



## **Cisco Secure Firewall ASA Series Syslog Messages**

**First Published:** 2017-08-28

**Last Modified:** 2024-09-16

### **Americas Headquarters**

Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
<http://www.cisco.com>  
Tel: 408 526-4000  
800 553-NETS (6387)  
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2024 Cisco Systems, Inc. All rights reserved.



## About This Guide

---

The following topics explain how to use this guide.

- [What's New in Each Release](#), on page iii
- [About ASA Syslog Messages](#), on page xviii
- [Communications, Services, and Additional Information](#), on page xxi

## What's New in Each Release

This section provides the following new or changed logging information for ASA.

- **Timestamp Logging:** Beginning with version 9.10(1), ASA provides the option to enable timestamp as per RFC 5424 in eventing syslogs. When this option is enabled, all timestamp of syslog messages would be displaying the time, in UTC, as per RFC 5424 format. Following is a sample output with RFC 5424 format:

```
<166>2018-06-27T12:17:46Z asa : %ASA-6-110002: Failed to locate egress interface for protocol from src interface :src IP/src port to dest IP/dest port
```

The following section provides new, changed, and deprecated syslog messages for the following ASA releases:

- [Version 9.22\(1\)](#)
- [Version 9.20\(2\)](#)
- [Table 1: New, Changed, and Deprecated Syslog Messages for Version 9.20\(1\)](#)
- [Version 9.19\(1\)](#)
- [Version 9.18\(1\)](#)
- [Table 2: New, Changed, and Deprecated Syslog Messages for Version 9.17\(1\)](#)
- [Table 3: New, Changed, and Deprecated Syslog Messages for Version 9.16\(1\)](#)
- [Table 4: New, Changed, and Deprecated Syslog Messages for Version 9.15\(1\)](#)
- [Table 5: New, Changed, and Deprecated Syslog Messages for Version 9.14\(1\)](#)
- [Table 6: New, Changed, and Deprecated Syslog Messages for Version 9.13\(1\)](#)
- [Table 7: New, Changed, and Deprecated Syslog Messages for Version 9.12\(1\)](#)
- [Table 7: New, Changed, and Deprecated Syslog Messages for Version 9.12\(1\)](#)

- [Table 7: New, Changed, and Deprecated Syslog Messages for Version 9.12\(1\)](#)
- [Table 10: New, Changed, and Deprecated Syslog Messages for Version 9.9\(1\)](#)
- [Table 11: New, Changed, and Deprecated Syslog Messages for Version 9.8\(2\)](#)
- [Table 12: New, Changed, and Deprecated Syslog Messages for Version 9.8\(1\)](#)
- [Table 13: New, Changed, and Deprecated Syslog Messages for Version 9.7\(1\)](#)
- [Table 14: New, Changed, and Deprecated Syslog Messages for Version 9.6\(2\)](#)
- [Table 15: New, Changed, and Deprecated Syslog Messages for Version 9.6\(1\)](#)
- [Table 16: New, Changed, and Deprecated Syslog Messages for Version 9.5\(2\)](#)
- [Table 17: New, Changed, and Deprecated Syslog Messages for Version 9.5\(1\)](#)
- [Table 18: New, Changed, and Deprecated Syslog Messages for Version 9.4\(1.225\)](#)
- [Table 19: New, Changed, and Deprecated Syslog Messages for Version 9.4\(1.150\)](#)
- [Table 20: New, Changed, and Deprecated Syslog Messages for Version 9.4\(1\)](#)
- [Table 21: New, Changed, and Deprecated Syslog Messages for Version 9.3\(3\)](#)
- [Table 22: New, Changed, and Deprecated Syslog Messages for Version 9.3\(2\)](#)
- [Table 23: New, Changed, and Deprecated Syslog Messages for Version 9.3\(1\)](#)
- [Table 24: New, Changed, and Deprecated Syslog Messages for Version 9.2\(1\)](#)
- [Table 25: New, Changed, and Deprecated Syslog Messages for Version 9.1\(7\)](#)
- [Table 26: New, Changed, and Deprecated Syslog Messages for Version 9.1\(5\)](#)
- [Table 27: New, Changed, and Deprecated Syslog Messages for Version 9.1\(4\)](#)
- [Table 28: New, Changed, and Deprecated Syslog Messages for Version 9.1\(3\)](#)
- [Table 29: New, Changed, and Deprecated Syslog Messages for Version 9.1\(2\)](#)
- [Table 30: New, Changed, and Deprecated Syslog Messages for Version 9.1\(1\)](#)
- [Table 31: New, Changed, and Deprecated Syslog Messages for Version 9.0\(3\)](#)
- [Table 32: New, Changed, and Deprecated Syslog Messages for Version 9.0\(2\)](#)
- [Table 33: New, Changed, and Deprecated Syslog Messages for Version 9.0\(1\)](#)
- [Table 34: New, Changed, and Deprecated Syslog Messages for Version 8.7\(1\)](#)
- [Table 35: New, Changed, and Deprecated Syslog Messages for Version 8.4\(6\)](#)
- [Table 36: New, Changed, and Deprecated Syslog Messages for Version 8.4\(5\)](#)
- [Table 37: New, Changed, and Deprecated Syslog Messages for Version 8.4.4\(1\)](#)
- [Table 38: New, Changed, and Deprecated Syslog Messages for Version 8.3\(3\)](#)
- [Table 39: New, Changed, and Deprecated Syslog Messages for Version 8.2\(5\)](#)
- [Table 40: New, Changed, and Deprecated Syslog Messages for Version 8.0\(1\)](#)

- [Table 41: New, Changed, and Deprecated Syslog Messages for pre-8.0\(1\) Release](#)
- [Table 42: New, Changed, and Deprecated Syslog Messages for Version 7.0.7\(8\)](#)

For Version 9.22(1), there are no new, changed, or deprecated syslog messages.

For Version 9.20(2), there are no new, changed, or deprecated syslog messages.

The following table lists the new, changed, and deprecated syslog message for Version 9.20(1). For complete syslog message descriptions, see respective chapters.

**Table 1: New, Changed, and Deprecated Syslog Messages for Version 9.20(1)**

<b>New Syslog Messages</b>	870001, 880001
<b>Changed Syslog Messages (Document)</b>	None
<b>Changed Syslog Messages (Code)</b>	302020, 302021

For Version 9.19(1), there are no new, changed, or deprecated syslog messages.

For Version 9.18(1), there are no new, changed, or deprecated syslog messages.

The following table lists the new, changed, and deprecated syslog message for Version 9.17(1). For complete syslog message descriptions, see respective chapters.

**Table 2: New, Changed, and Deprecated Syslog Messages for Version 9.17(1)**

<b>New Syslog Messages</b>	709009, 709010, 709011, 709012, 709013
<b>Changed Syslog Messages (Document)</b>	None
<b>Changed Syslog Messages (Code)</b>	None

The following table lists the new, changed, and deprecated syslog message for Version 9.16(1). For complete syslog message descriptions, see respective chapters.

**Table 3: New, Changed, and Deprecated Syslog Messages for Version 9.16(1)**

<b>New Syslog Messages</b>	717032, 305021, 305022, 317077, 317077, 324302, 324303, 733201, 812005, 812006
<b>Changed Syslog Messages (Document)</b>	717009
<b>Changed Syslog Messages (Code)</b>	None
<b>Deprecated Syslog Messages</b>	716055 and 716056

The following table lists the new, changed, and deprecated syslog message for Version 9.15(1). For complete syslog message descriptions, see respective chapters.

**Table 4: New, Changed, and Deprecated Syslog Messages for Version 9.15(1)**

<b>New Syslog Messages</b>	None
<b>Changed Syslog Messages (Document)</b>	105042, 105003, 105004, 105043, 305006, 414004

<b>Changed Syslog Messages (Code)</b>	302013, 302014
---------------------------------------	----------------

The following table lists the new, changed, and deprecated syslog message for Version 9.14(1). For complete syslog message descriptions, see respective chapters.

**Table 5: New, Changed, and Deprecated Syslog Messages for Version 9.14(1)**

<b>New Syslog Messages</b>	209006, 324012
----------------------------	----------------

The following table lists the new, changed, and deprecated syslog message for Version 9.13(1). For complete syslog message descriptions, see respective chapters.

**Table 6: New, Changed, and Deprecated Syslog Messages for Version 9.13(1)**

<b>New Syslog Messages</b>	113045, 121001, 121002, 121003, 302311, 305018, 305019, 305020, 324010, 324011, 769007, 769009
<b>Changed Syslog Messages</b>	
<b>Deprecated Syslog Messages</b>	717008, 717009, 717012, 717018, 717024, 717031

The following table lists the new, changed, and deprecated syslog messages for Version 9.12(1). For complete syslog message descriptions, see respective chapters.

**Table 7: New, Changed, and Deprecated Syslog Messages for Version 9.12(1)**

<b>New Syslog Messages</b>	305017, 308003, 308004, 339006, 339007, 339008, 408101, 408102, 409014, 409015, 409016, 409017, 419004-419006, 503002, 503003, 503004, 503005, 716165, 737038, 737200-737206, 737400-737407, 747042, 747043, 747044, 768003, 768004, 815002, 815003, 815004
<b>Changed Syslog Messages</b>	737001-737019, 737026, 737031-737036
<b>Deprecated Syslog Messages</b>	

The following table lists the new, changed, and deprecated syslog messages for Version 9.10(1). For complete syslog message descriptions, see respective chapters.

**Table 8: New, Changed, and Deprecated Syslog Messages for Version 9.10(1)**

<b>New Syslog Messages</b>	339001, 339002, 339003, 339004, 339005, 850001, 850002
<b>Changed Syslog Messages</b>	725002
<b>Deprecated Syslog Messages</b>	

The following table lists the new, changed, and deprecated syslog messages for Version 9.9(1). For complete syslog message descriptions, see respective chapters.

**Table 9: New, Changed, and Deprecated Syslog Messages for Version 9.9(2)**

<b>New Syslog Messages</b>	199027, 747037, 747038, 747039, 747040, 747041
<b>Changed Syslog Messages (Documentation)</b>	321006, 747023, 747024, 747034, 747035, 747036
<b>Changed Syslog Messages (Code)</b>	747023, 747024, 747034, 747035, 747036
<b>Deprecated Syslog Messages</b>	815001, 815002

**Table 10: New, Changed, and Deprecated Syslog Messages for Version 9.9(1)**

<b>New Syslog Messages</b>	104500, 104501, 104502, 105500, 105501, 105502, 105503, 105504, 105505, 105506, 105507, 105508, 105509, 105510, 105511, 105512, 105513, 105514, 105515, 105516, 105517, 105518, 105519, 105520, 105521, 105522, 105523, 105524, 105525, 105526, 105527, 105528, 105529, 105530, 105531, 105532, 105533, 105534, 105535, 105536, 105537, 105538, 105539, 105540, 105541, 105542, 105543, 105544, 105545, 105546, 105547, 105548, 105549, 105550, 105551, 105552, 105553, 418018, 418019, 418040, 750015, 751028
<b>Changed Syslog Messages (Documentation)</b>	302014
<b>Changed Syslog Messages (Code)</b>	302014
<b>Deprecated Syslog Messages</b>	

The following table lists the new, changed, and deprecated syslog messages for Version 9.8(2). For complete syslog message descriptions, see respective chapters.

**Table 11: New, Changed, and Deprecated Syslog Messages for Version 9.8(2)**

<b>New Syslog Messages</b>	753001, 840001, 8300001, 8300002, 8300003, 8300004, 8300005, 8300006
<b>Changed Syslog Messages (Documentation)</b>	
<b>Changed Syslog Messages (Code)</b>	
<b>Deprecated Syslog Messages</b>	

The following table lists the new, changed, and deprecated syslog messages for Version 9.8(1). For complete syslog message descriptions, see respective chapters.

**Table 12: New, Changed, and Deprecated Syslog Messages for Version 9.8(1)**

<b>New Syslog Messages</b>	109105, 602306, 750013
<b>Changed Syslog Messages (Documentation)</b>	302020, 302021
<b>Changed Syslog Messages (Code)</b>	302020, 302021
<b>Deprecated Syslog Messages</b>	

The following table lists the new, changed, and deprecated syslog messages for Version 9.7(1). For complete syslog message descriptions, see respective chapters.

**Table 13: New, Changed, and Deprecated Syslog Messages for Version 9.7(1)**

<b>New Syslog Messages</b>	717061, 717062, 717063, 717064, 4302310, 806001, 806002, 806003, 806004, 806005, 806006, 806007, 806008, 806009, 806010, 806011, 806012, 815001, 815002
<b>Changed Syslog Messages (Documentation)</b>	304001
<b>Changed Syslog Messages (Code)</b>	304001
<b>Deprecated Syslog Messages</b>	

The following table lists the new, changed, and deprecated syslog messages for Version 9.6(2). For complete syslog message descriptions, see respective chapters.

**Table 14: New, Changed, and Deprecated Syslog Messages for Version 9.6(2)**

<b>New Syslog Messages</b>	315013, 337000, 337001, 717059, 717060, 769005, 769006
<b>Changed Syslog Messages (Documentation)</b>	103001, 769004
<b>Changed Syslog Messages (Code)</b>	103001, 113015, 113016, 113017, 769004
<b>Deprecated Syslog Messages</b>	

The following table lists the new, changed, and deprecated syslog messages for Version 9.6(1). For complete syslog message descriptions, see respective chapters.



**Table 15: New, Changed, and Deprecated Syslog Messages for Version 9.6(1)**

<b>New Syslog Messages</b>	604201-604208, 618001, 703008
<b>Changed Syslog Messages (Documentation)</b>	
<b>Changed Syslog Messages (Code)</b>	776005, 776014, 776015, 776017, 776018, 776019, 776251, 776252, 776253, 776254
<b>Deprecated Syslog Messages</b>	

The following table lists the new, changed, and deprecated syslog messages for Version 9.5(2). For complete syslog message descriptions, see respective chapters.

**Table 16: New, Changed, and Deprecated Syslog Messages for Version 9.5(2)**

<b>New Syslog Messages</b>	717057, 717058, 722056, 747036, 748201-748203, 785001
<b>Changed Syslog Messages (Documentation)</b>	None
<b>Changed Syslog Messages (Code)</b>	None
<b>Deprecated Syslog Messages</b>	None

The following table lists the new, changed, and deprecated syslog messages for Version 9.5(1). For complete syslog message descriptions, see respective chapters.

**Table 17: New, Changed, and Deprecated Syslog Messages for Version 9.5(1)**

<b>New Syslog Messages</b>	302035, 302036, 302305, 302306, 305014, 305016, 725017, 747034, 747035, 748100-748103
<b>Changed Syslog Messages (Documentation)</b>	500001, 500002
<b>Changed Syslog Messages (Code)</b>	500001, 500002
<b>Deprecated Syslog Messages</b>	None

The following table lists the new, changed, and deprecated syslog messages for Version 9.4(1.225). For complete syslog message descriptions, see respective chapters.

**Table 18: New, Changed, and Deprecated Syslog Messages for Version 9.4(1.225)**

<b>New Syslog Messages</b>	218005, 804001-804002, 803003
----------------------------	-------------------------------

<b>Changed Syslog Messages (Documentation)</b>	None
<b>Changed Syslog Messages (Code)</b>	803001, 803002
<b>Deprecated Syslog Messages</b>	None

The following table lists the new, changed, and deprecated syslog messages for Version 9.4(1.150). For complete syslog message descriptions, see respective chapters.

**Table 19: New, Changed, and Deprecated Syslog Messages for Version 9.4(1.150)**

<b>New Syslog Messages</b>	748001-748009, 803001-803002
<b>Changed Syslog Messages (Documentation)</b>	None
<b>Changed Syslog Messages (Code)</b>	None
<b>Deprecated Syslog Messages</b>	None

The following table lists the new, changed, and deprecated syslog messages for Version 9.4(1). For complete syslog message descriptions, see respective chapters.

**Table 20: New, Changed, and Deprecated Syslog Messages for Version 9.4(1)**

<b>New Syslog Messages</b>	109040, 315012, 402149, 402150, 717052-717056, 751027
<b>Changed Syslog Messages (Documentation)</b>	405001, 730005
<b>Changed Syslog Messages (Code)</b>	730005
<b>Deprecated Syslog Messages</b>	337001-337009, 339001-339009, 608006

The following table lists the new, changed, and deprecated syslog messages for Version 9.3(3). For complete syslog message descriptions, see respective chapters.

**Table 21: New, Changed, and Deprecated Syslog Messages for Version 9.3(3)**

<b>New Syslog Messages</b>	None
<b>Changed Syslog Messages (Documentation)</b>	109006, 113005, 113014-113016, 315011, 603106, 605004, 611101, 611102, 716039

<b>Changed Syslog Messages (Code)</b>	109006, 113005, 113014-113016, 315011, 603106, 605004, 611101, 611102, 716039
<b>Deprecated Syslog Messages</b>	None

The following table lists the new, changed, and deprecated syslog messages for Version 9.3(2). For complete syslog message descriptions, see respective chapters.

**Table 22: New, Changed, and Deprecated Syslog Messages for Version 9.3(2)**

<b>New Syslog Messages</b>	110004, 342001-342008, 607004, 608006, 725016, 802001-802006
<b>Changed Syslog Messages (Documentation)</b>	210005, 302014, 505005, 609001, 609002, 725001-725010, 725012, 725013, 734004, 750003
<b>Changed Syslog Messages (Code)</b>	210005, 302014, 302016, 302018, 302021, 302304, 609001, 609002, 725001-725010, 725012, 725013, 734004
<b>Deprecated Syslog Messages</b>	734005

The following table lists the new, changed, and deprecated syslog messages for Version 9.3(1). For complete syslog message descriptions, see respective chapters.

**Table 23: New, Changed, and Deprecated Syslog Messages for Version 9.3(1)**

<b>New Syslog Messages</b>	103008, 105033, 105041, 302022-302027, 434004, 709008, 725016, 722055, 751025, 751026, 780001-780004
<b>Changed Syslog Messages (Documentation)</b>	725002
<b>Changed Syslog Messages (Code)</b>	725002
<b>Deprecated Syslog Messages</b>	None

The following table lists the new, changed, and deprecated syslog messages for Version 9.2(1). For complete syslog message descriptions, see respective chapters.

**Table 24: New, Changed, and Deprecated Syslog Messages for Version 9.2(1)**

<b>New Syslog Messages</b>	113041, 113042, 213007, 328002, 336012-336016, 336018, 336019, 434001-434004, 434007, 520001-520005, 520010, 520011, 520013, 520020-520025, 613004-613008, 613011, 613013-613019, 613021-613043 722054, 778001-778007, 779001-779007
----------------------------	--

<b>Changed Syslog Messages (Documentation)</b>	201010, 602101, 611101, 611102, 713903, 734004
<b>Changed Syslog Messages (Code)</b>	611101, 611102, 713903, 734004
<b>Deprecated Syslog Messages</b>	210011, 202011, 321008, 321009

The following table lists the new, changed, and deprecated syslog messages for Version 9.1(7). For complete syslog message descriptions, see respective chapters.

**Table 25: New, Changed, and Deprecated Syslog Messages for Version 9.1(7)**

<b>New Syslog Messages</b>	202016, 737034, 737035, 737036
<b>Changed Syslog Messages (Documentation)</b>	None
<b>Changed Syslog Messages (Code)</b>	None
<b>Deprecated Syslog Messages</b>	337005

The following table lists the new, changed, and deprecated syslog messages for Version 9.1(5). For complete syslog message descriptions, see respective chapters.

**Table 26: New, Changed, and Deprecated Syslog Messages for Version 9.1(5)**

<b>New Syslog Messages</b>	780001, 780002
<b>Changed Syslog Messages (Documentation)</b>	113005, 113015, 113016, 113017, 210007, 611102, 720073
<b>Changed Syslog Messages (Code)</b>	113005, 113015, 113016, 113017, 210007, 611102, 720073
<b>Deprecated Syslog Messages</b>	None

The following table lists the new, changed, and deprecated syslog messages for Version 9.1(4). For complete syslog message descriptions, see respective chapters.

**Table 27: New, Changed, and Deprecated Syslog Messages for Version 9.1(4)**

<b>New Syslog Messages</b>	109100-109104, 321008, 321009, 444008, 444009, 716061, 743010, 743011, 747031-747033, 750010, 751024
<b>Changed Syslog Messages (Documentation)</b>	702307

<b>Changed Syslog Messages (Code)</b>	713902
<b>Deprecated Syslog Messages</b>	None

The following table lists the new, changed, and deprecated syslog messages for Version 9.1(3). For complete syslog message descriptions, see respective chapters.

**Table 28: New, Changed, and Deprecated Syslog Messages for Version 9.1(3)**

<b>New Syslog Messages</b>	None
<b>Changed Syslog Messages (Documentation)</b>	106100, 715080, 746001-746019, 747021
<b>Changed Syslog Messages (Code)</b>	747021
<b>Deprecated Syslog Messages</b>	102001

The following table lists the new, changed, and deprecated syslog messages for Version 9.1(2). For complete syslog message descriptions, see respective chapters.

**Table 29: New, Changed, and Deprecated Syslog Messages for Version 9.1(2)**

<b>New Syslog Messages</b>	109100-109104, 402140-402148, 405003, 711006, 716600-716603, 730003, 730006-730009, 750011, 750012, 751023, 768001-768003, 769001-769004, 771001-771002, 772002-772006, 774001-774002
<b>Changed Syslog Messages (Documentation)</b>	315011, 713191, 751022
<b>Changed Syslog Messages (Code)</b>	103005, 315011, 713191, 751022
<b>Deprecated Syslog Messages</b>	None

The following table lists the new, changed, and deprecated syslog messages for Version 9.1(1). For complete syslog message descriptions, see respective chapters.

**Table 30: New, Changed, and Deprecated Syslog Messages for Version 9.1(1)**

<b>New Syslog Messages</b>	105050, 341001, 341002, 341004-341008, 341010, 341011, 751022
<b>Changed Syslog Messages (Documentation)</b>	None

<b>Changed Syslog Messages (Code)</b>	None
<b>Deprecated Syslog Messages</b>	None

The following table lists the new, changed, and deprecated syslog messages for Version 9.0(3). For complete syslog message descriptions, see respective chapters.

**Table 31: New, Changed, and Deprecated Syslog Messages for Version 9.0(3)**

<b>New Syslog Messages</b>	747030
<b>Changed Syslog Messages (Documentation)</b>	747022
<b>Changed Syslog Messages (Code)</b>	747022
<b>Deprecated Syslog Messages</b>	None

The following table lists the new, changed, and deprecated syslog messages for Version 9.0(2). For complete syslog message descriptions, see respective chapters.

**Table 32: New, Changed, and Deprecated Syslog Messages for Version 9.0(2)**

<b>New Syslog Messages</b>	199020, 199021, 747001-747029
<b>Changed Syslog Messages (Documentation)</b>	None
<b>Changed Syslog Messages (Code)</b>	None
<b>Deprecated Syslog Messages</b>	None

The following table lists the new, changed, and deprecated syslog messages for Version 9.0(1). For complete syslog message descriptions, see respective chapters.

**Table 33: New, Changed, and Deprecated Syslog Messages for Version 9.0(1)**

<b>New Syslog Messages</b>	109038, 109039, 114023, 302022-302027, 313009, 317007, 317008, 318101-318123, 318125-318128, 325004-325006, 402131, 409101-409123, 409125, 409128, 426101-426104, 429007, 503101, 613101-613104, 751019, 751020, 751021, 776001-776020, 776201-776204, 776251-776254, 776301-776313, 767001, 775001-775007
----------------------------	--

<b>Changed Syslog Messages (Documentation)</b>	103004, 103005, 106023, 106100, 106010, 106014, 109014, 113019, 313005, 418001, 424001, 509001, 713900-713906, 722051, 725001-725006, 735026-735029, 737009-737011, 737013, 737014, 737016
<b>Changed Syslog Messages (Code)</b>	103005, 109014, 106100, 113019, 722051, 725001-725006, 735026-735029, 737009-737011, 737013, 737014, 737016
<b>Deprecated Syslog Messages</b>	302009

The following table lists the new, changed, and deprecated syslog messages for Version 8.7(1). For complete syslog message descriptions, see respective chapters.

**Table 34: New, Changed, and Deprecated Syslog Messages for Version 8.7(1)**

<b>New Syslog Messages</b>	341001-341003
<b>Changed Syslog Messages (Documentation)</b>	713900-713906
<b>Deprecated Syslog Messages</b>	None

The following table lists the new, changed, and deprecated syslog messages for Version 8.4(6). For complete syslog message descriptions, see respective chapters.

**Table 35: New, Changed, and Deprecated Syslog Messages for Version 8.4(6)**

<b>New Syslog Messages</b>	716600-716603
<b>Changed Syslog Messages (Documentation)</b>	302014
<b>Changed Syslog Messages (Code)</b>	None
<b>Deprecated Syslog Messages</b>	None

The following table lists the new, changed, and deprecated syslog messages for Version 8.4(5). For complete syslog message descriptions, see Chapter 1.

**Table 36: New, Changed, and Deprecated Syslog Messages for Version 8.4(5)**

<b>New Syslog Messages</b>	None
<b>Changed Syslog Messages (Documentation)</b>	103004, 103005
<b>Changed Syslog Messages (Code)</b>	103005

<b>Deprecated Syslog Messages</b>	None
-----------------------------------	------

The following table lists the new, changed, and deprecated syslog messages for Version 8.4.4(1). For complete syslog message descriptions, see respective chapters.

**Table 37: New, Changed, and Deprecated Syslog Messages for Version 8.4.4(1)**

<b>New Syslog Messages</b>	402140-402148, 429001-429006, 429008, 602303-602305, 752001-752017, 768001-768003, 769001-769004, 771001-771002, 772002-772006, 774001-774002
<b>Changed Syslog Messages (Documentation)</b>	113019, 315011
<b>Changed Syslog Messages (Code)</b>	315011
<b>Deprecated Syslog Messages</b>	None

The following table lists the new, changed, and deprecated syslog messages for Version 8.3(3). For complete syslog message descriptions, see respective chapters.

**Table 38: New, Changed, and Deprecated Syslog Messages for Version 8.3(3)**

<b>New Syslog Messages</b>	114023, 120012, 313009
<b>Changed Syslog Messages (Documentation)</b>	722036
<b>Changed Syslog Messages (Code)</b>	None
<b>Deprecated Syslog Messages</b>	None

The following table lists the new, changed, and deprecated syslog messages for Version 8.2(5). For complete syslog message descriptions, see respective chapters.

**Table 39: New, Changed, and Deprecated Syslog Messages for Version 8.2(5)**

<b>New Syslog Messages</b>	103005, 114023, 120012, 313009, 413007, 413008, 447001, 735024-735027
<b>Changed Syslog Messages (Documentation)</b>	722036
<b>Changed Syslog Messages (Code)</b>	None
<b>Deprecated Syslog Messages</b>	None



The following table lists the new, changed, and deprecated syslog messages for Version 8.0(1). For complete syslog message descriptions, see respective chapters.

**Table 40: New, Changed, and Deprecated Syslog Messages for Version 8.0(1)**

<b>New Syslog Messages</b>	109035
<b>Changed Syslog Messages (Documentation)</b>	None
<b>Changed Syslog Messages (Code)</b>	None
<b>Deprecated Syslog Messages</b>	None

The following table lists the new, changed, and deprecated syslog messages for pre-8.0(1) release. For complete syslog message descriptions, see respective chapters.

**Table 41: New, Changed, and Deprecated Syslog Messages for pre-8.0(1) Release**

<b>New Syslog Messages</b>	713207, 713275, 713276, 715018, 715031, 715032, 715078, 715079
<b>Changed Syslog Messages (Documentation)</b>	None
<b>Changed Syslog Messages (Code)</b>	None
<b>Deprecated Syslog Messages</b>	None

The following table lists the new, changed, and deprecated syslog messages for Version 7.0.7(8). For complete syslog message descriptions, see respective chapters.

**Table 42: New, Changed, and Deprecated Syslog Messages for Version 7.0.7(8)**

<b>New Syslog Messages</b>	419003
<b>Changed Syslog Messages (Documentation)</b>	None
<b>Changed Syslog Messages (Code)</b>	None
<b>Deprecated Syslog Messages</b>	None

# About ASA Syslog Messages

This section provides information about the ASA syslog messages; lists the message classes and their ID ranges.

- The valid range for message IDs is between 100000 and 999999.




---

**Note** When a number is skipped in a sequence, the message is no longer in the ASA code.

---

- For information about how to configure logging, SNMP, and NetFlow, see the *CLI configuration guide*.
- Most of the ISAKMP messages have a common set of prepended objects to help identify the tunnel. These objects precede the descriptive text of a message when available. If the object is not known at the time the message is generated, the specific **heading = value** combination will not be displayed.

The objects will be prepended as follows:

Group = **groupname**, Username = **user**, IP = **IP\_address**,...

Where the Group identifies the tunnel group, the Username is the username from the local database or AAA server, and the IP address is the public IP address of the remote access client or L2L peer.

- Typically, a traffic session displays the connection numbers/IDs for each flow in the syslog messages. However, for some of the connections, though the connection ID is incremented, the syslog messages does not display the ID. Thus, you may find missing sequence numbers in the connection IDs of the subsequent messages.

For example, during a TCP traffic flow, the syslog messages display the connection IDs as 201, 202, 203, and 204 for each flow. When an ICMP flow begins, though the connection ID is internally incremented to 205 and 206, the syslog messages does not display the numbers. When another TCP flow follows, its connection numbers are now displayed as 207, 208, and so on, giving an impression of skipping sequence.

The following table lists the message classes and the ranges of message IDs that are associated with each class.

**Table 43: Syslog Message Classes and Associated Message ID Numbers**

Logging Class	Definition	Syslog Message ID Numbers
<b>auth</b>	User Authentication	109, 113
—	Access Lists	106
—	Application Firewall	415
<b>bridge</b>	Transparent Firewall	110, 220
<b>ca</b>	PKI Certification Authority	717
citrix	Citrix Client	723

Logging Class	Definition	Syslog Message ID Numbers
—	Clustering	747
—	Card Management	323
<b>config</b>	Command Interface	111, 112, 208, 308
csd	Secure Desktop	724
cts	Cisco TrustSec	776
<b>dap</b>	Dynamic Access Policies	734
eap, eapoudp	EAP or EAPoUDP for Network Admission Control	333, 334
eigrp	EIGRP Routing	336
<b>email</b>	E-mail Proxy	719
—	Environment Monitoring	735
<b>ha</b>	Failover	101, 102, 103, 104, 105, 210, 311, 709
—	Identity-based Firewall	746
ids	Intrusion Detection System	400, 733
—	IKEv2 Toolkit	750, 751, 752
<b>ip</b>	IP Stack	209, 215, 313, 317, 408
<b>ipaa</b>	IP Address Assignment	735
<b>ips</b>	Intrusion Protection System	400, 401, 420
—	IPv6	325
—	Block lists, Allow lists, and Graylists	338
—	Licensing	444
mdm-proxy	MDM Proxy	802
nac	Network Admission Control	731, 732
nacpolicy	NAC Policy	731
nacsettings	NAC Settings to apply NAC Policy	732
—	Network Access Point	713
<b>np</b>	Network Processor	319
—	NP SSL	725
<b>ospf</b>	OSPF Routing	318, 409, 503, 613

Logging Class	Definition	Syslog Message ID Numbers
—	Password Encryption	742
—	Phone Proxy	337
<b>rip</b>	RIP Routing	107, 312
<b>rm</b>	Resource Manager	321
—	Smart Call Home	120
<b>session</b>	User Session	106, 108, 201, 202, 204, 302, 303, 304, 305, 314, 405, 406, 407, 500, 502, 607, 608, 609, 616, 620, 703, 710
<b>snmp</b>	SNMP	212
—	ScanSafe	775
ssl	SSL Stack	725
svc	SSL VPN Client	722
<b>sys</b>	System	199, 211, 214, 216, 306, 307, 315, 414, 604, 605, 606, 610, 612, 614, 615, 701, 711, 741
—	Threat Detection	733
tre	Transactional Rule Engine	780
—	UC-IME	339
tag-switching	Service Tag Switching	779
vm	VLAN Mapping	730
<b>vpdn</b>	PPTP and L2TP Sessions	213, 403, 603
<b>vpn</b>	IKE and IPsec	316, 320, 402, 404, 501, 602, 702, 713, 714, 715
<b>vpnc</b>	VPN Client	611
<b>vpnfo</b>	VPN Failover	720
<b>vpnlb</b>	VPN Load Balancing	718
—	VXLAN	778
webfo	WebVPN Failover	721
<b>webvpn</b>	WebVPN and AnyConnect Client	716
—	NAT and PAT	305

## Syslog Message Format

Syslog messages are structured as follows:

```
[<PRI>] [Timestamp] [Device-ID] : %ASA-Level-Message_number: Message_text
```

Field descriptions are as follows:

<i>&lt;PRI&gt;</i>	Priority value. When the logging EMBLEM is enabled, this value is displayed in the syslog message. Logging EMBLEM is compatible with UDP and not with TCP.
<i>Timestamp</i>	Date and time of the event is displayed. When logging of timestamps is enabled, and if the timestamp is configured to be in the RFC 5424 format, all timestamp in syslog messages display the time in UTC, as indicated by the RFC 5424 standard.
<i>Device-ID</i>	The device identifier string that was configured while enabling the logging device-id option through the user interface. If enabled, the device ID does not appear in EMBLEM-formatted syslog messages.
<i>ASA</i>	The syslog message facility code for messages that are generated by the ASA. This value is always <code>ASA</code> .
<i>Level</i>	0 through 7. The level reflects the severity of the condition described by the syslog message—the lower the number, the more severe the condition.
<i>Message_number</i>	A unique six-digit number that identifies the syslog message.
<i>Message_text</i>	A text string that describes the condition. This portion of the syslog message sometimes includes IP addresses, port numbers, or usernames.

All syslog messages that are generated by the device are documented in this guide.

Example of a syslog message with logging EMBLEM, logging timestamp rfc5424, and device-id enabled.

```
<166>2018-06-27T12:17:46Z: %ASA-6-110002: Failed to locate egress interface for protocol
from src interface :src IP/src port to dest IP/dest port
```

Example of a syslog message with logging timestamp rfc5424 and device-id enabled.

```
2018-06-27T12:17:46Z asa : %ASA-6-110002: Failed to locate egress interface for protocol
from src interface :src IP/src port to dest IP/dest port
```

## Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at [Cisco Profile Manager](#).
- To get the business impact you're looking for with the technologies that matter, visit [Cisco Services](#).
- To submit a service request, visit [Cisco Support](#).
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit [Cisco DevNet](#).
- To obtain general networking, training, and certification titles, visit [Cisco Press](#).
- To find warranty information for a specific product or product family, access [Cisco Warranty Finder](#).

### Cisco Bug Search Tool

[Cisco Bug Search Tool](#) (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.



# CHAPTER 1

## Syslog Messages 101001 to 199027

This chapter contains the following sections:

- [Messages 101001 to 109213, on page 1](#)
- [Messages 110002 to 113045, on page 45](#)
- [Messages 114001 to 199027, on page 61](#)

### Messages 101001 to 109213

This section includes messages from 101001 to 109213.

#### 101001

**Error Message** %ASA-1-101001: (Primary) Failover cable OK.

**Explanation** The failover cable is present and functioning correctly. Primary can also be listed as Secondary for the secondary unit.

**Recommended Action** None required.

#### 101002

**Error Message** %ASA-1-101002: (Primary) Bad failover cable.

**Explanation** The failover cable is present, but not functioning correctly. Primary can also be listed as Secondary for the secondary unit.

**Recommended Action** Replace the failover cable.

#### 101003, 101004

**Error Message** %ASA-1-101003: (Primary) Failover cable not connected (this unit).

**Error Message** %ASA-1-101004: (Primary) Failover cable not connected (other unit).

**Explanation** Failover mode is enabled, but the failover cable is not connected to one unit of the failover pair. Primary can also be listed as Secondary for the secondary unit.

**Recommended Action** Connect the failover cable to both units of the failover pair.

## 101005

**Error Message** %ASA-1-101005: (Primary) Error reading failover cable status.

**Explanation** The failover cable is connected, but the primary unit is unable to determine its status.

**Recommended Action** Replace the cable.

## 103001

**Error Message** %ASA-1-103001: (Primary) No response from other firewall (reason code = code).

**Explanation** The primary unit is unable to communicate with the secondary unit over the failover cable. Primary can also be listed as Secondary for the secondary unit. The following table lists the reason codes and the descriptions to determine why the failover occurred.

Reason Code	Description
1	The local unit is not receiving the hello packet on the failover LAN interface when LAN failover occurs or on the serial failover cable when serial failover occurs, and declares that the peer is down.
2	An interface did not pass one of the four failover tests, which are as follows: 1) Link Up, 2) Monitor for Network Traffic, 3) ARP, and 4) Broadcast Ping.
3	No proper ACK for 15+ seconds after a command was sent on the serial cable.
4	The failover LAN interface is down, and other data interfaces are not responding to additional interface testing. In addition, the local unit is declaring that the peer is down.



Reason Code	Description
5	The standby peer went down during the configuration synchronization process.
6	Replication is not complete; the failover unit is not synchronized.

**Recommended Action** Verify that the failover cable is connected correctly and both units have the same hardware, software, and configuration. If the problem persists, contact the Cisco TAC.

## 103002

**Error Message** %ASA-1-103002: (Primary) Other firewall network interface interface\_number OK.

**Explanation** The primary unit has detected that the network interface on the secondary unit is okay. Primary can also be listed as Secondary for the secondary unit.

**Recommended Action** None required.

## 103003

**Error Message** %ASA-1-103003: (Primary) Other firewall network interface interface\_number failed.

**Explanation** The primary unit has detected a bad network interface on the secondary unit. Primary can also be listed as Secondary for the secondary unit.

**Recommended Action** Check the network connections on the secondary unit and the network hub connection. If necessary, replace the failed network interface.

## 103004

**Error Message** %ASA-1-103004: (Primary) Other firewall reports this firewall failed. Reason: reason-string

**Explanation** The primary unit received a message from the secondary unit indicating that the primary unit has failed. Primary can also be listed as Secondary for the secondary unit. The reason can be one of the following:

- Missed poll packets on failover command interface exceeded threshold.
- LAN failover interface failed.
- Peer failed to enter Standby Ready state.
- Failed to complete configuration replication. This firewall's configuration may be out of sync.
- Failover message transmit failure and no ACK for busy condition received.

**Recommended Action** Verify the status of the primary unit.

## 103005

**Error Message** %ASA-1-103005: (Primary) Other firewall reporting failure. Reason: SSM card failure

**Explanation** The secondary unit has reported an SSM card failure to the primary unit. Primary can also be listed as Secondary for the secondary unit.

**Recommended Action** Verify the status of the secondary unit.

## 103006

**Error Message** %ASA-1-103006: (Primary|Secondary) Mate version *ver\_num* is not compatible with ours *ver\_num*

**Explanation** The Secure Firewall ASA has detected a peer unit that is running a version that is different than the local unit and is not compatible with the HA Hitless Upgrade feature.

- *ver\_num* —Version number.

**Recommended Action** Install the same or a compatible version image on both units.

## 103007

**Error Message** %ASA-1-103007: (Primary|Secondary) Mate version *ver\_num* is not identical with ours *ver\_num*

**Explanation** The Secure Firewall ASA has detected that the peer unit is running a version that is not identical, but supports Hitless Upgrade and is compatible with the local unit. The system performance may be degraded because the image version is not identical, and the Secure Firewall ASA may develop a stability issue if the nonidentical image runs for an extended period.

- *ver\_num*—Version number

**Recommended Action** Install the same image version on both units as soon as possible.

## 103008

**Error Message** %ASA-1-103008: Mate hwidb index is not compatible

**Explanation** The number of interfaces on the active and standby units is not the same.

**Recommended Action** Verify that the units have the same number of interfaces. You might need to install additional interface modules, or use different devices. After the physical interfaces match, force a configuration sync by entering the **write standby** command.

## 104001, 104002

**Error Message** %ASA-1-104001: (Primary) Switching to ACTIVE (cause: *string* ).

**Error Message** %ASA-1-104002: (Primary) Switching to STANDBY (cause: *string* ).

**Explanation** You have forced the failover pair to switch roles, either by entering the **failover active** command on the standby unit, or the **no failover active** command on the active unit. Primary can also be listed as Secondary for the secondary unit. Possible values for the string variable are as follows:

- state check
- bad/incomplete config
- ifc [interface] check, mate is healthier
- the other side wants me to standby
- in failed state, cannot be active
- switch to failed state
- other unit set to active by CLI config command fail active

**Recommended Action** If the message occurs because of manual intervention, no action is required. Otherwise, use the cause reported by the secondary unit to verify the status of both units of the pair.

## 104003

**Error Message** %ASA-1-104003: (Primary) Switching to FAILED.

**Explanation** The primary unit has failed.

**Recommended Action** Check the messages for the primary unit for an indication of the nature of the problem (see message 104001). Primary can also be listed as Secondary for the secondary unit.

## 104004

**Error Message** %ASA-1-104004: (Primary) Switching to OK.

**Explanation** A previously failed unit reports that it is operating again. Primary can also be listed as Secondary for the secondary unit.

**Recommended Action** None required.

## 104500

**Error Message** %ASA-1-104500: (Primary|Secondary) Switching to ACTIVE (cause: reason)

### Explanation

This HA unit is assuming the Active role for the Cloud HA pair. Possible values for the reason string are:

- no existing Active unit present
- unable to send message to Active unit
- no response to Hello message received from Active unit
- user initiated failover on this unit
- user initiated failover on peer unit
- invalid message received on failover connection

**Recommended Action** None required.

## 104501

**Error Message** %ASA-1-104501: (Primary|Secondary) Switching to BACKUP (cause: reason).

**Explanation** This HA unit is assuming the Backup role for the Cloud HA pair. Possible values for the reason string are:

- existing Active unit present
- user initiated failover on this unit
- user initiated failover on peer unit

**Recommended Action** None required.

## 104502

**Error Message** %ASA-1-104502: (Primary|Secondary) Becoming Backup unit failed.

**Explanation** This HA unit failed to assume the Backup role for the Cloud HA pair. The reason being the same as that of 104500 and 104501.

**Recommended Action** None required.

## 105001

**Error Message** %ASA-1-105001: (Primary) Disabling failover.

**Explanation** In version 7.x and later, this message may indicate the following: failover has been automatically disabled because of a mode mismatch (single or multiple), a license mismatch (encryption or context), or a hardware difference (one unit has an IPS SSM installed, and its peer has a CSC SSM installed). Primary can also be listed as Secondary for the secondary unit.

**Recommended Action** None required.

## 105002

**Error Message** %ASA-1-105002: (Primary) Enabling failover.

**Explanation** You have used the **failover** command with no arguments on the console, after having previously disabled failover. Primary can also be listed as Secondary for the secondary unit.

**Recommended Action** None required.

## 105003

**Error Message** %ASA-1-105003: (Primary) Monitoring on interface interface\_name waiting

**Explanation** The Secure Firewall ASA is testing the specified network interface with the other unit of the failover pair. Primary can also be listed as Secondary for the secondary unit.



---

**Note** There could be delay in the logging of syslog when compared to the actual status change. This delay is due to the poll time and hold time that is configured for the interface monitoring.

---

**Recommended Action** None required. The Secure Firewall ASA monitors its network interfaces frequently during normal operation.

## 105004

**Error Message** %ASA-1-105004: (Primary) Monitoring on interface interface\_name normal

**Explanation** The test of the specified network interface was successful. Primary can also be listed as Secondary for the secondary unit.



---

**Note** There could be delay in the logging of syslog when compared to the actual status change. This delay is due to the poll time and hold time that is configured for the interface monitoring.

---

**Recommended Action** None required.

## 105005

**Error Message** %ASA-1-105005: (Primary) Lost Failover communications with mate on interface interface\_name.

**Explanation** One unit of the failover pair can no longer communicate with the other unit of the pair. Primary can also be listed as Secondary for the secondary unit.

**Recommended Action** Verify that the network connected to the specified interface is functioning correctly.

## 105006, 105007

**Error Message** %ASA-1-105006: (Primary) Link status Up on interface interface\_name.

**Error Message** %ASA-1-105007: (Primary) Link status Down on interface interface\_name.

**Explanation** The results of monitoring the link status of the specified interface have been reported. Primary can also be listed as Secondary for the secondary unit.

**Recommended Action** If the link status is down, verify that the network connected to the specified interface is operating correctly.

## 105008

**Error Message** %ASA-1-105008: (Primary) Testing interface interface\_name.

**Explanation** Testing of a specified network interface has occurred. This testing is performed only if the Secure Firewall ASA fails to receive a message from the standby unit on that interface after the expected interval. Primary can also be listed as Secondary for the secondary unit.

**Recommended Action** None required.

## 105009

**Error Message** %ASA-1-105009: (Primary) Testing on interface interface\_name {Passed|Failed}.

**Explanation** The result (either Passed or Failed) of a previous interface test has been reported. Primary can also be listed as Secondary for the secondary unit.

**Recommended Action** None required if the result is Passed. If the result is Failed, you should check the network cable connection to both failover units, that the network itself is functioning correctly, and verify the status of the standby unit.

## 105010

**Error Message** %ASA-3-105010: (Primary) Failover message block alloc failed.

**Explanation** Block memory was depleted. This is a transient message and the Secure Firewall ASA should recover. Primary can also be listed as Secondary for the secondary unit.

**Recommended Action** Use the show blocks command to monitor the current block memory.

## 105011

**Error Message** %ASA-1-105011: (Primary) Failover cable communication failure

**Explanation** The failover cable is not permitting communication between the primary and secondary units. Primary can also be listed as Secondary for the secondary unit.

**Recommended Action** Ensure that the cable is connected correctly.

## 105020

**Error Message** %ASA-1-105020: (Primary) Incomplete/slow config replication

**Explanation** When a failover occurs, the active Secure Firewall ASA detects a partial configuration in memory. Normally, this is caused by an interruption in the replication service. Primary can also be listed as Secondary for the secondary unit.

**Recommended Action** After the Secure Firewall ASA detects the failover, the Secure Firewall ASA automatically reboots and loads the configuration from flash memory and/or resynchronizes with another Secure Firewall ASA. If failovers occurs continuously, check the failover configuration and make sure that both Secure Firewall ASAs can communicate with each other.

## 105021

**Error Message** %ASA-1-105021: (failover\_unit ) Standby unit failed to sync due to a locked context\_name config. Lock held by lock\_owner\_name

**Explanation** During configuration synchronization, a standby unit will reload itself if some other process locks the configuration for more than five minutes, which prevents the failover process from applying the new configuration. This can occur when an administrator pages through a running configuration on the standby unit while configuration synchronization is in process. See also the **show running-config** command in privileged EXEC mode and the **pager lines num** command in global configuration mode in the *Command Reference Guides* .

**Recommended Action** Avoid viewing or modifying the configuration on the standby unit when it first boots up and is in the process of establishing a failover connection with the active unit.

## 105022

**Error Message** %ASA-1-105022: (host) Config replication failed with reason = (reason)

**Explanation** When high availability replication fails, the message is generated. Where,

- *host*—Indicates the current failover unit, namely, primary or secondary.
- *reason*—The time out expiry reason for termination of the failover configuration replication:
  - CFG\_SYNC\_TIMEOUT—Where, the 60-second timer for the configuration to be replicated from active to standby lapses, and the device starts to reboot.
  - CFG\_PROGRESSION\_TIMEOUT—Where, the interval timer of 6 hours which governs the high availability configuration replication lapses.

**Recommended Action** None.

## 105031

**Error Message** %ASA-1-105031: Failover LAN interface is up

**Explanation** The LAN failover interface link is up.

**Recommended Action** None required.

## 105032

**Error Message** %ASA-1-105032: LAN Failover interface is down

**Explanation** The LAN failover interface link is down.

**Recommended Action** Check the connectivity of the LAN failover interface. Make sure that the speed or duplex setting is correct.

## 105033

**Error Message** %ASA-1-105033: LAN FO cmd Iface down and up again

**Explanation** LAN interface of failover gone down.

**Recommended Action** Verify the failover link, might be a communication problem.

## 105034

**Error Message** %ASA-1-105034: Receive a LAN\_FAILOVER\_UP message from peer.

**Explanation** The peer has just booted and sent the initial contact message.

**Recommended Action** None required.

## 105035

**Error Message** %ASA-1-105035: Receive a LAN failover interface down msg from peer.

**Explanation** The peer LAN failover interface link is down. The unit switches to active mode if it is in standby mode.

**Recommended Action** Check the connectivity of the peer LAN failover interface.

## 105036

**Error Message** %ASA-1-105036: dropped a LAN Failover command message.

**Explanation** The Secure Firewall ASA dropped an unacknowledged LAN failover command message, indicating a connectivity problem exists on the LAN failover interface.

**Recommended Action** Check that the LAN interface cable is connected.

## 105037

**Error Message** %ASA-1-105037: The primary and standby units are switching back and forth as the active unit.

**Explanation** The primary and standby units are switching back and forth as the active unit, indicating a LAN failover connectivity problem or software bug exists.

**Recommended Action** Make sure that the LAN interface cable is connected.

## 105038

**Error Message** %ASA-1-105038: (Primary) Interface count mismatch

**Explanation** When a failover occurs, the active Secure Firewall ASA detects a partial configuration in memory. Normally, this is caused by an interruption in the replication service. Primary can also be listed as Secondary for the secondary unit.

**Recommended Action** Once the failover is detected by the Secure Firewall ASA, the Secure Firewall ASA automatically reboots and loads the configuration from flash memory and/or resynchronizes with another Secure Firewall ASA. If failovers occur continuously, check the failover configuration and make sure that both Secure Firewall ASAs can communicate with each other.

## 105039

**Error Message** %ASA-1-105039: (Primary) Unable to verify the Interface count with mate. Failover may be disabled in mate.

**Explanation** Failover initially verifies that the number of interfaces configured on the primary and secondary Secure Firewall ASAs are the same. This message indicates that the primary Secure Firewall ASA is not able to verify the number of interfaces configured on the secondary Secure Firewall ASA. This message indicates that the primary Secure Firewall ASA is not able to communicate with the secondary Secure Firewall ASA over the failover interface. Primary can also be listed as Secondary for the secondary unit.



**Recommended Action** Verify the failover LAN, interface configuration, and status on the primary and secondary Secure Firewall ASAs. Make sure that the secondary Secure Firewall ASA is running the Secure Firewall ASA application and that failover is enabled.

## 105040

**Error Message** %ASA-1-105040: (Primary) Mate failover version is not compatible.

**Explanation** The primary and secondary Secure Firewall ASAs should run the same failover software version to act as a failover pair. This message indicates that the secondary Secure Firewall ASA failover software version is not compatible with the primary Secure Firewall ASA. Failover is disabled on the primary Secure Firewall ASA. Primary can also be listed as Secondary for the secondary Secure Firewall ASA.

**Recommended Action** Maintain consistent software versions between the primary and secondary Secure Firewall ASAs to enable failover.

## 105041

**Error Message** %ASA-1-105041: cmd failed during sync

**Explanation** Replication of the nameif command failed, because the number of interfaces on the active and standby units is not the same.

**Recommended Action** Verify that the units have the same number of interfaces. You might need to install additional interface modules, or use different devices. After the physical interfaces match, force a configuration sync by entering the **write standby** command.

## 105042

**Error Message** %ASA-1-105042: (Primary) Failover interface OK

**Explanation** The interface that sends failover messages could go down when physical status of the failover link is down or when L2 connectivity between the failover peers is lost resulting in dropping of ARP packets. This message is generated after restoring the L2 ARP connectivity.

**Recommended Action** None required.

## 105043

**Error Message** %ASA-1-105043: (Primary) Failover interface failed

**Explanation** This syslog is generated when physical status of the failover link is down or when L2 connectivity between the failover peers is lost. The disconnection results in loss of ARP packets flowing between the units.

**Recommended Action**

- Check the physical status of the failover link, ensure its physical and operational status is functional.
- Ensure ARP packets flow through the transit path of the failover links between the failover pairs.

## 105044

**Error Message** %ASA-1-105044: (Primary) Mate operational mode mode is not compatible with my mode mode.

**Explanation** When the operational mode (single or multiple) does not match between failover peers, failover will be disabled.

**Recommended Action** Configure the failover peers to have the same operational mode, and then reenoble failover.

## 105045

**Error Message** %ASA-1-105045: (Primary) Mate license (number contexts) is not compatible with my license (number contexts).

**Explanation** When the feature licenses do not match between failover peers, failover will be disabled.

**Recommended Action** Configure the failover peers to have the same feature license, and then reenoble failover.

## 105046

**Error Message** %ASA-1-105046: (Primary|Secondary) Mate has a different chassis

**Explanation** Two failover units have a different type of chassis. For example, one has a three-slot chassis; the other has a six-slot chassis.

**Recommended Action** Make sure that the two failover units are the same.

## 105047

**Error Message** %ASA-1-105047: Mate has a *io\_card\_name1* card in slot *slot\_number* which is different from my *io\_card\_name2*

**Explanation** The two failover units have different types of cards in their respective slots.

**Recommended Action** Make sure that the card configurations for the failover units are the same.

## 105048

**Error Message** %ASA-1-105048: (*unit* ) Mate's service module (*application* ) is different from mine (*application* )

**Explanation** The failover process detected that different applications are running on the service modules in the active and standby units. The two failover units are incompatible if different service modules are used.

- **unit**—Primary or secondary
- **application**—The name of the application, such as InterScan Security Card

**Recommended Action** Make sure that both units have identical service modules before trying to reenoble failover.

## 105050

**Error Message** %ASA-3-105050: ASAv ethernet interface mismatch

**Explanation** Number of Ethernet interfaces on standby unit is less than that on active unit.

**Recommended Action** Secure Firewall ASA with same number of interfaces should be paired up with each other. Verify that the units have the same number of interfaces. You might need to install additional interface modules, or use different devices. After the physical interfaces match, force a configuration sync by entering the **write standby** command.

## 105052

**Error Message** %ASA-3-105052 HA: cipher in use *algorithm name* strong encryption is AVAILABLE, please reboot to use strong cipher and preferably change the key in use.

**Explanation** When the failover key is configured prior to a license update, the weaker cipher is not switched to a stronger cipher automatically. This syslog is generated, every 30 seconds to alert that a weaker cipher is still being used when a stronger cipher is available.

**Example** %ASA-3-105052 HA cipher in use DES strong encryption is AVAILABLE, please reboot to use strong cipher and preferably change the key in use.

**Recommended Action** Remove the failover key configuration and reconfigure the key. Reload the standby, and then reload the active device.

## 105500

**Error Message** %ASA-5-105500: (Primary|Secondary) Started HA.

**Explanation** Cloud HA has been enabled on this ASA virtual.

**Recommended Action** None required.

## 105501

**Error Message** %ASA-5-105501: (Primary|Secondary) Stopped HA.

**Explanation** Cloud HA has been disabled on this ASA virtual.

**Recommended Action** None required.

## 105502

**Error Message** %ASA-1-105502: (Primary|Secondary) Restarting Cloud HA on this unit, reason: *string*.

**Explanation** An error occurred and caused this HA unit to restart Cloud HA. Possible values for the reason string are:

- failed to become Backup unit
- unable to create failover connection

**Recommended Action** None required.

## 105503

**Error Message** %ASA-5-105503: (Primary|Secondary) Internal state change from previous\_state to new\_state

**Explanation** There was a change to the internal HA state.

**Recommended Action** None required.

## 105504

**Error Message** %ASA-5-105504: (Primary|Secondary) Connected to peer peer-ip:port

**Explanation** This HA unit has established communication with its HA peer.

**Recommended Action** None required.

## 105505

**Error Message** %ASA-4-105505: (Primary|Secondary) Failed to connect to peer unit peer-ip:port

**Explanation** This HA unit has failed to establish communication with its HA peer.

**Recommended Action**

This may occur if there is no HA peer present. If there is an HA peer present with failover enabled there could be connectivity issue between peers. Verify using the show failover command that:

- The peer IP address configured on each unit is matches an interface IP address on the peer
- The peer port number on each unit matches the failover control (server) port on the peer
- The interfaces used for the peer connection are not shutdown
- Any IP routes required for IP connectivity are present

## 105506

**Error Message** %ASA-2-105506: (Primary|Secondary) Unable to create socket on port port for (failover connection | load balancer probes), error: error\_string

**Explanation** An internal error occurred while attempting to create a socket needed for the failover connection or resending to Azure load balancer probes.

**Recommended Action** Copy the error message, the configuration, and any details about the events leading up to the error, and contact Cisco TAC.

## 105507

**Error Message** %ASA-2-105507: (Primary|Secondary) Unable to bind socket on port port for (failover connection | load balancer probes), error: error\_string

**Explanation** An internal error occurred while attempting to start a socket needed for the failover connection or resending to Azure load balancer probes.

**Recommended Action** Copy the error message, the configuration, and any details about the events leading up to the error, and contact Cisco TAC.

## 105508

**Error Message** %ASA-2-105508: (Primary|Secondary) Error creating failover connection socket on port port

**Explanation** An internal error occurred while attempting to create a socket on the Active unit for exchanging failover control messages with the Backup unit.

**Recommended Action** This message is preceded by a 104509 or 104510 message. Follow the Recommended Action for the message that precedes this one.

## 105509

**Error Message** %ASA-3-105509: (Primary|Secondary) Error sending message\_name message to peer unit peer-ip, error: error\_string

**Explanation** An error occurred while attempting to send a failover control message to the peer unit.

**Recommended Action** If the error was not caused by the failure of the peer unit, copy the error message, the configuration, and any details about the events leading up to the error, and contact Cisco TAC.

## 105510

**Error Message** %ASA-3-105510: (Primary|Secondary) Error receiving message from peer unit peer-ip, error: error\_string

**Explanation** An error occurred while attempting to receive a failover control message to the peer unit.

**Recommended Action** If the error was not caused by the failure of the peer unit, copy the error message, the configuration, and any details about the events leading up to the error, and contact Cisco TAC.

## 105511

**Error Message** %ASA-3-105511: (Primary|Secondary) Incomplete read of message header of message from peer unit peer-ip: bytes bytes read of expected header\_length header bytes.

**Explanation** An error occurred while attempting to receive a failover control message to the peer unit.

**Recommended Action** If the error was not caused by the failure of the peer unit, copy the error message, the configuration, and any details about the events leading up to the error, and contact Cisco TAC.

## 105512

**Error Message** %ASA-3-105512: (Primary|Secondary) Error receiving message body of message from peer unit peer-ip, error: error\_string

**Explanation** An error occurred while attempting to receive a failover control message to the peer unit.

**Recommended Action** If the error was not caused by the failure of the peer unit, copy the error message, the configuration, and any details about the events leading up to the error, and contact Cisco TAC.

## 105513

**Error Message** %ASA-3-105513: (Primary|Secondary) Incomplete read of message body of message from peer unit peer-ip: bytes bytes read of expected message\_length message body bytes

**Explanation** An error occurred while attempting to receive a failover control message to the peer unit.

**Recommended Action** If the error was not caused by the failure of the peer unit, copy the error message, the configuration, and any details about the events leading up to the error, and contact Cisco TAC.

## 105514

**Error Message** %ASA-3-105514: (Primary|Secondary) Error occurred when responding to message\_name message received from peer unit peer-ip, error: error\_string

**Explanation** An error occurred while attempting to receive a failover control message to the peer unit.

**Recommended Action** If the error was not caused by the failure of the peer unit, copy the error message, the configuration, and any details about the events leading up to the error, and contact Cisco TAC.

## 105515

**Error Message** %ASA-3-105515: (Primary|Secondary) Error receiving message\_name message from peer unit peer-ip, error: error\_string

**Explanation** An error occurred while attempting to receive a failover control message to the peer unit.

**Recommended Action** If the error was not caused by the failure of the peer unit, copy the error message, the configuration, and any details about the events leading up to the error, and contact Cisco TAC.

## 105516

**Error Message** %ASA-3-105516: (Primary|Secondary) Incomplete read of message header of message\_name message from peer unit peer-ip: bytes bytes read of expected header\_length header bytes

**Explanation** An error occurred while attempting to receive a failover control message to the peer unit.

**Recommended Action** If the error was not caused by the failure of the peer unit, copy the error message, the configuration, and any details about the events leading up to the error, and contact Cisco TAC.

## 105517

**Error Message** %ASA-3-105517: (Primary|Secondary) Error receiving message body of message\_name message from peer unit peer-ip, error: error\_string

**Explanation** An error occurred while attempting to receive a failover control message to the peer unit.

**Recommended Action** If the error was not caused by the failure of the peer unit, copy the error message, the configuration, and any details about the events leading up to the error, and contact Cisco TAC.

## 105518

**Error Message** %ASA-3-105518: (Primary|Secondary) Incomplete read of message body of message\_name message from peer unit peer-ip: bytes bytes read of expected message\_length message body bytes

**Explanation** An error occurred while attempting to receive a failover control message to the peer unit.

**Recommended Action** If the error was not caused by the failure of the peer unit, copy the error message, the configuration, and any details about the events leading up to the error, and contact Cisco TAC.

## 105519

**Error Message** %ASA-3-105519: (Primary|Secondary) Invalid response to message\_name message received from peer unit peer-ip: type message\_type, version message\_version, length message\_length

**Explanation** An unexpected message was received in response to a failover control message.

**Recommended Action** Copy the error message, the configuration, and any details about the events leading up to the error, and contact Cisco TAC.

## 105520

**Error Message** %ASA-5-105520: (Primary|Secondary) Responding to Azure Load Balancer probes

**Explanation** The Active unit has begun responding to Azure Load Balancer probes.

**Recommended Action** None required

## 105521

**Error Message** %ASA-5-105521: (Primary|Secondary) No longer responding to Azure Load Balancer probes

**Explanation** The Backup unit has stopped responding to Azure Load Balancer probes.

**Recommended Action** None required

## 105522

**Error Message** %ASA-5-105522: (Primary|Secondary) Updating route route\_table\_name

**Explanation** The Active unit has started the process of updating an Azure route-table.

**Recommended Action** None required

## 105523

**Error Message** %ASA-5-105523: (Primary|Secondary) Updated route route\_table\_name

**Explanation** The Active unit has completed the process of updating an Azure route-table.

**Recommended Action** None required

## 105524

**Error Message** %ASA-4-105524: (Primary|Secondary) Transitioning to Negotiating state due to the presence of another Active HA unit.

**Explanation** Another Active HA unit was detected, transitioning unit to negotiating state.

**Recommended Action** None required

## 105524

**Error Message** %ASA-4-105524: (Primary|Secondary) Transitioning to Negotiating state due to the presence of another Active HA unit.

**Explanation** Another Active HA unit was detected, transitioning unit to negotiating state.

**Recommended Action** None required

## 105525

**Error Message** %ASA-2-105525: (Primary|Secondary) Incomplete configuration to initiate access token change request.

**Explanation** An attempt was made to acquire an access token but there was not enough configuration information need to initiate the request.

**Recommended Action** Ensure that an Azure authentication client ID, tenant ID and secret key are all present in the ASA configuration.

## 105526

**Error Message** %ASA-2-105526: (Primary|Secondary) Unexpected status in response to access token request: status\_string.

**Explanation** A response to an Azure access token request was received but the HTTP status code in the response was not 200 (OK).

**Recommended Action** Ensure that the Azure authentication client ID, tenant ID and secret key are all correct in the ASA configuration.

## 105527

**Error Message** %ASA-2-105527: (Primary|Secondary) Failure reading response to access token request

**Explanation** An internal error occurred while receiving a response to an Azure access token request.

**Recommended Action** Copy the error message, the configuration, and any details about the events leading up to the error, and contact Cisco TAC.



## 105528

**Error Message** %ASA-2-105528: (Primary|Secondary) No access token in response to access token request

**Explanation** A response to an Azure route change request was received but it did not contain an access\_token value.

**Recommended Action** Verify that the Azure authentication client ID, tenant ID and secret key are all correct in the ASA configuration.

## 105529

**Error Message** %ASA-2-105529: (Primary|Secondary) Error creating authentication header from access token

**Explanation** An internal error occurred while attempting to create an authentication header needed for changing Azure routes.

**Recommended Action** Copy the error message, the configuration, and any details about the events leading up to the error, and contact Cisco TAC.

## 105530

**Error Message** %ASA-2-105530: (Primary|Secondary) No response to access token request url

**Explanation** Azure route-table information was not able to be obtained for an Azure route-table change.

**Recommended Action** Verify route-table name is correct in ASA configuration and exists in Azure.

## 105531

**Error Message** %ASA-2-105531: (Primary|Secondary) Failed to obtain route-table information needed for change request for route-table route\_table\_name

**Explanation** Azure route-table information was not able to be obtained for an Azure route-table change.

**Recommended Action** Verify route-table name is correct in ASA configuration and exists in Azure.

## 105532

**Error Message** %ASA-2-105532: (Primary|Secondary) Unexpected status in response to route-table change request for route-table route\_table\_name: status\_string

**Explanation** A response to an Azure route-tablechange request was received but the HTTP status code in the response was not 200 (OK).

**Recommended Action** Verify that the configured Azure subscription ID, route-table name and route-table resource group are correct.

## 105533

**Error Message** %ASA-2-105533: (Primary|Secondary) Failure reading response to route-table change request for route-table route\_table\_name

**Explanation** An internal error occurred while receiving a response to an Azure route-table change request.

**Recommended Action** Copy the error message, the configuration, and any details about the events leading up to the error, and contact Cisco TAC.

## 105534

**Error Message** %ASA-2-105534: (Primary|Secondary) No provisioning state in response to route-table change request route-table route\_table\_name

**Explanation** A response to an Azure route-table change request was received but it did not contain a provisioningState value containing the route-table change status.

**Recommended Action** Copy the error message, the configuration, and any details about the events leading up to the error, and contact Cisco TAC.

## 105535

**Error Message** %ASA-2-105535: (Primary|Secondary) No response to route-table change request for route-table route\_table\_name from url

**Explanation** No response was received to an Azure route-table change request.

**Recommended Action** Verify that management.azure.com is reachable from the ASA virtual.

## 105536

**Error Message** %ASA-2-105536: (Primary|Secondary) Failed to obtain Azure authentication header for route status request for route route\_name

**Explanation** An Azure access token was not able to be obtained for an Azure route status query.

**Recommended Action** See the Recommended Action of access token related message that precedes this message.

## 105537

**Error Message** %ASA-2-105537: (Primary|Secondary) Unexpected status in response to route state request for route route\_name: status\_string

**Explanation** A response to an Azure route state request was received but the HTTP status code in the response was not 200 (OK).

**Recommended Action** Verify that the configured Azure subscription ID, route table name and route table resource group are correct.

## 105538

**Error Message** %ASA-2-105538: (Primary|Secondary) Failure reading response to route state request for route route\_name

**Explanation** An internal error occurred while receiving a response to an Azure route state request.

**Recommended Action** Copy the error message, the configuration, and any details about the events leading up to the error, and contact Cisco TAC.

## 105539

**Error Message** %ASA-2-105539: (Primary|Secondary) No response to route state request for route route\_name from url

**Explanation** No response was received to an Azure route state request.

**Recommended Action** Verify that management.azure.com is reachable from the ASA virtual.

## 105540

**Error Message** %ASA-2-105540: (Primary|Secondary) No route-tables configured

**Explanation** No Azure route-tables were detected to change.

**Recommended Action** Confirm that route-tables are correctly configured in ASA configuration.

## 105541

**Error Message** %ASA-2-105541: (Primary|Secondary) Failed to update route-table route\_table\_name, provisioning state: state\_string

**Explanation** A response to an Azure route-table state request was received that contained a provisioningState that indicated a failure to update the route-table.

**Recommended Action** The Active unit will make three attempts to update an Azure route-table. If all three attempts fail, copy the error message, the configuration, and any details about the events leading up to the error, and contact Cisco TAC.

## 105542

**Error Message** %ASA-5-105542: (Primary|Secondary) Enabling load balancer probe responses

**Explanation** The Active unit is will now respond to probes from the Azure Load Balancer.

**Recommended Action** None required.

## 105543

**Error Message** %%ASA-5-105543: (Primary|Secondary) Disabling load balancer probe responses

**Explanation** The Active unit is no longer responding to probes from the Azure Load Balancer.

**Recommended Action** None required.

## 105544

**Error Message** %ASA-2-105544: (Primary|Secondary) Error creating load balancer probe socket on port port

**Explanation** An internal error occurred while attempting to create a socket for responding to probes from an Azure Load Balancer.

**Recommended Action** This message will be preceded by a 104509 or 104510 message. Follow the Recommended Action for the message that precedes this one.

## 105545

**Error Message** %ASA-3-105545: (Primary|Secondary) Error starting load balancer probe socket on port port, error code: error\_code

**Explanation** An internal error occurred while attempting to start receiving probes from an Azure Load Balancer. The Active unit will continue to attempt to enable the receiving of probes.

**Recommended Action** If this condition persists copy the error message, the configuration, and any details about the events leading up to the error, and contact Cisco TAC.

## 105546

**Error Message** %ASA-3-105546: (Primary|Secondary) Error starting load balancer probe handler

**Explanation** An internal error occurred while attempting to create a process for receiving probes from an Azure Load Balancer.

**Recommended Action** Copy the error message, the configuration, and any details about the events leading up to the error, and contact Cisco TAC.

## 105547

**Error Message** %ASA-3-105547: (Primary|Secondary) Error generating encryption key for Azure secret key

**Explanation** An internal error occurred while attempting to generate the encryption key used for encrypting the Azure secret key in the configuration.

**Recommended Action** Copy the error message, the configuration, and any details about the events leading up to the error, and contact Cisco TAC.

## 105548

**Error Message** %ASA-3-105548: (Primary|Secondary) Error storing encryption key for Azure secret key

**Explanation** An internal error occurred while attempting to store the encryption key used for encrypting the Azure secret key in the configuration.

**Recommended Action** Copy the error message, the configuration, and any details about the events leading up to the error, and contact Cisco TAC.

## 105549

**Error Message** %ASA-3-105549: (Primary|Secondary) Error retrieving encryption key for Azure secret key

**Explanation** An internal error occurred while attempting to retrieve the encryption key used for encrypting the Azure secret key in the configuration.

**Recommended Action** Copy the error message, the configuration, and any details about the events leading up to the error, and contact Cisco TAC.

## 105550

**Error Message** %ASA-3-105550: (Primary|Secondary) Error encrypting Azure secret key

**Explanation** An internal error occurred while encrypting the Azure secret key in the configuration.

**Recommended Action** Copy the error message, the configuration, and any details about the events leading up to the error, and contact Cisco TAC.

## 105551

**Error Message** %ASA-3-105551: (Primary|Secondary) Error encrypting Azure secret key

**Explanation** An internal error occurred while decrypting the Azure secret key in the configuration.

**Recommended Action** Copy the error message, the configuration, and any details about the events leading up to the error, and contact Cisco TAC.

## 105552

**Error Message** %ASA-5-105552: (Primary|Secondary) Stopped HA

**Explanation** Cloud HA has been disabled on this ASA virtual.

**Recommended Action** None required.

## 105553

**Error Message** %ASA-4-105553: (Primary|Secondary) Detected another Active HA unit

**Explanation** Another Active HA unit was detected.

**Recommended Action** None required

## 106001

**Error Message** %ASA-2-106001: Inbound TCP connection denied from *IP\_address/port* to *IP\_address/port* flags *tcp\_flags* on interface *interface\_name*

**Explanation** An attempt was made to connect to an inside address is denied by the security policy that is defined for the specified traffic type. The IP address displayed is the real IP address instead of the IP address that appears through NAT. Possible *tcp\_flags* values correspond to the flags in the TCP header that were

present when the connection was denied. For example, a TCP packet arrived for which no connection state exists in the Secure Firewall ASA, and it was dropped. The `tcp_flags` in this packet are FIN and ACK.

The `tcp_flags` are as follows:

- ACK—The acknowledgment number was received
- FIN—Data was sent
- PSH—The receiver passed data to the application
- RST—The connection was reset
- SYN—Sequence numbers were synchronized to start a connection
- URG—The urgent pointer was declared valid

**Recommended Action** None required.

## 106002

**Error Message** %ASA-2-106002: *protocol* Connection denied by outbound list `acl_ID` src `inside_address` dest `outside_address`

**Explanation** The specified connection failed because of an **outbound deny** command. The **protocol** variable can be ICMP, TCP, or UDP.

**Recommended Action** Use the **show outbound** command to check outbound lists.

## 106006

**Error Message** %ASA-2-106006: Deny inbound UDP from `outside_address/outside_port` to `inside_address/inside_port` on interface `interface_name`.

**Explanation** An inbound UDP packet was denied by the security policy that is defined for the specified traffic type.

**Recommended Action** None required.

## 106007

**Error Message** %ASA-2-106007: Deny inbound UDP from `outside_address/outside_port` to `inside_address/inside_port` due to DNS {Response|Query}.

**Explanation** A UDP packet containing a DNS query or response was denied.

**Recommended Action** If the inside port number is 53, the inside host probably is set up as a caching name server. Add an **access-list** command statement to permit traffic on UDP port 53 and a translation entry for the inside host. If the outside port number is 53, a DNS server was probably too slow to respond, and the query was answered by another server.

## 106010

**Error Message** %ASA-3-106010: Deny inbound *protocol* src `[interface_name : source_address/source_port ]` `[[[idfw_user | FQDN_string ], sg_info ]]` dst `[interface_name : dest_address /dest_port ]` `[[[idfw_user | FQDN_string ], sg_info ]]`

**Explanation** An inbound connection was denied by your security policy.

**Recommended Action** Modify the security policy if traffic should be permitted. If the message occurs at regular intervals, contact the remote peer administrator.

## 106011

**Error Message** %ASA-3-106011: Deny inbound (No xlate) protocol src Interface:IP/port dst Interface-nameif:IP/port

**Explanation** The message appears under normal traffic conditions if there are internal users that are accessing the Internet through a web browser. Any time a connection is reset, when the host at the end of the connection sends a packet after the Secure Firewall ASA receives the connection reset, this message appears. It can typically be ignored.

**Recommended Action** Prevent this message from getting logged to the syslog server by entering the **no logging message 106011** command.

## 106012

**Error Message** %ASA-6-106012: Deny IP from *IP\_address* to *IP\_address* , IP options hex.

**Explanation** An IP packet was seen with IP options. Because IP options are considered a security risk, the packet was discarded.

**Recommended Action** Contact the remote host system administrator to determine the problem. Check the local site for loose source routing or strict source routing.

## 106013

**Error Message** %ASA-2-106013: Dropping echo request from *IP\_address* to PAT address *IP\_address*

**Explanation** The Secure Firewall ASA discarded an inbound ICMP Echo Request packet with a destination address that corresponds to a PAT global address. The inbound packet is discarded because it cannot specify which PAT host should receive the packet.

**Recommended Action** None required.

## 106014

**Error Message** %ASA-3-106014: Deny inbound icmp src *interface\_name* : *IP\_address* ([[*idfw\_user* | *FQDN\_string* ], *sg\_info* ]) dst *interface\_name* : *IP\_address* ([[*idfw\_user* | *FQDN\_string* ], *sg\_info* ]) (type *dec* , code *dec* )

**Explanation** The Secure Firewall ASA denied any inbound ICMP packet access. By default, all ICMP packets are denied access unless specifically allowed.

**Recommended Action** None required.

## 106015

**Error Message** %ASA-6-106015: Deny TCP (no connection) from *IP\_address* /port to *IP\_address* /port flags *tcp\_flags* on interface *interface\_name*.

**Explanation** The Secure Firewall ASA discarded a TCP packet that has no associated connection in the Secure Firewall ASA connection table. The Secure Firewall ASA looks for a SYN flag in the packet, which indicates a request to establish a new connection. If the SYN flag is not set, and there is no existing connection, the Secure Firewall ASA discards the packet.

**Recommended Action** None required unless the Secure Firewall ASA receives a large volume of these invalid TCP packets. If this is the case, trace the packets to the source and determine the reason these packets were sent.

## 106016

**Error Message** %ASA-2-106016: Deny IP spoof from (IP\_address ) to IP\_address on interface interface\_name.

**Explanation** A packet arrived at the Secure Firewall ASA interface that has a destination IP address of 0.0.0.0 and a destination MAC address of the Secure Firewall ASA interface. In addition, this message is generated when the Secure Firewall ASA discarded a packet with an invalid source address, which may include one of the following or some other invalid address:

- Loopback network (127.0.0.0)
- Broadcast (limited, net-directed, subnet-directed, and all-subnets-directed)
- The destination host (land.c)

To further enhance spoof packet detection, use the **icmp** command to configure the Secure Firewall ASA to discard packets with source addresses belonging to the internal network, because the **access-list** command has been deprecated and is no longer guaranteed to work correctly.

**Recommended Action** Determine if an external user is trying to compromise the protected network. Check for misconfigured clients.

## 106017

**Error Message** %ASA-2-106017: Deny IP due to Land Attack from IP\_address to IP\_address

**Explanation** The Secure Firewall ASA received a packet with the IP source address equal to the IP destination, and the destination port equal to the source port. This message indicates a spoofed packet that is designed to attack systems. This attack is referred to as a Land Attack.

**Recommended Action** If this message persists, an attack may be in progress. The packet does not provide enough information to determine where the attack originates.

## 106018

**Error Message** %ASA-2-106018: ICMP packet type ICMP\_type denied by outbound list acl\_ID src inside\_address dest outside\_address

**Explanation** The outgoing ICMP packet with the specified ICMP from local host (inside\_address) to the foreign host (outside\_address) was denied by the outbound ACL list.

**Recommended Action** None required.



## 106020

**Error Message** %ASA-2-106020: Deny IP teardrop fragment (size = number, offset = number) from *IP\_address* to *IP\_address*

**Explanation** The Secure Firewall ASA discarded an IP packet with a teardrop signature containing either a small offset or fragment overlapping. This is a hostile event that circumvents the Secure Firewall ASA or an Intrusion Detection System.

**Recommended Action** Contact the remote peer administrator or escalate this issue according to your security policy.

## 106021

**Error Message** %ASA-1-106021: Deny protocol reverse path check from *source\_address* to *dest\_address* on interface *interface\_name*

**Explanation** An attack is in progress. Someone is attempting to spoof an IP address on an inbound connection. Unicast RPF, also known as reverse route lookup, detected a packet that does not have a source address represented by a route and assumes that it is part of an attack on your Secure Firewall ASA.

This message appears when you have enabled Unicast RPF with the `ip verify reverse-path` command. This feature works on packets input to an interface; if it is configured on the outside, then the Secure Firewall ASA checks packets arriving from the outside.

The Secure Firewall ASA looks up a route based on the *source\_address*. If an entry is not found and a route is not defined, then this message appears and the connection is dropped.

If there is a route, the Secure Firewall ASA checks which interface it corresponds to. If the packet arrived on another interface, it is either a spoof or there is an asymmetric routing environment that has more than one path to a destination. The Secure Firewall ASA does not support asymmetric routing.

If the Secure Firewall ASA is configured on an internal interface, it checks static route command statements or RIP, and if the *source\_address* is not found, then an internal user is spoofing their address.

**Recommended Action** Even though an attack is in progress, if this feature is enabled, no user action is required. The Secure Firewall ASA repels the attack.

## 106022

**Error Message** %ASA-1-106022: Deny protocol connection spoof from *source\_address* to *dest\_address* on interface *interface\_name*

**Explanation** A packet matching a connection arrived on a different interface from the interface on which the connection began. In addition, the `ip verify reverse-path` command is not configured.

For example, if a user starts a connection on the inside interface, but the Secure Firewall ASA detects the same connection arriving on a perimeter interface, the Secure Firewall ASA has more than one path to a destination. This is known as asymmetric routing and is not supported on the Secure Firewall ASA.

An attacker also might be attempting to append packets from one connection to another as a way to break into the Secure Firewall ASA. In either case, the Secure Firewall ASA shows this message and drops the connection.

**Recommended Action** Check that the routing is not asymmetric.

## 106023

**Error Message** %ASA-4-106023: Deny protocol src [interface\_name :source\_address /source\_port] [(idfw\_user |FQDN\_string ), sg\_info ]) dst interface\_name :dest\_address /dest\_port [(idfw\_user |FQDN\_string ), sg\_info ]) [type {string }, code {code }] by access\_group acl\_ID [0x8ed66b60, 0xf8852875]

**Explanation** A real IP packet was denied by the ACL. This message appears even if you do not have the **log** option enabled for an ACL. The IP address is the real IP address instead of the values that display through NAT. Both user identity information and FQDN information is provided for the IP addresses if a matched one is found. The Secure Firewall ASA logs either identity information (domain\user) or FQDN (if the username is not available). If the identity information or FQDN is available, the Secure Firewall ASA logs this information for both the source and destination.

**Recommended Action** If messages persist from the same source address, a footprinting or port scanning attempt might be occurring. Contact the remote host administrator.

## 106024

**Error Message** %ASA-2-106024: Access rules memory exhausted

**Explanation** The access list compilation process has run out of memory. All configuration information that has been added since the last successful access list was removed from the Secure Firewall ASA, and the most recently compiled set of access lists will continue to be used.

**Recommended Action** Access lists, AAA, ICMP, SSH, Telnet, and other rule types are stored and compiled as access list rule types. Remove some of these rule types so that others can be added.

## 106025, 106026

**Error Message** %ASA-6-106025: Failed to determine the security context for the packet:sourceVlan:source\_address dest\_address source\_port dest\_port protocol

**Error Message** %ASA-6-106026: Failed to determine the security context for the packet:sourceVlan:source\_address dest\_address source\_port dest\_port protocol

**Explanation** The security context of the packet in multiple context mode cannot be determined. Both messages can be generated for IP packets being dropped in either router and transparent mode.

**Recommended Action** None required.

## 106027

**Error Message** %ASA-4-106027:acl\_ID: Deny src [source address] dst [destination address] by access-group "access-list name"

**Explanation** An non IP packet was denied by the ACL. This message is displayed even if you do not have the log option enabled for an extended ACL.

**Recommended Action** If messages persist from the same source address, it might indicate a foot-printing or port-scanning attempt. Contact the remote host administrator.

## 106100

**Error Message** %ASA-6-106100: access-list *acl\_ID* {permitted | denied | est-allowed} *protocol interface\_name /source\_address (source\_port) (idfw\_user , sg\_info) interface\_name /dest\_address (dest\_port) (idfw\_user , sg\_info) hit-cnt number* ({first hit | *number* -second interval}) hash codes

**Explanation** The initial occurrence or the total number of occurrences during an interval are listed. This message provides more information than message 106023, which only logs denied packets, and does not include the hit count or a configurable level.

When an access-list line has the *log* argument, it is expected that this message ID might be triggered because of a nonsynchronized packet reaching the Secure Firewall ASA and being evaluated by the access list. For example, if an ACK packet is received on the Secure Firewall ASA (for which no TCP connection exists in the connection table), the Secure Firewall ASA might generate message 106100, indicating that the packet was permitted; however, the packet is later correctly dropped because of no matching connection.

The following list describes the message values:

- *permitted | denied | est-allowed*—These values specify if the packet was permitted or denied by the ACL. If the value is *est-allowed*, the packet was denied by the ACL but was allowed for an already established session (for example, an internal user is allowed to access the Internet, and responding packets that would normally be denied by the ACL are accepted).
- *protocol*—TCP, UDP, ICMP, or an IP protocol number.
- *interface\_name*—The interface name for the source or destination of the logged flow. The VLAN interfaces are supported.
- *source\_address*—The source IP address of the logged flow. The IP address is the real IP address instead of the values that display through NAT.
- *dest\_address*—The destination IP address of the logged flow. The IP address is the real IP address instead of the values that display through NAT.
- *source\_port*—The source port of the logged flow (TCP or UDP). For ICMP, the number after the source port is the message type.
- *idfw\_user*—The user identity username, including the domain name that is added to the existing syslog when the Secure Firewall ASA can find the username for the IP address.
- *sg\_info*—The security group tag that is added to the syslog when the Secure Firewall ASA can find a security group tag for the IP address. The security group name is displayed with the security group tag, if available.
- *dest\_port*—The destination port of the logged flow (TCP or UDP). For ICMP, the number after the destination port is the ICMP message code, which is available for some message types. For type 8, it is always 0. For a list of ICMP message types, see the following URL:  
<http://www.iana.org/assignments/icmp-parameters/icmp-parameters.xml>.
- *hit-cnt number*—The number of times this flow was permitted or denied by this ACL entry in the configured time interval. The value is 1 when the Secure Firewall ASA generates the first message for this flow.
- *first hit*—The first message generated for this flow.
- *number -second interval*—The interval in which the hit count is accumulated. Set this interval using the **access-list** command with the **interval** option.
- *hash codes*—Two are always printed for the object group ACE and the constituent regular ACE. Values are determined on which ACE that the packet hit. To display these hash codes, enter the **show-access list** command.

**Recommended Action** None required.

## 106101

**Error Message** %ASA-1-106101 Number of cached deny-flows for ACL log has reached limit (*number*).

**Explanation** If you configured the **log** option for an ACL **deny** statement (**access-list id deny** command), and a traffic flow matches the ACL statement, the Secure Firewall ASA caches the flow information. This message indicates that the number of matching flows that are cached on the Secure Firewall ASA exceeds the user-configured limit (using the **access-list deny-flow-max** command). This message might be generated as a result of a DoS attack.

- *number*— The limit configured using the **access-list deny-flow-max** command

**Recommended Action** None required.

## 106102

**Error Message** %ASA-6-106102: access-list *acl\_ID* {permitted|denied} protocol for user *username* *interface\_name* /*source\_address* *source\_port* *interface\_name* /*dest\_address* *dest\_port* hit-cnt *number* {first hit|*number* -second interval} hash codes

**Explanation** A packet was either permitted or denied by an access-list that was applied through a VPN filter. This message is the VPN/AAA filter equivalent of message 106100.

**Recommended Action** None required.

## 106103

**Error Message** %ASA-4-106103: access-list *acl\_ID* denied protocol for user *username* *interface\_name* /*source\_address* *source\_port* *interface\_name* /*dest\_address* *dest\_port* hit-cnt *number* first hit hash codes

**Explanation** A packet was denied by an access-list that was applied through a VPN filter. This message is the VPN/AAA filter equivalent of message 106023.

**Recommended Action** None required.

## 107001

**Error Message** %ASA-1-107001: RIP auth failed from *IP\_address* : version=*number*, type=*string*, mode=*string*, sequence=*number* on interface *interface\_name*

**Explanation** The Secure Firewall ASA received a RIP reply message with bad authentication. This message might be caused by a misconfiguration on the router or the Secure Firewall ASA or by an unsuccessful attempt to attack the routing table of the Secure Firewall ASA.

**Recommended Action** This message indicates a possible attack and should be monitored. If you are not familiar with the source IP address listed in this message, change your RIP authentication keys between trusted entities. An attacker might be trying to determine the existing keys.

## 107002

**Error Message** %ASA-1-107002: RIP pkt failed from *IP\_address* : version=number on interface *interface\_name*

**Explanation** A router bug, a packet with non-RFC values inside, or a malformed entry may have caused this message to appear. This should not happen, and may be an attempt to exploit the routing table of the ASA.

**Recommended Action** This message indicates a possible attack and should be monitored. The packet has passed authentication, if enabled, and bad data is in the packet. Monitor the situation and change the keys if there are any doubts about the originator of the packet.

## 108002

**Error Message** %ASA-2-108002: SMTP replaced string: out *source\_address* in *inside\_address* data: *string*

**Explanation** A Mail Guard (SMTP) message has been generated by the inspect esmtp command. The ASA has replaced an invalid character in an e-mail address with a space.

**Recommended Action** None required.

## 108003

**Error Message** %ASA-2-108003: Terminating ESMTP/SMTP connection; malicious pattern detected in the mail address from *source\_interface:source\_address/source\_port* to *dest\_interface:dest\_address/dset\_port* . Data:*string*

**Explanation** The ASA has detected a malicious pattern in an e-mail address and drops the connection. An attack is in progress.

**Recommended Action** None required.

## 108004

**Error Message** %ASA-4-108004: *action\_class: action* ESMTP *req\_resp* from *src\_ifc:sip |sport* to *dest\_ifc:dip |dport;further\_info*

**Explanation** An ESMTP classification is performed on an ESMTP message, and the specified criteria are satisfied. The configured action is taken.

- **action\_class**—The class of action: ESMTP Classification for ESMTP match commands; ESMTP Parameter for parameter commands
- **action**—Action taken: Dropped, Dropped connection for, Reset connection for, or Masked header flags for
- **req\_resp**—Request or Response
- **src\_ifc**—Source interface name
- **sip|sport**—Source IP address or source port
- **dest\_ifc**—Destination interface name
- **dip|dport**—Destination IP address or destination port
- **further info**—One of the following:

For a single match command: matched Class *id* : *match\_command* (for example, matched Class 1234: match body length 100).

For parameter commands: *parameter-command* : *descriptive-message* (for example, mail-relay: No Mail Relay allowed)

**Recommended Action** None required.

## 108005

**Error Message** %ASA-6-108005: *action\_class*: Received ESMTP req\_resp from *src\_ifc:sip* |*sport* to *dest\_ifc:dip* |*dport*; *further\_info*

**Explanation** An ESMTP classification is performed on an ESMTP message, and the specified criteria are satisfied. The standalone log action is taken.

- **action\_class**—The class of action: ESMTP Classification for ESMTP match commands; ESMTP Parameter for parameter commands
- **req\_resp**—Request or Response
- **src\_ifc**—Source interface name
- **sip|sport**—Source IP address or source port
- **dest\_ifc**—Destination interface name
- **dip|dport**—Destination IP address or destination port
- **further\_info**—One of the following:

For a single match command: matched Class *id* : *match\_command* (for example, matched Class 1234: match body length 100)

For parameter commands (commands under the parameter section): *parameter-command* : *descriptive-message* (for example, mail-relay: No Mail Relay allowed)

**Recommended Action** None required.

## 108006

**Error Message** %ASA-7-108006: Detected ESMTP size violation from *src\_ifc:sip* |*sport* to *dest\_ifc:dip* |*dport*; declared size is: *decl\_size*, actual size is *act\_size*.

**Explanation** This event is generated when an ESMTP message size exceeds the size declared in the RCPT command.

- **src\_ifc**—Source interface name
- **sip|sport**—Source IP address or source port
- **dest\_ifc**—Destination interface name
- **dip|dport**—Destination IP address or destination port
- **decl\_size**—Declared size
- **act\_size**—Actual size

**Recommended Action** None required.

## 108007

**Error Message** %ASA-6-108007: TLS started on ESMTP session between client *client-side interface-name* : *client IP address /client port* and server *server-side interface-name* : *server IP address /server port*

**Explanation** On an ESMTP connection, the server has responded with a 220 reply code to the client STARTTLS command. The ESMTP inspection engine no longer inspects the traffic on this connection.

- *client-side interface-name* —The name for the interface that faces the client side
- *client IP address* —The IP address of the client
- *client port* —The TCP port number for the client
- *server-side interface-name* —The name for the interface that faces the server side
- *server IP address* —The IP address of the server
- *server port* —The TCP port number for the server

**Recommended Action** Log and review the message. Check whether the ESMTP policy map associated with this connection has the allow-tls action log setting. If not, contact the Cisco TAC.

## 109001

**Error Message** %ASA-6-109001: Auth start for user *user* from *inside\_address/inside\_port* to *outside\_address/outside\_port*

**Explanation** The ASA is configured for AAA and detects an authentication request by the specified user.

**Recommended Action** None required.

## 109002

**Error Message** %ASA-6-109002: Auth from *inside\_address/inside\_port* to *outside\_address/outside\_port* failed (*server IP\_address* failed) on interface *interface\_name*.

**Explanation** An authentication request failed because the specified authentication server cannot be contacted by the module.

**Recommended Action** Check that the authentication daemon is running on the specified authentication server.

## 109003

**Error Message** %ASA-6-109003: Auth from *inside\_address* to *outside\_address/outside\_port* failed (all servers failed) on interface *interface\_name*, so marking all servers ACTIVE again.

**Explanation** No authentication server can be found.

**Recommended Action** Ping the authentication servers from the ASA. Make sure that the daemons are running.

## 109005

**Error Message** %ASA-6-109005: Authentication succeeded for user *user* from *inside\_address/inside\_port* to *outside\_address/outside\_port* on interface *interface\_name*.

**Explanation** The specified authentication request succeeded.

**Recommended Action** None required.

## 109006

**Error Message** %ASA-6-109006: Authentication failed for user user from inside\_address/inside\_port to outside\_address/outside\_port on interface interface\_name.

**Explanation** The specified authentication request failed, possibly because of an incorrect password. The username is hidden when invalid or unknown, but appears when valid or the **no logging hide username** command has been configured.

**Recommended Action** None required.

## 109007

**Error Message** %ASA-6-109007: Authorization permitted for user user from inside\_address/inside\_port to outside\_address/outside\_port on interface interface\_name.

**Explanation** The specified authorization request succeeded.

**Recommended Action** None required.

## 109008

**Error Message** %ASA-6-109008: Authorization denied for user user from outside\_address/outside\_port to inside\_address/ inside\_port on interface interface\_name.

**Explanation** A user is not authorized to access the specified address, possibly because of an incorrect password.

**Recommended Action** None required.

## 109010

**Error Message** %ASA-3-109010: Auth from inside\_address/inside\_port to outside\_address/outside\_port failed (too many pending auths) on interface interface\_name.

**Explanation** An authentication request cannot be processed because the server has too many requests pending.

**Recommended Action** Check to see if the authentication server is too slow to respond to authentication requests. Enable the Flood Defender feature with the floodguard enable command.

## 109011

**Error Message** %ASA-2-109011: Authen Session Start: user 'user ', sid number

**Explanation** An authentication session started between the host and the Secure Firewall ASA and has not yet completed.

**Recommended Action** None required.



## 109012

**Error Message** %ASA-5-109012: Authen Session End: user 'user', sid number, elapsed number seconds

**Explanation** The authentication cache has timed out. Users must reauthenticate on their next connection. You can change the duration of this timer with the timeout uauth command.

**Recommended Action** None required.

## 109013

**Error Message** %ASA-3-109013: User must authenticate before using this service

**Explanation** The user must be authenticated before using the service.

**Recommended Action** Authenticate using FTP, Telnet, or HTTP before using the service.

## 109014

**Error Message** %ASA-7-109014: A non-Telnet connection was denied to the configured virtual Telnet IP address.

**Explanation** A request to authenticate did not have a corresponding request for authorization.

**Recommended Action** Ensure that both the aaa authentication and aaa authorization command statements are included in the configuration.

## 109016

**Error Message** %ASA-3-109016: Can't find authorization ACL *acl\_ID* for user 'user '

**Explanation** The specified on the AAA server for this user does not exist on the Secure Firewall ASA. This error can occur if you configure the AAA server before you configure the Secure Firewall ASA. The Vendor-Specific Attribute (VSA) on your AAA server might be one of the following values:

- `acl=acl_ID`
- `shell:acl=acl_ID`
- `ACS:CiscoSecured-Defined-ACL=acl_ID`

**Recommended Action** Add the ACL to the Secure Firewall ASA, making sure to use the same name specified on the AAA server.

## 109017

**Error Message** %ASA-4-109017: User at *IP\_address* exceeded auth proxy connection limit (max)

**Explanation** A user has exceeded the user authentication proxy limit, and has opened too many connections to the proxy.

**Recommended Action** Increase the proxy limit by entering the **proxy-limit** *proxy\_limit* command, or ask the user to close unused connections. If the error persists, it may indicate a possible DoS attack.

## 109018

**Error Message** %ASA-3-109018: Downloaded ACL *acl\_ID* is empty

**Explanation** The downloaded authorization has no ACEs. This situation might be caused by misspelling the attribute string *ip:inacl#* or omitting the access-list command.

```
junk:junk# 1=permit tcp any any eq junk ip:inacl#1=
```

**Recommended Action** Correct the ACL components that have the indicated error on the AAA server.

## 109019

**Error Message** %ASA-3-109019: Downloaded ACL *acl\_ID* has parsing error; ACE string

**Explanation** An error occurred during parsing the sequence number NNN in the attribute string *ip:inacl#NNN=* of a downloaded authorization. The reasons include: - missing = - contains nonnumeric, nonpace characters between # and = - NNN is greater than 999999999.

```
ip:inacl# 1 permit tcp any any
ip:inacl# 1junk2=permit tcp any any
ip:inacl# 1000000000=permit tcp any any
```

**Recommended Action** Correct the ACL element that has the indicated error on the AAA server.

## 109020

**Error Message** %ASA-3-109020: Downloaded ACL has config error; ACE

**Explanation** One of the components of the downloaded authorization has a configuration error. The entire text of the element is included in the message. This message is usually caused by an invalid access-list command statement.

**Recommended Action** Correct the ACL component that has the indicated error on the AAA server.

## 109021

**Error Message** %ASA-7-109021: Uauth null proxy error

**Explanation** An internal user authentication error has occurred.

**Recommended Action** None required. However, if this error appears repeatedly, contact the Cisco TAC.

## 109022

**Error Message** %ASA-4-109022: exceeded HTTPS proxy process limit

**Explanation** For each HTTPS authentication, the ASA dedicates a process to service the authentication request. When the number of concurrently running processes exceeds the system-imposed limit, the ASA does not perform the authentication, and this message appears.

**Recommended Action** None required.

## 109023

**Error Message** %ASA-3-109023: User from *source\_address /source\_port* to *dest\_address /dest\_port* on interface *outside\_interface* must authenticate before using this service.

**Explanation** Based on the configured policies, you need to be authenticated before you can use this service port.

**Recommended Action** Authenticate using Telnet, FTP, or HTTP before attempting to use this service port.

## 109024

**Error Message** %ASA-6-109024: Authorization denied from *source\_address /source\_port* to *dest\_address /dest\_port* (not authenticated) on interface *interface\_name* using *protocol*

**Explanation** The ASA is configured for AAA and a user attempted to make a TCP connection across the ASA without prior authentication.

**Recommended Action** None required.

## 109025

**Error Message** %ASA-6-109025: Authorization denied (acl=**acl\_ID**) for user '**user**' from *source\_address /source\_port* to *dest\_address /dest\_port* on interface *interface\_name* using *protocol*

**Explanation** The check failed. The check either matched a deny or did not match anything, such as an implicit deny. The connection was denied by the user **acl\_ID**, which was defined according to the AAA authorization policy on the Cisco Secure Access Control Server (ACS).

**Recommended Action** None required.

## 109026

**Error Message** %ASA-3-109026: [*aaa protocol*] Invalid reply digest received; shared server key may be mismatched.

**Explanation** The response from the AAA server cannot be validated. The configured server key is probably incorrect. This message may be generated during transactions with RADIUS or TACACS+ servers.

Verify that the server key, configured using the **aaa-server** command, is correct.

## 109027

**Error Message** %ASA-4-109027: [*aaa protocol*] Unable to decipher response message Server = *server\_IP\_address* , User = *user*

**Explanation** The response from the AAA server cannot be validated. The configured server key is probably incorrect. This message may be displayed during transactions with RADIUS or TACACS+ servers. The *server\_IP\_address* is the IP address of the relevant AAA server. The user is the user name associated with the connection.

**Recommended Action** Verify that the server key, configured using the **aaa-server** command, is correct.

## 109028

**Error Message** %ASA-4-109028: aaa bypassed for same-security traffic from ingress\_ interface:source\_address/source\_port to egress\_interface:dest\_address/dest\_port

**Explanation** AAA is being bypassed for same security traffic that matches a configured AAA rule. This can only occur when traffic passes between two interfaces that have the same configured security level, when the same security traffic is permitted, and if the AAA configuration uses the include or exclude syntax.

**Recommended Action** None required.

## 109029

**Error Message** %ASA-5-109029: Parsing downloaded ACL: string

**Explanation** A syntax error occurred while parsing an access list that was downloaded from a RADIUS server during user authentication.

- *string* —An error message detailing the syntax error that prevented the access list from parsing correctly

**Recommended Action** Use the information presented in this message to identify and correct the syntax error in the access list definition within the RADIUS server configuration.

## 109030

**Error Message** %ASA-4-109030: Autodetect ACL convert wildcard did not convert ACL access\_list source |dest netmask netmask .

**Explanation** A dynamic ACL that is configured on a RADIUS server is not converted by the mechanism for automatically detecting wildcard netmasks. The problem occurs because this mechanism cannot determine if the netmask is a wildcard or a normal netmask.

- **access\_list**—The access list that cannot be converted
- **source**—The source IP address
- **dest**—The destination IP address
- **netmask**—The subnet mask for the destination or source address in dotted-decimal notation

**Recommended Action** Check the access list netmask on the RADIUS server for the wildcard configuration. If the netmask is supposed to be a wildcard, and if all access list netmasks on that server are wildcards, then use the wildcard setting for **acl-netmask-convert** for the AAA server. Otherwise, change the netmask to a normal netmask or to a wildcard netmask that does not contain holes (that is, where the netmask presents consecutive binary 1s. For example, 00000000.00000000.00011111.11111111 or hex 0.0.31.255). If the mask is supposed to be normal and all access list netmasks on that server are normal, then use the normal setting for **acl-netmask-convert** for the AAA server.

## 109031

**Error Message** %ASA-4-109031: NT Domain Authentication Failed: rejecting guest login for username .

**Explanation** A user has tried to authenticate to an NT domain that was configured for guest account access and the username is not a valid username on the NT server. The connection is denied.

**Recommended Action** If the user is a valid user, add an account to the NT server. If the user is not allowed access, no action is required.

## 109032

**Error Message** %ASA-3-109032: Unable to install ACL *access\_list* , downloaded for user *username* ; Error in ACE: *ace* .

**Explanation** The Secure Firewall ASA received an access control list from a RADIUS server to apply to a user connection, but an entry in the list contains a syntax error. The use of a list containing an error could result in the violation of a security policy, so the Secure Firewall ASA failed to authenticate the user.

- *access\_list* —The name assigned to the dynamic access list as it would appear in the output of the **show access-list** command
- *username* —The name of the user whose connection will be subject to this access list
- *ace* —The access list entry that was being processed when the error was detected

**Recommended Action** Correct the access list definition in the RADIUS server configuration.

## 109033

**Error Message** %ASA-4-109033: Authentication failed for admin user *user* from *src\_IP* . Interactive challenge processing is not supported for *protocol* connections

**Explanation** AAA challenge processing was triggered during authentication of an administrative connection, but the Secure Firewall ASA cannot initiate interactive challenge processing with the client application. When this occurs, the authentication attempt will be rejected and the connection denied.

- *user* —The name of the user being authenticated
- *src\_IP* —The IP address of the client host
- *protocol* —The client connection protocol (SSH v1 or administrative HTTP)

**Recommended Action** Reconfigure AAA so that challenge processing does not occur for these connection types. This generally means to avoid authenticating these connection types to RSA SecurID servers or to any token-based AAA server via RADIUS.

## 109034

**Error Message** %ASA-4-109034: Authentication failed for network user *user* from *src\_IP/port* to *dst\_IP/port* . Interactive challenge processing is not supported for *protocol* connections

**Explanation** AAA challenge processing was triggered during authentication of a network connection, but the Secure Firewall ASA cannot initiate interactive challenge processing with the client application. When this occurs, the authentication attempt will be rejected and the connection denied.

- *user* —The name of the user being authenticated
- *src\_IP/port* —The IP address and port of the client host
- *dst\_IP/port* —The IP address and port of the server to which the client is attempting to connect
- *protocol* —The client connection protocol (for example, FTP)

**Recommended Action** Reconfigure AAA so that challenge processing does not occur for these connection types. This generally means to avoid authenticating these connection types to RSA SecurID servers or to any token-based AAA server via RADIUS.

## 109035

**Error Message** %ASA-3-109035: Exceeded maximum number (<max\_num>) of DAP attribute instances for user <user>

**Explanation** This log is generated when the number of DAP attributes received from the RADIUS server exceeds the maximum number allowed when authenticating a connection for the specified user.

**Recommended Action** Modify the DAP attribute configuration to reduce the number of DAP attributes below the maximum number allowed as specified in the log so that the specified user can connect.

## 109036

**Error Message** %ASA-6-109036: Exceeded 1000 attribute values for the *attribute name* attribute for user *username* .

**Explanation** The LDAP response message contains an attribute that has more than 1000 values.

- *attribute\_name* —The LDAP attribute name
- *username* —The username at login

**Recommended Action** None required.

## 109037

**Error Message** %ASA-3-109037: Exceeded 5000 attribute values for the *attribute name* attribute for user *username* .

**Explanation** The Secure Firewall ASA supports multiple values of the same attribute received from a AAA server. If the AAA server sends a response containing more than 5000 values for the same attribute, then the Secure Firewall ASA treats this response message as being malformed and rejects the authentication. This condition has only been seen in lab environments using specialized test tools. It is unlikely that the condition would occur in a real-world production network.

- *attribute\_name* —The LDAP attribute name
- *username* —The username at login

**Recommended Action** Capture the authentication traffic between the Secure Firewall ASA and AAA server using a protocol sniffer (such as WireShark), then forward the trace file to the Cisco TAC for analysis.

## 109038

**Error Message** %ASA-3-109038: Attribute *internal-attribute-name* value *string-from-server* from AAA server could not be parsed as a *type internal-attribute-name* string representation of the attribute name

**Explanation** The AAA subsystem tried to parse an attribute from the AAA server into an internal representation and failed.

- *string-from-server*— String received from the AAA server, truncated to 40 characters.
- *type* —The type of the specified attribute

**Recommended Action** Verify that the attribute is being generated correctly on the AAA server. For additional information, use the **debug ldap** and **debug radius** commands.

## 109039

**Error Message** %ASA-5-109039: AAA Authentication:Dropping an unsupported IPv6/IPv4/IPv6 packet from *lifc* :*laddr* to *fifc* :*faddr*

**Explanation** A packet containing IPv6 addresses or IPv4 addresses translated to IPv6 addresses by NAT requires AAA authentication or authorization. AAA authentication and authorization do not support IPv6 addresses. The packet is dropped.

- *lifc* —The ingress interface
- *laddr* —The source IP address
- *fifc* —The egress interface
- *faddr* —The destination IP address after NAT translation, if any

**Recommended Action** None required.

## 109040

**Error Message** %ASA-4-109040: User at *IP* exceeded auth proxy rate limit of 10 connections/sec

**Explanation** A connection attempt has been rejected because the ASA has detected a high frequency of HTTPS authentication requests from the same host.

- *IP* —The IP address of the host from which the connection was initiated

**Recommended Action** Limit the number of cut-through proxy authentication attempts from users.

## 109100

**Error Message** %ASA-6-109100: Received CoA update from *coa-source-ip* for user *username* , with session ID: *audit-session-id* , changing authorization attributes

**Explanation** The Secure Firewall ASA has successfully processed the CoA policy update request from *coa-source-ip* for user *username* with session id *audit-session-id* . This syslog message is generated after a change of authorization policy update has been received by the Secure Firewall ASA, validated and applied. In a non-error case, this is the only syslog message that is generated when a change of authorization is received and processed.

- *coa-source-ip* —Originating IP address of the change of authorization request
- *username* —User whose session is being changed
- *audit-session-id* —The global ID of the session being modified

**Recommended Action** None required.

## 109101

**Error Message** %ASA-6-109101: Received CoA disconnect request from *coa-source-ip* for user *username* , with audit-session-id: *audit-session-id*

**Explanation** The Secure Firewall ASA has received a correctly formatted Disconnect-Request for an active VPN session and has successfully terminated the connection.

- *coa-source-ip* —Originating IP address of the change of authorization request
- *username* —User whose session is being changed

- *audit-session-id*—The global ID of the session being modified

**Recommended Action** None required.

## 109102

**Error Message** %ASA-4-109102: Received CoA *action-type* from *coa-source-ip* , but cannot find named session *audit-session-id*

**Explanation** The Secure Firewall ASA has received a valid change of authorization request, but the session ID specified in the request does not match any active sessions on the Secure Firewall ASA. This could be the result of the change of authorization server attempting to issue a change of authorization on a session that has already been closed by the user.

- *action-type* —The requested change of authorization action (update or disconnect)
- *coa-source-ip* —Originating IP address of the change of authorization request
- *audit-session-id* —The global ID of the session being modified

**Recommended Action** None required.

## 109103

**Error Message** %ASA-3-109103: CoA *action-type* from *coa-source-ip* failed for user *username* , with session ID: *audit-session-id* .

**Explanation** The Secure Firewall ASA has received a correctly formatted change of authorization request, but was unable to process it successfully.

- *action-type* —The requested change of authorization action (update or disconnect)
- *coa-source-ip* —Originating IP address of the change of authorization request
- *username* —User whose session is being changed
- *audit-session-id* —The global ID of the session being modified

**Recommended Action** Investigate the relevant VPN subsystem logs to determine why the updated attributes could not be applied or why the session could not be terminated.

## 109104

**Error Message** %ASA-3-109104: CoA *action-type* from *coa-source-ip* failed for user *username* , session ID: *audit-session-id* . Action not supported.

**Explanation** The Secure Firewall ASA has received a correctly formatted change of authorization request, but did not process it because the indicated action is not supported by the Secure Firewall ASA.

- *action-type* —The requested change of authorization action (update or disconnect)
- *coa-source-ip* —Originating IP address of the change of authorization request
- *username* —User whose session is being changed
- *audit-session-id* —The global ID of the session being modified

**Recommended Action** None required.



## 109105

**Error Message** %ASA-3-109105: Failed to determine the egress interface for locally generated traffic destined to <protocol> <IP>:<port>.

**Explanation** It is necessary for Secure Firewall ASA to log a syslog if no routes are present when the interface is BVI. Apparently, if default route is present and it does not route packet to the correct interface then it becomes impossible to track it.

**Recommended Action** It is highly recommended to add default route for correct destination or add static routes.

## 109201

**Error Message** %ASA-5-109201: UAUTH Session *session*, User *username*, Assigned IP *IP Address*, Succeeded adding entry.

**Explanation** When a VPN user is successfully added, this message is generated.

**Recommended Action** None.

## 109202

**Error Message** %ASA-6-109202: UAUTH Session *session*, User *username*, Assigned IP *IP Address*, Succeeded incrementing entry use.

**Explanation** The VPN user account already exists and successfully incremented the reference count.

**Recommended Action** None.

## 109203

**Error Message** %ASA-3-109203: UAUTH Session *session*, User *username*, Assigned IP *IP Address*, Failed adding entry.

**Explanation** This message is generated when the device failed to apply ACL rules for newly created user entry.

**Recommended Action** Try to reconnect.

## 109204

**Error Message** %ASA-5-109204: UAUTH Session *session*, User *username*, Assigned IP *IP Address*, Succeeded applying filter.

**Explanation** This message is generated when the device failed to apply ACL rules for newly created user entry.

**Recommended Action** None.

## 109205

**Error Message** %ASA-3-109205: UAUTH Session *session*, User *username*, Assigned IP *IP Address*, Failed applying filter.

**Explanation** This message is generated when the user entry already exists and failed to apply new rules to session on interface.

**Recommended Action** Try to reconnect.

## 109206

**Error Message** %ASA-3-109206: UAUTH Session *session*, User *username*, Assigned IP *IP Address*, Removing stale entry added *hours* ago.

**Explanation** This message is generated when the device failed to add user entry due to collision and has removed stale entry.

**Recommended Action** Try to reconnect.

## 109207

**Error Message** %ASA-5-109207: UAUTH Session *session*, User *username*, Assigned IP *IP Address*, Succeeded updating entry.

**Explanation** This message is generated when the device has successfully applied rules for user on interface.

**Recommended Action** None.

## 109208

**Error Message** %ASA-3-109208: UAUTH Session *session*, User *username*, Assigned IP *IP Address*, Failed updating entry - no entry.

**Explanation** This message is generated when the device has failed to update user entry with new rules.

**Recommended Action** Try to reconnect again.

## 109209

**Error Message** %ASA-3-109209: UAUTH Session *session*, User *username*, Assigned IP *IP Address*, Failed updating filter for entry.

**Explanation** This message is generated when the device has failed to update the rules in user entry due to collision.

**Recommended Action** Try to reconnect again.

## 109210

**Error Message** %ASA-5-109210: UAUTH Session *session*, User *username*, Assigned IP *IP Address*, Successfully removed the rules for user during tunnel torn down.

**Explanation** This message is generated when the device has successfully removed the rules for user during tunnel torn down.

**Recommended Action** None.

## 109211

**Error Message** %ASA-6-109211: UAUTH Session *session*, User *username*, Assigned IP *IP Address*, Successfully removed the rules for user during tunnel torn down.

**Explanation** This message is generated when the reference count decremented successfully after tunnel removal.

**Recommended Action** None.

## 109212

**Error Message** %ASA-3-109212: UAUTH Session *session*, User *username*, Assigned IP *IP Address*, Failed removing entry.

**Explanation** This message is generated when the device fails to delete due to invalid address or bad entry.

**Recommended Action** Try to disconnect again.

## 109213

**Error Message** %ASA-3-109213: UAUTH Session *session*, User *username*, Assigned IP *IP Address*, Failed removing entry.

**Explanation** This message is generated when the device fails to delete due to collision in user entry.

**Recommended Action** Try to disconnect again.

## Messages 110002 to 113045

This section includes messages from 110002 to 113045.

## 110002

**Error Message** %ASA-6-110002: Failed to locate egress interface for *protocol* from *src interface* :*src IP/src port* to *dest IP/dest port*

**Explanation** An error occurred when the Secure Firewall ASA tried to find the interface through which to send the packet.

- *protocol* —The protocol of the packet
- *src interface* —The interface from which the packet was received
- *src IP* —The source IP address of the packet
- *src port* —The source port number
- *dest IP* —The destination IP address of the packet
- *dest port* —The destination port number

**Recommended Action** Copy the error message, the configuration, and any details about the events leading up to the error, and contact Cisco TAC.

## 110003

**Error Message** %ASA-6-110003: Routing failed to locate next-hop for protocol from *src interface* :*src IP/src port* to *dest interface* :*dest IP/dest port*

**Explanation** An error occurred when the Secure Firewall ASA tried to find the next hop on an interface routing table.

- *protocol* —The protocol of the packet
- *src interface* —The interface from which the packet was received
- *src IP* —The source IP address of the packet
- *src port* —The source port number
- *dest IP* —The destination IP address of the packet
- *dest port* —The destination port number

**Recommended Action** Copy the error message, the configuration, and any details about the events leading up to the error, and contact Cisco TAC. During debugging, use the **show asp table routing** command to view the routing table details.

## 110004

**Error Message** %ASA-6-110004: Egress interface changed from *old\_active\_ifc* to *new\_active\_ifc* on *ip\_protocol* connection *conn\_id* for *outside\_zone* /*parent\_outside\_ifc* :*outside\_addr* /*outside\_port* (*mapped\_addr* /*mapped\_port* ) to *inside\_zone* /*parent\_inside\_ifc* :*inside\_addr* /*inside\_port* (*mapped\_addr* /*mapped\_port* )

**Explanation** A flow changed on the egress interface.

**Recommended Action** None required.

## 111001

**Error Message** %ASA-5-111001: Begin configuration: *IP\_address* writing to device

**Explanation** You have entered the **write** command to store your configuration on a device (either floppy, flash memory, TFTP, the failover standby unit, or the console terminal). The **IP\_address** indicates whether the login was made at the console port or with a Telnet connection.

**Recommended Action** None required.

## 111002

**Error Message** %ASA-5-111002: Begin configuration: *IP\_address* reading from device

**Explanation** You have entered the **read** command to read your configuration from a device (either floppy disk, flash memory, TFTP, the failover standby unit, or the console terminal). The **IP\_address** indicates whether the login was made at the console port or with a Telnet connection.

**Recommended Action** None required.

## 111003

**Error Message** %ASA-5-111003: *IP\_address* Erase configuration

**Explanation** You have erased the contents of flash memory by entering the **write erase** command at the console. The **IP\_address** value indicates whether the login was made at the console port or through a Telnet connection.

**Recommended Action** After erasing the configuration, reconfigure the Secure Firewall ASA and save the new configuration. Alternatively, you can restore information from a configuration that was previously saved, either on a floppy disk or on a TFTP server elsewhere on the network.

## 111004

**Error Message** %ASA-5-111004: *IP\_address* end configuration: {FAILED|OK}

**Explanation** You have entered the **config floppy/memory/ network** command or the **write floppy/memory/network/standby** command. The **IP\_address** value indicates whether the login was made at the console port or through a Telnet connection.

**Recommended Action** None required if the message ends with OK. If the message indicates a failure, try to fix the problem. For example, if writing to a floppy disk, ensure that the floppy disk is not write protected; if writing to a TFTP server, ensure that the server is up.

## 111005

**Error Message** %ASA-5-111005: *IP\_address* end configuration: OK

**Explanation** You have exited the configuration mode. The **IP\_address** value indicates whether the login was made at the console port or through a Telnet connection.

**Recommended Action** None required.

## 111007

**Error Message** %ASA-5-111007: Begin configuration: *IP\_address* reading from device.

**Explanation** You have entered the **reload** or **configure** command to read in a configuration. The device text can be floppy, memory, net, standby, or terminal. The **IP\_address** value indicates whether the login was made at the console port or through a Telnet connection.

**Recommended Action** None required.

## 111008

**Error Message** %ASA-5-111008: User *user* executed the command *string*

**Explanation** The user entered any command, with the exception of a **show** command.

**Recommended Action** None required.

## 111009

**Error Message** %ASA-7-111009:User *user* executed cmd:*string*

**Explanation** The user entered a command that does not modify the configuration. This message appears only for **show** commands.

**Recommended Action** None required.

## 111010

**Error Message** %ASA-5-111010: User *username* , running *application-name* from IP *ip addr* , executed *cmd*

**Explanation** A user made a configuration change.

- *username* —The user making the configuration change
- *application-name* —The application that the user is running
- *ip addr* —The IP address of the management station
- *cmd* —The command that the user has executed

**Recommended Action** None required.

## 111111

**Error Message** % ASA-1-111111 *error\_message*

**Explanation** A system or infrastructure error has occurred.

**Recommended Action** If the problem persists, contact the Cisco TAC.

## 112001

**Error Message** %ASA-2-112001: (*string* :*dec* ) Clear complete.

**Explanation** A request to clear the module configuration was completed. The source file and line number are identified.

**Recommended Action** None required.

## 113001

**Error Message** %ASA-3-113001: Unable to open AAA session. Session limit [*limit* ] reached.

**Explanation** The AAA operation on an IPsec tunnel or WebVPN connection cannot be performed because of the unavailability of AAA resources. The **limit** value indicates the maximum number of concurrent AAA transactions.

**Recommended Action** Reduce the demand for AAA resources, if possible.

## 113003

**Error Message** %ASA-6-113003: AAA group policy for user *user* is being set to *policy\_name* .

**Explanation** The group policy that is associated with the tunnel group is being overridden with a user-specific policy, *policy\_name*. The *policy\_name* is specified using the **username** command when LOCAL authentication is configured or is returned in the RADIUS CLASS attribute when RADIUS authentication is configured.

**Recommended Action** None required.

## 113004

**Error Message** %ASA-6-113004: AAA user *aaa\_type* Successful: server = *server\_IP\_address* , User = *user*

**Explanation** The AAA operation on an IPsec or WebVPN connection has been completed successfully. The AAA types are authentication, authorization, or accounting. The **server\_IP\_address** is the IP address of the relevant AAA server. The **user** is the user name associated with the connection.

**Recommended Action** None required.

## 113005

**Error Message** %ASA-6-113005: AAA user authentication Rejected: reason = AAA failure: server = *ip\_addr* : user = \*\*\*\*\*: user IP = *ip\_addr*

**Explanation** The AAA authentication on a connection has failed. The username is hidden when invalid or unknown, but appears when valid or the **no logging hide username** command has been configured.

**Recommended Action** Retry the authentication.

## 113005

**Error Message** %ASA-6-113005: AAA user authentication Rejected: reason = AAA failure: server = *ip\_addr* : user = \*\*\*\*\*: user IP = *ip\_addr*

**Explanation** The AAA authentication on a connection has failed. The username is hidden when invalid or unknown, but appears when valid or the **no logging hide username** command has been configured.

**Recommended Action** Retry the authentication.

## 113006

**Error Message** %ASA-6-113006: User *user* locked out on exceeding *number* successive failed authentication attempts

**Explanation** A locally configured user is being locked out. This happens when a configured number of consecutive authentication failures have occurred for this user and indicates that all future authentication attempts by this user will be rejected until an administrator unlocks the user using the **clear aaa local user lockout** command. The **user** is the user that is now locked, and the **number** is the consecutive failure threshold configured using the **aaa local authentication attempts max-fail** command.

**Recommended Action** Try unlocking the user using the **clear\_aaa\_local\_user\_lockout** command or adjusting the maximum number of consecutive authentication failures that are tolerated.

## 113007

**Error Message** %ASA-6-113007: User *user* unlocked by *administrator*

**Explanation** A locally configured user that was locked out after exceeding the maximum number of consecutive authentication failures set by using the **aaa local authentication attempts max-fail** command has been unlocked by the indicated administrator.

**Recommended Action** None required.

## 113008

**Error Message** %ASA-6-113008: AAA transaction status ACCEPT: user = *user*

**Explanation** The AAA transaction for a user associated with an IPsec or WebVPN connection was completed successfully. The user is the username associated with the connection.

**Recommended Action** None required.

## 113009

**Error Message** %ASA-6-113009: AAA retrieved default group policy *policy* for user *user*

**Explanation** The authentication or authorization of an IPsec or WebVPN connection has occurred. The attributes of the group policy that were specified with the **tunnel-group** or **webvpn** commands have been retrieved.

**Recommended Action** None required.

## 113010

**Error Message** %ASA-6-113010: AAA challenge received for user *user* from server *server\_IP\_address*

**Explanation** The authentication of an IPsec connection has occurred with a SecurID server. The user will be prompted to provide further information before being authenticated.

- **user**—The username associated with the connection
- **server\_IP\_address**—The IP address of the relevant AAA server

**Recommended Action** None required.

## 113011

**Error Message** %ASA-6-113011: AAA retrieved user specific group policy *policy* for user *user*

**Explanation** The authentication or authorization of an IPsec or WebVPN connection has occurred. The attributes of the group policy that was specified with the **tunnel-group** or **webvpn** commands have been retrieved.

**Recommended Action** None required.



## 113012

**Error Message** %ASA-6-113012: AAA user authentication Successful: local database: user = *user*

**Explanation** The user associated with a IPsec or WebVPN connection has been successfully authenticated to the local user database.

- **user**—The username associated with the connection

**Recommended Action** None required.

## 113013

**Error Message** %ASA-6-113013: AAA unable to complete the request Error: reason = *reason* : user = *user*

**Explanation** The AAA transaction for a user associated with an IPsec or WebVPN connection has failed because of an error or has been rejected because of a policy violation.

- **reason**—The reason details
- **user**—The username associated with the connection

**Recommended Action** None required.

## 113014

**Error Message** %ASA-6-113014: AAA authentication server not accessible: server = *server\_IP\_address* : user = *user*

**Explanation** The device was unable to communicate with the configured AAA server during the AAA transaction associated with an IPsec or WebVPN connection. This may or may not result in a failure of the user connection attempt depending on the backup servers configured in the **aaa-server** group and the availability of those servers. The username is hidden when invalid or unknown, but appears when valid or the **no logging hide username** command has been configured.

**Recommended Action** Verify connectivity with the configured AAA servers.

## 113015

**Error Message** %ASA-6-113015: AAA user authentication Rejected: reason = *reason* : local database: user = *user*: user IP = *xxx.xxx.xxx.xxx*

**Explanation** A request for authentication to the local user database for a user associated with an IPsec or WebVPN connection has been rejected. The username is hidden when invalid or unknown, but appears when valid or the **no logging hide username** command has been configured.

- **reason**—The details of why the request was rejected
- **user**—The username associated with the connection
- **user\_ip**—The IP address of the user who initiated the authentication or authorization request<915CLI>

**Recommended Action** None required.

## 113016

**Error Message** %ASA-6-113016: AAA credentials rejected: reason = *reason* : server = *server\_IP\_address* : user = *user*<915CLI>: user IP = *xxx.xxx.xxx.xxx*

**Explanation** The AAA transaction for a user associated with an IPsec or WebVPN connection has failed because of an error or rejected due to a policy violation. The username is hidden when invalid or unknown, but appears when valid or the **no logging hide username** command has been configured.

- **reason**—The details of why the request was rejected
- **server\_IP\_address**—The IP address of the relevant AAA server
- **user**—The username associated with the connection
- <915CLI>*user\_ip*—The IP address of the user who initiated the authentication or authorization request

**Recommended Action** None required.

## 113017

**Error Message** %ASA-6-113017: AAA credentials rejected: reason = *reason* : local database: user = *user*: user IP = *xxx.xxx.xxx.xxx*

**Explanation** The AAA transaction for a user associated with an IPsec or WebVPN connection has failed because of an error or rejected because of a policy violation. This event only appears when the AAA transaction is with the local user database rather than with an external AAA server.

- **reason**—The details of why the request was rejected
- **user**—The username associated with the connection
- **user\_ip**—The IP address of the user who initiated the authentication or authorization request

**Recommended Action** None required.

## 113018

**Error Message** %ASA-3-113018: User: *user* , Unsupported downloaded ACL Entry: *ACL\_entry* , Action: *action*

**Explanation** An ACL entry in unsupported format was downloaded from the authentication server. The following list describes the message values:

- **user**—User trying to log in
- **ACL\_entry**—Unsupported ACL entry downloaded from the authentication server
- **action**—Action taken when encountering the unsupported ACL entry

**Recommended Action** The ACL entry on the authentication server has to be changed by the administrator to conform to the supported ACL entry formats.

## 113019

**Error Message** %ASA-4-113019: Group = *group* , Username = *username* , IP = *peer\_address* , Session disconnected. Session Type: *type* , Duration: *duration* , Bytes xmt: *count* , Bytes rcv: *count* , Reason: *reason*

**Explanation** An indication of when and why the longest idle user is disconnected.

- **group**—Group name
- **username**—Username
- **IP**—Peer address
- **Session Type**—Session type (for example, IPsec or UDP)
- **duration**—Connection duration in hours, minutes, and seconds
- **Bytes xmt**—Number of bytes transmitted
- *Bytes rcv*—Number of bytes received
- **reason**—Reason for disconnection

User Requested. Indicates a disconnection from client.

Lost Carrier

Lost Service. The service loss could be due to an issue from ISP during a SSL session establishment.

Idle Timeout

Max time exceeded

Administrator Reset- Indicates disconnection from secure gateway through vpn-sessiondb logoff

Administrator Reboot

Administrator Shutdown

Port Error

NAS Error

NAS Request

NAS Reboot

Port unneeded

Connection preempted. Indicates that the allowed number of simultaneous (same user) logins has been exceeded. To resolve this problem, increase the number of simultaneous logins or have users only log in once with a given username and password.

Port Suspended

Service Unavailable

Callback

User error

Host Requested

SA Expired

IKE Delete

Bandwidth Management Error

Certificate Expired

Phase 2 Mismatch

Firewall Mismatch

Peer Address Changed

ACL Parse Error

Phase 2 Error  
 Configuration Error  
 Peer Reconnected  
 Internal Error  
 Crypto map policy not found  
 L2TP initiated  
 VLAN Mapping Error  
 NAC-Policy Error  
 Dynamic Access Policy terminate  
 Client type not supported  
 Unknown

**Recommended Action** Unless the reason indicates a problem, then no action is required.

## 113020

**Error Message** %ASA-3-113020: Kerberos error: Clock skew with server *ip\_address* greater than 300 seconds

**Explanation** Authentication for an IPsec or WebVPN user through a Kerberos server has failed because the clocks on the Secure Firewall ASA and the server are more than five minutes (300 seconds) apart. When this occurs, the connection attempt is rejected.

- *ip\_address* —The IP address of the Kerberos server

**Recommended Action** Synchronize the clocks on the Secure Firewall ASA and the Kerberos server.

## 113021

**Error Message** %ASA-3-113021: Attempted console login failed. User *username* did NOT have appropriate Admin Rights.

**Explanation** A user has tried to access the management console and was denied.

- *username* —The username entered by the user

**Recommended Action** If the user is a newly added admin rights user, check that the service type (LOCAL or RADIUS authentication server) for that user is set to allow access:

- *nas-prompt*—Allows login to the console and exec privileges at the required level, but not enable (configuration modification) access
- *admin*—Allows all access and can be further constrained by command privileges

Otherwise, the user is inappropriately trying to access the management console; the action to be taken should be consistent with company policy for these matters.

## 113022

**Error Message** %ASA-2-113022: AAA Marking RADIUS server *servername* in aaa-server group AAA-Using-DNS as FAILED

**Explanation** The Secure Firewall ASA has tried an authentication, authorization, or accounting request to the AAA server and did not receive a response within the configured timeout window. The AAA server will be marked as failed and has been removed from service.

- *protocol* —The type of authentication protocol, which can be one of the following:

- RADIUS
- TACACS+
- NT
- RSA SecurID
- Kerberos
- LDAP

- *ip-addr* —The IP address of the AAA server
- *tag* —The server group name

**Recommended Action** Verify that the AAA server is online and is accessible from the Secure Firewall ASA.

## 113023

**Error Message** %ASA-2-113023: AAA Marking *protocol* server *ip-addr* in server group *tag* as ACTIVE

**Explanation** The Secure Firewall ASA has reactivated the AAA server that was previously marked as failed. The AAA server is now available to service AAA requests.

- *protocol* —The type of authentication protocol, which can be one of the following:

- RADIUS
- TACACS+
- NT
- RSA SecurID
- Kerberos
- LDAP

- *ip-addr* —The IP address of the AAA server
- *tag* —The server group name

**Recommended Action** None required.

## 113024

**Error Message** %ASA-5-113024: Group *tg* : Authenticating *type* connection from *ip* with username, *user\_name* , from client certificate

**Explanation** The prefill username feature overrides the username with one derived from the client certificate for use in AAA.

- *tg* —The tunnel group
- *type* —The type of connection (ssl-client or clientless)
- *ip* —The IP address of the connecting user
- *user\_name* —The name extracted from the client certificate for use in AAA

**Recommended Action** None required.

## 113025

**Error Message** %ASA-5-113025: Group *tg* : *fields* Could not authenticate *connection type* connection from *ip*

**Explanation** A username cannot be successfully extracted from the certificate.

- *tg* —The tunnel group
- *fields* —The DN fields being searched for
- *connection type* —The type of connection (SSL client or clientless)
- *ip* —The IP address of the connecting user

**Recommended Action** The administrator should check that the **authentication aaa certificate**, **ssl certificate-authentication**, and **authorization-dn-attributes** keywords have been set correctly.

## 113026

**Error Message** %ASA-4-113026: Error *error* while executing Lua script for group *tunnel group*

**Explanation** An error occurred while extracting a username from the client certificate for use in AAA. This message is only generated when the username-from-certificate use-script option is enabled.

- *error* —Error string returned from the Lua environment
- *tunnel group* —The tunnel group attempting to extract a username from a certificate

**Recommended Action** Examine the script being used by the username-from-certificate use-script option for errors.

## 113027

**Error Message** %ASA-2-113027: Error activating tunnel-group scripts

**Explanation** The script file cannot be loaded successfully. No tunnel groups using the username-from-certificate use-script option work correctly.

**Recommended Action** The administrator should check the script file for errors using ASDM. Use the **debug aaa** command to obtain a more detailed error message that may be useful.

## 113028

**Error Message** %ASA-7-113028: Extraction of username from VPN client certificate has *string*.  
[Request *num* ]

**Explanation** The processing request of a username from a certificate is running or has finished.

- *num* —The ID of the request (the value of the pointer to the fiber), which is a monotonically increasing number.
- *string* —The status message, which can one of the following:
  - been requested
  - started
  - finished with error
  - finished successfully
  - completed

**Recommended Action** None required.

## 113029

**Error Message** %ASA-4-113029: Group *group* User *user* IP *ipaddr* Session could not be established: session limit of *num* reached

**Explanation** The user session cannot be established because the current number of sessions exceeds the maximum session load.

**Recommended Action** Increase the configured limit, if possible, to create a load-balanced cluster.

## 113030

**Error Message** %ASA-4-113030: Group *group* User *user* IP *ipaddr* User ACL *acl* from AAA doesn't exist on the device, terminating connection.

**Explanation** The specified ACL was not found on the Secure Firewall ASA.

- **group**—The name of the group
- **user**—The name of the user
- **ipaddr**—The IP address
- **acl**—The name of the ACL

**Recommended Action** Modify the configuration to add the specified ACL or to correct the ACL name.

## 113031

**Error Message** %ASA-4-113031: Group *group* User *user* IP *ipaddr* AnyConnect vpn-filter *filter* is an IPv6 ACL; ACL not applied.

**Explanation** The type of ACL to be applied is incorrect. An IPv6 ACL has been configured as an IPv4 ACL through the **vpn-filter** command.

- *group* —The group policy name of the user
- *user* —The username
- *ipaddr* —The public (not assigned) IP address of the user
- *filter* —The name of the VPN filter

**Recommended Action** Validate the VPN filter and IPv6 VPN filter configurations on the Secure Firewall ASA, and the filter parameters on the AAA (RADIUS) server. Make sure that the correct type of ACL is specified.

## 113032

**Error Message** %ASA-4-113032: Group *group* User *user* IP *ipaddr* AnyConnect *ipv6-vpn-filter* *filter* is an IPv4 ACL; ACL not applied.

**Explanation** The type of ACL to be applied is incorrect. An IPv4 ACL has been configured as an IPv6 ACL through the **ipv6-vpn-filter** command.

- *group* —The group policy name of the user
- *user* —The username
- *ipaddr* —The public (not assigned) IP address of the user
- *filter* —The name of the VPN filter

**Recommended Action** Validate the VPN filter and IPv6 VPN filter configurations on the Secure Firewall ASA and the filter parameters on the AAA (RADIUS) server. Make sure that the correct type of ACL is specified.

## 113033

**Error Message** %ASA-6-113033: Group *group* User *user* IP *ipaddr* AnyConnect session not allowed. ACL parse error.

**Explanation** The WebVPN session for the specified user in this group is not allowed because the associated ACL did not parse. The user will not be allowed to log in via WebVPN until this error has been corrected.

- *group* —The group policy name of the user
- *user* —The username
- *ipaddr* —The public (not assigned) IP address of the user

**Recommended Action** Correct the WebVPN ACL.

## 113034

**Error Message** %ASA-4-113034: Group *group* User *user* IP *ipaddr* User ACL *acl* from AAA ignored, AV-PAIR ACL used instead.

**Explanation** The specified ACL was not used because a Cisco AV-PAIR ACL was used.

- **group**—The name of the group
- **user**—The name of the user
- **ipaddr**—The IP address
- **acl**—The name of the ACL

**Recommended Action** Determine the correct ACL to use and correct the configuration.



## 113035

**Error Message** %ASA-4-113035: Group *group* User *user* IP *ipaddr* Session terminated: AnyConnect not enabled or invalid AnyConnect image on the ASA.

**Explanation** The user logged in via the AnyConnect client. The SVC service is not enabled globally, or the SVC image is invalid or corrupted. The session connection has been terminated.

- *group*—The name of the group policy with which the user is trying to connect
- *user*—The name of the user who is trying to connect
- *ipaddr*—The IP address of the user who is trying to connect

**Recommended Action** Enable the SVC globally using the **svc-enable** command. Validate the integrity and versions of the SVC images by reloading new images using the **svc image** command.

## 113036

**Error Message** %ASA-4-113036: Group *group* User *user* IP *ipaddr* AAA parameter *name* value invalid.

**Explanation** The given parameter has a bad value. The value is not shown because it might be very long.

- **group**—The name of the group
- **user**—The name of the user
- **ipaddr**—The IP address
- **name**—The name of the parameter

**Recommended Action** Modify the configuration to correct the indicated parameter.

## 113037

**Error Message** %ASA-6-113037: Reboot pending, new sessions disabled. Denied user login.

**Explanation** A user was unable to log in to WebVPN because the Secure Firewall ASA is in the process of rebooting.

**Recommended Action** None required.

## 113038

**Error Message** %ASA-4-113038: Group *group* User *user* IP *ipaddr* Unable to create AnyConnect parent session.

**Explanation** The AnyConnect session was not created for the user in the specified group because of resource issues. For example, the user may have reached the maximum login limit.

- **group**—The name of the group
- **user**—The name of the user
- **ipaddr**—The IP address

**Recommended Action** None required.

## 113039

**Error Message** %ASA-6-113039: Group *group* User *user* IP *ipaddr* AnyConnect parent session started.

**Explanation** The AnyConnect session has started for the user in this group at the specified IP address. When the user logs in via the AnyConnect login page, the AnyConnect session starts.

- **group**—The name of the group
- **user**—The name of the user
- **ipaddr**—The IP address

**Recommended Action** None required.

## 113040

**Error Message** %ASA-4-113040: Terminating the VPN connection attempt from *attempted group* . Reason: This connection is group locked to *locked group*.

**Explanation** The tunnel group over which the connection is attempted is not the same as the tunnel group set in the group lock.

- *attempted group* —The tunnel group over which the connection came in
- *locked group* —The tunnel group for which the connection is locked or restricted

**Recommended Action** Check the group-lock value in the group policy or the user attributes.

## 113041

**Error Message** %ASA-4-113041: Redirect ACL configured for *assigned IP* does not exist on the device.

**Explanation** An error occurred when the redirect URL was installed and the ACL was received from the ISE, but the redirect ACL does not exist on the Secure Firewall ASA.

- *assigned IP* —The IP address that is assigned to the client

**Recommended Action** Configure the redirect ACL on the Secure Firewall ASA.

## 113042

**Error Message** %ASA-4-113042: CoA: Non-HTTP connection from *src\_if* :*src\_ip* /*src\_port* to *dest\_if* :*dest\_ip* /*dest\_port* for user *username* at *client\_IP* denied by redirect filter; only HTTP connections are supported for redirection.

**Explanation** For the CoA feature, the redirect ACL filter drops the matching non-HTTP traffic during the redirect processing and provides information about the terminated traffic flow.

- *src\_if*, *src\_ip*, *src\_port* —The source interface, IP address, and port of the flow
- *dest\_if*, *dest\_ip*, *dest\_port* —The destination interface, IP address, and port of the flow
- *username* —The name of the user
- *client\_IP* —The IP address of the client

**Recommended Action** Validate the redirect ACL configuration on the Secure Firewall ASA. Make sure that the correct filter is used to match the traffic to redirect and does not block the flow that is intended to be allowed through.

## 113045

**Error Message** %ASA-6-113045: AAA SDI server *IP\_address* in aaa-server group *group\_name*: status changed from *previous-state* to *current-state*

### Explanation

When servers are administratively added to or removed from SDI cluster, a new state `REMOVED` is added to the status transition message.

### Example

During initial transition:

```
%ASA-6-113045: AAA SDI server 10.x.x.x in aaa-server group test-SDI-group: status changed from REMOVED to OK
```

When server fails to respond after several attempts:

```
%ASA-6-113045: AAA SDI server 10.x.x.x in aaa-server group test-SDI-group: status changed from OK to SUSPENDED
```

When server finally responds:

```
%ASA-6-113045: AAA SDI server 10.x.x.x in aaa-server group test-SDI-group: status changed from SUSPENDED to OK
```

When server is administratively removed from the SDI cluster:

```
%ASA-6-113045: AAA SDI server 10.x.x.x in aaa-server group test-SDI-group: status changed from OK to REMOVED
```

**Recommended Action** None required.

## Messages 114001 to 199027

This section includes messages from 114001 to 199027.

### 114001

**Error Message** %ASA-1-114001: Failed to initialize 4GE SSM I/O card (error *error\_string*).

**Explanation** The system failed to initialize a 4GE SSM I/O card because of an I2C error or a switch initialization error.

- *syslog\_id* —Message identifier
- *>error\_string* —An I2C serial bus error or a switch access error, which is a decimal error code. The following are I2C serial bus errors:
  - I2C\_BUS\_TRANSACTION\_ERROR
  - I2C\_CHKSUM\_ERROR
  - I2C\_TIMEOUT\_ERROR
  - I2C\_BUS\_COLLISION\_ERROR

- I2C\_HOST\_BUSY\_ERROR
- I2C\_UNPOPULATED\_ERROR
- I2C\_SMBUS\_UNSUPPORT
- I2C\_BYTE\_COUNT\_ERROR
- I2C\_DATA\_PTR\_ERROR

**Recommended Action** Perform the following steps:

1. Log and review the messages and the errors associated with the event.
2. Reboot the software running on the Secure Firewall ASA.
3. Power cycle the device. When you turn off the power, make sure you wait several seconds before turning the power on.
4. If the problem persists, contact the Cisco TAC.

## 114002

**Error Message** %ASA-1-114002: Failed to initialize SFP in 4GE SSM I/O card (error *error\_string* ).

**Explanation** The system failed to initialize an SFP connector in a 4GE SSM I/O card because of an I2C error or a switch initialization error.

- >*syslog\_id* —Message identifier
- >*error\_string* —An I2C serial bus error or a switch access error, which is a decimal error code. The following are the I2C serial bus errors:
  - I2C\_BUS\_TRANSACTION\_ERROR
  - I2C\_CHKSUM\_ERROR
  - I2C\_TIMEOUT\_ERROR
  - I2C\_BUS\_COLLISION\_ERROR
  - I2C\_HOST\_BUSY\_ERROR
  - I2C\_UNPOPULATED\_ERROR
  - I2C\_SMBUS\_UNSUPPORT
  - I2C\_BYTE\_COUNT\_ERROR
  - I2C\_DATA\_PTR\_ERROR

**Recommended Action** Perform the following steps:

1. Log and review the messages and the errors associated with the event.
2. Reboot the software running on the Secure Firewall ASA.
3. Power cycle the device. When you turn off the power, make sure you wait several seconds before turning the power on.
4. If the problem persists, contact the Cisco TAC.

## 114003

**Error Message** %ASA-1-114003: Failed to run cached commands in 4GE SSM I/O card (error *error\_string* ).

**Explanation** The system failed to run cached commands in a 4GE SSM I/O card because of an I2C error or a switch initialization error.

- >*syslog\_id* —Message identifier
- >*error\_string* —An I2C serial bus error or a switch access error, which is a decimal error code. The following are the I2C serial bus errors:
  - I2C\_BUS\_TRANSACTION\_ERROR
  - I2C\_CHKSUM\_ERROR
  - I2C\_TIMEOUT\_ERROR
  - I2C\_BUS\_COLLISION\_ERROR
  - I2C\_HOST\_BUSY\_ERROR
  - I2C\_UNPOPULATED\_ERROR
  - I2C\_SMBUS\_UNSUPPORT
  - I2C\_BYTE\_COUNT\_ERROR
  - I2C\_DATA\_PTR\_ERROR

**Recommended Action** Perform the following steps:

1. Log and review the messages and the errors associated with the event.
2. Reboot the software running on the Secure Firewall ASA.
3. Power cycle the device. When you turn off the power, make sure you wait several seconds before turning the power on.
4. If the problem persists, contact the Cisco TAC.

## 114004

**Error Message** %ASA-6-114004: 4GE SSM I/O Initialization start.

**Explanation** The user has been notified that a 4GE SSM I/O initialization is starting.

- >*syslog\_id* —Message identifier

**Recommended Action** None required.

## 114005

**Error Message** %ASA-6-114005: 4GE SSM I/O Initialization end.

**Explanation** The user has been notified that an 4GE SSM I/O initialization is finished.

- >*syslog\_id* —Message identifier

**Recommended Action** None required.

## 114006

**Error Message** %ASA-3-114006: Failed to get port statistics in 4GE SSM I/O card (error *error\_string* ).

**Explanation** The Secure Firewall ASA failed to obtain port statistics in a 4GE SSM I/O card because of an I2C error or a switch initialization error.

- >*syslog\_id* —Message identifier
- >*error\_string* —An I2C serial bus error or a switch access error, which is a decimal error code. The following are the I2C serial bus errors:

- I2C\_BUS\_TRANSACTION\_ERROR
- I2C\_CHKSUM\_ERROR
- I2C\_TIMEOUT\_ERROR
- I2C\_BUS\_COLLISION\_ERROR
- I2C\_HOST\_BUSY\_ERROR
- I2C\_UNPOPULATED\_ERROR
- I2C\_SMBUS\_UNSUPPORT
- I2C\_BYTE\_COUNT\_ERROR
- I2C\_DATA\_PTR\_ERROR

**Recommended Action** Perform the following steps:

1. Log and review the messages and the errors associated with the event.
2. Reboot the software running on the Secure Firewall ASA.
3. Power cycle the device. When you turn off the power, make sure you wait several seconds before turning the power on.
4. If the problem persists, contact the Cisco TAC.

## 114007

**Error Message** %ASA-3-114007: Failed to get current msr in 4GE SSM I/O card (error *error\_string* ).

**Explanation** The Secure Firewall ASA failed to obtain the current module status register information in a 4GE SSM I/O card because of an I2C error or a switch initialization error.

- >*syslog\_id*—Message identifier
- >*error\_string*—An I2C serial bus error or a switch access error, which is a decimal error code. The following are the I2C serial bus errors:
  - I2C\_BUS\_TRANSACTION\_ERROR
  - I2C\_CHKSUM\_ERROR
  - I2C\_TIMEOUT\_ERROR
  - I2C\_BUS\_COLLISION\_ERROR
  - I2C\_HOST\_BUSY\_ERROR
  - I2C\_UNPOPULATED\_ERROR
  - I2C\_SMBUS\_UNSUPPORT
  - I2C\_BYTE\_COUNT\_ERROR
  - I2C\_DATA\_PTR\_ERROR

**Recommended Action** Perform the following steps:

1. Log and review the messages and the errors associated with the event.
2. Reboot the software running on the Secure Firewall ASA.
3. Power cycle the device. When you turn off the power, make sure you wait several seconds before turning the power on.
4. If the problem persists, contact the Cisco TAC.

## 114008

**Error Message** %ASA-3-114008: Failed to enable port after link is up in 4GE SSM I/O card due to either I2C serial bus access error or switch access error.

**Explanation** The Secure Firewall ASA failed to enable a port after the link transition to Up state is detected in a 4GE SSM I/O card because of either an I2C serial bus access error or a switch access error.

- >*syslog\_id* —Message identifier
- >*error\_string* —An I2C serial bus error or a switch access error, which is a decimal error code. The following are I2C serial bus errors:
  - I2C\_BUS\_TRANSACTION\_ERROR
  - I2C\_CHKSUM\_ERROR
  - I2C\_TIMEOUT\_ERROR
  - I2C\_BUS\_COLLISION\_ERROR
  - I2C\_HOST\_BUSY\_ERROR
  - I2C\_UNPOPULATED\_ERROR
  - I2C\_SMBUS\_UN SUPPORT
  - I2C\_BYTE\_COUNT\_ERROR
  - I2C\_DATA\_PTR\_ERROR

**Recommended Action** Perform the following steps:

1. Log and review the messages and the errors associated with the event.
2. Reboot the software running on the Secure Firewall ASA.
3. Power cycle the device. When you turn off the power, make sure you wait several seconds before turning the power on.
4. If the problem persists, contact the Cisco TAC.

## 114009

**Error Message** %ASA-3-114009: Failed to set multicast address in 4GE SSM I/O card (error *error\_string* ).

**Explanation** The Secure Firewall ASA failed to set the multicast address in a 4GE SSM I/O card because of an I2C error or a switch initialization error.

- >*syslog\_id* —Message identifier
- >*error\_string* —An I2C serial bus error or a switch access error, which is a decimal error code. The following are I2C serial bus errors:
  - I2C\_BUS\_TRANSACTION\_ERROR
  - I2C\_CHKSUM\_ERROR
  - I2C\_TIMEOUT\_ERROR
  - I2C\_BUS\_COLLISION\_ERROR
  - I2C\_HOST\_BUSY\_ERROR
  - I2C\_UNPOPULATED\_ERROR
  - I2C\_SMBUS\_UN SUPPORT
  - I2C\_BYTE\_COUNT\_ERROR
  - I2C\_DATA\_PTR\_ERROR

**Recommended Action** Perform the following steps:

1. Log and review the messages and the errors associated with the event.
2. Reboot the software running on the Secure Firewall ASA.
3. Power cycle the device. When you turn off the power, make sure you wait several seconds before turning the power on.
4. If the problem persists, contact the Cisco TAC.

## 114010

**Error Message** %ASA-3-114010: Failed to set multicast hardware address in 4GE SSM I/O card (error *error\_string* ).

**Explanation** The Secure Firewall ASA failed to set the multicast hardware address in a 4GE SSM I/O card because of an I2C error or a switch initialization error.

- >*syslog\_id* —Message identifier
- >*error\_string* —An I2C serial bus error or a switch access error, which is a decimal error code. The following are I2C serial bus errors:
  - I2C\_BUS\_TRANSACTION\_ERROR
  - I2C\_CHKSUM\_ERROR
  - I2C\_TIMEOUT\_ERROR
  - I2C\_BUS\_COLLISION\_ERROR
  - I2C\_HOST\_BUSY\_ERROR
  - I2C\_UNPOPULATED\_ERROR
  - I2C\_SMBUS\_UNSUPPORT
  - I2C\_BYTE\_COUNT\_ERROR
  - I2C\_DATA\_PTR\_ERROR
  - I2C\_DATA\_PTR\_ERROR

**Recommended Action** Perform the following steps:

1. Log and review the messages and the errors associated with the event.
2. Reboot the software running on the Secure Firewall ASA.
3. Power cycle the device. When you turn off the power, make sure you wait several seconds before turning the power on.
4. If the problem persists, contact the Cisco TAC.

## 114011

**Error Message** %ASA-3-114011: Failed to delete multicast address in 4GE SSM I/O card (error *error\_string* ).

**Explanation** The Secure Firewall ASA failed to delete the multicast address in a 4GE SSM I/O card because of either an I2C error or a switch initialization error.

- >*syslog\_id* —Message identifier
- >*error\_string* —An I2C serial bus error or a switch access error, which is a decimal error code. The following are I2C serial bus errors:
  - I2C\_BUS\_TRANSACTION\_ERROR



- I2C\_CHKSUM\_ERROR
- I2C\_TIMEOUT\_ERROR
- I2C\_BUS\_COLLISION\_ERROR
- I2C\_HOST\_BUSY\_ERROR
- I2C\_UNPOPULATED\_ERROR
- I2C\_SMBUS\_UNSUPPORT
- I2C\_BYTE\_COUNT\_ERROR
- I2C\_DATA\_PTR\_ERROR

**Recommended Action** Perform the following steps:

1. Log and review the messages and the errors associated with the event.
2. Reboot the software running on the Secure Firewall ASA.
3. Power cycle the device. When you turn off the power, make sure you wait several seconds before turning the power on.
4. If the problem persists, contact the Cisco TAC.

## 114012

**Error Message** %ASA-3-114012: Failed to delete multicast hardware address in 4GE SSM I/O card (error *error\_string* ).

**Explanation** The Secure Firewall ASA failed to delete the multicast hardware address in a 4GE SSM I/O card because of an I2C error or a switch initialization error.

- >*syslog\_id* —Message identifier
- >*error\_string* —An I2C serial bus error or a switch access error, which is a decimal error code. The following are I2C serial bus errors:
  - I2C\_BUS\_TRANSACTION\_ERROR
  - I2C\_CHKSUM\_ERROR
  - I2C\_TIMEOUT\_ERROR
  - I2C\_BUS\_COLLISION\_ERROR
  - I2C\_HOST\_BUSY\_ERROR
  - I2C\_UNPOPULATED\_ERROR
  - I2C\_SMBUS\_UNSUPPORT
  - I2C\_BYTE\_COUNT\_ERROR
  - I2C\_DATA\_PTR\_ERROR

**Recommended Action** Perform the following steps:

1. Log and review the messages and the errors associated with the event.
2. Reboot the software running on the Secure Firewall ASA.
3. Power cycle the device. When you turn off the power, make sure you wait several seconds before turning the power on.
4. If the problem persists, contact the Cisco TAC.

## 114013

**Error Message** %ASA-3-114013: Failed to set mac address table in 4GE SSM I/O card (error *error\_string* ).

**Explanation** The Secure Firewall ASA failed to set the MAC address table in a 4GE SSM I/O card because of an I2C error or a switch initialization error.

- >*syslog\_id*—Message identifier
- >*error\_string*—An I2C serial bus error or a switch access error, which is a decimal error code. The following are I2C serial bus errors:

- I2C\_BUS\_TRANSACTION\_ERROR
- I2C\_CHKSUM\_ERROR
- I2C\_TIMEOUT\_ERROR
- I2C\_BUS\_COLLISION\_ERROR
- I2C\_HOST\_BUSY\_ERROR
- I2C\_UNPOPULATED\_ERROR
- I2C\_SMBUS\_UNSUPPORT
- I2C\_BYTE\_COUNT\_ERROR
- I2C\_DATA\_PTR\_ERROR

**Recommended Action** Perform the following steps:

1. Log and review the messages and the errors associated with the event.
2. Reboot the software running on the Secure Firewall ASA.
3. Power cycle the device. When you turn off the power, make sure you wait several seconds before turning the power on.
4. If the problem persists, contact the Cisco TAC.

## 114014

**Error Message** %ASA-3-114014: Failed to set mac address in 4GE SSM I/O card (error *error\_string* ).

**Explanation** The Secure Firewall ASA failed to set the MAC address in a 4GE SSM I/O card because of an I2C error or a switch initialization error.

- >*syslog\_id*—Message identifier
- >*error\_string*—An I2C serial bus error or a switch access error, which is a decimal error code. The following are I2C serial bus errors:

- I2C\_BUS\_TRANSACTION\_ERROR
- I2C\_CHKSUM\_ERROR
- I2C\_TIMEOUT\_ERROR
- I2C\_BUS\_COLLISION\_ERROR
- I2C\_HOST\_BUSY\_ERROR

- I2C\_UNPOPULATED\_ERROR
- I2C\_SMBUS\_UN SUPPORT
- I2C\_BYTE\_COUNT\_ERROR
- I2C\_DATA\_PTR\_ERROR

**Recommended Action** Perform the following steps:

1. Log and review the messages and the errors associated with the event.
2. Reboot the software running on the Secure Firewall ASA.
3. Power cycle the device. When you turn off the power, make sure you wait several seconds before turning the power on.
4. If the problem persists, contact the Cisco TAC.

## 114015

**Error Message** %ASA-3-114015: Failed to set mode in 4GE SSM I/O card (error *error\_string* ).

**Explanation** The Secure Firewall ASA failed to set individual or promiscuous mode in a 4GE SSM I/O card because of an I2C error or a switch initialization error.

- >*syslog\_id*—Message identifier
- >*error\_string*—An I2C serial bus error or a switch access error, which is a decimal error code. The following are I2C serial bus errors:

- I2C\_BUS\_TRANSACTION\_ERROR
- I2C\_CHKSUM\_ERROR
- I2C\_TIMEOUT\_ERROR
- I2C\_BUS\_COLLISION\_ERROR
- I2C\_HOST\_BUSY\_ERROR
- I2C\_UNPOPULATED\_ERROR
- I2C\_SMBUS\_UN SUPPORT
- I2C\_BYTE\_COUNT\_ERROR
- I2C\_DATA\_PTR\_ERROR

**Recommended Action** Perform the following steps:

1. Log and review the messages and the errors associated with the event.
2. Reboot the software running on the Secure Firewall ASA.
3. Power cycle the device. When you turn off the power, make sure you wait several seconds before turning the power on.
4. If the problem persists, contact the Cisco TAC.

## 114016

**Error Message** %ASA-3-114016: Failed to set multicast mode in 4GE SSM I/O card (error *error\_string* ).

**Explanation**The Secure Firewall ASA failed to set the multicast mode in a 4GE SSM I/O card because of an I2C error or a switch initialization error.

- >*syslog\_id* —Message identifier
- >*error\_string* —An I2C serial bus error or a switch access error, which is a decimal error code. The following are the I2C serial bus errors:

- I2C\_BUS\_TRANSACTION\_ERROR
- I2C\_CHKSUM\_ERROR
- I2C\_TIMEOUT\_ERROR
- I2C\_BUS\_COLLISION\_ERROR
- I2C\_HOST\_BUSY\_ERROR
- I2C\_UNPOPULATED\_ERROR
- I2C\_SMBUS\_UN SUPPORT
- I2C\_BYTE\_COUNT\_ERROR
- I2C\_DATA\_PTR\_ERROR

**Recommended Action** Perform the following steps:

1. Log and review the messages and the errors associated with the event.
2. Reboot the software running on the Secure Firewall ASA.
3. Power cycle the device. When you turn off the power, make sure you wait several seconds before turning the power on.
4. If the problem persists, contact the Cisco TAC.

## 114017

**Error Message** %ASA-3-114017: Failed to get link status in 4GE SSM I/O card (error *error\_string* ).

**Explanation**The Secure Firewall ASA failed to obtain link status in a 4GE SSM I/O card because of an I2C serial bus access error or a switch access error.

- >*syslog\_id* —Message identifier
- >*error\_string* —An I2C serial bus error or a switch access error, which is a decimal error code. The following are the I2C serial bus errors:

- I2C\_BUS\_TRANSACTION\_ERROR
- I2C\_CHKSUM\_ERROR
- I2C\_TIMEOUT\_ERROR
- I2C\_BUS\_COLLISION\_ERROR
- I2C\_HOST\_BUSY\_ERROR
- I2C\_UNPOPULATED\_ERROR
- I2C\_SMBUS\_UN SUPPORT
- I2C\_BYTE\_COUNT\_ERROR
- I2C\_DATA\_PTR\_ERROR

**Recommended Action** Perform the following steps:

1. Notify the system administrator.
2. Log and review the messages and the errors associated with the event.
3. Reboot the software running on the Secure Firewall ASA.
4. Power cycle the device. When you turn off the power, make sure you wait several seconds before turning the power on.
5. If the problem persists, contact the Cisco TAC.

## 114018

**Error Message** %ASA-3-114018: Failed to set port speed in 4GE SSM I/O card (error *error\_string* ).

**Explanation** The Secure Firewall ASA failed to set the port speed in a 4GE SSM I/O card because of an I2C error or a switch initialization error.

- >*syslog\_id* —Message identifier
- >*error\_string* —An I2C serial bus error or a switch access error, which is a decimal error code. The following are the I2C serial bus errors:

- I2C\_BUS\_TRANSACTION\_ERROR
- I2C\_CHKSUM\_ERROR
- I2C\_TIMEOUT\_ERROR
- I2C\_BUS\_COLLISION\_ERROR
- I2C\_HOST\_BUSY\_ERROR
- I2C\_UNPOPULATED\_ERROR
- I2C\_SMBUS\_UN SUPPORT
- I2C\_BYTE\_COUNT\_ERROR
- I2C\_DATA\_PTR\_ERROR

**Recommended Action** Perform the following steps:

1. Log and review the messages and the errors associated with the event.
2. Reboot the software running on the Secure Firewall ASA.
3. Power cycle the device. When you turn off the power, make sure you wait several seconds before turning the power on.
4. If the problem persists, contact the Cisco TAC.

## 114019

**Error Message** %ASA-3-114019: Failed to set media type in 4GE SSM I/O card (error *error\_string* ).

**Explanation** The Secure Firewall ASA failed to set the media type in a 4GE SSM I/O card because of an I2C error or a switch initialization error.

- >*syslog\_id* —Message identifier

- *>error\_string*—An I2C serial bus error or a switch access error, which is a decimal error code. The following are the I2C serial bus errors:

- I2C\_BUS\_TRANSACTION\_ERROR
- I2C\_CHKSUM\_ERROR
- I2C\_TIMEOUT\_ERROR
- I2C\_BUS\_COLLISION\_ERROR
- I2C\_HOST\_BUSY\_ERROR
- I2C\_UNPOPULATED\_ERROR
- I2C\_SMBUS\_UN SUPPORT
- I2C\_BYTE\_COUNT\_ERROR
- I2C\_DATA\_PTR\_ERROR

**Recommended Action** Perform the following steps:

1. Log and review the messages and the errors associated with the event.
2. Reboot the software running on the Secure Firewall ASA.
3. Power cycle the device. When you turn off the power, make sure you wait several seconds before turning the power on.
4. If the problem persists, contact the Cisco TAC.

## 114020

**Error Message** %ASA-3-114020: Port link speed is unknown in 4GE SSM I/O card.

**Explanation**The Secure Firewall ASA cannot detect the port link speed in a 4GE SSM I/O card.

**Recommended Action** Perform the following steps:

1. Log and review the messages associated with the event.
2. Reset the 4GE SSM I/O card and observe whether or not the software automatically recovers from the event.
3. If the software does not recover automatically, power cycle the device. When you turn off the power, make sure you wait several seconds before you turn the power on.
4. If the problem persists, contact the Cisco TAC.

## 114021

**Error Message** %ASA-3-114021: Failed to set multicast address table in 4GE SSM I/O card due to *error* .

**Explanation**The Secure Firewall ASA failed to set the multicast address table in the 4GE SSM I/O card because of either an I2C serial bus access error or a switch access error.

- **error**—A switch access error (a decimal error code) or an I2C serial bus error. Possible I2C serial bus errors include:

- I2C\_BUS\_TRANSACTION\_ERROR
- I2C\_CHKSUM\_ERROR

- I2C\_TIMEOUT\_ERROR
- I2C\_BUS\_COLLISION\_ERROR
- I2C\_HOST\_BUSY\_ERROR
- I2C\_UNPOPULATED\_ERROR
- I2C\_SMBUS\_UN SUPPORT
- I2C\_BYTE\_COUNT\_ERROR
- I2C\_DATA\_PTR\_ERROR

**Recommended Action** Perform the following steps:

1. Log and review the messages associated with the event.
2. Try to reboot the Secure Firewall ASA.
3. If the software does not recover automatically, power cycle the device. When you turn off the power, make sure you wait several seconds before you turn the power on.
4. If the problem persists, contact the Cisco TAC.

## 114022

**Error Message** %ASA-3-114022: Failed to pass broadcast traffic in 4GE SSM I/O card due to *error\_string*

**Explanation** The Secure Firewall ASA failed to pass broadcast traffic in the 4GE SSM I/O card because of a switch access error.

- *error\_string* —A switch access error, which will be a decimal error code

**Recommended Action** Perform the following steps:

1. Log the message and errors surrounding the event.
2. Retrieve the ssm4ge\_dump file from the compact flash, and send it to Cisco TAC.
3. Contact Cisco TAC with the information collected in Steps 1 and 2.




---

**Note** The 4GE SSM will be automatically reset and recover.

---

## 114023

**Error Message** %ASA-3-114023: Failed to cache/flush mac table in 4GE SSM I/O card due to *error\_string* .

**Explanation** A failure to cache or flush the MAC table in a 4GE SSM I/O card occurred because of an I2C serial bus access error or a switch access error. This message rarely occurs.

- **error\_string**— Either an I2C serial bus error (see the second bullet for possible values) or a switch access error (which is a decimal error code).
- I2C serial bus errors are as follows:

I2C\_BUS\_TRANSACTION\_ERROR

I2C\_CHKSUM\_ERROR

I2C\_TIMEOUT\_ERROR  
 I2C\_BUS\_COLLISION\_ERROR  
 I2C\_HOST\_BUSY\_ERROR  
 I2C\_UNPOPULATED\_ERROR  
 I2C\_SMBUS\_UN SUPPORT  
 I2C\_BYTE\_COUNT\_ERROR  
 I2C\_DATA\_PTR\_ERROR

**Recommended Action** Perform the following steps:

1. Log the syslog message and the errors surrounding the event.
2. Try to software reboot the Secure Firewall ASA.
3. Power cycle the Secure Firewall ASA.




---

**Note** When you turn off the power, make sure that you wait several seconds before powering on again. After you complete steps 1-3, if the problem persists, contact the Cisco TAC and provide the information described in step 1. You may need to RMA the Secure Firewall ASA.

---

## 115000

**Error Message** %ASA-2-115000: Critical assertion in process: *process name* fiber: *fiber name* , component: *component name* , subcomponent: *subcomponent name* , file: *filename* , line: *line number* , cond: *condition*

**Explanation** The critical assertion has gone off and is used during development in checked builds only, but never in production builds.

- **process name**— The name of the process
- *fiber name* —The name of the fiber
- *component name* —The name of the specified component
- *subcomponent name* —The name of the specified subcomponent
- *filename* —The name of the specified file
- *line number* —The line number for the specified line
- *condition* —The specified condition

**Recommended Action** A high priority defect should be filed, the reason for the assertion should be investigated, and the problem corrected.

## 115001

**Error Message** %ASA-3-115001: Error in process: *process name* fiber: *fiber name* , component: *component name* , subcomponent: *subcomponent name* , file: *filename* , line: *line number* , cond: *condition*

**Explanation** An error assertion has gone off and is used during development in checked builds only, but never in production builds.



- **process name**— The name of the process
- *fiber name* —The name of the fiber
- *component name* —The name of the specified component
- *subcomponent name* —The name of the specified subcomponent
- *filename* —The name of the specified file
- *line number* —The line number for the specified line
- *condition* —The specified condition

**Recommended Action** A defect should be filed, the reason for the assertion should be investigated, and the problem fixed.

## 115002

**Error Message** %ASA-4-115002: Warning in process: *process name* fiber: *fiber name* , component: *component name* , subcomponent: *subcomponent name* , file: *filename* , line: *line number* , cond: *condition*

**Explanation** A warning assertion has gone off and is used during development in checked builds only, but never in production builds.

- **process name**— The name of the process
- *fiber name* —The name of the fiber
- *component name* —The name of the specified component
- *subcomponent name* —The name of the specified subcomponent
- *filename* —The name of the specified file
- *line number* —The line number for the specified line
- *condition* —The specified condition

**Recommended Action** The reason for the assertion should be investigated and if a problem is found, a defect should be filed, and the problem corrected.

## 120001

**Error Message** %ASA-5-120001: Smart Call-Home Module is started.

**Explanation** The Smart Call-Home module started successfully after system bootup and failover in a stable state, and is ready to process Smart-Call Home events.

**Recommended Action** None required.

## 120002

**Error Message** %ASA-5-120002: Smart Call-Home Module is terminated.

**Explanation** When the Smart Call-Home module is disabled, it is then terminated.

**Recommended Action** None required.

## 120003

**Error Message** %ASA-6-120003: Process event *group title*

**Explanation** The Smart Call-Home module retrieved an event from the queue to process.

- *group*—The event group, which may be the following: inventory, configuration, diagnostic, environment, snapshot, telemetry, threat, and test.
- *title*—The event title

**Recommended Action** None required.

## 120004

**Error Message** %ASA-4-120004: Event *group title* is dropped. Reason *reason*

**Explanation** A Smart Call-Home event was dropped. The event may have been dropped because of an internal error, the event queue is full, or the Smart Call-Home module was disabled after the message was generated, but before it was processed.

- *group*—The event group, which can be any of the following: inventory, configuration, diagnostic, environment, snapshot, telemetry, threat, and test.
- *title*—The event title
- *reason*—The drop reason, which can any of the following:

Internal Error—Various internal system errors occurred, such as being out of memory or parsing a CLI failed.

Queue Full—The number of events reached the configured limit.

Cancelled—The event was cancelled because the Smart Call-Home module is disabled.

**Recommended Action** If the drop reason is Queue Full, try to increase the event queue size and the rate-limit configuration to avoid event queue buildup. If the drop reason is Internal Error, turn on debugging by entering the **debug sch fail** command to obtain more detailed debugging information.

## 120005

**Error Message** %ASA-4-120005: Message *group to destination* is dropped. Reason *reason*

**Explanation** A Smart Call-Home message was dropped. The message may have been dropped because of an internal error, a network error, or the Smart Call-Home module was disabled after the message was generated, but before it was delivered.

- *group*—The event group, which can be any of the following: inventory, configuration, diagnostic, environment, snapshot, telemetry, threat, and test.
- *destination*—The e-mail or URL destination
- *reason*—The drop reason, which can any of the following:

Internal Error—Various internal system errors occurred.

Delivery Failed—The packets cannot be delivered because a network error occurred.

Cancelled—The event was cancelled because the Smart Call-Home module is disabled.

**Recommended Action** If the drop reason is Delivery Failed, the message is dropped after three unsuccessful retransmissions, or because the error is local (such as no route to destination). Search message 120006 for the delivery failure reason, or turn on debugging by entering the **debug sch fail** command to obtain more detailed debugging information.

## 120006

**Error Message** %ASA-4-120006: Delivering message *group* to *destination* failed. Reason *reason*

**Explanation** An error occurred while the Smart Call Home module tried to deliver a message. The error may be transient. The message is not dropped when message 120006 is generated. The message may be queued for retransmission. The message is only dropped when message 120005 is generated.

- *group* —The event group, which can be any of the following: inventory, configuration, diagnostic, environment, snapshot, telemetry, threat, and test
- *destination*— The e-mail or URL destination
- *reason* —The failure reason

**Recommended Action** Check the error reason in the message. If the reason is NO\_ROUTE, INVALID\_ADDRESS, or INVALID\_URL, check the system configuration, DNS, and the name setting.

## 120007

**Error Message** %ASA-6-120007: Message *group* to *destination* delivered.

**Explanation** A Smart Call Home message was successfully delivered.

- *group* —The event group, which can be any of the following: inventory, configuration, diagnostic, environment, snapshot, telemetry, threat, and test
- *destination*— The e-mail or URL destination

**Recommended Action** None required.

## 120008

**Error Message** %ASA-5-120008: SCH client *client* is activated.

**Explanation** The Smart Call Home module is enabled, an event group is also enabled, and that event group is subscribed to by at least one active profile. If these conditions are met, then all clients of that group will be activated.

- *client* —The name of the Smart Call Home client

**Recommended Action** None required.

## 120009

**Error Message** %ASA-5-120009: SCH client *client* is deactivated.

**Explanation** The Smart Call Home module is disabled, an event group is enabled, or an event group is no longer subscribed to by any active profile. If these conditions are met, clients of that event group will be deactivated.

- *client* —The name of the Smart Call Home client

**Recommended Action** None required.

## 120010

**Error Message** %ASA-3-120010: Notify command *command* to SCH client *client* failed. Reason *reason* .

**Explanation** The Smart Call Home module notified Smart Call Home clients of certain events through the callback function. If the client does not interpret the command correctly, does not understand the command, or cannot process the command, an error will be returned.

- *command*— ENABLE, DISABLE, or READY
- *client* —The name of the Smart Call Home client
- *reason* —The reason for failure

**Recommended Action** Turn on debugging by entering the **debug sch fail** command to obtain more detailed debugging information.

## 120011

**Error Message** %ASA-4-120011: To ensure Smart Call Home can properly communicate with Cisco, use the command **dns name-server** to configure at least one DNS server.

**Recommended Action** Once this syslog is generated, run the **dns name-server** command to configure at least one DNS server. Otherwise, network-local DNS server or Cisco DNS server will be used.

## 120012

**Error Message** %ASA-5-120012: User *username* chose to *choice* call-home anonymous reporting at the prompt.

**Explanation** The administrator was notified that a user has responded to the Smart Call Home prompt to enable, disable, or postpone anonymous reporting.

- *username* —The user who responded to the prompt
- *choice* —The available entries are enable, disable, or postpone

**Recommended Action** To enable anonymous reporting in the future, enter the **call-home reporting anonymous** command. To disable anonymous reporting, enter the **no call-home reporting anonymous** command.

## 121001

**Error Message** %ASA-5-121001: msgId *id*. Telemetry support on the chassis: *status*.

**Explanation** Whenever telemetry support is enabled or disabled on the chassis, this message is displayed.

- *id*—The message identifier as in the appAG-appAgent message
- *status*— The available values are enabled or disabled

### Example

```
%ASA-5-121001: msgId 1. Telemetry support on the chassis: disabled
```

**Recommended Action** None required.

## 121002

**Error Message** %ASA-5-121002: Telemetry support on the blade: *status*.

**Explanation** Whenever telemetry support is enabled or disabled on the blade, this message is displayed.

- *status*—The available entries are enable or disable

### Example

```
%ASA-5-121002: Telemetry support on the blade: enabled
%ASA-5-121002: Telemetry support on the blade: disabled
```

**Recommended Action** None required.

## 121003

**Error Message** %ASA-6-121003: msgId *id*. Telemetry request from the chassis received. SSE connector status: *connector status*. Telemetry config on the blade: *blade status*. Telemetry data *data status*.

**Explanation** The message is displayed whenever ASA receives a telemetry request from FXOS. The message displays the SSE connector status, telemetry support status on the blade, and whether the telemetry data was sent to FXOS.

- *id*—The message identifier as in the appAG-appAgent message
- *connector status*—Whether telemetry support is enabled or disabled on the chassis
- *blade status*—Whether telemetry support is enabled or disabled on the blade
- *data status*—Whether telemetry data is sent or not

### Example

```
%ASA-6-121003: msgId 2. Telemetry request from the chassis received. SSE connector status:
enabled. Telemetry config on the blade: enabled. Telemetry data Sent
%ASA-6-121003: msgId 1. Telemetry request from the chassis received. SSE connector status:
enabled. Telemetry config on the blade: enabled. Telemetry data Sent
```

**Recommended Action** None required.

## 199001

**Error Message** %ASA-5-199001: Reload command executed from Telnet (remote *IP\_address* ).

**Explanation** The address of the host that is initiating an Secure Firewall ASA reboot with the **reload** command has been recorded.

**Recommended Action** None required.

## 199002

**Error Message** %ASA-6-199002: startup completed. Beginning operation.

**Explanation** The Secure Firewall ASA finished its initial boot and the flash memory reading sequence, and is ready to begin operating normally.




---

**Note** You cannot block this message by using the no logging message command.

---

**Recommended Action** None required.

## 199003

**Error Message** %ASA-6-199003: Reducing link MTU dec .

**Explanation** The Secure Firewall ASA received a packet from the outside network that uses a larger MTU than the inside network. The Secure Firewall ASA then sent an ICMP message to the outside host to negotiate an appropriate MTU. The log message includes the sequence number of the ICMP message.

**Recommended Action** None required.

## 199005

**Error Message** %ASA-6-199005: Startup begin

**Explanation** The Secure Firewall ASA started.

**Recommended Action** None required.

## 199010

**Error Message** %ASA-1-199010: Signal 11 caught in process/fiber(rtcli async executor process)/(rtcli async executor) at address 0xf132e03b, corrective action at 0xcal961a0

**Explanation** The system has recovered from a serious error.

**Recommended Action** Contact the Cisco TAC.

## 199011

**Error Message** %ASA-2-199011: Close on bad channel in process/fiber process/fiber , channel ID p , channel state s process/fiber name of the process/fiber that caused the bad channel close operation.

**Explanation** An unexpected channel close condition has been detected.

- **p**—The channel ID
- *process/fiber* —The name of the process/fiber that caused the bad channel close operation
- **s**—The channel state

**Recommended Action** Contact the Cisco TAC and attach a log file.

## 199012

**Error Message** %ASA-1-1199012: Stack overflow during new\_stack\_call in process/fiber process/fiber , call target f , stack size s , process/fiber name of the process/fiber that caused the stack overflow

**Explanation** A stack overflow condition has been detected.

- **f**—The target of the `new_stack_call`
- *process/fiber* —The name of the process/fiber that caused the stack overflow
- **s**—The new stack size specified in `new_stack_call`

**Recommended Action** Contact the Cisco TAC and attach the log file.

## 199013

**Error Message** %ASA-1-199013: *syslog*

**Explanation** A variable syslog was generated by an assistive process.

- **syslog**—The alert syslog passed verbatim from an external process

**Recommended Action** Contact the Cisco TAC.

## 199014

**Error Message** %ASA-2-199014: *syslog*

**Explanation** A variable syslog was generated by an assistive process.

- **syslog**—The critical syslog passed verbatim from an external process

**Recommended Action** Contact the Cisco TAC.

## 199015

**Error Message** %ASA-3-199015: *syslog*

**Explanation** A variable syslog was generated by an assistive process.

- **syslog**—The error syslog passed verbatim from an external process

**Recommended Action** Contact the Cisco TAC.

## 199016

**Error Message** %ASA-4-199016: *syslog*

**Explanation** A variable syslog was generated by an assistive process.

- **syslog**—The warning syslog passed verbatim from an external process

In some instances, the message may appear to be an issue that is internal to the device platform process. For example, in the following message though it indicates to be an internal device issue, it is related to an internal virtual device which is not used on the device platform, and it does not cause any functionality impact.

```
%ASA-4-199016: mm dd HH:MM:SS acpid: input device has been disconnected, fd 4
```

**Recommended Action** Contact the Cisco TAC.

## 199017

**Error Message** %ASA-5-199017: *syslog*

**Explanation** A variable syslog was generated by an assistive process.

- **syslog**—The notification syslog passed verbatim from an external process

**Recommended Action** None required.

## 199018

**Error Message** %ASA-6-199018: *syslog*

**Explanation** A variable syslog was generated by an assistive process.

- **syslog**—The informational syslog passed verbatim from an external process

**Recommended Action** None required.

## 199019

**Error Message** %ASA-7-199019: *syslog*

**Explanation** A variable syslog was generated by an assistive process.

- **syslog**—The debugging syslog passed verbatim from an external process

**Recommended Action** None required.

## 199020

**Error Message** %ASA-2-199020: System memory utilization has reached X %. System will reload if memory usage reaches the configured trigger level of Y %.

**Explanation** The system memory utilization has reached 80% of the system memory watchdog facility's configured value.

**Recommended Action** Reduce system memory utilization by reducing traffic load, removing traffic inspections, reducing the number of ACL entries, and so on. If a memory leak is suspected, contact Cisco TAC.

## 199021

**Error Message** %ASA-1-199021: System memory utilization has reached the configured watchdog trigger level of Y %. System will now reload

**Explanation** The system memory utilization has reached 100% of the system memory watchdog facility's configured value. The system will automatically reload.

**Recommended Action** Reduce system memory utilization by reducing traffic load, removing traffic inspections, reducing the number of ACL entries, and so on. If a memory leak is suspected, contact Cisco TAC.



## 199027

**Error Message** %ASA-5-199027: Restore operation was aborted at <HH:MM:SS> UTC <DD:MM:YY>

**Explanation** This message indicates that the backup restoration failed while using the 'restore' command.

**Recommended Action** None





## CHAPTER 2

# Syslog Messages 201002 to 219002

This chapter contains the following sections:

- [Messages 201002 to 210022, on page 85](#)
- [Messages 211001 to 219002, on page 93](#)

## Messages 201002 to 210022

This chapter includes messages from 201002 to 210022.

### 201002

**Error Message** %ASA-3-201002: Too many TCP connections on {static|xlate} *global\_address* !  
*econns nconns*

**Explanation** The maximum number of TCP connections to the specified global address was exceeded.

- *econns*—The maximum number of embryonic connections
- *nconns*—The maximum number of connections permitted for the static or xlate global address

**Recommended Action** Use the **show static** or **show nat** command to check the limit imposed on connections to a static address. The limit is configurable.

### 201003

**Error Message** %ASA-2-201003: Embryonic limit exceeded *nconns/elimit* for  
*outside\_address/outside\_port (global\_address) inside\_address /inside\_port* on interface  
*interface\_name*

**Explanation** The number of embryonic connections from the specified foreign address with the specified static global address to the specified local address exceeds the embryonic limit. When the limit on embryonic connections to the Secure Firewall ASA is reached, the Secure Firewall ASA attempts to accept them anyway, but puts a time limit on the connections. This situation allows some connections to succeed even if the Secure Firewall ASA is very busy. This message indicates a more serious overload than message 201002, which can be caused by a SYN attack, or by a very heavy load of legitimate traffic.

- *nconns*—The maximum number of embryonic connections received
- *elimit*—The maximum number of embryonic connections specified in the static or nat command

**Recommended Action** Use the show static command to check the limit imposed on embryonic connections to a static address.

## 201004

**Error Message** %ASA-3-201004: Too many UDP connections on {static|xlate} *global\_address!udp connections limit*

**Explanation** The maximum number of UDP connections to the specified global address was exceeded.

- udp conn limit—The maximum number of UDP connections permitted for the static address or translation

**Recommended Action** Use the **show static** or show nat command to check the limit imposed on connections to a static address. You can configure the limit.

## 201005

**Error Message** %ASA-3-201005: FTP data connection failed for IP\_address *IP\_address*

**Explanation** The Secure Firewall ASA cannot allocate a structure to track the data connection for FTP because of insufficient memory.

**Recommended Action** Reduce the amount of memory usage or purchase additional memory.

## 201006

**Error Message** %ASA-3-201006: RCMD backconnection failed for *IP\_address/port*.

**Explanation** The Secure Firewall ASA cannot preallocate connections for inbound standard output for **rsh** commands because of insufficient memory.

**Recommended Action** Check the **rsh** client version; the Secure Firewall ASA only supports the Berkeley **rsh** client version. You can also reduce the amount of memory usage, or purchase additional memory.

## 201008

**Error Message** %ASA-3-201008: Disallowing new connections.

**Explanation** You have enabled TCP system log messaging and the syslog server cannot be reached, or when using the ASA syslog server (PFSS) and the disk on the Windows NT system is full, or when the auto-update timeout is configured and the auto-update server is not reachable.

**Recommended Action** Disable TCP syslog messaging. If using PFSS, free up space on the Windows NT system where PFSS resides. Also, make sure that the syslog server is up and you can ping the host from the ASA console. Then restart TCP system message logging to allow traffic. If the Auto Update Server has not been contacted for a certain period of time, enter the **[no] auto-update timeout period** command to have it stop sending packets.

## 201009

**Error Message** %ASA-3-201009: TCP connection limit of *number* for host *IP\_address* on *interface\_name* exceeded

**Explanation** The maximum number of connections to the specified static address was exceeded.

- **number**—The maximum of connections permitted for the host
- **IP\_address**—The host IP address
- **interface\_name**— The name of the interface to which the host is connected

**Recommended Action** Use the show static and show nat commands to check the limit imposed on connections to an address. The limit is configurable.

## 201010

**Error Message** %ASA-6-201010: Embryonic connection limit exceeded econns/limit for dir packet from source\_address/source\_port to dest\_address/dest\_port on interface interface\_name

**Explanation** An attempt to establish a TCP connection failed because of an exceeded embryonic connection limit, which was configured with the **set connection embryonic-conn-max** MPC command for a traffic class.

To reduce the impact of anomalous incoming traffic on ASA's different management or data interfaces and protocols, the interfaces are configured with a default embryonic limit of 100. This syslog message appears when the embryonic connections to ASA interface exceeds 100. This default value cannot be modified or disabled.

- **econnns**—The current count of embryonic connections associated to the configured traffic class
- **limit**—The configured embryonic connection limit for the traffic class
- **dir**—input: The first packet that initiates the connection is an input packet on the interface **interface\_name**  
output: The first packet that initiates the connection is an output packet on the interface **interface\_name**
- **source\_address/source\_port**—The source real IP address and the source port of the packet initiating the connection
- **dest\_address/dest\_port**—The destination real IP address and the destination port of the packet initiating the connection
- **interface\_name**—The name of the interface on which the policy limit is enforced

**Recommended Action** None required.

## 201011

**Error Message** %ASA-3-201011: Connection limit exceeded cnt /limit for dir packet from sip /sport to dip /dport on interface if\_name .

**Explanation** A new connection through the Secure Firewall ASA resulted in exceeding at least one of the configured maximum connection limits. This message applies both to connection limits configured using a **static** command, or to those configured using Cisco Modular Policy Framework. The new connection will not be allowed through the Secure Firewall ASA until one of the existing connections is torn down, which brings the current connection count below the configured maximum.

- **cnt**—Current connection count
- **limit**—Configured connection limit
- **dir**—Direction of traffic, inbound or outbound
- **sip**—Source real IP address
- **sport**—Source port
- **dip**—Destination real IP address
- **dport**—Destination port

- *if\_name* —Name of the interface on which the traffic was received

**Recommended Action** None required.

## 201012

**Error Message** %ASA-6-201012: Per-client embryonic connection limit exceeded *curr num /limit* for [input|output] packet from *IP\_address / port* to *ip /port* on interface *interface\_name*

**Explanation** An attempt to establish a TCP connection failed because the per-client embryonic connection limit was exceeded. By default, this message is rate limited to 1 message every 10 seconds.

- **curr num**—The current number
- **limit**—The configured limit
- [input|output]—Input or output packet on interface **interface\_name**
- **IP\_address**—Real IP address
- **port**—TCP or UDP port
- **interface\_name**—The name of the interface on which the policy is applied

**Recommended Action** When the limit is reached, any new connection request will be proxied by the Secure Firewall ASA to prevent a SYN flood attack. The Secure Firewall ASA will only connect to the server if the client is able to finish the three-way handshake. This usually does not affect the end user or the application. However, if this creates a problem for any application that has a legitimate need for a higher number of embryonic connections, you can adjust the setting by entering the **set connection per-client-embryonic-max** command.

## 201013

**Error Message** %ASA-3-201013: Per-client connection limit exceeded *curr num /limit* for [input|output] packet from *ip /port* to *ip /port* on interface *interface\_name*

**Explanation** A connection was rejected because the per-client connection limit was exceeded.

- **curr num**—The current number
- **limit**—The configured limit
- [input|output]—The input or output packet on interface **interface\_name**
- **ip**—The real IP address
- **port**—The TCP or UDP port
- **interface\_name**—The name of the interface on which the policy is applied

**Recommended Action** When the limit is reached, any new connection request will be silently dropped. Normally an application will retry the connection, which will cause a delay or even a timeout if all retries also fail. If an application has a legitimate need for a higher number of concurrent connections, you can adjust the setting by entering the **set connection per-client-max** command.

## 202001

**Error Message** %ASA-3-202001: Out of address translation slots!

**Explanation** The ASA has no more address translation slots available.

**Recommended Action** Check the size of the global pool compared to the number of inside network clients. A PAT address may be necessary. Alternatively, shorten the timeout interval of translates and connections.

This error message can also be caused by insufficient memory; reduce the amount of memory usage, or purchase additional memory, if possible.

## 202005

**Error Message** %ASA-3-202005: Non-embryonic in embryonic list outside\_address/outside\_port inside\_address/inside\_port

**Explanation** A connection object (xlate) is in the wrong list.

**Recommended Action** Contact the Cisco TAC.

## 202010

(With flow) **Error Message** %ASA-3-202010: [NAT | PAT] pool exhausted in pool *pool-name* IP *ip\_address*, port range [1-511 | 512-1023 | 1024-65535]. Unable to create *protocol* connection from *in-interface* :*src-ip* /*src-port* to *out-interface* :*dst-ip* /*dst-port*

(Without flow) **Error Message** %ASA-3-202010: [NAT | PAT] pool exhausted in pool *pool-name* IP *ip\_address*. Unable to create connection.

### Explanation

- *pool-name* —The name of the NAT or PAT pool. If the interface PAT or mapped IP is a raw address, pool name is logged as empty string ("").
- *protocol* —The protocol used to create the connection
- *in-interface* —The ingress interface
- *src-ip* —The source IP address
- *src-port* —The source port
- *out-interface* —The egress interface
- *dest-ip* —The destination IP address
- *dst-port* —The destination port

The Secure Firewall ASA has no more address translation pools available.

**Recommended Action** Use the **show nat pool** and **show nat detail** commands to determine why all addresses and ports in the pool are used up. If this occurs under normal conditions, then add additional IP addresses to the NAT/PAT pool.

## 202016

**Error Message** %ASA-3-202016: "%d: Unable to pre-allocate SIP %s secondary channel for message" \ "from %s:%A/%d to %s:%A/%d with PAT and missing port information.\n"

### Explanation

When SIP application generates an SDP payload with Media port set to 0, you cannot allocate a PAT xlate for such invalid port request and drop the packet with this syslog.

**Recommended Action** None. This is an application specific issue.

## 208005

**Error Message** %ASA-3-208005: (function:line\_num) clear command return code

**Explanation** The Secure Firewall ASA received a nonzero value (an internal error) when attempting to clear the configuration in flash memory. The message includes the reporting subroutine filename and line number.

**Recommended Action** For performance reasons, the end host should be configured not to inject IP fragments. This configuration change is probably because of NFS. Set the read and write size equal to the interface MTU for NFS.

## 209003

**Error Message** %ASA-4-209003: Fragment database limit of *number* exceeded: src = *source\_address* , dest = *dest\_address* , proto = *protocol* , id = *number*

**Explanation** Too many IP fragments are currently awaiting reassembly. By default, the maximum number of fragments is 200 (to raise the maximum, see the **fragment size** command in the command reference guide). The Secure Firewall ASA limits the number of IP fragments that can be concurrently reassembled. This restriction prevents memory depletion at the Secure Firewall ASA under abnormal network conditions. In general, fragmented traffic should be a small percentage of the total traffic mix. An exception is in a network environment with NFS over UDP where a large percentage is fragmented traffic; if this type of traffic is relayed through the Secure Firewall ASA, consider using NFS over TCP instead. To prevent fragmentation, see the **sysopt connection tcpmss bytes** command in the command reference guide.

**Recommended Action** If this message persists, a denial of service (DoS) attack might be in progress. Contact the remote peer administrator or upstream provider.

## 209004

**Error Message** %ASA-4-209004: Invalid IP fragment, size = *bytes* exceeds maximum size = *bytes* : src = *source\_address* , dest = *dest\_address* , proto = *protocol* , id = *number*

**Explanation** An IP fragment is malformed. The total size of the reassembled IP packet exceeds the maximum possible size of 65,535 bytes.

**Recommended Action** A possible intrusion event may be in progress. If this message persists, contact the remote peer administrator or upstream provider.

## 209005

**Error Message** %ASA-4-209005: Discard IP fragment set with more than *number* elements: src =  
Too many elements are in a fragment set.

**Explanation** The Secure Firewall ASA disallows any IP packet that is fragmented into more than 24 fragments. For more information, see the **fragment** command in the command reference guide.

**Recommended Action** A possible intrusion event may be in progress. If the message persists, contact the remote peer administrator or upstream provider. You can change the number of fragments per packet by using the **fragment chain xxx interface\_name** command.



## 209006

**Error Message** %ASA-4-209006: Fragment queue threshold exceeded, dropped *protocol* fragment from IP address/port to IP address/port on outside interface.

**Explanation** The Secure Firewall ASA drops the fragmented packets when the fragment database threshold, that is 2/3 of the queue size per interface, has exceeded.

**Recommended Action** None required.

## 210001

**Error Message** %ASA-3-210001: LU *sw\_module\_name* error = *number*

**Explanation** A Stateful Failover error occurred.

**Recommended Action** If this error persists after traffic lessens through the Secure Firewall ASA, report this error to the Cisco TAC.

## 210002

**Error Message** %ASA-3-210002: LU allocate block (*bytes*) failed.

**Explanation** Stateful Failover cannot allocate a block of memory to transmit stateful information to the standby Secure Firewall ASA.

**Recommended Action** Check the failover interface using the **show interface** command to make sure its transmit is normal. Also check the current block memory using the **show block** command. If current available count is 0 within any of the blocks of memory, then reload the Secure Firewall ASA software to recover the lost blocks of memory.

## 210003

**Error Message** %ASA-3-210003: Unknown LU Object *number*

**Explanation** Stateful Failover received an unsupported Logical Update object and was unable to process it. This can be caused by corrupted memory, LAN transmissions, and other events.

**Recommended Action** If you see this error infrequently, then no action is required. If this error occurs frequently, check the Stateful Failover link LAN connection. If the error was not caused by a faulty failover link LAN connection, determine if an external user is trying to compromise the protected network. Also check for misconfigured clients.

## 210005

**Error Message** %ASA-3-210005: LU allocate *secondary (optional)* connection failed for *protocol* [TCP |UDP] connection from *ingress interface name* :Real IP Address /Real Port to *egress interface name* :Real IP Address /Real Port

**Explanation** Stateful Failover cannot allocate a new connection on the standby unit. This may be caused by little or no RAM memory available within the Secure Firewall ASA. This could additionally be caused by flow creation failure due to resource limitation or reaching configured resource usage limits.



**Note** The *secondary* field in the syslog message is optional and appears only if the connection is a secondary connection.

**Recommended Action** Check the available memory using the **show memory** command to make sure that the Secure Firewall ASA has free memory. If there is no available memory, add more physical memory to the Secure Firewall ASA. Check resource limitation using the **show resource usage** command and **show asp drop** to ensure that the device is not reaching the resource limitation.

## 210006

**Error Message** %ASA-3-210006: LU look NAT for *IP\_address* failed

**Explanation** Stateful Failover was unable to locate a NAT group for the IP address on the standby unit. The active and standby Secure Firewall ASAs may be out-of-sync with each other.

**Recommended Action** Use the **write standby** command on the active unit to synchronize system memory with the standby unit.

## 210007

**Error Message** %ASA-3-210007: LU allocate xlate failed for type [*static | dynamic*]-[*NAT | PAT*] *secondary(optional) protocol* translation from *ingress interface name :Real IP Address /real port (Mapped IP Address /Mapped Port )* to *egress interface name :Real IP Address /Real Port (Mapped IP Address /Mapped Port )*

**Explanation** Stateful Failover failed to allocate a translation slot record.

**Recommended Action** Check the available memory by using the **show memory** command to make sure that the Secure Firewall ASA has free memory available. If no memory is available, add more memory.

## 210008

**Error Message** %ASA-3-210008: LU no xlate for *inside\_address /inside\_port outside\_address /outside\_port*

**Explanation** The Secure Firewall ASA cannot find a translation slot record for a Stateful Failover connection; as a result, the Secure Firewall ASA cannot process the connection information.

**Recommended Action** Use the **write standby** command on the active unit to synchronize system memory between the active and standby units.

## 210010

**Error Message** %ASA-3-210010: LU make UDP connection for *outside\_address :outside\_port inside\_address :inside\_port* failed

**Explanation** Stateful Failover was unable to allocate a new record for a UDP connection.

**Recommended Action** Check the available memory by using the **show memory** command to make sure that the Secure Firewall ASA has free memory available. If no memory is available, add more memory.

## 210020

**Error Message** %ASA-3-210020: LU PAT port *port* reserve failed

**Explanation** Stateful Failover is unable to allocate a specific PAT address that is in use.

**Recommended Action** Use the **write standby** command on the active unit to synchronize system memory between the active and standby units.

## 210021

**Error Message** %ASA-3-210021: LU create static xlate *global\_address* ifc *interface\_name* failed

**Explanation** Stateful Failover is unable to create a translation slot.

**Recommended Action** Enter the **write standby** command on the active unit to synchronize system memory between the active and standby units.

## 210022

**Error Message** %ASA-6-210022: LU missed *number* updates

**Explanation** Stateful Failover assigns a sequence number for each record sent to the standby unit. When a received record sequence number is out of sequence with the last updated record, the information in between is assumed to be lost, and this error message is sent as a result.

**Recommended Action** Unless LAN interruptions occur, check the available memory on both Secure Firewall ASA units to ensure that enough memory is available to process the stateful information. Use the **show failover** command to monitor the quality of stateful information updates.

# Messages 211001 to 219002

This chapter includes messages from 211001 to 219002.

## 211001

**Error Message** %ASA-3-211001: Memory allocation Error

**Explanation** The Secure Firewall ASA failed to allocate RAM system memory.

**Recommended Action** If this message occurs periodically, it can be ignored. If it repeats frequently, contact the Cisco TAC.

## 211003

**Error Message** %ASA-3-211003: Error in computed percentage CPU usage value

**Explanation** The percentage of CPU usage is greater than 100 percent.

**Recommended Action** If this message occurs periodically, it can be ignored. If it repeats frequently, contact the Cisco TAC.

## 211004

**Error Message** %ASA-1-211004: WARNING: Minimum Memory Requirement for ASA version *ver* not met for ASA image. *min* MB required, *actual* MB found.

**Explanation** The Secure Firewall ASA does not meet the minimum memory requirements for this version.

- **ver**—Running image version number
- **min**—Minimum required amount of RAM to run the installed image.
- **actual**—Amount of RAM currently installed in the system

**Recommended Action** Install the required amount of RAM.

## 212001

**Error Message** %ASA-3-212001: Unable to open SNMP channel (UDP port *port* ) on interface *interface\_number* , error code = *code*

**Explanation** The Secure Firewall ASA is unable to receive SNMP requests destined for the Secure Firewall ASA from SNMP management stations located on this interface. The SNMP traffic passing through the Secure Firewall ASA on any interface is not affected. The error codes are as follows:

- An error code of -1 indicates that the Secure Firewall ASA cannot open the SNMP transport for the interface. This can occur when the user attempts to change the port on which SNMP accepts queries to one that is already in use by another feature. In this case, the port used by SNMP will be reset to the default port for incoming SNMP queries (UDP 161).
- An error code of -2 indicates that the Secure Firewall ASA cannot bind the SNMP transport for the interface.

**Recommended Action** After the Secure Firewall ASA reclaims some of its resources when traffic is lighter, reenter the `snmp-server host` command for that interface.

## 212002

**Error Message** %ASA-3-212002: Unable to open SNMP trap channel (UDP port *port* ) on interface *interface\_number* , error code = *code*

**Explanation** The Secure Firewall ASA is unable to send its SNMP traps from the Secure Firewall ASA to SNMP management stations located on this interface. The SNMP traffic passing through the Secure Firewall ASA on any interface is not affected. The error codes are as follows:

- An error code of -1 indicates that the Secure Firewall ASA cannot open the SNMP trap transport for the interface.
- An error code of -2 indicates that the Secure Firewall ASA cannot bind the SNMP trap transport for the interface.
- An error code of -3 indicates that the Secure Firewall ASA cannot set the trap channel as write-only.

**Recommended Action** After the Secure Firewall ASA reclaims some of its resources when traffic is lighter, reenter the `snmp-server host` command for that interface.

## 212003

**Error Message** %ASA-3-212003: Unable to receive an SNMP request on interface *interface\_number* , error code = *code* , will try again.

**Explanation** An internal error occurred in receiving an SNMP request destined for the Secure Firewall ASA on the specified interface. The error codes are as follows:

- An error code of -1 indicates that the Secure Firewall ASA cannot find a supported transport type for the interface.
- An error code of -5 indicates that the Secure Firewall ASA received no data from the UDP channel for the interface.
- An error code of -7 indicates that the Secure Firewall ASA received an incoming request that exceeded the supported buffer size.
- An error code of -14 indicates that the Secure Firewall ASA cannot determine the source IP address from the UDP channel.
- An error code of -22 indicates that the Secure Firewall ASA received an invalid parameter.

**Recommended Action** None required. The Secure Firewall ASA SNMP agent goes back to wait for the next SNMP request.

## 212004

**Error Message** %ASA-3-212004: Unable to send an SNMP response to IP Address *IP\_address* Port *port* interface *interface\_number* , error code = *code*

**Explanation** An internal error occurred in sending an SNMP response from the Secure Firewall ASA to the specified host on the specified interface. The error codes are as follows:

- An error code of -1 indicates that the Secure Firewall ASA cannot find a supported transport type for the interface.
- An error code of -2 indicates that the Secure Firewall ASA sent an invalid parameter.
- An error code of -3 indicates that the Secure Firewall ASA was unable to set the destination IP address in the UDP channel.
- An error code of -4 indicates that the Secure Firewall ASA sent a PDU length that exceeded the supported UDP segment size.
- An error code of -5 indicates that the Secure Firewall ASA was unable to allocate a system block to construct the PDU.

**Recommended Action** None required.

## 212005

**Error Message** %ASA-3-212005: incoming SNMP request (*number bytes*) on interface *interface\_name* exceeds data buffer size, discarding this SNMP request.

**Explanation** The length of the incoming SNMP request that is destined for the Secure Firewall ASA exceeds the size of the internal data buffer (512 bytes) used for storing the request during internal processing. The Secure Firewall ASA is unable to process this request. The SNMP traffic passing through the Secure Firewall ASA on any interface is not affected.

**Recommended Action** Have the SNMP management station resend the request with a shorter length. For example, instead of querying multiple MIB variables in one request, try querying only one MIB variable in a request. You may need to modify the configuration of the SNMP manager software.

## 212006

**Error Message** %ASA-3-212006: Dropping SNMP request from *src\_addr /src\_port* to *ifc :dst\_addr /dst\_port* because: *reason username*

**Explanation** The Secure Firewall ASA cannot process the SNMP request being sent to it for the following reasons:

- user not found—The username cannot be located in the local SNMP user database.
- username exceeds maximum length—The username embedded in the PDU exceeds the maximum length allowed by the SNMP RFCs.
- authentication algorithm failure—An authentication failure caused by an invalid password or a packet authenticated using the incorrect algorithm.
- privacy algorithm failure—A privacy failure caused by an invalid password or a packet encrypted using the incorrect algorithm.
- error decrypting request—An error occurred in the platform crypto module decrypting the user request.
- error encrypting response—An error occurred in the platform crypto module encrypting the user response or trap notification.
- engineBoots has reached maximum value—The engineBoots variable has reached the maximum allowed value. For more information, see message 212011.




---

**Note** The username appears after each reason listed.

---

**Recommended Action** Check the Secure Firewall ASA SNMP server settings and confirm that the NMS configuration is using the expected user, authentication, and encryption settings. Enter the **show crypto accelerator statistics** command to isolate errors in the platform crypto module.

## 212009

**Error Message** %ASA-5-212009: Configuration request for SNMP group *groupname* failed. User *username* , *reason* .

**Explanation** A user has tried to change the SNMP server group configuration. One or more users that refer to the group have insufficient settings to comply with the requested group changes.

- **groupname**—A string that represents the group name
- **username** —A string that represents the username
- **reason**—A string that represents one of the following reasons:
  - *missing auth-password* —A user has tried to add authentication to the group, and the user has not specified an authentication password
  - *missing priv-password* —A user has tried to add privacy to the group, and the user has not specified an encryption password
  - *reference group intended for removal* —A user has tried to remove a group that has users belonging to it

**Recommended Action** The user must update the indicated user configurations before changing the group or removing indicated users, and then add them again after making changes to the group.

## 212010

**Error Message** %ASA-3-212010: Configuration request for SNMP user %s failed. Host %s reason .

**Explanation** A user has tried to change the SNMP server user configuration by removing one or more hosts that reference the user. One message is generated per host.

- %s—A string that represents the username or hostname
- reason —A string the represents the following reason:

- *references user intended for removal*— The name of the user to be removed from the host.

**Recommended Action** The user must either update the indicated host configuration before changing a user or remove the indicated hosts, then add them again after making changes to the user.

## 212011

**Error Message** %ASA-3-212011: SNMP engineBoots is set to maximum value. Reason : %s User intervention necessary.

For example:

```
%ASA-3-212011: SNMP engineBoots is set to maximum value. Reason: error accessing persistent data. User intervention necessary.
```

**Explanation** The device has rebooted 214783647 times, which is the maximum allowed value of the engineBoots variable, or an error reading the persistent value from flash memory has occurred. The engineBoots value is stored in flash memory in the flash:/snmp/*ctx-name* file, where *ctx-name* is the name of the context. In single mode, the name of this file is flash:/snmp/single\_vf. In multi-mode, the name of the file for the admin context is flash:/snmp/admin. During a reboot, if the device is unable to read from the file or write to the file, the engineBoots value is set to the maximum.

- %s—A string that represents the reason that the engineBoots value is set to the maximum allowed value. The two valid strings are “device reboots” and “error accessing persistent data.”

**Recommended Action** For the first string, the administrator must delete all SNMP Version 3 users and add them again to reset the engineBoots variable to 1. All subsequent Version 3 queries will fail until all users have been removed. For the second string, the administrator must delete the context-specific file, then delete all SNMP Version users, and add them again to reset the engineBoots variable to 1. All subsequent Version 3 queries will fail until all users have been removed.

## 212012

**Error Message** %ASA-3-212012: Unable to write SNMP engine data to persistent storage.

**Explanation** The SNMP engine data is written to the file, flash:/snmp/*context-name* . For example: in single mode, the data is written to the file, flash:/snmp/single\_vf. In the admin context in multi-mode, the file is written to the directory, flash:/snmp/admin. The error may be caused by a failure to create the flash:/snmp directory or the flash:/snmp/*context-name* file. The error may also be caused by a failure to write to the file.

**Recommended Action** The system administrator should remove the `flash:/snmp/context-name` file, then remove all SNMP Version 3 users, and add them again. This procedure should recreate the `flash:/snmp/context-name` file. If the problem persists, the system administrator should try reformatting the flash.

## 213001

**Error Message** %ASA-3-213001: PPTP control daemon socket io *string* , errno = *number* .

**Explanation** An internal TCP socket I/O error occurred.

**Recommended Action** Contact the Cisco TAC.

## 213002

**Error Message** %ASA-3-213002: PPTP tunnel hashtable insert failed, peer = *IP\_address* .

**Explanation** An internal software error occurred while creating a new PPTP tunnel.

**Recommended Action** Contact the Cisco TAC.

## 213003

**Error Message** %ASA-3-213003: PPP virtual interface *interface\_number* isn't opened.

**Explanation** An internal software error occurred while closing a PPP virtual interface.

**Recommended Action** Contact the Cisco TAC.

## 213004

**Error Message** %ASA-3-213004: PPP virtual interface *interface\_number* client ip allocation failed.

**Explanation** An internal software error occurred while allocating an IP address to the PPTP client when the IP local address pool was depleted.

**Recommended Action** Consider allocating a larger pool with the `ip local pool` command.

## 213005

**Error Message** %ASA-3-213005%: Dynamic-Access-Policy action (DAP) action aborted

**Explanation** The DAP is dynamically created by selecting configured access policies based on the authorization rights of the user and the posture assessment results of the remote endpoint device. The resulting dynamic policy indicates that the session should be terminated.

**Recommended Action** None required.

## 213006

**Error Message** %ASA-3-213006: Unable to read dynamic access policy record.



**Explanation** There was either an error in retrieving the DAP policy record data, or the action configuration was missing.

**Recommended Action** A configuration change might have resulted in deleting a DAP record. Use ASDM to recreate the DAP record.

## 213007

**Error Message** %ASA-4-213007: L2TP: Failed to install Redirect URL: *redirect URL* Redirect ACL: *non\_exist* for *assigned IP* .

**Explanation** An error occurred for an L2TP connection when the redirect URL was installed and the ACL was received from the ISE, but the redirect ACL does not exist on the ASA.

- *redirect URL* —The URL for the HTTP traffic redirection
- *assigned IP* —The IP address that is assigned to the user

**Recommended Action** Configure the redirect ACL on the ASA.

## 214001

**Error Message** %ASA-2-214001: Terminating manager session from *IP\_address* on interface *interface\_name* . Reason: incoming encrypted data (*number* bytes) longer than *number* bytes

**Explanation** An incoming encrypted data packet destined for the Secure Firewall ASA management port indicates a packet length exceeding the specified upper limit. This may be a hostile event. The Secure Firewall ASA immediately terminates this management connection.

**Recommended Action** Ensure that the management connection was initiated by Cisco Secure Policy Manager.

## 215001

**Error Message** %ASA-2-215001:Bad route\_compress() call, sdb = *number*

**Explanation** An internal software error occurred.

**Recommended Action** Contact the Cisco TAC.

## 217001

**Error Message** %ASA-2-217001: No memory for *string* in *string*

**Explanation** An operation failed because of low memory.

**Recommended Action** If sufficient memory exists, then send the error message, the configuration, and any details about the events leading up to the error to the Cisco TAC.

## 216001

**Error Message** %ASA-*n*-216001: internal error in: *function* : *message*

**Explanation** Various internal errors have occurred that should not appear during normal operation. The severity level varies depending on the cause of the message.

- **n**—The message severity
- **function**—The affected component
- **message**—A message describing the cause of the problem

**Recommended Action** Search the Bug Toolkit for the specific text message and try to use the Output Interpreter to resolve the problem. If the problem persists, contact the Cisco TAC.

## 216002

**Error Message** %ASA-3-216002: Unexpected event (major: *major\_id* , minor: *minor\_id* ) received by *task\_string* in *function* at line: *line\_num*

**Explanation** A task registers for event notification, but the task cannot handle the specific event. Events that can be watched include those associated with queues, booleans, and timer services. If any of the registered events occur, the scheduler wakes up the task to process the event. This message is generated if an unexpected event woke up the task, but it does not know how to handle the event.

If an event is left unprocessed, it can wake up the task very often to make sure that it is processed, but this should not occur under normal conditions. If this message appears, it does not necessarily mean the device is unusable, but something unusual has occurred and needs to be investigated.

- *major\_id* —Event identifier
- *minor\_id* —Event identifier
- *task\_string* —Custom string passed by the task to identify itself
- *function* —The function that received the unexpected event
- *line\_num* —Line number in the code

**Recommended Action** If the problem persists, contact the Cisco TAC.

## 216003

**Error Message** %ASA-3-216003: Unrecognized timer *timer\_ptr* , *timer\_id* received by *task\_string* in *function* at line: *line\_num*

**Explanation** An unexpected timer event woke up the task, but the task does not know how to handle the event. A task can register a set of timer services with the scheduler. If any of the timers expire, the scheduler wakes up the task to take action. This message is generated if the task is awakened by an unrecognized timer event.

An expired timer, if left unprocessed, wakes up the task continuously to make sure that it is processed, and this is undesirable. This should not occur under normal conditions. If this message appears, it does not necessarily mean the device is unusable, but something unusual has occurred and needs to be investigated.

- *timer\_ptr* —Pointer to the timer
- *timer\_id* —Timer identifier
- *task\_string* —Custom string passed by the task to identify itself
- *function* —The function that received the unexpected event
- *line\_num* —Line number in the code

**Recommended Action** If the problem persists, contact the Cisco TAC.

## 216004

**Error Message** %ASA-4-216004:prevented: error in function at file (line ) - stack trace

**Explanation** An internal logic error has occurred, which should not occur during normal operation.

- *error* —Internal logic error. Possible errors include the following:

- Exception
- Dereferencing null pointer
- Array index out of bounds
- Invalid buffer size
- Writing from input
- Source and destination overlap
- Invalid date
- Access offset from array indices

- *function* —The calling function that generated the error
- *file(line)* —The file and line number that generated the error
- *stack trace* —Full call stack traceback, starting with the calling function. For example: (“0x001010a4 0x00304e58 0x00670060 0x00130b04”)

**Recommended Action** If the problem persists, contact the Cisco TAC.

## 216005

**Error Message** %ASA-1-216005: ERROR: Duplex-mismatch on *interface\_name* resulted in transmitter lockup. A soft reset of the switch was performed.

**Explanation** A duplex mismatch on the port caused a problem in which the port can no longer transmit packets. This condition was detected, and the switch was reset to autorecover. This message applies only to the ASA 5505.

- *interface\_name* —The interface name that was locked up

**Recommended Action** A duplex mismatch exists between the specified port and the ASA 5505 that is connected to it. Correct the duplex mismatch by either setting both devices to autorecover, or hard coding the duplex mismatch for both devices to be the same.

## 218001

**Error Message** %ASA-2-218001: Failed Identification Test in *slot#* [*fail #/res* ].

**Explanation** The module in *slot#* of the Secure Firewall ASA cannot be identified as a genuine Cisco product. Cisco warranties and support programs apply only to genuine Cisco products. If Cisco determines that the cause of a support issue is related to non-Cisco memory, SSM modules, SSC modules, or other modules, Cisco may deny support under your warranty or under a Cisco support program such as SmartNet.

**Recommended Action** If this message recurs, copy it exactly as it appears on the console or in the system log. Research and try to resolve the error using the Output Interpreter. Also perform a search with the Bug Toolkit. If the problem persists, contact the Cisco TAC.

## 218002

**Error Message** %ASA-2-218002: Module (slot# ) is a registered proto-type for Cisco Lab use only, and not certified for live network operation.

**Explanation** The hardware in the specified location is a prototype module that came from a Cisco lab.

**Recommended Action** If this message reoccurs, copy it exactly as it appears on the console or in the system log. Research and try to resolve the error using the Output Interpreter. Also perform a search with the Bug Toolkit. If the problem persists, contact the Cisco TAC.

## 218003

**Error Message** %ASA-2-218003: Module Version in slot# is obsolete. The module in slot = slot# is obsolete and must be returned via RMA to Cisco Manufacturing. If it is a lab unit, it must be returned to Proto Services for upgrade.

**Explanation** Obsolete hardware has been detected or the **show module** command has been run for the module. This message is generated once per minute after it first appears.

**Recommended Action** If this message recurs, copy it exactly as it appears on the console or in the system log. Research and try to resolve the error using the Output Interpreter. Also perform a search with the Bug Toolkit. If the problem persists, contact the Cisco TAC.

## 218004

**Error Message** %ASA-2-218004: Failed Identification Test in slot# [fail# /res ]

**Explanation** A problem occurred while identifying hardware in the specified location.

**Recommended Action** If this message recurs, copy it exactly as it appears on the console or in the system log. Research and try to resolve the error using the Output Interpreter. Also perform a search with the Bug Toolkit. If the problem persists, contact the Cisco TAC.

## 218005

**Error Message** %ASA-2-218005: Inconsistency detected in the system information programmed in non-volatile memory

**Explanation** System information programmed in non-volatile memory is not consistent. This syslog will be generated during bootup if Secure Firewall ASA detects that the contents of the IDPROM are not identical to the contents of ACT2 EEPROM. Since the IDPROM and ACT2 EEPROM are programmed with exactly the same contents in manufacturing, this would happen either due to an error in manufacturing or if the IDPROM contents are tampered with.

**Recommended Action** If the message recurs, collect the output of the show tech-support command and contact Cisco TAC.

## 219002

**Error Message** %ASA-3-219002: I2C\_API\_name error, slot = slot\_number , device = device\_number , address = address , byte count = count . Reason: reason\_string

**Explanation** The I2C serial bus API has failed because of a hardware or software problem.

- *I2C\_API\_name* —The I2C API that failed, which can be one of the following:
  - I2C\_read\_byte\_w\_wait()
  - I2C\_read\_word\_w\_wait()
  - I2C\_read\_block\_w\_wait()
  - I2C\_write\_byte\_w\_wait()
  - I2C\_write\_word\_w\_wait()
  - I2C\_write\_block\_w\_wait()
  - I2C\_read\_byte\_w\_suspend()
  - I2C\_read\_word\_w\_suspend()
  - I2C\_read\_block\_w\_suspend()
  - I2C\_write\_byte\_w\_suspend()
  - I2C\_write\_word\_w\_suspend()
  - I2C\_write\_block\_w\_suspend()
- *slot\_number* —The hexadecimal number of the slot where the I/O operation that generated the message occurred. The slot number cannot be unique to a slot in the chassis. Depending on the chassis, two different slots might have the same I2C slot number. Also, the value is not necessarily less than or equal to the number of slots. The value depends on the way the I2C hardware is wired.
- *device\_number* —The hexadecimal number of the device on the slot for which the I/O operation was performed
- *address* —The hexadecimal address of the device on which the I/O operation occurred
- *byte\_count* —The byte count in decimal format of the I/O operation
- *error\_string* —The reason for the error, which can be one of the following:
  - I2C\_BUS\_TRANSACTION\_ERROR
  - I2C\_CHKSUM\_ERROR
  - I2C\_TIMEOUT\_ERROR
  - I2C\_BUS\_COLLISION\_ERROR
  - I2C\_HOST\_BUSY\_ERROR
  - I2C\_UNPOPULATED\_ERROR
  - I2C\_SMBUS\_UNSUPPORT
  - I2C\_BYTE\_COUNT\_ERROR
  - I2C\_DATA\_PTR\_ERROR

**Recommended Action** Perform the following steps:

1. Log and review the messages and the errors associated with the event. If the message does not occur continuously and disappears after a few minutes, it might be because the I2C serial bus is busy.
2. Reboot the software running on the Secure Firewall ASA.
3. Power cycle the device. When you turn off the power, make sure that you wait several seconds before turning the power on.
4. If the problem persists, contact the Cisco TAC.





## CHAPTER 3

# Syslog Messages 302003 to 342008

This chapter contains the following sections:

- [Messages 302003 to 319004, on page 105](#)
- [Messages 320001 to 342008, on page 143](#)

## Messages 302003 to 319004

This chapter includes messages from 302003 to 319004 .

### 302003

**Error Message** %ASA-6-302003: Built H245 connection for foreign\_address *outside\_address* /*outside\_port* local\_address *inside\_address* /*inside\_port*

**Explanation** An H.245 connection has been started from the **outside\_address** to the **inside\_address**. The Secure Firewall ASA has detected the use of an Intel Internet Phone. The foreign port (*outside\_port*) only appears on connections from outside the Secure Firewall ASA. The local port value (*inside\_port*) only appears on connections that were started on an internal interface.

**Recommended Action** None required.

### 302004

**Error Message** %ASA-6-302004: Pre-allocate H323 UDP backconnection for foreign\_address *outside\_address* /*outside\_port* to local\_address *inside\_address* /*inside\_port*

**Explanation** An H.323 UDP back connection has been preallocated to the foreign address (**outside\_address**) from the local address (**inside\_address**). The Secure Firewall ASA has detected the use of an Intel Internet Phone. The foreign port (**outside\_port**) only appears on connections from outside the Secure Firewall ASA. The local port value (**inside\_port**) only appears on connections that were started on an internal interface.

**Recommended Action** None required.

### 302010

**Error Message** %ASA-6-302010: *connections* in use, *connections* most used

**Explanation** Provides information on the number of connections that are in use and most used.

- **connections**—The number of connections

**Recommended Action** None required.

## 302012

**Error Message** %ASA-6-302012: Pre-allocate H225 Call Signalling Connection for faddr *IP\_address* /port to laddr *IP\_address*

**Explanation** An H.225 secondary channel has been preallocated.

**Recommended Action** None required.

## 302013

**Error Message** %ASA-6-302013: Built {inbound|outbound} [Probe] TCP *connection\_id* for interface :*real-address* /*real-port* (*mapped-address/mapped-port*) [(*idfw\_user*)] to interface :*real-address* /*real-port* (*mapped-address/mapped-port*) [(*idfw\_user*)] [(*user*)]

**Explanation** A TCP connection slot between two hosts was created.

- **probe**—Indicates the TCP connection is a probe connection
- **connection\_id** —A unique identifier
- **interface, real-address, real-port**—The actual sockets
- **mapped-address, mapped-port**—The mapped sockets
- **user**—The AAA name of the user
- **idfw\_user**—The name of the identity firewall user

If inbound is specified, the original control connection was initiated from the outside. For example, for FTP, all data transfer channels are inbound if the original control channel is inbound. If outbound is specified, the original control connection was initiated from the inside.

**Recommended Action** None required.

## 302014

**Error Message** %ASA-6-302014: Teardown [Probe] TCP connection id for interface :*real-address* /*real-port* [(*idfw\_user*)] to interface :*real-address* /*real-port* [(*idfw\_user*)] duration hh:mm:ss bytes bytes [reason [from teardown-initiator]] [(*user*)]

**Explanation** A TCP connection between two hosts was deleted. The following list describes the message values:

- **probe**—Indicates the TCP connection is a probe connection
- **id** —A unique identifier
- **interface, real-address, real-port**—The actual socket
- **duration**—The lifetime of the connection
- **bytes**— The data transfer of the connection



- **User**—The AAA name of the user
- **idfw\_user** —The name of the identity firewall user
- **reason**—The action that causes the connection to terminate. Set the **reason** variable to one of the TCP termination reasons listed in the following table.
- **teardown-initiator**—Interface name of the side that initiated the teardown.

**Table 44: TCP Termination Reasons**

Reason	Description
Conn-timeout	The connection ended when a flow is closed because of the expiration of its inactivity timer.
Deny Terminate	Flow was terminated by application inspection.
Failover primary closed	The standby unit in a failover pair deleted a connection because of a message received from the active unit.
FIN Timeout	Force termination after 10 minutes awaiting the last ACK or after half-closed timeout.
Flow closed by inspection	Flow was terminated by the inspection feature.
Flow terminated by IPS	Flow was terminated by IPS.
Flow reset by IPS	Flow was reset by IPS.
Flow terminated by TCP Intercept	Flow was terminated by TCP Intercept.
Flow timed out	Flow has timed out.
Flow timed out with reset	Flow has timed out, but was reset.
Flow is a loopback	Flow is a loopback.
Free the flow created as result of packet injection	The connection was built because the packet tracer feature sent a simulated packet through the Secure Firewall ASA.
Invalid SYN	The SYN packet was not valid.
IPS fail-close	Flow was terminated because the IPS card is down.
No interfaces associated with zone	Flows were torn down after the “no nameif” or “no zone-member” leaves a zone with no interface members.
No valid adjacency	This counter is incremented when the Secure Firewall ASA tried to obtain an adjacency and could not obtain the MAC address for the next hop. The packet is dropped.

Reason	Description
Pinhole Timeout	The counter is incremented to report that the Secure Firewall ASA opened a secondary flow, but no packets passed through this flow within the timeout interval, and so it was removed. An example of a secondary flow is the FTP data channel that is created after successful negotiation on the FTP control channel.
Probe maximum retries of retransmission exceeded	The connection was torn down because the TCP packet exceeded maximum probe retries of retransmission.
Probe maximum retransmission time elapsed	The connection was torn down because the maximum probing time for TCP packet had elapsed.
Probe received RST	The connection was torn down because probe connection received RST from server.
Probe received FIN	The connection was torn down because probe connection received FIN from server and complete FIN closure process was completed.
Probe completed	The probe connection was successful.
Route change	When the Secure Firewall ASA adds a lower cost (better metric) route, packets arriving that match the new route cause their existing connection to be torn down after the user-configured timeout (floating-conn) value. Subsequent packets rebuild the connection out of the interface with the better metric. To prevent the addition of lower cost routes from affecting active flows, you can set the floating-conn configuration timeout value to 0:0:0.
SYN Control	A back channel initiation occurred from the wrong side.
SYN Timeout	Force termination after 30 seconds, awaiting three-way handshake completion.
TCP bad retransmission	The connection was terminated because of a bad TCP retransmission.
TCP FINs	A normal close-down sequence occurred.
TCP Invalid SYN	Invalid TCP SYN packet.
TCP Reset - APPLIANCE	The flow is closed when a TCP reset is generated by the Secure Firewall ASA.
TCP Reset - I	Reset was from the inside.
TCP Reset - O	Reset was from the outside.
TCP segment partial overlap	A partially overlapping segment was detected.
TCP unexpected window size variation	A connection was terminated due to variation in the TCP window size.
Tunnel has been torn down	Flow was terminated because the tunnel is down.

Reason	Description
Unauth Deny	An authorization was denied by a URL filter.
Unknown	An unknown error has occurred.
VPN reclassify failed	When connections fail to be reclassified for passing through a VPN tunnel.
Xlate Clear	A command line was removed.

**Recommended Action** None required.

## 302015

**Error Message** %ASA-6-302015: Built {inbound|outbound} UDP connection *number* for *interface\_name* :*real\_address* /*real\_port* (*mapped\_address* /*mapped\_port* ) [(*idfw\_user* )] to *interface\_name* :*real\_address* /*real\_port* (*mapped\_address* /*mapped\_port* )[(*idfw\_user* )] [(*user* )]

**Explanation** A UDP connection slot between two hosts was created. The following list describes the message values:

- **number**—A unique identifier
- **interface, real\_address, real\_port**—The actual sockets
- **mapped\_address and mapped\_port**—The mapped sockets
- **user**—The AAA name of the user
- **idfw\_user**—The name of the identity firewall user

If inbound is specified, then the original control connection is initiated from the outside. For example, for UDP, all data transfer channels are inbound if the original control channel is inbound. If outbound is specified, then the original control connection is initiated from the inside.

**Recommended Action** None required.

## 302016

**Error Message** %ASA-6-302016: Teardown UDP connection *number* for *interface* :*real-address* /*real-port* [(*idfw\_user* )] to *interface* :*real-address* /*real-port* [(*idfw\_user* )] duration *hh* :*mm* :*ss* bytes *bytes* [(*user* )]

**Explanation** A UDP connection slot between two hosts was deleted. The following list describes the message values:

- **number**—A unique identifier
- **interface, real\_address, real\_port**—The actual sockets
- **time**—The lifetime of the connection
- **bytes**—The data transfer of the connection
- **id**—A unique identifier
- **interface, real-address, real-port**—The actual sockets
- **duration**— The lifetime of the connection
- **bytes**—The data transfer of the connection
- **user**—The AAA name of the user

- *idfw\_user*—The name of the identity firewall user

**Recommended Action** None required.

## 302017

**Error Message** %ASA-6-302017: Built {inbound|outbound} GRE connection *id* from *interface* :*real\_address* (*translated\_address*) [(*idfw\_user*)] to *interface* :*real\_address* /*real\_cid* (*translated\_address* /*translated\_cid*) [(*idfw\_user*)] [(*user*)]

**Explanation** A GRE connection slot between two hosts was created. The **id** is a unique identifier. The **interface**, **real\_address**, **real\_cid** tuple identifies the one of the two simplex PPTP GRE streams. The parenthetical **translated\_address**, **translated\_cid** tuple identifies the translated value with NAT. If inbound is indicated, then the connection can only be used inbound. If outbound is indicated, then the connection can only be used for outbound. The following list describes the message values:

- **id**—Unique number identifying the connection
- **inbound**—Control connection is for inbound PPTP GRE flow
- **outbound**—Control connection is for outbound PPTP GRE flow
- **interface\_name**—The interface name
- **real\_address**—IP address of the actual host
- **real\_cid**—Untranslated call ID for the connection
- **translated\_address**—IP address after translation
- **translated\_cid**—Translated call
- **user**—AAA user name
- *idfw\_user*—The name of the identity firewall user

**Recommended Action** None required.

## 302018

**Error Message** %ASA-6-302018: Teardown GRE connection *id* from *interface* :*real\_address* (*translated\_address*) [(*idfw\_user*)] to *interface* :*real\_address* /*real\_cid* (*translated\_address* /*translated\_cid*) [(*idfw\_user*)] duration *hh* :*mm* :*ss* bytes *bytes* [(*user*)]

**Explanation** A GRE connection slot between two hosts was deleted. The **interface**, **real\_address**, **real\_port** tuples identify the actual sockets. **Duration** identifies the lifetime of the connection. The following list describes the message values:

- **id**—Unique number identifying the connection
- **interface**—The interface name
- **real\_address**—IP address of the actual host
- **real\_port**—Port number of the actual host.
- **hh:mm:ss**—Time in hour:minute:second format
- **bytes**—Number of PPP bytes transferred in the GRE session
- **reason**—Reason why the connection was terminated
- **user**—AAA user name
- *idfw\_user*—The name of the identity firewall user

**Recommended Action** None required.

## 302019

**Error Message** %ASA-3-302019: H.323 *library\_name* ASN Library failed to initialize, error code *number*

**Explanation** The specified ASN library that the Secure Firewall ASA uses for decoding the H.323 messages failed to initialize; the Secure Firewall ASA cannot decode or inspect the arriving H.323 packet. The Secure Firewall ASA allows the H.323 packet to pass through without any modification. When the next H.323 message arrives, the Secure Firewall ASA tries to initialize the library again.

**Recommended Action** If this message is generated consistently for a particular library, contact the Cisco TAC and provide them with all log messages (preferably with timestamps).

## 302020

**Error Message** %ASA-6-302020: Built {in | out} bound ICMP connection for *faddr* {*faddr* | *icmp\_seq\_num* } [(*idfw\_user* )] *gaddr* {*gaddr* | *icmp\_type* } *laddr* *laddr* [(*idfw\_user* )] *type* {*type* } *code* {*code* } Rx [{*circular\_buffer\_size* }]

**Explanation** This message is generated when an ICMP session was established in the fast-path. The following list describes the message values:

- *faddr*—Specifies the IP address of the foreign host
- *gaddr*—Specifies the IP address of the global host
- *laddr*—Specifies the IP address of the local host
- *idfw\_user*—The name of the identity firewall user
- *user*—The username associated with the host from where the connection was initiated
- *type*—Specifies the ICMP type
- *code*—Specifies the ICMP code
- *Rx*—Specifies the received data circular-buffer size, where the buffer is overwritten, starting from the beginning, when the buffer is full.

**Recommended Action** None required.

## 302021

**Error Message** %ASA-6-302021: Teardown ICMP connection for *faddr* {*faddr* | *icmp\_seq\_num* } [(*idfw\_user* )] *gaddr* {*gaddr* | *icmp\_type* } *laddr* *laddr* [(*idfw\_user* )] *type* {*type* } *code* {*code* } Rx [{*circular\_buffer\_size* }]

**Explanation** This message is generated when an ICMP session is removed in the fast-path. The following list describes the message values:

- *faddr*—Specifies the IP address of the foreign host
- *gaddr*—Specifies the IP address of the global host
- *laddr*—Specifies the IP address of the local host
- *idfw\_user*—The name of the identity firewall user
- *user*—The username associated with the host from where the connection was initiated
- *type*—Specifies the ICMP type
- *code*—Specifies the ICMP code
- *Rx*—Specifies the received data circular-buffer size, where the buffer is overwritten, starting from the beginning, when the buffer is full.

**Recommended Action** None required.

## 302022

**Error Message** %ASA-6-302022: Built *role* stub TCP connection for *interface :real-address /real-port (mapped-address /mapped-port )* to *interface :real-address /real-port (mapped-address /mapped-port)*

**Explanation** A TCP director/backup/forwarder flow has been created.

**Recommended Action** None required.

## 302023

**Error Message** %ASA-6-302023: Teardown stub TCP connection for *interface :real-address /real-port* to *interface :real-address /real-port* duration *hh:mm:ss* forwarded bytes *bytes* reason

**Explanation** A TCP director/backup/forwarder flow has been torn down.

**Recommended Action** None required.

## 302024

**Error Message** %ASA-6-302024: Built *role* stub UDP connection for *interface :real-address /real-port (mapped-address /mapped-port )* to *interface :real-address /real-port (mapped-address /mapped-port )*

**Explanation** A UDP director/backup/forwarder flow has been created.

**Recommended Action** None required.

## 302025

**Error Message** %ASA-6-302025: Teardown stub UDP connection for *interface :real-address /real-port* to *interface :real-address /real-port* duration *hh:mm:ss* forwarded bytes *bytes* reason

**Explanation** A UDP director/backup/forwarder flow has been torn down.

**Recommended Action** None required.

## 302026

**Error Message** %ASA-6-302026: Built *role* stub ICMP connection for *interface :real-address /real-port (mapped-address )* to *interface :real-address /real-port (mapped-address )*

**Explanation** An ICMP director/backup/forwarder flow has been created.

**Recommended Action** None required.

## 302027

**Error Message** %ASA-6-302027: Teardown stub ICMP connection for interface *:real-address* /*real-port* to interface *:real-address* /*real-port* duration *hh:mm:ss* forwarded bytes *bytes* reason

**Explanation** An ICMP director/backup/forwarder flow has been torn down.

**Recommended Action** None required.

## 302033

**Error Message** %ASA-6-302033:Pre-allocated H323 GUP Connection for faddr interface *:foreign address* /*foreign-port* to laddr interface *:local-address* /*local-port*

**Explanation** A GUP connection was started from the foreign address to the local address. The foreign port (outside port) only appears on connections from outside the security device. The local port value (inside port) only appears on connections started on an internal interface.

- **interface**—The interface name
- *foreign-address* —IP address of the foreign host
- *foreign-port* —Port number of the foreign host
- *local-address* —IP address of the local host
- *local-port* —Port number of the local host

**Recommended Action** None required.

## 302034

**Error Message** %ASA-4-302034: Unable to pre-allocate H323 GUP Connection for faddr interface *:foreign address* /*foreign-port* to laddr interface *:local-address* /*local-port*

**Explanation** The module failed to allocate RAM system memory while starting a connection or has no more address translation slots available.

- **interface**—The interface name
- *foreign-address* —IP address of the foreign host
- *foreign-port* —Port number of the foreign host
- *local-address* —IP address of the local host
- *local-port* —Port number of the local host

**Recommended Action** If this message occurs periodically, it can be ignored. If it repeats frequently, contact the Cisco TAC. You can check the size of the global pool compared to the number of inside network clients. Alternatively, shorten the timeout interval of translations and connections. This message may also be caused by insufficient memory; try reducing the amount of memory usage, or purchasing additional memory.

## 302035

**Error Message** %ASA-6-302035: Built {inbound|outbound} SCTP connection *conn\_id* for *outside\_interface* *:outside\_ip* /*outside\_port* (*mapped\_outside\_ip* /*mapped\_outside\_port*) [(*outside\_idfw\_user* ], [*outside\_sg\_info* ])] to *inside\_interface* *:inside\_ip* /*inside\_port* (*mapped\_inside\_ip* /*mapped\_inside\_port*) [(*inside\_idfw\_user* ], [*inside\_sg\_info* ])] [(*user* )]

**Explanation** SCTP flow creation is logged when SCTP-state-bypass is not configured.

- *conn\_id* —The unique connection ID
- *outside\_interface* —The interface with the lower security level
- *outside\_ip* —The IP address of the host on the lower security level side of the ASA
- *outside\_port* —The port number of the host on the lower security level side of the ASA
- *mapped\_outside\_ip* —The mapped IP address of the host on the lower security level side of the ASA
- *mapped\_outside\_port* —The mapped port number of the host on the lower security level side of the ASA
- *outside\_idfw\_user* —The IDFW username associated with the host on the lower security level side of the ASA
- *outside\_sg\_info* —The SGT and SG name associated with the host on the lower security level side of the ASA
- *inside\_interface* —The interface with the higher security level
- *inside\_ip* —The IP address of the host on the higher security level side of the ASA
- *inside\_port* —The port number of the host on the higher security level side of the ASA
- *mapped\_inside\_ip* —The mapped IP address of the host on the higher security level side of the ASA
- *mapped\_inside\_port* —The mapped port number of the host on the higher security level side of the ASA
- *inside\_idfw\_user* —The IDFW username associated with the host on the higher security level side of the ASA
- *inside\_sg\_info* —The SGT and SG name associated with the host on the higher security level side of the ASA
- *user* —The username associated with the host from where the connection was initiated

**Recommended Action** None required.

## 302036

951 complete topic

**Error Message** %ASA-6-302036: Teardown SCTP connection *conn\_id* for *outside\_interface* :*outside\_ip* /*outside\_port* [[*outside\_idfw\_user* ],*outside\_sg\_info* ]] to *inside\_interface* :*inside\_ip* /*inside\_port* [[*inside\_idfw\_user* ],*inside\_sg\_info* ]] duration *time* bytes *bytes* reason [*user* ]

**Explanation** SCTP flow deletion is logged when SCTP-state-bypass is not configured.

- *conn\_id* —The unique connection ID
- *outside\_interface* —The interface with the lower security level
- *outside\_ip* —The IP address of the host on the lower security level side of the ASA
- *outside\_port* —The port number of the host on the lower security level side of the ASA
- *outside\_idfw\_user* —The IDFW username associated with the host on the lower security level side of the ASA
- *outside\_sg\_info* —The SGT and SG name associated with the host on the lower security level side of the ASA
- *inside\_interface* —The interface with the higher security level
- *inside\_ip* —The IP address of the host on the higher security level side of the ASA
- *inside\_port* —The port number of the host on the higher security level side of the ASA
- *inside\_idfw\_user* —The IDFW username associated with the host on the higher security level side of the ASA



- *inside\_sg\_info* —The SGT and SG name associated with the host on the higher security level side of the ASA
- *user* —The username associated with the host from where the connection was initiated
- *time* —The amount of the flow stayed alive in hh:mm:ss
- *bytes* —The number of bytes passed on the flow
- *reason* —The reason the connection was torn down

**Recommended Action** None required.

## 302302

**Error Message** %ASA-3-302302: ACL = deny; no sa created

**Explanation** IPsec proxy mismatches have occurred. Proxy hosts for the negotiated SA correspond to a deny access-list command policy.

**Recommended Action** Check the access-list command statement in the configuration. Contact the administrator for the peer.

## 302303

**Error Message** %ASA-6-302303: Built TCP state-bypass connection *conn\_id* from *initiator\_interface* :*real\_ip* /*real\_port* (*mapped\_ip* /*mapped\_port* ) to *responder\_interface* :*real\_ip* /*real\_port* (*mapped\_ip* /*mapped\_port* )

**Explanation** A new TCP connection has been created, and this connection is a TCP-state-bypass connection. This type of connection bypasses all the TCP state checks and additional security checks and inspections.

**Recommended Action** If you need to secure TCP traffic with all the normal TCP state checks as well as all other security checks and inspections, you can use the **no set connection advanced-options tcp-state-bypass** command to disable this feature for TCP traffic.

## 302304

**Error Message** %ASA-6-302304: Teardown TCP state-bypass connection *conn\_id* from *initiator\_interface* :*ip*/*port* to *responder\_interface* :*ip*/*port* *duration* , *bytes* , *teardown reason* .

**Explanation** A new TCP connection has been torn down, and this connection is a TCP-state-bypass connection. This type of connection bypasses all the TCP state checks and additional security checks and inspections.

- *duration* —The duration of the TCP connection
- *bytes* —The total number of bytes transmitted over the TCP connection
- *teardown reason* —The reason for the teardown of the TCP connection

**Recommended Action** If you need to secure TCP traffic with all the normal TCP state checks as well as all other security checks and inspections, you can use the **no set connection advanced-options tcp-state-bypass** command to disable this feature for TCP traffic.

## 302305

**Error Message** %ASA-6-302305: Built SCTP state-bypass connection *conn\_id* for *outside\_interface* :*outside\_ip* /*outside\_port* (*mapped\_outside\_ip* /*mapped\_outside\_port* )([[*outside\_idfw\_user* ],[*outside\_sg\_info* ]]) to *inside\_interface* :*inside\_ip* /*inside\_port* (*mapped\_inside\_ip* /*mapped\_inside\_port* )([[*inside\_idfw\_user* ],[*inside\_sg\_info* ]])

**Explanation** SCTP flow creation is logged when SCTP-state-bypass is configured.

- *conn\_id* —The unique connection ID
- *outside\_interface* —The interface with the lower security level
- *outside\_ip* —The IP address of the host on the lower security level side of the ASA
- *outside\_port* —The port number of the host on the lower security level side of the ASA
- *mapped\_outside\_ip* —The mapped IP address of the host on the lower security level side of the ASA
- *mapped\_outside\_port* —The mapped port number of the host on the lower security level side of the ASA
- *outside\_idfw\_user* —The IDFW username associated with the host on the lower security level side of the ASA
- *outside\_sg\_info* —The SGT and SG name associated with the host on the lower security level side of the ASA
- *inside\_interface* —The interface with the higher security level
- *inside\_ip* —The IP address of the host on the higher security level side of the ASA
- *inside\_port* —The port number of the host on the higher security level side of the ASA
- *mapped\_inside\_ip* —The mapped IP address of the host on the higher security level side of the ASA
- *mapped\_inside\_port* —The mapped port number of the host on the higher security level side of the ASA
- *inside\_idfw\_user* —The IDFW username associated with the host on the higher security level side of the ASA
- *inside\_sg\_info* —The SGT and SG name associated with the host on the higher security level side of the ASA

**Recommended Action** None required.

## 302306

**Error Message** %ASA-6-302306: Teardown SCTP state-bypass connection *conn\_id* for *outside\_interface* :*outside\_ip* /*outside\_port* ([[*outside\_idfw\_user* ],[*outside\_sg\_info* ]]) to *inside\_interface* :*inside\_ip* /*inside\_port* ([[*inside\_idfw\_user* ],[*inside\_sg\_info* ]]) duration *time* bytes *bytes* reason

**Explanation** SCTP flow deletion is logged when SCTP-state-bypass is configured.

- *conn\_id* —The unique connection ID
- *outside\_interface* —The interface with the lower security level
- *outside\_ip* —The IP address of the host on the lower security level side of the ASA
- *outside\_port* —The port number of the host on the lower security level side of the ASA
- *outside\_idfw\_user* —The IDFW username associated with the host on the lower security level side of the ASA
- *outside\_sg\_info* —The SGT and SG name associated with the host on the lower security level side of the ASA
- *inside\_interface* —The interface with the higher security level
- *inside\_ip* —The IP address of the host on the higher security level side of the ASA

- *inside\_port*—The port number of the host on the higher security level side of the ASA
- *inside\_outside\_ip*—The mapped IP address of the host on the higher security level side of the ASA
- *inside\_idfw\_user*—The IDFW username associated with the host on the higher security level side of the ASA
- *inside\_sg\_info*—The SGT and SG name associated with the host on the higher security level side of the ASA
- *time*—The amount of time that the flow stayed alive in hh:mm:ss
- *bytes*—The number of bytes passed on the flow
- *reason*—The reason the connection was torn down

**Recommended Action** None required.

## 4302310

**Error Message** %ASA-4-302310: SCTP packet received from *src\_ifc:src\_ip/src\_port* to *dst\_ifc:dst\_ip/dst\_port* contains unsupported Hostname Parameter.

**Explanation** A init/init-ack packet is received with the hostname parameter.

- **packet init/init-ack**—The message carrying the hostname parameter
- **src-ifc**— Indicates the ingress interface
- **src-ip/src-port**— Indicates the Source IP and Port in the packet
- **dst-ifc**—Indicates the egress interface
- **dst\_ip/dst\_port**—Indicates the Source IP and Port in the packet

**Recommended Action** Use the real IP addresses of endpoints rather than the hostname. Disable the hostname parameter.

## 302311

**Error Message** %ASA-4-302311: Failed to create a new *protocol* connection from *ingress interface:source IP/source port* to *egress interface:destination IP/destination port* due to application cache memory allocation failure. The app-cache memory threshold level is *threshold%* and threshold check is *enabled/disabled*.

**Explanation** A new connection could not be created due to app-cache memory allocation failure. The failure could be due to system running out of memory or exceeding app-cache memory threshold.

- **protocol**—The name of the protocol used to create the connection
- **ingress interface**—The interface name
- **source IP**—The source IP address
- **source port**—The source port number
- **egress interface**—The interface name
- **destination IP**— The destination address
- **destination port**—The destination port number
- **threshold%**—The percentage value of memory threshold
- **enabled/disabled**—app-cache memory threshold feature enabled/disabled

**Recommended Action** Disable memory intensive features on the device or reduce the number of through-the-box connections.

## 303002

**Error Message** %ASA-6-303002: FTP connection from *src\_ifc* :*src\_ip* /*src\_port* to *dst\_ifc* :*dst\_ip* /*dst\_port* , user *username* action *file filename*

**Explanation** A client has uploaded or downloaded a file from the FTP server.

- **src\_ifc**—The interface where the client resides.
- **src\_ip**—The IP address of the client.
- **src\_port**—The client port.
- **dst\_ifc**—The interface where the server resides.
- **dst\_ip**—The IP address of the FTP server.
- **dst\_port**—The server port.
- **username**—The FTP username.
- **action**—The stored or retrieved actions.
- **filename**—The file stored or retrieved.

**Recommended Action** None required.

## 303004

**Error Message** %ASA-5-303004: FTP *cmd\_string* command unsupported - failed strict inspection, terminating connection from *source\_interface* :*source\_address* /*source\_port* to *dest\_interface* :*dest\_address*/*dest\_interface*

**Explanation** Strict FTP inspection on FTP traffic has been used, and an FTP request message contains a command that is not recognized by the device.

**Recommended Action** None required.

## 303005

**Error Message** %ASA-5-303005: Strict FTP inspection matched *match\_string* in policy-map *policy-name* , action\_string from *src\_ifc* :*sip* /*sport* to *dest\_ifc* :*dip* /*dport*

**Explanation** When FTP inspection matches any of the following configured values: filename, file type, request command, server, or username, then the action specified by the *action\_string* in this message occurs.

- **match\_string** —The match clause in the policy map
- **policy-name**—The policy map that matched
- **action\_string**—The action to take; for example, Reset Connection
- **src\_ifc**—The source interface name
- **sip**—The source IP address
- **sport**—The source port
- **dest\_ifc**—The destination interface name
- **dip**—The destination IP address
- **dport**—The destination port

**Recommended Action** None required.

## 304001

**Error Message** %ASA-5-304001: *user@source\_address [(idfw\_user )] Accessed URL dest\_address : url .*

**Explanation** The specified host tried to access the specified URL. If you enable the HTTP inspection with custom HTTP policy map, the following possibilities are seen. When the packet of GET request does not have the hostname parameter, instead of printing the URI, it prints the following message: %ASA-5-304001: client IP Accessed URL server ip: Hostname not present URI: URI. If a large URI which cannot be printed in a single syslog, you can print partial wherever it is being chopped down. For instance, when the URL is to be divided into multiple chunks and logged, the following message is printed: %ASA-5-304001: client IP Accessed URL server ip: http(ftp)://hostname/URI\_CHUNK1 partial %ASA-5-304001: client IP Accessed URL server ip: partial URI\_CHUNK1 partial..... %ASA-5-304001: client IP Accessed URL server ip: partial URI\_CHUNKn. The limit for URI is 1024 bytes. If the current packet contains partial URI at the beginning or end, use the same logic as explained above.

**Recommended Action** None required.

## 304002

**Error Message** %ASA-5-304002: *Access denied URL chars SRC IP\_address [(idfw\_user )] DEST IP\_address : chars*

**Explanation** Access from the source address to the specified URL or FTP site was denied.

**Recommended Action** None required.

## 304003

**Error Message** %ASA-3-304003: *URL Server IP\_address timed out URL url*

**Explanation** A URL server timed out.

**Recommended Action** None required.

## 304004

**Error Message** %ASA-6-304004: *URL Server IP\_address request failed URL url*

**Explanation** A Websense server request failed.

**Recommended Action** None required.

## 304005

**Error Message** %ASA-7-304005: *URL Server IP\_address request pending URL url*

**Explanation** A Websense server request is pending.

**Recommended Action** None required.

## 304006

**Error Message** %ASA-3-304006: URL Server *IP\_address* not responding

**Explanation** The Websense server is unavailable for access, and the ASA attempts to either try to access the same server if it is the only server installed, or another server if there is more than one.

**Recommended Action** None required.

## 304007

**Error Message** %ASA-2-304007: URL Server *IP\_address* not responding, ENTERING ALLOW mode.

**Explanation** You used the allow option of the filter command, and the Websense servers are not responding. The ASA allows all web requests to continue without filtering while the servers are not available.

**Recommended Action** None required.

## 304008

**Error Message** %ASA-2-304008: LEAVING ALLOW mode, URL Server is up.

**Explanation** You used the allow option of the filter command, and the ASA receives a response message from a Websense server that previously was not responding. With this response message, the ASA exits the allow mode, which enables the URL filtering feature again.

**Recommended Action** None required.

## 304009

**Error Message** %ASA-7-304009: Ran out of buffer blocks specified by url-block command

**Explanation** The URL pending buffer block is running out of space.

**Recommended Action** Change the buffer block size by entering the **url-block block block\_size** command.

## 305005

**Error Message** %ASA-3-305005: No translation group found for protocol src interface\_name: source\_address/source\_port [(idfw\_user )] dst interface\_name: dest\_address /dest\_port [(idfw\_user )]

**Explanation** A packet does not match any of the outbound nat command rules. If NAT is not configured for the specified source and destination systems, the message will be generated frequently.

**Recommended Action** This message indicates a configuration error. If dynamic NAT is desired for the source host, ensure that the **nat** command matches the source IP address. If static NAT is desired for the source host, ensure that the local IP address of the **static** command matches. If no NAT is desired for the source host, check the ACL bound to the NAT 0 ACL.

## 305006

**Error Message** %ASA-3-305006: {outbound static|identity|portmap|regular) translation creation failed for protocol src interface\_name:source\_address/source\_port [(idfw\_user)] dst interface\_name:dest\_address/dest\_port [(idfw\_user)]

**Explanation** The ICMP error inspection was enabled and the following conditions were met:

- There was a connection established through the device with forward and reverse flows having different protocols. For example, forward flow is UDP or TCP, reverse flow is ICMP. The switch in protocols occurs when either the receiver or any intermediary device in the path returns ICMP error messages, for example type 3 code 3.
- There was a dynamic NAT/PAT statement that matched the packets of the reverse flow and failed to translate the outer header IP addresses because the device does not apply PAT to all ICMP message types; it only applies PAT ICMP echo and echo-reply packets (types 8 and 0).

**Recommended Action** None required.

## 305007

**Error Message** %ASA-6-305007: addrpool\_free(): Orphan IP IP\_address on interface interface\_number

**Explanation** The ASA has attempted to translate an address that it cannot find in any of its global pools. The ASA assumes that the address was deleted and drops the request.

**Recommended Action** None required.

## 305008

**Error Message** %ASA-3-305008: Free unallocated global IP address.

**Explanation** The ASA kernel detected an inconsistency condition when trying to free an unallocated global IP address back to the address pool. This abnormal condition may occur if the ASA is running a Stateful Failover setup, and some of the internal states are momentarily out of sync between the active unit and the standby unit. This condition is not catastrophic, and the synchronization recovers automatically.

**Recommended Action** If the problem persists, contact the Cisco TAC.

## 305009

**Error Message** %ASA-6-305009: Built {dynamic|static} translation from interface\_name [(acl-name)]:real\_address [(idfw\_user)] to interface\_name :mapped\_address

**Explanation** An address translation slot was created. The slot translates the source address from the local side to the global side. In reverse, the slot translates the destination address from the global side to the local side.

**Recommended Action** None required.

## 305010

**Error Message** %ASA-6-305010: Teardown {dynamic|static} translation from *interface\_name* :*real\_address* [(*idfw\_user*)] to *interface\_name* :*mapped\_address* duration *time*

**Explanation** The address translation slot was deleted.

**Recommended Action** None required.

## 305011

**Error Message** %ASA-6-305011: Built {dynamic|static} {TCP|UDP|ICMP} translation from *interface\_name* :*real\_address/real\_port* [(*idfw\_user*)] to *interface\_name* :*mapped\_address/mapped\_port*

**Explanation** A TCP, UDP, or ICMP address translation slot was created. The slot translates the source socket from the local side to the global side. In reverse, the slot translates the destination socket from the global side to the local side.

**Recommended Action** None required.

## 305012

**Error Message** %ASA-6-305012: Teardown {dynamic|static} {TCP|UDP|ICMP} translation from *interface\_name* [(*acl-name*)] :*real\_address* /{*real\_port* |*real\_ICMP\_ID* } [(*idfw\_user*)] to *interface\_name* :*mapped\_address* /{*mapped\_port* |*mapped\_ICMP\_ID* } duration *time*

**Explanation** The address translation slot was deleted.

**Recommended Action** None required.

## 305013

**Error Message** %ASA-5-305013: Asymmetric NAT rules matched for forward and reverse flows; Connection protocol *src interface\_name* :*source\_address* /*source\_port* [(*idfw\_user*)] *dst interface\_name* :*dst\_address* /*dst\_port* [(*idfw\_user*)] denied due to NAT reverse path failure.

**Explanation** An attempt to connect to a mapped host using its actual address was rejected.

**Recommended Action** When not on the same interface as the host using NAT, use the mapped address instead of the actual address to connect to the host. In addition, enable the **inspect** command if the application embeds the IP address.

## 305014

**Error Message** %ASA-6-305014: Allocated block of ports for translation from *real\_interface* :*real\_host\_ip* /*real\_source\_port* to *real\_dest\_interface* :*real\_dest\_ip* /*real\_dest\_port*.

**Explanation** When CGNAT “block-allocation” is configured, this syslog will be generated on allocation of a new port block.

**Recommended Action** None.



## 305015

**Error Message** %ASA-6-305015: Released block of ports for translation from *real\_interface* :*real\_host\_ip* /*real\_source\_port* to *real\_dest\_interface* :*real\_dest\_ip* /*real\_dest\_port*.

**Explanation** When CGNAT “block-allocation” is configured, this syslog will be generated on release of an allocated port block.

**Recommended Action** None.

## 305016

**Error Message** %ASA-3-305016: Unable to create *protocol* connection from *real\_interface* :*real\_host\_ip* /*real\_source\_port* to *real\_dest\_interface* :*real\_dest\_ip* /*real\_dest\_port* due to *reason* .

**Explanation** The maximum port blocks per host limit has been reached for a host or the port blocks have been exhausted.

- *reason* —May be one of the following:
  - reaching per-host PAT port block limit of *value*
  - port block exhaustion in PAT pool

**Recommended Action** For reaching the per-host PAT port block limit, review the maximum blocks per host limit by entering the following command:

```
xlate block-allocation maximum-per-host 4
```

For the port block exhaustion in the PAT pool, we recommend increasing the pool size. Also, review the block size by entering the following command:

```
xlate block-allocation size 512
```

## 305017

**Error Message** %ASA-3-305017: Pba-interim-logging: Active ICMP block of ports for translation from <*source device IP*> to <*destination device IP*>/<*Active Port Block*>

**Explanation** When CGNAT interim logging feature is turned on. This syslog specifies the Active Port Block from a particular source IP address to a destination IP address at that time.

**Recommended Action**None.

## 305018

**Error Message** %ASA-6-305018: MAP translation from *src\_ifc:src\_ip/src\_port-dst\_ifc:dst\_ip/dst\_port* to *src\_ifc:translated\_src\_ip/src\_port-dst\_ifc:translated\_dst\_ip/dst\_port*

**Explanation** MAP style address translation has been applied to a connection being established, their source and destination have been translated

Example:

```
%ASA-6-305018: MAP translation from
inside:2001:DB8:0000:0000:0000:0000:0002/57964-outside:2001:DB8:FFFF:0000:0000:0000:0001/22
to inside:192.168.101.210/57964-outside:192.168.100.203/22
```

**Recommended Action**None.

## 305019

**Error Message** %ASA-3-305019: MAP node address *ip/port* has inconsistent Port Set ID encoding

**Explanation**A packet has an address that matches MAP basic mapping rules (meaning it is meant to be translated) but the Port Set ID encoded within the address is inconsistent (per RFC7599). This could be due to a software fault on the MAP node where this packet originates.

Example

```
%ASA-3-305019: MAP node address 2001:DB8:0000:FFFF:0000:0000:0000:0002/57964 has inconsistent
Port Set ID encoding
```

**Recommended Action**None.

## 305020

**Error Message** %ASA-3-305020: MAP node with address *ip* is not allowed to use port *port*\n

**Explanation** A packet has an address that matches MAP basic mapping rules (meaning it is meant to be translated) but the associated port does not fall within the range allocated to that address. This likely means there is misconfiguration on the MAP node where this packet originates.

Example:

```
%ASA-3-305020: MAP node with address 2001:DB8:0000:0000:0000:0000:0000:0002 is not allowed
to use port 37964\n
```

**Recommended Action**None.

## 305021

**Error Message** %ASA-4-305021: Ports exhausted in pre-allocated PAT pool IP *mapped\_ip\_address* for host *real\_host\_ip*. Allocating from new PAT pool IP *mapped\_ip\_address*.

**Explanation** This message is generated when all ports are exhausted in the sticky IP on a cluster node and allocation moves to the next available IP with free ports.

**Example:**

```
%ASA-4-305021: Ports exhausted in pre-allocated PAT pool IP 174.0.1.1 for host 192.168.1.20.
Allocating from new PAT pool IP 174.0.1.2.
```

**Recommended Action** None.

## 305022

**Error Message** %ASA-4-305022: Cluster unit *unit\_name* has been allocated *num\_of\_port\_blocks* port blocks for PAT usage. All units should have at least *min\_num\_of\_port\_blocks* port blocks.

**Explanation** This message is generated on a node when it joins cluster and does not get any or unequal share of port blocks.

**Examples**

%ASA-4-305022: Cluster unit ASA-4 has been allocated 0 port blocks for PAT usage. All units should have at least 32 port blocks.

%ASA-4-305022: Cluster unit ASA-4 has been allocated 12 port blocks for PAT usage. All units should have at least 32 port blocks.

**Recommended Action** None.

## 308001

**Error Message** %ASA-6-308001: console enable password incorrect for *number* tries (from *IP\_address* )

**Explanation** This is a Secure Firewall ASA management message. This message appears after the specified number of times a user incorrectly types the password to enter privileged mode. The maximum is three attempts.

**Recommended Action** Verify the password and try again.

## 308002

**Error Message** %ASA-4-308002: static *global\_address inside\_address netmask netmask* overlapped with *global\_address inside\_address*

**Explanation** The IP addresses in one or more static command statements overlap. **global\_address** is the global address, which is the address on the lower security interface, and **inside\_address** is the local address, which is the address on the higher security-level interface.

**Recommended Action** Use the show static command to view the static command statements in your configuration and fix the commands that overlap. The most common overlap occurs if you specify a network address such as 10.1.1.0, and in another static command you specify a host within that range, such as 10.1.1.5.

## 308003

**Error Message** %ASA-4-308003: WARNING: The enable password is not configured

**Explanation** When entering enable mode (privilege level 2 or greater), you are forced to configure the enable password for privilege level 15 when the enable password is not already set.

**Recommended Action** Set the enable password. The permitted length of password is between 3 and 15.

## 308004

**Error Message** %ASA-4-308004: The enable password has been configured by user *admin*

**Explanation** You have configured the enable password for the first time. This message will not be displayed when you are modifying an existing enable password.

**Recommended Action** None.

## 311001

**Error Message** %ASA-6-311001: LU loading standby start

**Explanation** Stateful Failover update information was sent to the standby Secure Firewall ASA when the standby Secure Firewall ASA is first to be online.

**Recommended Action** None required.

## 311002

**Error Message** %ASA-6-311002: LU loading standby end

**Explanation** Stateful Failover update information stopped sending to the standby Secure Firewall ASA.

**Recommended Action** None required.

## 311003

**Error Message** %ASA-6-311003: LU recv thread up

**Explanation** An update acknowledgment was received from the standby Secure Firewall ASA.

**Recommended Action** None required.

## 311004

**Error Message** %ASA-6-311004: LU xmit thread up

**Explanation** A Stateful Failover update was transmitted to the standby Secure Firewall ASA.

**Recommended Action** None required.

## 312001

**Error Message** %ASA-6-312001: RIP hdr failed from *IP\_address* : cmd=*string* , version=*number* domain=*string* on interface *interface\_name*

**Explanation** The Secure Firewall ASA received a RIP message with an operation code other than reply, the message has a version number different from what is expected on this interface, and the routing domain entry was nonzero. Another RIP device may not be configured correctly to communicate with the Secure Firewall ASA.

**Recommended Action** None required.

## 313001

**Error Message** %ASA-3-313001: Denied ICMP type=*number* , code=*code* from *IP\_address* on interface *interface\_name*

**Explanation** When using the icmp command with an access list, if the first matched entry is a permit entry, the ICMP packet continues processing. If the first matched entry is a deny entry, or an entry is not matched, the Secure Firewall ASA discards the ICMP packet and generates this message. The **icmp** command enables

or disables pinging to an interface. With pinging disabled, the Secure Firewall ASA cannot be detected on the network. This feature is also referred to as configurable proxy pinging.

**Recommended Action** Contact the administrator of the peer device.

## 313004

**Error Message** %ASA-4-313004:Denied ICMP type=*icmp\_type* , from *source\_address* on interface *interface\_name* to *dest\_address* :no matching session

**Explanation** ICMP packets were dropped by the Secure Firewall ASA because of security checks added by the stateful ICMP feature that are usually either ICMP echo replies without a valid echo request already passed across the Secure Firewall ASA or ICMP error messages not related to any TCP, UDP, or ICMP session already established in the Secure Firewall ASA.

**Recommended Action** None required.

## 313005

**Error Message** %ASA-4-313005: No matching connection for ICMP error message: *icmp\_msg\_info* on *interface\_name* interface. Original IP payload: *embedded\_frame\_info icmp\_msg\_info* = icmp *src src\_interface\_name :src\_address* [(*idfw\_user* | *FQDN\_string*), *sg\_info*] *dst dest\_interface\_name :dest\_address* [(*idfw\_user* | *FQDN\_string*), *sg\_info*] (type *icmp\_type*, code *icmp\_code*) *embedded\_frame\_info* = prot *src source\_address /source\_port* [(*idfw\_user* | *FQDN\_string*), *sg\_info*] *dst dest\_address /dest\_port* [(*idfw\_user* | *FQDN\_string*), *sg\_info*]

**Explanation** ICMP error packets were dropped by the Secure Firewall ASA because the ICMP error messages are not related to any session already established in the Secure Firewall ASA.

**Recommended Action** If the cause is an attack, you can deny the host by using ACLs.

## 313008

**Error Message** %ASA-3-313008: Denied ICMPv6 type=*number* , code=*code* from *IP\_address* on interface *interface\_name*

**Explanation** When using the **icmp** command with an access list, if the first matched entry is a permit entry, the ICMPv6 packet continues processing. If the first matched entry is a deny entry, or an entry is not matched, the Secure Firewall ASA discards the ICMPv6 packet and generates this message.

The **icmp** command enables or disables pinging to an interface. When pinging is disabled, the Secure Firewall ASA is undetectable on the network. This feature is also referred to as “configurable proxy pinging.”

**Recommended Action** Contact the administrator of the peer device.

## 313009

**Error Message** %ASA-4-313009: Denied invalid ICMP code *icmp-code* , for *src-ifc :src-address /src-port* (mapped-src-address/mapped-src-port) to *dest-ifc :dest-address /dest-port* (mapped-dest-address/mapped-dest-port) [*user*], ICMP id *icmp-id* , ICMP type *icmp-type*

**Explanation** An ICMP echo request/reply packet was received with a malformed code(non-zero).

**Recommended Action** If it is an intermittent event, no action is required. If the cause is an attack, you can deny the host using the ACLs.

## 314001

**Error Message** %ASA-6-314001: Pre-allocated RTSP UDP backconnection for *src\_intf* :*src\_IP* to *dst\_intf* :*dst\_IP* /*dst\_port*.

**Explanation** The Secure Firewall ASA opened a UDP media channel for the RTSP client that was receiving data from the server.

- *src\_intf*—Source interface name
- *src\_IP*—Source interface IP address
- *dst\_intf*—Destination interface name
- *dst\_IP*—Destination IP address
- *dst\_port*—Destination port

**Recommended Action** None required.

## 314002

**Error Message** %ASA-6-314002: RTSP failed to allocate UDP media connection from *src\_intf* :*src\_IP* to *dst\_intf* :*dst\_IP* /*dst\_port* : *reason\_string*.

**Explanation** The Secure Firewall ASA cannot open a new pinhole for the media channel.

- *src\_intf*—Source interface name
- *src\_IP*—Source interface IP address
- *dst\_intf*—Destination interface name
- *dst\_IP*—Destination IP address
- *dst\_port*—Destination port
- *reason\_string*—Pinhole already exists/Unknown

**Recommended Action** If the reason is unknown, check the free memory available by running the **show memory** command, or the number of connections used by running the **show conn** command, because the Secure Firewall ASA is low on memory.

## 314003

**Error Message** %ASA-6-314003: Dropped RTSP traffic from *src\_intf* :*src\_ip* due to: *reason*.

**Explanation** The RTSP message violated the user-configured RTSP security policy, either because it contains a port from the reserve port range, or it contains a URL with a length greater than the maximum limit allowed.

- *src\_intf*—Source interface name
- *src\_IP*—Source interface IP address
- *reason*—The reasons may be one of the following:
  - Endpoint negotiating media ports in the reserved port range from 0 to 1024
  - URL length of *url length* bytes exceeds the maximum *url length limit* bytes

**Recommended Action** Investigate why the RTSP client sends messages that violate the security policy. If the requested URL is legitimate, you can relax the policy by specifying a longer URL length limit in the RTSP policy map.

## 314004

**Error Message** %ASA-6-314004: RTSP client *src\_intf:src\_IP* accessed RTSP URL *RTSP\_URL*

**Explanation** An RTSP client tried to access an RTSP server.

- *src\_intf*—Source interface name
- *src\_IP*—Source interface IP address
- *RTSP\_URL*—RTSP server URL

**Recommended Action** None required.

## 314005

**Error Message** %ASA-6-314005: RTSP client *src\_intf:src\_IP* denied access to URL *RTSP\_URL*.

**Explanation** An RTSP client tried to access a prohibited site.

- *src\_intf*—Source interface name
- *src\_IP*—Source interface IP address
- *RTSP\_URL*—RTSP server URL

**Recommended Action** None required.

## 314006

**Error Message** %ASA-6-314006: RTSP client *src\_intf:src\_IP* exceeds configured rate limit of *rate* for *request\_method* messages.

**Explanation** A specific RTSP request message exceeded the configured rate limit of RTSP policy.

- *src\_intf*—Source interface name
- *src\_IP*—Source interface IP address
- *rate*—Configured rate limit
- *request\_method*—Type of request message

**Recommended Action** Investigate why the specific RTSP request message from the client exceeded the rate limit.

## 315004

**Error Message** %ASA-3-315004: Fail to establish SSH session because RSA host key retrieval failed.

**Explanation** The ASA cannot find the RSA host key, which is required for establishing an SSH session. The ASA host key may be absent because it was not generated or because the license for this ASA does not allow DES or 3DES encryption.

**Recommended Action** From the ASA console, enter the **show crypto key mypubkey rsa** command to verify that the RSA host key is present. If the host key is not present, enter the **show version** command to verify that DES or 3DES is allowed. If an RSA host key is present, restart the SSH session. To generate the RSA host key, enter the **crypto key mypubkey rsa** command.

## 315011

**Error Message** %ASA-6-315011: SSH session from *IP\_address* on interface *interface\_name* for user *user* disconnected by SSH server, reason: *reason*

**Explanation** An SSH session has ended. If a user enters **quit** or **exit**, the **terminated normally** message appears. The username is hidden when invalid or unknown, but appears when valid or the **no logging hide username** command has been configured. If the session disconnected for another reason, the text describes the reason. The following table lists the possible reasons why a session is disconnected.

**Table 45: SSH Disconnect Reasons**

Text String	Explanation	Action
Bad checkbytes	A mismatch was detected in the check bytes during an SSH key exchange.	Restart the SSH session.
CRC check failed	The CRC value computed for a particular packet does not match the CRC value embedded in the packet; the packet is bad.	None required. If this message persists, call Cisco TAC.
Decryption failure	Decryption of an SSH session key failed during an SSH key exchange.	Check the RSA host key and try again.
Format error	A nonprotocol version message was received during an SSH version exchange.	Check the SSH client, to ensure it is a supported version.
Internal error	This message indicates either an error internal to SSH on the ASA or an RSA key may not have been entered on the ASA or cannot be retrieved.	From the ASA console, enter the <b>show crypto key mypubkey rsa</b> command to verify that the RSA host key is present. If the host key is not present, enter the <b>show version</b> command to verify that DES or 3DES is allowed. If an RSA host key is present, restart the SSH session. To generate the RSA host key, enter the <b>crypto key mypubkey rsa</b> command.
Invalid cipher type	The SSH client requested an unsupported cipher.	Enter the <b>show version</b> command to determine which features your license supports, then reconfigure the SSH client to use the supported cipher.
Invalid message length	The length of SSH message arriving at the ASA exceeds 262,144 bytes or is shorter than 4096 bytes. The data may be corrupted.	None required.



Text String	Explanation	Action
Invalid message type	The ASA received a non-SSH message, or an unsupported or unwanted SSH message.	Check whether the peer is an SSH client. If it is a client supporting SSHv1, and this message persists, from the ASA serial console enter the <b>debug ssh</b> command and capture the debugging messages. Then contact the Cisco TAC.
Out of memory	This message appears when the ASA cannot allocate memory for use by the SSH server, probably when the ASA is busy with high traffic.	Restart the SSH session later.
Rejected by server	User authentication failed.	Ask the user to verify username and password.
Reset by client	An SSH client sent the SSH_MSG_DISCONNECT message to the ASA.	None required.
status code: <b>hex (hex)</b>	Users closed the SSH client window (running on Windows) instead of entering <b>quit</b> or <b>exit</b> at the SSH console.	None required. Encourage users to exit the client gracefully instead of just exiting.
Terminated by operator	The SSH session was terminated by entering the <b>ssh disconnect</b> command at the ASA console.	None required.
Time-out activated	The SSH session timed out because the duration specified by the <b>ssh timeout</b> command was exceeded.	Restart the SSH connection. You can use the <b>ssh timeout</b> command to increase the default value of 5 minutes up to 60 minutes if required.

**Recommended Action** None required.

## 315012

**Error Message** %ASA-3-315012: Weak SSH type (alg) provided from client IP\_address on interface Int. Connection failed. Not FIPS 140-2 compliant.

**Explanation** As part of the FIPS 140-2 certification, when FIPS is enabled, SSH connections can only be brought up using aes128-cbc or aes256-cbc as the cipher and SHA1 as the MAC. This syslog is generated when an unacceptable cipher or MAC is used. This syslog will not be seen if FIPS mode is disabled.

- *type* —cipher or MAC
- *alg* —The name of the unacceptable cipher or MAC
- *IP\_address* —The IP address of the client
- *int* —The interface that the client is attempting to connect to

**Recommended Action** Provide an acceptable cipher or MAC

## 315013

**Error Message** %ASA-6-315013: SSH session from <SSH client address> on interface <interface name> for user "<user name>" rekeyed successfully.

**Explanation** This syslog is needed to indicate that an SSH rekey has successfully completed. This is a Common Criteria certification requirement.

- *SSH\_client\_address* —The IP address of the client
- *interface\_name* —The interface that the client is attempting to connect to
- *user\_name*—The user name associated with the session

**Recommended Action** None

## 316001

**Error Message** %ASA-3-316001: Denied new tunnel to *IP\_address* . VPN peer limit (*platform\_vpn\_peer\_limit*) exceeded

**Explanation** If more VPN tunnels (ISAKMP/IPsec) are concurrently trying to be established than are supported by the platform VPN peer limit, then the excess tunnels are aborted.

**Recommended Action** None required.

## 316002

**Error Message** %ASA-3-316002: VPN Handle error: protocol=*protocol* , src *in\_if\_num* :*src\_addr* , dst *out\_if\_num* :*dst\_addr*

**Explanation** The Secure Firewall ASA cannot create a VPN handle, because the VPN handle already exists.

- *protocol* —The protocol of the VPN flow
- *in\_if\_num* —The ingress interface number of the VPN flow
- *src\_addr* —The source IP address of the VPN flow
- *out\_if\_num* —The egress interface number of the VPN flow
- *dst\_addr* —The destination IP address of the VPN flow

**Recommended Action** This message may occur during normal operation; however, if the message occurs repeatedly and a major malfunction of VPN-based applications occurs, a software defect may be the cause. Enter the following commands to collect more information and contact the Cisco TAC to investigate the issue further:

```
capture
  name
  type asp-drop vpn-handle-error
show asp table classify crypto detail
show asp table vpn-context
```

## 317001

**Error Message** %ASA-3-317001: No memory available for limit\_slow

**Explanation** The requested operation failed because of a low-memory condition.

**Recommended Action** Reduce other system activity to ease memory demands. If conditions warrant, upgrade to a larger memory configuration.

## 317002

**Error Message** %ASA-3-317002: Bad path index of *number* for *IP\_address* , *number* max

**Explanation** A software error occurred.

**Recommended Action** If the problem persists, contact the Cisco TAC.

## 317003

**Error Message** %ASA-3-317003: IP routing table creation failure - *reason*

**Explanation** An internal software error occurred, which prevented the creation of a new IP routing table.

**Recommended Action** Copy the message exactly as it appears, and report it to Cisco TAC.

## 317004

**Error Message** %ASA-3-317004: IP routing table limit warning

**Explanation** The number of routes in the named IP routing table has reached the configured warning limit.

**Recommended Action** Reduce the number of routes in the table, or reconfigure the limit.

## 317005

**Error Message** %ASA-3-317005: IP routing table limit exceeded - *reason* , *IP\_address* *netmask*

**Explanation** Additional routes will be added to the table.

**Recommended Action** Reduce the number of routes in the table, or reconfigure the limit.

## 317006

**Error Message** %ASA-3-317006: Pdb index error *pdb* , *pdb\_index* , *pdb\_type*

**Explanation** The index into the PDB is out of range.

- **pdb**—Protocol Descriptor Block, the descriptor of the PDB index error
- **pdb\_index**—The PDB index identifier
- **pdb\_type**—The type of the PDB index error

**Recommended Action** If the problem persists, copy the error message exactly as it appears on the console or in the system log, contact the Cisco TAC, and provide the representative with the collected information.

## 317007

**Error Message** %ASA-6-317007: Added *route\_type* route *dest\_address* *netmask* via *gateway\_address* [*distance* /*metric* ] on *interface\_name* *route\_type*

**Explanation** A new route has been added to the routing table.

Routing protocol type:

C – connected, S – static, I – IGRP, R – RIP, M – mobile

B – BGP, D – EIGRP, EX - EIGRP external, O - OSPF

IA - OSPF inter area, N1 - OSPF NSSA external type 1

N2 - OSPF NSSA external type 2, E1 - OSPF external type 1

E2 - OSPF external type 2, E – EGP, i - IS-IS, L1 - IS-IS level-1

L2 - IS-IS level-2, ia - IS-IS inter area

- *dest\_address* —The destination network for this route
- *netmask* —The netmask for the destination network
- *gateway\_address* —The address of the gateway by which the destination network is reached
- *distance* —Administrative distance for this route
- *metric* —Metric for this route
- *interface\_name* —Network interface name through which the traffic is routed

**Recommended Action** None required.

## 317008

**Error Message** %ASA-6-317008: Community list check with bad list *list\_number*

**Explanation** When an out of range community list is identified, this message is generated along with the list number.

**Recommended Action** None required.

## 317012

**Error Message** %ASA-3-317012: Interface IP route counter negative - nameif-string-value

**Explanation** Indicates that the interface route count is negative.

- nameif-string-value—The interface name as specified by the nameif command

**Recommended Action** None required.

## 317077

**Error Message** %ASA-6-317077: Added <protocol\_name> route <destination\_address/subnet-mask> via <gateway-address> on <inf\_name>

**Explanation** This message is generated when a route is added successfully on the Secure Firewall Threat Defense device.

**Recommended Action** None required.

## 317078

**Error Message** %ASA-6-317078: Deleted <protocol\_name> route <destination\_address/subnet-mask> via <gateway-address> on <inf\_name>

**Explanation** This message is generated when a route is deleted from the Secure Firewall Threat Defense device.

**Recommended Action** None required.

## 317012

**Error Message** %ASA-3-317012: Interface IP route counter negative - nameif-string-value

**Explanation** Indicates that the interface route count is negative.

- nameif-string-value—The interface name as specified by the nameif command

**Recommended Action** None required.

## 318001

**Error Message** %ASA-3-318001: Internal error: reason

**Explanation** An internal software error occurred. This message occurs at five-second intervals.

**Recommended Action** Copy the message exactly as it appears, and report it to the Cisco TAC.

## 318002

**Error Message** %ASA-3-318002: Flagged as being an ABR without a backbone area

**Explanation** The router was flagged as an area border router without a backbone area configured in the router. This message occurs at five-second intervals.

**Recommended Action** Restart the OSPF process.

## 318003

**Error Message** %ASA-3-318003: Reached unknown state in neighbor state machine

**Explanation** An internal software error occurred. This message occurs at five-second intervals.

**Recommended Action** Copy the message exactly as it appears, and report it to the Cisco TAC.

## 318004

**Error Message** %ASA-3-318004: area string lsid IP\_address mask netmask adv IP\_address type number

**Explanation** The OSPF process had a problem locating the link state advertisement, which might lead to a memory leak.

**Recommended Action** If the problem persists, contact the Cisco TAC.

## 318005

**Error Message** %ASA-3-318005: lsid *ip\_address* adv *IP\_address* type *number* gateway *gateway\_address* metric *number* network *IP\_address* mask *netmask* protocol *hex* attr *hex* net-metric *number*

**Explanation** OSPF found an inconsistency between its database and the IP routing table.

**Recommended Action** If the problem persists, contact the Cisco TAC.

## 318006

**Error Message** %ASA-3-318006: if *interface\_name* if\_state *number*

**Explanation** An internal error occurred.

**Recommended Action** Copy the message exactly as it appears, and report it to the Cisco TAC.

## 318007

**Error Message** %ASA-3-318007: OSPF is enabled on *interface\_name* during idb initialization

**Explanation** An internal error occurred.

**Recommended Action** Copy the message exactly as it appears, and report it to the Cisco TAC.

## 318008

**Error Message** %ASA-3-318008: OSPF process *number* is changing router-id. Reconfigure virtual link neighbors with our new router-id

**Explanation** The OSPF process is being reset, and it is going to select a new router ID. This action will bring down all virtual links.

**Recommended Action** Change the virtual link configuration on all of the virtual link neighbors to reflect the new router ID.

## 318009

**Error Message** %ASA-3-318009: OSPF: Attempted reference of stale data encountered in *function*, line: *line\_num*

**Explanation** OSPF is running and has tried to reference some related data structures that have been removed elsewhere. Clearing interface and router configurations may resolve the problem. However, if this message appears, some sequence of steps caused premature deletion of data structures and this needs to be investigated.

- *function* —The function that received the unexpected event
- *line\_num* —Line number in the code

**Recommended Action** If the problem persists, contact the Cisco TAC.

## 318101

**Error Message** %ASA-3-318101: Internal error: *REASON*

**Explanation** An internal software error has occurred.

- *REASON* —The detailed cause of the event

**Recommended Action** None required.

## 318102

**Error Message** %ASA-3-318102: Flagged as being an ABR without a backbone area

**Explanation** The router was flagged as an Area Border Router (ABR) without a backbone area in the router.

**Recommended Action** Restart the OSPF process.

## 318103

**Error Message** %ASA-3-318103: Reached unknown state in neighbor state machine

**Explanation** An internal software error has occurred.

**Recommended Action** None required.

## 318104

**Error Message** %ASA-3-318104: DB already exist: area *AREA\_ID\_STR* lsid *i* adv *i* type 0x *x*

**Explanation** OSPF has a problem locating the LSA, which could lead to a memory leak.

- *AREA\_ID\_STR* —A string representing the area
- *i* —An integer value
- *x* —A hexadecimal representation of an integer value

**Recommended Action** None required.

## 318105

**Error Message** %ASA-3-318105: lsid *i* adv *i* type 0x *x* gateway *i* metric *d* network *i* mask *i* protocol #*x* attr #*x* net-metric *d*

**Explanation** OSPF found an inconsistency between its database and the IP routing table.

- *i* —An integer value
- *x* —A hexadecimal representation of an integer value
- *d* —A number

**Recommended Action** None required.

## 318106

**Error Message** %ASA-3-318106: if *IF\_NAME* if\_state *d*

**Explanation** An internal error has occurred.

- *IF\_NAME*— The name of the affected interface
- *d*—A number

**Recommended Action** None required.

## 318107

**Error Message** %ASA-3-318107: OSPF is enabled on *IF\_NAME* during idb initialization

**Explanation** An internal error has occurred.

- *IF\_NAME*— The name of the affected interface

**Recommended Action** None required.

## 318108

**Error Message** %ASA-3-318108: OSPF process *d* is changing router-id. Reconfigure virtual link neighbors with our new router-id

**Explanation** The OSPF process is being reset, and it is going to select a new router ID, which brings down all virtual links. To make them work again, you need to change the virtual link configuration on all virtual link neighbors.

- *d*—A number representing the process ID

**Recommended Action** Change the virtual link configuration on all the virtual link neighbors to include the new router ID.

## 318109

**Error Message** %ASA-3-318109: OSPFv3 has received an unexpected message: 0x / 0x

**Explanation** OSPFv3 has received an unexpected interprocess message.

- *x*—A hexadecimal representation of an integer value

**Recommended Action** None required.

## 318110

**Error Message** %ASA-3-318110: Invalid encrypted key *s* .

**Explanation** The specified encrypted key is not valid.

- *s*—A string representing the encrypted key

**Recommended Action** Either specify a clear text key and enter the **service password-encryption** command for encryption, or ensure that the specified encrypted key is valid. If the specified encrypted key is not valid, an error message appears during system configuration.



## 318111

**Error Message** %ASA-3-318111: SPI *u* is already in use with ospf process *d*

**Explanation** An attempt was made to use a SPI that has already been used.

- *u*—A number representing the SPI
- *d*—A number representing the process ID

**Recommended Action** Choose a different SPI.

## 318112

**Error Message** %ASA-3-318112: SPI *u* is already in use by a process other than ospf process *d* .

**Explanation** An attempt was made to use a SPI that has already been used.

- *u*—A number representing the SPI
- *d*—A number representing the process ID

**Recommended Action** Choose a different SPI. Enter the **show crypto ipv6 ipsec sa** command to view a list of SPIs that are already being used.

## 318113

**Error Message** %ASA-3-318113: *s s* is already configured with SPI *u* .

**Explanation** An attempt was made to use a SPI that has already been used.

- *s*— A string representing an interface
- *u*—A number representing the SPI

**Recommended Action** Unconfigure the SPI first, or choose a different one.

## 318114

**Error Message** %ASA-3-318114: The key length used with SPI *u* is not valid

**Explanation** The key length was incorrect.

- *u*—A number representing the SPI

**Recommended Action** Choose a valid IPsec key. An IPsec authentication key must be 32 (MD5) or 40 (SHA-1) hexadecimal digits long.

## 318115

**Error Message** %ASA-3-318115: *s* error occurred when attempting to create an IPsec policy for SPI *u*

**Explanation** An IPsec API (internal) error has occurred.

- *s*— A string representing the error
- *u*—A number representing the SPI

**Recommended Action** None required.

## 318116

**Error Message** %ASA-3-318116: SPI *u* is not being used by ospf process *d* .

**Explanation** An attempt was made to unconfigure a SPI that is not being used with OSPFv3.

- *u* —A number representing the SPI
- *d* —A number representing the process ID

**Recommended Action** Enter a **show** command to see which SPIs are used by OSPFv3.

## 318117

**Error Message** %ASA-3-318117: The policy for SPI *u* could not be removed because it is in use.

**Explanation** An attempt was made to remove the policy for the indicated SPI, but the policy was still being used by a secure socket.

- *u* —A number representing the SPI

**Recommended Action** None required.

## 318118

**Error Message** %ASA-3-318118: *s* error occurred when attempting to remove the IPsec policy with SPI *u*

**Explanation** An IPsec API (internal) error has occurred.

- *s* —A string representing the specified error
- *u* —A number representing the SPI

**Recommended Action** None required.

## 318119

**Error Message** %ASA-3-318119: Unable to close secure socket with SPI *u* on interface *s*

**Explanation** An IPsec API (internal) error has occurred.

- *u* —A number representing the SPI
- *s* —A string representing the specified interface

**Recommended Action** None required.

## 318120

**Error Message** %ASA-3-318120: OSPFv3 was unable to register with IPsec

**Explanation** An internal error has occurred.

**Recommended Action** None required.

## 318121

**Error Message** %ASA-3-318121: IPsec reported a GENERAL ERROR: message *s* , count *d*

**Explanation** An internal error has occurred.

- *s* —A string representing the specified message
- *d* —A number representing the total number of generated messages

**Recommended Action** None required.

## 318122

**Error Message** %ASA-3-318122: IPsec sent a *s* message *s* to OSPFv3 for interface *s* . Recovery attempt *d*

**Explanation** An internal error has occurred. The system is trying to reopen the secure socket and to recover.

- *s* —A string representing the specified message and specified interface
- *d* —A number representing the total number of recovery attempts

**Recommended Action** None required.

## 318123

**Error Message** %ASA-3-318123: IPsec sent a *s* message *s* to OSPFv3 for interface *IF\_NAME* . Recovery aborted

**Explanation** An internal error has occurred. The maximum number of recovery attempts has been exceeded.

- *s* —A string representing the specified message
- *IF\_NAME* —The specified interface

**Recommended Action** None required.

## 318125

**Error Message** %ASA-3-318125: Init failed for interface *IF\_NAME*

**Explanation** The interface initialization failed. Possible reasons include the following:

- The area to which the interface is being attached is being deleted.
- It was not possible to create the link scope database.
- It was not possible to create a neighbor datablock for the local router.

**Recommended Action** Remove the configuration command that initializes the interface and then try it again.

## 318126

**Error Message** %ASA-3-318126: Interface *IF\_NAME* is attached to more than one area

**Explanation** The interface is on the interface list for an area other than the one to which the interface links.

- *IF\_NAME* —The specified interface

**Recommended Action** None required.

## 318127

**Error Message** %ASA-3-318127: Could not allocate or find the neighbor

**Explanation** An internal error has occurred.

**Recommended Action** None required.

## 319001

**Error Message** %ASA-3-319001: Acknowledge for arp update for IP address *dest\_address* not received (*number*).

**Explanation** The ARP process in the ASA lost internal synchronization because the ASA was overloaded.

**Recommended Action** None required. The failure is only temporary. Check the average load of the ASA and make sure that it is not used beyond its capabilities.

## 319002

**Error Message** %ASA-3-319002: Acknowledge for route update for IP address *dest\_address* not received (*number*).

**Explanation** The routing module in the ASA lost internal synchronization because the ASA was overloaded.

**Recommended Action** None required. The failure is only temporary. Check the average load of the ASA and make sure that it is not used beyond its capabilities.

## 319003

**Error Message** %ASA-3-319003: Arp update for IP address *address* to NPn failed.

**Explanation** When an ARP entry has to be updated, a message is sent to the network processor (NP) in order to update the internal ARP table. If the module is experiencing high utilization of memory or if the internal table is full, the message to the NP may be rejected and this message generated.

**Recommended Action** Verify if the ARP table is full. If it is not full, check the load of the module by reviewing the CPU utilization and connections per second. If CPU utilization is high and/or there is a large number of connections per second, normal operations will resume when the load returns to normal.

## 319004

**Error Message** %ASA-3-319004: Route update for IP address *dest\_address* failed (*number*).

**Explanation** The routing module in the ASA lost internal synchronization because the system was overloaded.

**Recommended Action** None required. The failure is only temporary. Check the average load of the system and make sure that it is not used beyond its capabilities.

## Messages 320001 to 342008

This chapter includes messages from 320001 to 342008.

### 320001

**Error Message** %ASA-3-320001: The subject name of the peer cert is not allowed for connection

**Explanation** When the Secure Firewall ASA is an easy VPN remote device or server, the peer certificate includes a subject name that does not match the output of the **ca verifycertdn** command. A man-in-the-middle attack might be occurring, where a device spoofs the peer IP address and tries to intercept a VPN connection from the Secure Firewall ASA.

**Recommended Action** None required.

### 321001

**Error Message** %ASA-5-321001: Resource var1 limit of var2 reached.

**Explanation** A configured resource usage or rate limit for the indicated resource was reached.

**Recommended Action** If the platform maximum connections were reached, it takes some time to reallocate memory to free system memory, resulting in traffic failure. After memory space is released, you must reload the device. For further assistance, contact TAC team.

### 321002

**Error Message** %ASA-5-321002: Resource var1 rate limit of var2 reached.

**Explanation** A configured resource usage or rate limit for the indicated resource was reached.

**Recommended Action** If the platform maximum connections were reached, it takes some time to reallocate memory to free system memory, resulting in traffic failure. After memory space is released, you must reload the device. For further assistance, contact TAC team.

### 321003

**Error Message** %ASA-6-321003: Resource var1 log level of var2 reached.

**Explanation** A configured resource usage or rate logging level for the indicated resource was reached.

**Recommended Action** None required.

### 321004

**Error Message** %ASA-6-321004: Resource var1 rate log level of var2 reached

**Explanation** A configured resource usage or rate logging level for the indicated resource was reached.

**Recommended Action** None required.

## 321005

**Error Message** %ASA-2-321005: System CPU utilization reached *utilization* %

**Explanation** The system CPU utilization has reached 95 percent or more and remains at this level for five minutes.

- *utilization %* —The percentage of CPU being used

**Recommended Action** If this message occurs periodically, you can ignore it. If it repeats frequently, check the output of the **show cpu** command and verify the CPU usage. If it is high, contact the Cisco TAC.

## 321006

**Error Message** %ASA-2-321006: System memory usage reached *utilization* %

**Explanation** The system memory usage has reached 80 percent or more and remains at this level for five minutes.

- *utilization %* —The percentage of memory being used

**Recommended Action** If this message occurs periodically, you can ignore it. If it repeats frequently, check the output of the **show memory** command and verify the memory usage. If it is high, contact the Cisco TAC.

## 321007

**Error Message** %ASA-3-321007: System is low on free memory blocks of size *block\_size* (*free\_blocks* CNT out of *max\_blocks* MAX)

**Explanation** The system is low on free blocks of memory. Running out of blocks may result in traffic disruption.

- *block\_size* —The block size of memory (for example, 4, 1550, 8192)
- *free\_blocks* —The number of free blocks, as shown in the CNT column after using the **show blocks** command
- *max\_blocks* —The maximum number of blocks that the system can allocate, as shown in the MAX column after using the **show blocks** command

**Recommended Action** Use the **show blocks** command to monitor the amount of free blocks in the CNT column of the output for the indicated block size. If the CNT column remains zero, or very close to it for an extended period of time, then the Secure Firewall ASA may be overloaded or running into another issue that needs additional investigation.

## 322001

**Error Message** %ASA-3-322001: Deny MAC address *MAC\_address*, possible spoof attempt on interface *interface*

**Explanation** The Secure Firewall ASA received a packet from the offending MAC address on the specified interface, but the source MAC address in the packet is statically bound to another interface in the configuration. Either a MAC-spoofing attack or a misconfiguration may be the cause.

**Recommended Action** Check the configuration and take appropriate action by either finding the offending host or correcting the configuration.

## 322002

**Error Message** %ASA-3-322002: ARP inspection check failed for arp {request|response} received from host *MAC\_address* on interface *interface* . This host is advertising MAC Address *MAC\_address\_1* for IP Address *IP\_address* , which is {statically|dynamically} bound to MAC Address *MAC\_address\_2* .

**Explanation** If the ARP inspection module is enabled, it checks whether a new ARP entry advertised in the packet conforms to the statically configured or dynamically learned IP-MAC address binding before forwarding ARP packets across the Secure Firewall ASA. If this check fails, the ARP inspection module drops the ARP packet and generates this message. This situation may be caused by either ARP spoofing attacks in the network or an invalid configuration (IP-MAC binding).

**Recommended Action** If the cause is an attack, you can deny the host using the ACLs. If the cause is an invalid configuration, correct the binding.

## 322003

**Error Message** %ASA-3-322003:ARP inspection check failed for arp {request|response} received from host *MAC\_address* on interface *interface* . This host is advertising MAC Address *MAC\_address\_1* for IP Address *IP\_address* , which is not bound to any MAC Address.

**Explanation** If the ARP inspection module is enabled, it checks whether a new ARP entry advertised in the packet conforms to the statically configured IP-MAC address binding before forwarding ARP packets across the Secure Firewall ASA. If this check fails, the ARP inspection module drops the ARP packet and generates this message. This situation may be caused by either ARP spoofing attacks in the network or an invalid configuration (IP-MAC binding).

**Recommended Action** If the cause is an attack, you can deny the host using the ACLs. If the cause is an invalid configuration, correct the binding.

## 322004

**Error Message** %ASA-6-322004: No management IP address configured for transparent firewall. Dropping protocol *protocol* packet from *interface\_in* :*source\_address* /*source\_port* to *interface\_out* :*dest\_address* /*dest\_port*

**Explanation** The Secure Firewall ASA dropped a packet because no management IP address was configured in the transparent mode.

- **protocol**—Protocol string or value
- **interface\_in**—Input interface name
- **source\_address**—Source IP address of the packet
- **source\_port**—Source port of the packet
- **interface\_out**—Output interface name
- **dest\_address**—Destination IP address of the packet
- **dest\_port**—Destination port of the packet

**Recommended Action** Configure the device with the management IP address and mask values.

## 323001

**Error Message** %ASA-3-323001: Module *module\_id* experienced a control channel communications failure.

%ASA-3-323001: Module in slot *slot\_num* experienced a control channel communications failure.

**Explanation** The Secure Firewall ASA is unable to communicate via control channel with the module installed (in the specified slot).

- **module\_id**—For a software services module, specifies the services module name.
- **slot\_num**—For a hardware services module, specifies the slot in which the failure occurred. Slot 0 indicates the system main board, and slot 1 indicates the module installed in the expansion slot.

**Recommended Action** If the problem persists, contact the Cisco TAC.

## 323002

**Error Message** %ASA-3-323002: Module *module\_id* is not able to shut down, shut down request not answered.

%ASA-3-323002: Module in slot *slot\_num* is not able to shut down, shut down request not answered.

**Explanation** The module installed did not respond to a shutdown request.

- **module\_id**—For a software services module, specifies the service module name.
- **slot\_num**—For a hardware services module, specifies the slot in which the failure occurred. Slot 0 indicates the system main board, and slot 1 indicates the module installed in the expansion slot.

**Recommended Action** If the problem persists, contact the Cisco TAC.

## 323003

**Error Message** %ASA-3-323003: Module *module\_id* is not able to reload, reload request not answered.

%ASA-3-323003: Module in slot *slotnum* is not able to reload, reload request not answered.

**Explanation** The module installed did not respond to a reload request.

- **module\_id**—For a software services module, specifies the service module name.
- **slot\_num**—For a hardware services module, specifies the slot in which the failure occurred. Slot 0 indicates the system main board, and slot 1 indicates the module installed in the expansion slot.

**Recommended Action** If the problem persists, contact the Cisco TAC.

## 323004

**Error Message** %ASA-3-323004: Module *string one* failed to write software *newver* (currently *ver*), *reason*. Hw-module reset is required before further use.

**Explanation** The module failed to accept a software version, and will be transitioned to an UNRESPONSIVE state. The module is not usable until the software is updated.



- **string one**—The text string that specifies the module
- *>newver* —The new version number of software that was not successfully written to the module (for example, 1.0(1)0)
- *>ver* —The current version number of the software on the module (for example, 1.0(1)0)
- *>reason* —The reason the new version cannot be written to the module. The possible values for *>reason* include the following:

- write failure

- failed to create a thread to write the image

**Recommended Action** If the module software cannot be updated, it will not be usable. If the problem persists, contact the Cisco TAC.

## 323005

**Error Message** %ASA-3-323005: Module *module\_id* can not be started completely

%ASA-3-323005: Module in slot *slot\_num* cannot be started completely

**Explanation** This message indicates that the module cannot be started completely. The module will remain in the UNRESPONSIVE state until this condition is corrected. A module that is not fully seated in the slot is the most likely cause.

- **module\_id**—For a software services module, specifies the service module name.
- **slot\_num**—For a hardware services module, specifies the slot number that contains the module.

**Recommended Action** Verify that the module is fully seated and check to see if any status LEDs on the module are on. It may take a minute after fully reseating the module for the Secure Firewall ASA to recognize that it is powered up. If this message appears after verifying that the module is seated and after resetting the module using either the **sw-module module service-module-name reset** command or the **hw-module module slotnum reset** command, contact the Cisco TAC.

## 323006

**Error Message** %ASA-1-323006: Module *ips* experienced a data channel communication failure, data channel is DOWN.

**Explanation** A data channel communication failure occurred and the Secure Firewall ASA was unable to forward traffic to the services module. This failure triggers a failover when the failure occurs on the active Secure Firewall ASA in an HA configuration. The failure also results in the configured fail open or fail closed policy being enforced on traffic that would normally be sent to the services module. This message is generated whenever a communication problem over the Secure Firewall ASA dataplane occurs between the system module and the services module, which can be caused when the services module stops, resets, is removed or disabled.

**Recommended Action** For software services modules such as IPS, recover the module using the **sw-module module ips recover** command. For hardware services modules, if this message is not the result of the SSM reloading or resetting and the corresponding syslog message 505010 is not seen after the SSM returns to an UP state, reset the module using the **hw-module module 1 reset** command.

## 323007

**Error Message** %ASA-3-323007: Module in slot *slot* experienced a firware failure and the recovery is in progress.

**Explanation** An Secure Firewall ASA with a 4GE-SSM installed experienced a short power surge, then rebooted. As a result, the 4GE-SSM may come online in an unresponsive state. The Secure Firewall ASA has detected that the 4GE-SSM is unresponsive, and automatically restarts the 4GE-SSM.

**Recommended Action** None required.

## 324000

**Error Message** %ASA-3-324000: Drop GTPv *version* message *msg\_type* from *source\_interface* :*source\_address* /*source\_port* to *dest\_interface*:*dest\_address*/*dest\_port* Reason: *reason*

**Explanation** The packet being processed did not meet the filtering requirements as described in the **reason** variable and is being dropped.

**Recommended Action** None required.

## 324001

**Error Message** %ASA-3-324001: GTPv0 packet parsing error from *source\_interface* :*source\_address* /*source\_port* to *dest\_interface* :*dest\_address* /*dest\_port* , TID: *tid\_value* , Reason: *reason*

**Explanation** There was an error processing the packet. The following are possible reasons:

- Mandatory IE is missing
- Mandatory IE incorrect
- IE out of sequence
- Invalid message format.
- Optional IE incorrect
- Invalid TEID
- Unknown IE
- Bad length field
- Unknown GTP message.
- Message too short
- Unexpected message seen
- Null TID
- Version not supported

**Recommended Action** If this message is seen periodically, it can be ignored. If it is seen frequently, then the endpoint may be sending out bad packets as part of an attack.

## 324002

**Error Message** %ASA-3-324002: No PDP[MCB] exists to process GTPv0 *msg\_type* from *source\_interface* :*source\_address* /*source\_port* to *dest\_interface* :*dest\_address* /*dest\_port* , TID: *tid\_value*

**Explanation** If this message was preceded by message 321100, memory allocation error, the message indicates that there were not enough resources to create the PDP context. If not, it was not preceded by message 321100. For version 0, it indicates that the corresponding PDP context cannot be found. For version 1, if this message was preceded by message 324001, then a packet processing error occurred, and the operation stopped.

**Recommended Action** If the problem persists, determine why the source is sending packets without a valid PDP context.

## 324003

**Error Message** %ASA-3-324003: No matching request to process GTPv *version msg\_type* from *source\_interface:source\_address/source\_port* to *source\_interface:dest\_address/dest\_port*

**Explanation** The response received does not have a matching request in the request queue and should not be processed further.

**Recommended Action** If this message is seen periodically, it can be ignored. But if it is seen frequently, then the endpoint may be sending out bad packets as part of an attack.

## 324004

**Error Message** %ASA-3-324004: GTP packet with version%d from *source\_interface :source\_address /source\_port* to *dest\_interface :dest\_address /dest\_port* is not supported

**Explanation** The packet being processed has a version other than the currently supported version, which is 0 or 1. If the version number printed out is an incorrect number and is seen frequently, then the endpoint may be sending out bad packets as part of an attack.

**Recommended Action** None required.

## 324005

**Error Message** %ASA-3-324005: Unable to create tunnel from *source\_interface :source\_address /source\_port* to *dest\_interface :dest\_address /dest\_port*

**Explanation** An error occurred while trying to create the tunnel for the transport protocol data units.

**Recommended Action** If this message occurs periodically, it can be ignored. If it repeats frequently, contact the Cisco TAC.

## 324006

**Error Message** %ASA-3-324006:GSN *IP\_address* tunnel limit *tunnel\_limit* exceeded, PDP Context TID *tid* failed

**Explanation** The GPRS support node sending the request has exceeded the maximum allowed tunnels created, so no tunnel will be created.

**Recommended Action** Check to see whether the tunnel limit should be increased or if there is a possible attack on the network.

## 324007

**Error Message** %ASA-3-324007: Unable to create GTP connection for response from *source\_address* /0 to *dest\_address* /*dest\_port*

**Explanation** An error occurred while trying to create the tunnel for the transport protocol data units for a different servicing GPRS support node or gateway GPRS support node.

**Recommended Action** Check debugging messages to see why the connection was not created correctly. If the problem persists, contact the Cisco TAC.

## 324008

**Error Message** %ASA-3-324008: No PDP exists to update the data sgsn [ggsn] PDP MCB Info REID: *teid\_value* , Request TEID; *teid\_value* , Local GSN: IPaddress (*VPIfNum* ), Remove GSN: IPaddress (*VPIfNum* )

**Explanation** When a GTP HA message is received on the standby unit to update the PDP with data sgsn/ggsn PDP MCB information, the PDP is not found because of a previous PDP update message that was not successfully delivered or successfully processed on the standby unit.

**Recommended Action** If this message occurs periodically, you can ignore it. If it occurs frequently, contact the Cisco TAC.

## 324010

**Error Message** %ASA-5-324010: Subscriber *IMSI* PDP Context activated on network MCC/MNC *mccmnc* (*IE type*[/*IE type*]) [*CellID cellID*]

### Explanation

This message appears when the PDP Context is activated. MCC is always 3 digits and MNC is 2 or 3 digits.




---

**Note** The MCC, MNC, IE type, or Cell ID could be "Unknown" if the packet does not contain the location information IEs.

---

### Example:

```
%ASA-5-324010: Subscriber ID PDP Context activated on network MCC/MNC 11122 (v1 RAI/v1 ULI)
CellID 1
```

```
%ASA-5-324010: Subscriber ID PDP Context activated on network Unknown
```

**Recommended Action** None

## 324011

**Error Message** %ASA-5-324011: Subscriber *IMSI* location changed during handoff from MCC/MNC *mccmnc* (*IE type*[/*IE type*]) [*CellID cellID*] to MCC/MNC *mccmnc* (*IE type*[/*IE type*]) [*CellID cellID*]

### Explanation

A message appears when the location has changed. MCC is always 3 digits and MNC is 2 or 3 digits. This change could be triggered by handoff or a subsequent create request after the PDP is created and that the previous create request on ASA expired.



**Note** The MCC, MNC, IE type, or Cell ID could be "Unknown" if the packet does not contain the location information IEs.

Example:

```
%ASA-5-324011: Subscriber ID location changed during v1 handoff from MCC/MNC 11122 (v1 RAI/v1 ULI-CGI) CellID 1 to MCC/MNC 111222 (v1 RAI/v1 ULI-CGI) CellID 2
```

```
%ASA-5-324011: Subscriber ID location changed during v1 handoff from MCC/MNC 11122 (v2 ULI) CellID 1 to Unknown
```

```
%ASA-5-324011: Subscriber ID location changed during v1 handoff from Unknown to MCC/MNC 11122 (v1 RAI) CellID 1
```

**Recommended Action** None

## 324012

**Error Message** %ASA-5-324012: GTP\_PARSE: GTP IE TYPE:GTP IE TYPE NUMBER: Invalid Length Received Length: *Length Received*, Minimum Expected Length: *Expected Length*

### Explanation

When GTP IE length received is less than the minimum length, an error message appears with the following data:

- *GTP IE TYPE*: Name Of GTP IE.
- *GTP IE TYPE NUMBER*: Number Defined for GTP IE Type
- *Invalid Length Received*: Invalid Length Received in the Packet.
- *Minimum Expected Length*: Minimum Expected length for IE.

Example:

```
%ASA-5-324012: GTP_PARSE: GTPV2_PARSE: Presence Reporting Area Action[177]: Invalid Length Received Length: 4, Minimum Expected Length: 11
```

**Recommended Action** None

## 324300

**Error Message** %ASA-3-324300: Radius Accounting Request from *from\_addr* has an incorrect request authenticator

**Explanation** When a shared secret is configured for a host, the request authenticator is verified with that secret. If it fails, it is logged and packet processing stops.

- *from\_addr* —The IP address of the host sending the RADIUS accounting request

**Recommended Action** Check to see that the correct shared secret was configured. If it is, double-check the source of the packet to make sure that it was not spoofed.

## 324301

**Error Message** %ASA-3-324301: Radius Accounting Request has a bad header length *hdr\_len* , packet length *pkt\_len*

**Explanation** The accounting request message has a header length that is not the same as the actual packet length, so packet processing stops.

- *hdr\_len* —The length indicated in the request header
- *pkt\_len* —The actual packet length

**Recommended Action** Make sure the packet was not spoofed. If the packet is legitimate, then capture the packet and make sure the header length is incorrect, as indicated by the message. If the header length is correct, and if the problem persists, contact the Cisco TAC.

## 324302

**Error Message** %ASA-4-324302: Server=*IPaddr:port* ID=*id*: Rejecting the RADIUS response: *Reason*

**Explanation** This message is generated when RADIUS response is rejected either because the required message-authenticator payload is missing in the response or if the Message-Authenticator payload failed validation check.

- **IPaddr:port**—RADIUS server IP address and port
- **id**—RADIUS request ID
- **Reason**—Reason why the RADIUS response is rejected:
  - Required Message-Authenticator Payload Missing
  - Message-Authenticator payload failed validation check

**Recommended Action** None.

## 324303

**Error Message** %ASA-6-324303: Server=*IPaddr:port* ID=*id* The RADIUS server supports and included the Message-Authenticator payload in its response. To prevent Man-In-The-Middle attacks, consider enabling 'message-authenticator' on the aaa-server-group configuration for this server as a security best practice.

**Explanation** This message is generated to convey that the RADIUS server supports and included Message-authenticator payload in the RADIUS response. Also, provides best security practices that is configurable and could disable this syslog.

- **IPaddr:port**—RADIUS server IP address and port
- **id**—RADIUS request ID

In addition, this syslog is rate-limited to report not more than 10 syslog messages in a 5-minute interval window by default. You can configure custom rate-limit interval and count through CLI.

To view the existing rate limits, use:

```
show running-configuration all logging | grep 324303
```

To configure a custom value, use:

```
logging rate-limit 10 300 message 324303
```

**Recommended Action** Configure message-authenticator-required CLI under AAA server configuration.

## 325001

**Error Message** %ASA-3-325001: Router *ipv6\_address* on *interface* has conflicting ND (Neighbor Discovery) settings

**Explanation** Another router on the link sent router advertisements with conflicting parameters.

- **ipv6\_address**—IPv6 address of the other router
- **interface**—Interface name of the link with the other router

**Recommended Action** Verify that all IPv6 routers on the link have the same parameters in the router advertisement for **hop\_limit**, **managed\_config\_flag**, **other\_config\_flag**, **reachable\_time** and **ns\_interval**, and that preferred and valid lifetimes for the same prefix, advertised by several routers, are the same. To list the parameters per interface, enter the **show ipv6 interface** command.

## 325002

**Error Message** %ASA-4-325002: Duplicate address *ipv6\_address/MAC\_address* on *interface*

**Explanation** Another system is using your IPv6 address.

- **ipv6\_address**—The IPv6 address of the other router
- **MAC\_address**—The MAC address of the other system, if known; otherwise, it is considered unknown.
- **interface**—The interface name of the link with the other system

**Recommended Action** Change the IPv6 address of one of the two systems.

## 325004

**Error Message** %ASA-4-325004: IPv6 Extension Header *hdr\_type* action configuration. *protocol* from *src\_int* :*src\_ipv6\_addr* /*src\_port* to *dst\_interface* : *dst\_ipv6\_addr* /*dst\_port* .

**Explanation** A user has configured one or multiple actions over the specified IPv6 header extension.

- **hdr\_type** —Can be one of the following values:

ah—Configured action over the AH extension header

count—Configured action over the number of extension headers

destination-option—Configured action over the destination option extension header

esp—Configured action over the ESP extension header

fragment—Configured action over the fragment extension header

hop-by-hop—Configured action over the hop-by-hop extension header

routing-address count—Configured action over the number of addresses in the routing extension header

routing-type—Configured action over the routing type extension header

- *action*—Can be one of the following values:

denied—The packet is denied.

denied/logged—The packet is denied and logged.

logged—The packet is logged.

**Recommended Action** If the configured action is not expected, under the **policy-map** command, check the action in the **match header extension\_header\_type** command and the **parameters** command, and make the correct changes. For example:

```
ciscoasa (config)# policy-map type inspect ipv6 pname
ciscoasa (config-pmap)# parameters
ciscoasa (config-pmap-p)# no match header extension_header_type
! to remove the configuration
ciscoasa (config-pmap-p)# no drop ! so packets with the specified extension_header_type
are not dropped
ciscoasa (config-pmap-p)# no log ! so packets with the specified extension_header_type
are not logged
ciscoasa (config-pmap-p)# no drop log ! so packets with the specified extension_header_type
are not dropped or logged
```

## 325005

**Error Message** %ASA-4-325005: Invalid IPv6 Extension Header Content: *string* . detail regarding protocol, ingress and egress interface

**Explanation** An IPv6 packet with a bad extension header has been detected.

- *string*—Can be one of the following values:

- wrong extension header order

- duplicate extension header

- routing extension header

**Recommended Action** Configure the **capture** command to record the dropped packet, then analyze the cause of the dropped packet. If the validity check of the IPv6 extension header can be ignored, disable the validity check in the IPv6 policy map by entering the following commands:

```
ciscoasa (config)# policy-map type inspect ipv6 policy_name
ciscoasa (config-pmap)# parameters
ciscoasa (config-pmap-p)# no verify-header type
```

## 325006

**Error Message** %ASA-4-325006: IPv6 Extension Header not in order: Type *hdr\_type* occurs after Type *hdr\_type* . TCP prot from inside *src\_int* : *src\_ipv6\_addr* /*src\_port* to *dst\_interface* :*dst\_ipv6\_addr* /*dst\_port*



**Explanation** An IPv6 packet with out-of-order extension headers has been detected.

**Recommended Action** Configure the **capture** command to record the dropped packet, then analyze the extension header order of the dropped packet. If out-of-order header extensions are allowed, disable the out-of-order check in the IPv6 type policy map by entering the following commands:

```
ciscoasa (config)# policy-map type inspect ipv6 policy_name
ciscoasa (config-pmap)# parameters
ciscoasa (config-pmap-p)# no verify-header order
```

## 326001

**Error Message** %ASA-3-326001: Unexpected error in the timer library: *error\_message*

**Explanation** A managed timer event was received without a context or a correct type, or no handler exists. Alternatively, if the number of events queued exceeds a system limit, an attempt to process them will occur at a later time.

**Recommended Action** If the problem persists, contact the Cisco TAC.

## 326002

**Error Message** %ASA-3-326002: Error in *error\_message* : *error\_message*

**Explanation** The IGMP process failed to shut down upon request. Events that are performed in preparation for this shutdown may be out-of-sync.

**Recommended Action** If the problem persists, contact the Cisco TAC.

## 326004

**Error Message** %ASA-3-326004: An internal error occurred while processing a packet queue

**Explanation** The IGMP packet queue received a signal without a packet.

**Recommended Action** If the problem persists, contact the Cisco TAC.

## 326005

**Error Message** %ASA-3-326005: Mrib notification failed for (*IP\_address*, *IP\_address* )

**Explanation** A packet triggering a data-driven event was received, and the attempt to notify the MRIB failed.

**Recommended Action** If the problem persists, contact the Cisco TAC.

## 326006

**Error Message** %ASA-3-326006: Entry-creation failed for (*IP\_address*, *IP\_address* )

**Explanation** The MFIB received an entry update from the MRIB, but failed to create the entry related to the addresses displayed. The probable cause is insufficient memory.

**Recommended Action** If the problem persists, contact the Cisco TAC.

## 326007

**Error Message** %ASA-3-326007: Entry-update failed for (IP\_address, IP\_address )

**Explanation** The MFIB received an interface update from the MRIB, but failed to create the interface related to the addresses displayed. The probable cause is insufficient memory.

**Recommended Action** If the problem persists, contact the Cisco TAC.

## 326008

**Error Message** %ASA-3-326008: MRIB registration failed

**Explanation** The MFIB failed to register with the MRIB.

**Recommended Action** If the problem persists, contact the Cisco TAC.

## 326009

**Error Message** %ASA-3-326009: MRIB connection-open failed

**Explanation** The MFIB failed to open a connection to the MRIB.

**Recommended Action** If the problem persists, contact the Cisco TAC.

## 326010

**Error Message** %ASA-3-326010: MRIB unbind failed

**Explanation** The MFIB failed to unbind from the MRIB.

**Recommended Action** If the problem persists, contact the Cisco TAC.

## 326011

**Error Message** %ASA-3-326011: MRIB table deletion failed

**Explanation** The MFIB failed to retrieve the table that was supposed to be deleted.

**Recommended Action** If the problem persists, contact the Cisco TAC.

## 326012

**Error Message** %ASA-3-326012: Initialization of string functionality failed

**Explanation** The initialization of a specified functionality failed. This component might still operate without the functionality.

**Recommended Action** If the problem persists, contact the Cisco TAC.

## 326013

**Error Message** %ASA-3-326013: Internal error: string in string line %d (%s )

**Explanation** A fundamental error occurred in the MRIB.

**Recommended Action** If the problem persists, contact the Cisco TAC.

## 326014

**Error Message** %ASA-3-326014: Initialization failed: error\_message error\_message

**Explanation** The MRIB failed to initialize.

**Recommended Action** If the problem persists, contact the Cisco TAC.

## 326015

**Error Message** %ASA-3-326015: Communication error: error\_message error\_message

**Explanation** The MRIB received a malformed update.

**Recommended Action** If the problem persists, contact the Cisco TAC.

## 326016

**Error Message** %ASA-3-326016: Failed to set un-numbered interface for interface\_name (string )

**Explanation** The PIM tunnel is not usable without a source address. This situation occurs because a numbered interface cannot be found, or because of an internal error.

**Recommended Action** If the problem persists, contact the Cisco TAC.

## 326017

**Error Message** %ASA-3-326017: Interface Manager error - string in string : string

**Explanation** An error occurred while creating a PIM tunnel interface.

**Recommended Action** If the problem persists, contact the Cisco TAC.

## 326019

**Error Message** %ASA-3-326019: string in string : string

**Explanation** An error occurred while creating a PIM RP tunnel interface.

**Recommended Action** If the problem persists, contact the Cisco TAC.

## 326020

**Error Message** %ASA-3-326020: List error in string : string

**Explanation** An error occurred while processing a PIM interface list.

**Recommended Action** If the problem persists, contact the Cisco TAC.

## 326021

**Error Message** %ASA-3-326021: Error in *string* : *string*

**Explanation** An error occurred while setting the SRC of a PIM tunnel interface.

**Recommended Action** If the problem persists, contact the Cisco TAC.

## 326022

**Error Message** %ASA-3-326022: Error in *string* : *string*

**Explanation** The PIM process failed to shut down upon request. Events that are performed in preparation for this shutdown may be out-of-sync.

**Recommended Action** If the problem persists, contact the Cisco TAC.

## 326023

**Error Message** %ASA-3-326023: *string* - *IP\_address* : *string*

**Explanation** An error occurred while processing a PIM group range.

**Recommended Action** If the problem persists, contact the Cisco TAC.

## 326024

**Error Message** %ASA-3-326024: An internal error occurred while processing a packet queue.

**Explanation** The PIM packet queue received a signal without a packet.

**Recommended Action** If the problem persists, contact the Cisco TAC.

## 326025

**Error Message** %ASA-3-326025: *string*

**Explanation** An internal error occurred while trying to send a message. Events scheduled to occur on the receipt of a message, such as deletion of the PIM tunnel IDB, may not occur.

**Recommended Action** If the problem persists, contact the Cisco TAC.

## 326026

**Error Message** %ASA-3-326026: Server unexpected error: *error\_message*

**Explanation** The MRIB failed to register a client.

**Recommended Action** If the problem persists, contact the Cisco TAC.

## 326027

**Error Message** %ASA-3-326027: Corrupted update: *error\_message*

**Explanation**The MRIB received a corrupt update.

**Recommended Action** If the problem persists, contact the Cisco TAC.

## 326028

**Error Message** %ASA-3-326028: Asynchronous error: *error\_message*

**Explanation**An unhandled asynchronous error occurred in the MRIB API.

**Recommended Action** If the problem persists, contact the Cisco TAC.

## 327001

**Error Message** %ASA-3-327001: IP SLA Monitor: Cannot create a new process

**Explanation**The IP SLA monitor was unable to start a new process.

**Recommended Action** Check the system memory. If memory is low, then this is probably the cause. Try to reenter the commands when memory is available. If the problem persists, contact the Cisco TAC.

## 327002

**Error Message** %ASA-3-327002: IP SLA Monitor: Failed to initialize, IP SLA Monitor functionality will not work

**Explanation**The IP SLA monitor failed to initialize. This condition is caused by either the timer wheel function failing to initialize or a process not being created. Sufficient memory is probably not available to complete the task.

**Recommended Action** Check the system memory. If memory is low, then this is probably the cause. Try to reenter the commands when memory is available. If the problem persists, contact the Cisco TAC.

## 327003

**Error Message** %ASA-3-327003: IP SLA Monitor: Generic Timer wheel timer functionality failed to initialize

**Explanation**The IP SLA monitor cannot initialize the timer wheel.

**Recommended Action** Check the system memory. If memory is low, then the timer wheel function did not initialize. Try to reenter the commands when memory is available. If the problem persists, contact the Cisco TAC.

## 328001

**Error Message** %ASA-3-328001: Attempt made to overwrite a set stub function in *string* .

**Explanation**A single function can be set as a callback for when a stub with a check registry is invoked. An attempt to set a new callback failed because a callback function has already been set.

- **string**—The name of the function

**Recommended Action** If the problem persists, contact the Cisco TAC.

## 328002

**Error Message** %ASA-3-328002: Attempt made in *string* to register with out of bounds key

**Explanation** In the FASTCASE registry, the key has to be smaller than the size specified when the registry was created. An attempt was made to register with a key out-of-bounds.

**Recommended Action** Copy the error message exactly as it appears, and report it to the Cisco TAC.

## 329001

**Error Message** %ASA-3-329001: The *string0* subblock named *string1* was not removed

**Explanation** A software error has occurred. IDB subblocks cannot be removed.

- *string0* —SWIDB or HWIDB
- *string1* —The name of the subblock

**Recommended Action** If the problem persists, contact the Cisco TAC.

## 331001

**Error Message** %ASA-3-331001: Dynamic DNS Update for '*fqdn\_name*' = *ip\_address* failed

**Explanation** The dynamic DNS subsystem failed to update the resource records on the DNS server. This failure might occur if the Secure Firewall ASA is unable to contact the DNS server or the DNS service is not running on the destination system.

- *fqdn\_name* —The fully qualified domain name for which the DNS update was attempted
- *ip\_address* —The IP address of the DNS update

**Recommended Action** Make sure that a DNS server is configured and reachable by the Secure Firewall ASA. If the problem persists, contact the Cisco TAC.

## 331002

**Error Message** %ASA-5-331002: Dynamic DNS *type* RR for ('*fqdn\_name*' - *ip\_address* | *ip\_address* - '*fqdn\_name*') successfully updated in DNS server *dns\_server\_ip*

**Explanation** A dynamic DNS update succeeded in the DNS server.

- *type* —The type of resource record, which may be A or PTR
- *fqdn\_name* —The fully qualified domain name for which the DNS update was attempted
- *ip\_address* —The IP address of the DNS update
- *dns\_server\_ip* —The IP address of the DNS server

**Recommended Action** None required.

## 332001

**Error Message** %ASA-3-332001: Unable to open cache discovery socket, WCCP V2 closing down.

**Explanation** An internal error that indicates the WCCP process was unable to open the UDP socket used to listen for protocol messages from caches.

**Recommended Action** Ensure that the IP configuration is correct and that at least one IP address has been configured.

## 332002

**Error Message** %ASA-3-332002: Unable to allocate message buffer, WCCP V2 closing down.

**Explanation** An internal error that indicates the WCCP process was unable to allocate memory to hold incoming protocol messages.

**Recommended Action** Ensure that enough memory is available for all processes.

## 332003

**Error Message** %ASA-5-332003: Web Cache *IP\_address /service\_ID* acquired

**Explanation** A service from the web cache of the Secure Firewall ASA was acquired.

- **IP\_address**—The IP address of the web cache
- **service\_ID**—The WCCP service identifier

**Recommended Action** None required.

## 332004

**Error Message** %ASA-1-332004: Web Cache *IP\_address /service\_ID* lost

**Explanation** A service from the web cache of the Secure Firewall ASA was lost.

- **IP\_address**—The IP address of the web cache
- **service\_ID**—The WCCP service identifier

**Recommended Action** Verify operation of the specified web cache.

## 333001

**Error Message** %ASA-6-333001: EAP association initiated - context: *EAP-context*

**Explanation** An EAP association has been initiated with a remote host.

- *EAP-context* —A unique identifier for the EAP session, displayed as an eight-digit hexadecimal number (for example, 0x2D890AE0)

**Recommended Action** None required.

## 333002

**Error Message** %ASA-5-333002: Timeout waiting for EAP response - context:*EAP-context*

**Explanation** A timeout occurred while waiting for an EAP response.

- *EAP-context* —A unique identifier for the EAP session displayed as an eight-digit hexadecimal number (for example, 0x2D890AE0)

**Recommended Action** None required.

## 333003

**Error Message** %ASA-6-333003: EAP association terminated - context:*EAP-context*

**Explanation** The EAP association has been terminated with the remote host.

- *EAP-context*—A unique identifier for the EAP session displayed as an eight-digit hexadecimal number (for example, 0x2D890AE0)

**Recommended Action** None required.

## 333004

**Error Message** %ASA-7-333004: EAP-SQ response invalid - context:*EAP-context*

**Explanation** The EAP-Status Query response failed basic packet validation.

- *EAP-context*—A unique identifier for the EAP session displayed as an eight-digit hexadecimal number (for example, 0x2D890AE0)

**Recommended Action** If the problem persists, contact the Cisco TAC.

## 333005

**Error Message** %ASA-7-333005: EAP-SQ response contains invalid TLV(s) - context:*EAP-context*

**Explanation** The EAP-Status Query response has one or more invalid TLVs.

- *EAP-context*—A unique identifier for the EAP session displayed as an eight-digit hexadecimal number (for example, 0x2D890AE0)

**Recommended Action** If the problem persists, contact the Cisco TAC.

## 333006

**Error Message** %ASA-7-333006: EAP-SQ response with missing TLV(s) - context:*EAP-context*

**Explanation** The EAP-Status Query response is missing one or more mandatory TLVs.

- *EAP-context*—A unique identifier for the EAP session displayed as an eight-digit hexadecimal number (for example, 0x2D890AE0)

**Recommended Action** If the problem persists, contact the Cisco TAC.

## 333007

**Error Message** %ASA-7-333007: EAP-SQ response TLV has invalid length - context:*EAP-context*

**Explanation** The EAP-Status Query response includes a TLV with an invalid length.

- *EAP-context*—A unique identifier for the EAP session displayed as an eight-digit hexadecimal number (for example, 0x2D890AE0)

**Recommended Action** If the problem persists, contact the Cisco TAC.



## 333008

**Error Message** %ASA-7-333008: EAP-SQ response has invalid nonce TLV - context:*EAP-context*

**Explanation** The EAP-Status Query response includes an invalid nonce TLV.

- *EAP-context* —A unique identifier for the EAP session displayed as an eight-digit hexadecimal number (for example, 0x2D890AE0)

**Recommended Action** If the problem persists, contact the Cisco TAC.

## 333009

**Error Message** %ASA-6-333009: EAP-SQ response MAC TLV is invalid - context:*EAP-context*

**Explanation** The EAP-Status Query response includes a MAC that does not match the calculated MAC.

- *EAP-context* —A unique identifier for the EAP session displayed as an eight-digit hexadecimal number (for example, 0x2D890AE0)

**Recommended Action** If the problem persists, contact the Cisco TAC.

## 333010

**Error Message** %ASA-5-333010: EAP-SQ response Validation Flags TLV indicates PV request - context:*EAP-context*

**Explanation** The EAP-Status Query response includes a validation flags TLV, which indicates that the peer requested a full posture validation.

**Recommended Action** None required.

## 334001

**Error Message** %ASA-6-334001: EAPoUDP association initiated - host-address

**Explanation** An EAPoUDP association has been initiated with a remote host.

- *host-address* —The IP address of the host in dotted decimal format (for example, 10.86.7.101)

**Recommended Action** None required.

## 334002

**Error Message** %ASA-5-334002: EAPoUDP association successfully established - host-address

**Explanation** An EAPoUDP association has been successfully established with the host.

- *host-address* —The IP address of the host in dotted decimal format (for example, 10.86.7.101)

**Recommended Action** None required.

## 334003

**Error Message** %ASA-5-334003: EAPoUDP association failed to establish - host-address

**Explanation** An EAPoUDP association has failed to establish with the host.

- *host-address* —The IP address of the host in dotted decimal format (for example, 10.86.7.101)

**Recommended Action** Verify the configuration of the Cisco Secure Access Control Server.

## 334004

**Error Message** %ASA-6-334004: Authentication request for NAC Clientless host - *host-address*

**Explanation** An authentication request was made for a NAC clientless host.

- *host-address* —The IP address of the host in dotted decimal format (for example, 10.86.7.101)

**Recommended Action** None required.

## 334005

**Error Message** %ASA-5-334005: Host put into NAC Hold state - *host-address*

**Explanation** The NAC session for the host was put into the Hold state.

- *host-address* —The IP address of the host in dotted decimal format (for example, 10.86.7.101)

**Recommended Action** None required.

## 334006

**Error Message** %ASA-5-334006: EAPoUDP failed to get a response from host - *host-address*

**Explanation** An EAPoUDP response was not received from the host.

- *host-address* —The IP address of the host in dotted decimal format (for example, 10.86.7.101)

**Recommended Action** None required.

## 334007

**Error Message** %ASA-6-334007: EAPoUDP association terminated - *host-address*

**Explanation** An EAPoUDP association has terminated with the host.

- *host-address* —The IP address of the host in dotted decimal format (for example, 10.86.7.101)

**Recommended Action** None required.

## 334008

**Error Message** %ASA-6-334008: NAC EAP association initiated - *host-address* , EAP context: *EAP-context*

**Explanation** EAPoUDP has initiated EAP with the host.

- *host-address* —The IP address of the host in dotted decimal format (for example, 10.86.7.101)
- *EAP-context* —A unique identifier for the EAP session displayed as an eight-digit, hexadecimal number (for example, 0x2D890AE0)

**Recommended Action** None required.

## 334009

**Error Message** %ASA-6-334009: Audit request for NAC Clientless host - *Assigned\_IP*.

**Explanation** An audit request is being sent for the specified assigned IP address.

- *Assigned\_IP* —The IP address assigned to the client

**Recommended Action** None required.

## 335001

**Error Message** %ASA-6-335001: NAC session initialized - *host-address*

**Explanation** A NAC session has started for a remote host.

- *host-address* —The IP address of the host in dotted decimal format (for example, 10.86.7.101)

**Recommended Action** None required.

## 335002

**Error Message** %ASA-5-335002: Host is on the NAC Exception List - *host-address* , OS: *oper-sys*

**Explanation** The client is on the NAC Exception List and is therefore not subject to posture validation.

- *host-address* —The IP address of the host in dotted decimal format (for example, 10.1.1.1)
- *oper-sys* —The operating system (for example, Windows XP) of the host

**Recommended Action** None required.

## 335003

**Error Message** %ASA-5-335003: NAC Default ACL applied, ACL:*ACL-name* - *host-address*

**Explanation** The NAC default ACL has been applied for the client.

- *ACL-name* —The name of the ACL being applied
- *host-address* —The IP address of the host in dotted decimal format (for example, 10.1.1.1)

**Recommended Action** None required.

## 335004

**Error Message** %ASA-6-335004: NAC is disabled for host - *host-address*

**Explanation** NAC is disabled for the remote host.

- *host-address* —The IP address of the host in dotted decimal format (for example, 10.1.1.1)

**Recommended Action** None required.

## 335005

**Error Message** %ASA-4-335005: NAC Downloaded ACL parse failure - *host-address*

**Explanation** Parsing of a downloaded ACL failed.

- *host-address* —The IP address of the host in dotted decimal format (for example, 10.1.1.1)

**Recommended Action** Verify the configuration of the Cisco Secure Access Control Server.

## 335006

**Error Message** %ASA-6-335006: NAC Applying ACL: *ACL-name* - *host-address*

**Explanation** The name of the ACL that is being applied as a result of NAC posture validation.

- *ACL-name* —The name of the ACL being applied
- *host-address* —The IP address of the host in dotted decimal format (for example, 10.1.1.1)

**Recommended Action** None required.

## 335007

**Error Message** %ASA-7-335007: NAC Default ACL not configured - *host-address*

**Explanation** A NAC default ACL has not been configured.

- *host-address* —The IP address of the host in dotted decimal format (for example, 10.1.1.1)

**Recommended Action** None required.

## 335008

**Error Message** %ASA-5-335008: NAC IPsec terminate from dynamic ACL: *ACL-name* - *host-address*

**Explanation** A dynamic ACL obtained as a result of PV requires IPsec termination.

- *ACL-name* —The name of the ACL being applied
- *host-address* —The IP address of the host in dotted decimal format (for example, 10.1.1.1)

**Recommended Action** None required.

## 335009

**Error Message** %ASA-6-335009: NAC Revalidate request by administrative action - *host-address*

**Explanation** A NAC Revalidate action was requested by the administrator.

- *host-address* —The IP address of the host in dotted decimal format (for example, 10.1.1.1)

**Recommended Action** None required.

## 335010

**Error Message** %ASA-6-335010: NAC Revalidate All request by administrative action - *num* sessions

**Explanation** A NAC Revalidate All action was requested by the administrator.

- *num* —A decimal integer that indicates the number of sessions to be revalidated

**Recommended Action** None required.

## 335011

**Error Message** %ASA-6-335011: NAC Revalidate Group request by administrative action for *group-name* group - *num* sessions

**Explanation** A NAC Revalidate Group action was requested by the administrator.

- *group-name* —The VPN group name
- *num* —A decimal integer that indicates the number of sessions to be revalidated

**Recommended Action** None required.

## 335012

**Error Message** %ASA-6-335012: NAC Initialize request by administrative action - *host-address*

**Explanation** A NAC Initialize action was requested by the administrator.

- *host-address* —The IP address of the host in dotted decimal format (for example, 10.1.1.1)

**Recommended Action** None required.

## 335013

**Error Message** %ASA-6-335013: NAC Initialize All request by administrative action - *num* sessions

**Explanation** A NAC Initialize All action was requested by the administrator.

- *num* —A decimal integer that indicates the number of sessions to be revalidated

**Recommended Action** None required.

## 335014

**Error Message** %ASA-6-335014: NAC Initialize Group request by administrative action for *group-name* group - *num* sessions

**Explanation** A NAC Initialize Group action was requested by the administrator.

- *group-name* —The VPN group name
- *num* —A decimal integer that indicates the number of sessions to be revalidated

**Recommended Action** None required.

## 336001

**Error Message** %ASA-3-336001 Route *desination\_network* stuck-in-active state in EIGRP-*ddb\_name* *as\_num*. Cleaning up

**Explanation** The SIA state means that an EIGRP router has not received a reply to a query from one or more neighbors within the time allotted (approximately three minutes). When this happens, EIGRP clears the neighbors that did not send a reply and logs an error message for the route that became active.

- *destination\_network* —The route that became active
- *ddb\_name* —IPv4
- *as\_num* —The EIGRP router

**Recommended Action** Check to see why the router did not get a response from all of its neighbors and why the route disappeared.

## 336002

**Error Message** %ASA-3-336002: Handle *handle\_id* is not allocated in pool.

**Explanation** The EIGRP router is unable to find the handle for the next hop.

- *handle\_id* —The identity of the missing handle

**Recommended Action** If the problem persists, contact the Cisco TAC.

## 336003

**Error Message** %ASA-3-336003: No buffers available for *bytes* byte packet

**Explanation** The DUAL software was unable to allocate a packet buffer. The Secure Firewall ASA may be out of memory.

- *bytes* —Number of bytes in the packet

**Recommended Action** Check to see if the Secure Firewall ASA is out of memory by entering the **show mem** or **show tech** command. If the problem persists, contact the Cisco TAC.

## 336004

**Error Message** %ASA-3-336004: Negative refcount in pakdesc *pakdesc*.

**Explanation** The reference count packet count became negative.

- *pakdesc* —Packet identifier

**Recommended Action** If the problem persists, contact the Cisco TAC.

## 336005

**Error Message** %ASA-3-336005: Flow control error, *error* , on *interface\_name*.

**Explanation** The interface is flow blocked for multicast. Qelm is the queue element, and in this case, the last multicast packet on the queue for this particular interface.

- *error* —Error statement: Qelm on flow ready
- *interface\_name* —Name of the interface on which the error occurred

**Recommended Action** If the problem persists, contact the Cisco TAC.

## 336006

**Error Message** %ASA-3-336006: *num* peers exist on IIDB *interface\_name*.

**Explanation** Peers still exist on a particular interface during or after cleanup of the IDB of the EIGRP.

- *num* —The number of peers
- *interface\_name* —The interface name

**Recommended Action** If the problem persists, contact the Cisco TAC.

## 336007

**Error Message** %ASA-3-336007: Anchor count negative

**Explanation** An error occurred and the count of the anchor became negative when it was released.

**Recommended Action** If the problem persists, contact the Cisco TAC.

## 336008

**Error Message** %ASA-3-336008: Lingering DRDB deleting IIDB, dest network, nexthop address (interface), origin origin\_str

**Explanation** An interface is being deleted and some lingering DRDB exists.

- *network*—The destination network
- *address*—The nexthop address
- *interface*—The nexthop interface
- *origin\_str*—String defining the origin

**Recommended Action** If the problem persists, contact the Cisco TAC.

## 336009

**Error Message** %ASA-3-336009 ddb\_name as\_id: Internal Error

**Explanation** An internal error occurred.

- *ddb\_name* —PDM name (for example, IPv4 PDM)
- *as\_id* —Autonomous system ID

**Recommended Action** If the problem persists, contact the Cisco TAC.

## 336010

**Error Message** %ASA-5-336010 EIGRP-*ddb\_name* tableid as\_id: Neighbor address (%interface) is event\_msg: msg

**Explanation** A neighbor went up or down.

- *ddb\_name* —IPv4
- *tableid* — Internal ID for the RIB
- *as\_id* —Autonomous system ID
- *address* —IP address of the neighbor
- *interface* —Name of the interface
- *event\_msg* — Event that is occurring for the neighbor (that is, up or down)
- *msg* —Reason for the event. Possible *event\_msg* and *msg* value pairs include:
  - resync: peer graceful-restart
  - down: holding timer expired
  - up: new adjacency
  - down: Auth failure
  - down: Stuck in Active
  - down: Interface PEER-TERMINATION received
  - down: K-value mismatch
  - down: Peer Termination received
  - down: stuck in INIT state
  - down: peer info changed
  - down: summary configured
  - down: Max hopcount changed
  - down: metric changed
  - down: [No reason]

**Recommended Action** Check to see why the link on the neighbor is going down or is flapping. This may be a sign of a problem, or a problem may occur because of this.

## 336011

**Error Message** %ASA-6-336011: *event event*

**Explanation** A dual event occurred. The events can be one of the following:

- Redist rt change
- SIA Query while Active

**Recommended Action** If the problem persists, contact the Cisco TAC.

## 336012

**Error Message** %ASA-3-336012: Interface *interface\_names* going down and *neighbor\_links* links exist

**Explanation** An interface is going down or is being removed from routing through IGRP, but not all links (neighbors) have been removed from the topology table.



**Recommended Action** If the problem persists, contact the Cisco TAC.

## 336013

**Error Message** %ASA-3-336013: Route iproute, iproute\_successors successors, db\_successors rdfs

**Explanation** A hardware or software error occurred.

**Recommended Action** If the problem persists, contact the Cisco TAC.

## 336014

**Error Message** %ASA-3-336014: "EIGRP\_PDM\_Process\_name, event\_log"

**Explanation** A hardware or software error occurred.

**Recommended Action** If the problem persists, contact the Cisco TAC.

## 336015

**Error Message** %ASA-3-336015: "Unable to open socket for AS as\_number"

**Explanation** A hardware or software error occurred.

**Recommended Action** If the problem persists, contact the Cisco TAC.

## 336016

**Error Message** %ASA-3-336016: Unknown timer type timer\_type expiration

**Explanation** A hardware or software error occurred.

**Recommended Action** If the problem persists, contact the Cisco TAC.

## 336019

**Error Message** %ASA-3-336019: process\_name as\_number: prefix\_source threshold prefix level (prefix\_threshold) reached

**Explanation** The number of prefixes in the topology database has reached the configured or default threshold level. The prefix source may be any of the following:

- Neighbor
- Redistributed
- Aggregate

**Recommended Action** Use the **show eigrp accounting** command to obtain details about the source of the prefixes and take corrective action.

## 337000

**Error Message** %ASA-6-337000: Created BFD session with local discriminator <id> on <real\_interface> with neighbor <real\_host\_ip>

**Explanation** This syslog message indicates that a BFD active session has been created.

- id— A numerical field that denotes the local discriminator value for a particular BFD session
- real\_interface— The interface nameif on which the BFD session is running
- real\_host\_ip— The IP address of the neighbor with which the BFD session has come up

**Recommended Action** None.

## 337001

**Error Message** %ASA-6-337001: Terminated BFD session with local discriminator <id> on <real\_interface> with neighbor <real\_host\_ip> due to <failure\_reason>

**Explanation** This syslog message indicates that an active BFD session has been terminated.

- id— A numerical field that denotes the local discriminator value for a particular BFD session
- real\_interface— The interface nameif on which the BFD session is running
- real\_host\_ip— The IP address of the neighbor with which the BFD session has come up
- failure\_reason— One of the following failure reasons: BFD going down on peer's side, BFD configuration removal on peer's side, Detection timer expiration, Echo function failure, Path to peer going down, Local BFD configuration removal, BFD client configuration removal

**Recommended Action** None.

## 337005

**Error Message** %ASA-4-337005: Phone Proxy SRTP: Media session not found for media\_term\_ip/media\_term\_port for packet from in\_ifc:src\_ip/src\_port to out\_ifc:dest\_ip/dest\_port

**Explanation** The adaptive security appliance received an SRTP or RTP packet that was destined to go to the media termination IP address and port, but the corresponding media session to process this packet was not found.

- in\_ifc—The input interface
- src\_ip—The source IP address of the packet
- src\_port—The source port of the packet
- out\_ifc—The output interface
- dest\_ip—The destination IP address of the packet
- dest\_port—The destination port of the packet.

**Recommended Action** If this message occurs at the end of the call, it is considered normal because the signaling messages may have released the media session, but the endpoint is continuing to send a few SRTP or RTP packets. If this message occurs for an odd-numbered media termination port, the endpoint is sending RTCP, which must be disabled from the CUCM. If this message happens continuously for a call, debug the signaling message transaction either using phone proxy debug commands or capture commands to determine if the signaling messages are being modified with the media termination IP address and port..

## 338001

**Error Message** %ASA-4-338001: Dynamic filter monitored blacklisted *protocol* traffic from *in\_interface* :*src\_ip\_addr* /*src\_port* (*mapped-ip* /*mapped-port*) to *out\_interface* :*dest\_ip\_addr* /*dest\_port* , (*mapped-ip* /*mapped-port*), source *malicious* address resolved from *local* or *dynamic* list: *domain name*, threat-level: *level\_value*, category: *category\_name*

**Explanation** Traffic from a domain, which is on an block list in the dynamic filter database, has appeared. The threat level is a string that shows one of the following values: none, very-low, low, moderate, high, and very-high. The category is a string that shows the reason why a domain name is on a block list (for example, botnet, Trojan, and spyware).

**Recommended Action** Access to a malicious site has been logged. Use the internal IP address to trace the infected machine, or enter the **dynamic-filter drop blacklist** command to automatically drop such traffic.

## 338002

**Error Message** %ASA-4-338002: Dynamic filter monitored blacklisted *protocol* traffic from *in\_interface* :*src\_ip\_addr* /*src\_port* (*mapped-ip* /*mapped-port* ) to *out\_interface* :*dest\_ip\_addr* /*dest\_port* (*mapped-ip* /*mapped-port* ), destination *malicious* address resolved from *local* or *dynamic* list: *domain name*, threat-level: *level\_value*, category: *category\_name*

**Explanation** Traffic to a domain, which is on an block list in the dynamic filter database, has appeared. The threat level is a string that shows one of the following values: none, very-low, low, moderate, high, and very-high. The category is a string that shows the reason why a domain name is on a block list (for example, botnet, Trojan, and spyware).

**Recommended Action** Access to a malicious site has been logged. Use the internal IP address to trace the infected machine, or enter the **dynamic-filter drop blacklist** command to automatically drop such traffic.

## 338003

**Error Message** %ASA-4-338003: Dynamic filter monitored blacklisted *protocol* traffic from *in\_interface* :*src\_ip\_addr* /*src\_port* (*mapped-ip* /*mapped-port*) to *out\_interface* :*dest\_ip\_addr* /*dest\_port* , (*mapped-ip* /*mapped-port*), source *malicious* address resolved from *local* or *dynamic* list: *ip address/netmask*, threat-level: *level\_value*, category: *category\_name*

**Explanation** Traffic from an IP address, which is on an block list in the dynamic filter database, has appeared. The threat level is a string that shows one of the following values: none, very-low, low, moderate, high, and very-high. The category is a string that shows the reason why a domain name is on a block list (for example, botnet, Trojan, and spyware).

**Recommended Action** Access to a malicious site has been logged. Use the internal IP address to trace the infected machine, or enter the **dynamic-filter drop blacklist** command to automatically drop such traffic.

## 338004

**Error Message** %ASA-4-338004: Dynamic filter monitored blacklisted *protocol* traffic from *in\_interface* :*src\_ip\_addr* /*src\_port* (*mapped-ip* /*mapped-port* ) to *out\_interface* :*dest\_ip\_addr* /*dest\_port* (*mapped-ip* /*mapped-port* ), destination *malicious* address resolved from *local* or *dynamic* list: *ip address/netmask*, threat-level: *level\_value*, category: *category\_name*

**Explanation** Traffic to an IP address, which is on a block list in the dynamic filter database, has appeared. The threat level is a string that shows one of the following values: none, very-low, low, moderate, high, and very-high. The category is a string that shows the reason why a domain name is on a block list (for example, botnet, Trojan, and spyware).

**Recommended Action** Access to a malicious site has been logged. Use the internal IP address to trace the infected machine, or enter the dynamic-filter drop command to automatically drop such traffic.

## 338005

**Error Message** %ASA-4-338005: Dynamic filter dropped blacklisted *protocol* traffic from *in\_interface :src\_ip\_addr /src\_port (mapped-ip /mapped-port )* to *out\_interface :dest\_ip\_addr /dest\_port (mapped-ip /mapped-port )*, source malicious address resolved from local or dynamic list: *domain name*, threat-level: *level\_value*, category: *category\_name*

**Explanation** Traffic from a domain name, which is on a block list in the dynamic filter database, was denied. The threat level is a string that shows one of the following values: none, very-low, low, moderate, high, and very-high. The category is a string that shows the reason why a domain name is on a block list (for example, botnet, Trojan, and spyware).

**Recommended Action** None required.

## 338006

**Error Message** %ASA-4-338006: Dynamic filter dropped blacklisted *protocol* traffic from *in\_interface :src\_ip\_addr /src\_port (mapped-ip /mapped-port )* to *out\_interface :dest\_ip\_addr /dest\_port (mapped-ip /mapped-port )*, destination malicious address resolved from local or dynamic list: *domain name*, threat-level: *level\_value*, category: *category\_name*

**Explanation** Traffic to a domain, which is on a block list in the dynamic filter database, was denied. The threat level is a string that shows one of the following values: none, very-low, low, moderate, high, and very-high. The category is a string that shows the reason why a domain name is on a block list (for example, botnet, Trojan, and spyware).

**Recommended Action** None required.

## 338007

**Error Message** %ASA-4-338007: Dynamic filter dropped blacklisted *protocol* traffic from *in\_interface :src\_ip\_addr /src\_port (mapped-ip /mapped-port )* to *out\_interface :dest\_ip\_addr /dest\_port (mapped-ip /mapped-port )*, source malicious address resolved from local or dynamic list: *ip address/netmask*, threat-level: *level\_value*, category: *category\_name*

**Explanation** Traffic from an IP address, which is on a block list in the dynamic filter database, was denied. The threat level is a string that shows one of the following values: none, very-low, low, moderate, high, and very-high. The category is a string that shows the reason why a domain name is on a block list (for example, botnet, Trojan, and spyware).

**Recommended Action** None required.

## 338008

**Error Message** %ASA-4-338008: Dynamic filter dropped blacklisted *protocol* traffic from *in\_interface :src\_ip\_addr /src\_port (mapped-ip /mapped-port )* to *out\_interface :dest\_ip\_addr /dest\_port (mapped-ip /mapped-port )*, destination *malicious address* resolved from *local or dynamic list: ip address/netmask*, threat-level: *level\_value*, category: *category\_name*

**Explanation** Traffic to an IP address, which is on a block list in the dynamic filter database, was denied. The threat level is a string that shows one of the following values: none, very-low, low, moderate, high, and very-high. The category is a string that shows the reason why a domain name is on a block list (for example, botnet, Trojan, and spyware).

**Recommended Action** None required.

## 338101

**Error Message** %ASA-4-338101: Dynamic filter *action* whitelisted *protocol* traffic from *in\_interface :src\_ip\_addr /src\_port (mapped-ip /mapped-port)* to *out\_interface :dest\_ip\_addr /dest\_port , (mapped-ip /mapped-port)*, source *malicious address* resolved from *local or dynamic list: domain name*

**Explanation** Traffic from a domain, which is on an allow list in the dynamic filter database, has appeared.

**Recommended Action** None required.

## 338102

**Error Message** %ASA-4-338102: Dynamic filter *action* whitelisted *protocol* traffic from *in\_interface :src\_ip\_addr /src\_port (mapped-ip /mapped-port )* to *out\_interface :dest\_ip\_addr /dest\_port (mapped-ip /mapped-port )*, destination *malicious address* resolved from *local or dynamic list: domain name*

**Explanation** Traffic to a domain name, which is on an allow list in the dynamic filter database, has appeared.

**Recommended Action** None required.

## 338103

**Error Message** %ASA-4-338103: Dynamic filter *action* whitelisted *protocol* traffic from *in\_interface :src\_ip\_addr /src\_port (mapped-ip /mapped-port)* to *out\_interface :dest\_ip\_addr /dest\_port , (mapped-ip /mapped-port)*, source *malicious address* resolved from *local or dynamic list: ip address/netmask*

**Explanation** Traffic from an IP address, which is on an allow list in the dynamic filter database, has appeared.

**Recommended Action** None required.

## 338104

**Error Message** %ASA-4-338104: Dynamic filter *action* whitelisted *protocol* traffic from *in\_interface :src\_ip\_addr /src\_port (mapped-ip /mapped-port )* to *out\_interface :dest\_ip\_addr /dest\_port (mapped-ip /mapped-port )*, destination *malicious address* resolved from *local or dynamic list: ip address/netmask*

**Explanation** Traffic to an IP address, which is on an allow list in the dynamic filter database, has appeared.

**Recommended Action** None required.

## 338201

**Error Message** %ASA-4-338201: Dynamic filter monitored greylisted protocol traffic from *in\_interface :src\_ip\_addr /src\_port (mapped-ip /mapped-port)* to *out\_interface :dest\_ip\_addr /dest\_port , (mapped-ip /mapped-port)*, source malicious address resolved from local or dynamic list: *domain name*, threat-level: *level\_value*, category: *category\_name*

**Explanation** Traffic from a domain, which is on a greylist in the dynamic filter database, has appeared. The threat level is a string that shows one of the following values: none, very-low, low, moderate, high, and very-high. The category is a string that shows the reason why a domain name is on a block list (for example, botnet, Trojan, and spyware).

**Recommended Action** Access to a malicious site has been logged. Use the internal IP address to trace the infected machine, or enter the **dynamic-filter drop blacklist** command and the **dynamic-filter ambiguous-is-black** command to automatically drop such traffic.

## 338202

**Error Message** %ASA-4-338202: Dynamic filter monitored greylisted protocol traffic from *in\_interface :src\_ip\_addr /src\_port (mapped-ip /mapped-port )* to *out\_interface :dest\_ip\_addr /dest\_port (mapped-ip /mapped-port )*, destination malicious address resolved from local or dynamic list: *domain name*, threat-level: *level\_value*, category: *category\_name*

**Explanation** Traffic to a domain name, which is on a gerylist in the dynamic filter database, has appeared. The threat level is a string that shows one of the following values: none, very-low, low, moderate, high, and very-high. The category is a string that shows the reason why a domain name is on a block list (for example, botnet, Trojan, and spyware).

**Recommended Action** Access to a malicious site has been logged. Use the internal IP address to trace the infected machine, or enter the **dynamic-filter drop blacklist** command and the **dynamic-filter ambiguous-is-black** command to automatically drop such traffic.

## 338203

**Error Message** %ASA-4-338203: Dynamic filter dropped greylisted protocol traffic from *in\_interface :src\_ip\_addr /src\_port (mapped-ip /mapped-port )* to *out\_interface :dest\_ip\_addr /dest\_port (mapped-ip /mapped-port )*, source malicious address resolved from local or dynamic list: *domain name*, threat-level: *level\_value*, category: *category\_name*

**Explanation** Traffic from a greylisted domain name in the dynamic filter database was denied; however, the malicious IP address was also resolved to domain names that are unknown to the dynamic filter database. The threat level is a string that shows one of the following values: none, very-low, low, moderate, high, and very-high. The category is a string that shows the reason why a domain name is on a block list (for example, botnet, Trojan, and spyware).

**Recommended Action** Access to a malicious site was dropped. If you do not want to automatically drop greylisted traffic whose IP address matches both unknown domain names, and domain names, which are on a block list, disable the **dynamic-filter ambiguous-is-black** command.

## 338204

**Error Message** %ASA-4-338204: Dynamic filter dropped greylisted *protocol* traffic from *in\_interface :src\_ip\_addr /src\_port (mapped-ip /mapped-port )* to *out\_interface :dest\_ip\_addr /dest\_port (mapped-ip /mapped-port )*, destination *malicious address* resolved from *local or dynamic list: domain name*, *threat-level: level\_value*, *category: category\_name*

**Explanation** Traffic to a greylisted domain name in the dynamic filter database was denied; however, the malicious IP address was also resolved to domain names that are unknown to the dynamic filter database. The threat level is a string that shows one of the following values: none, very-low, low, moderate, high, and very-high. The category is a string that shows the reason why a domain name is on a block list (for example, botnet, Trojan, and spyware).

**Recommended Action** Access to a malicious site was dropped. If you do not want to automatically drop greylisted traffic whose IP address matches both unknown domain names, and domain names, which are on a block list, disable the **dynamic-filter ambiguous-is-black** command.

## 338301

**Error Message** %ASA-4-338301: Intercepted DNS reply for domain *name* from *in\_interface :src\_ip\_addr /src\_port* to *out\_interface :dest\_ip\_addr /dest\_port* , matched *list*

**Explanation** A DNS reply that was present in an administrator's allow list, block list, or IronPort list was intercepted.

- *name*— The domain name
- *list* —The list that includes the domain name, administrator allow list, block list, or IronPort list

**Recommended Action** None required.

## 338302

**Error Message** %ASA-5-338302: Address *ipaddr* discovered for domain *name* from *list* , Adding rule

**Explanation** An IP address that was discovered from a DNS reply to the dynamic filter rule table was added.

- *ipaddr*— The IP address from the DNS reply
- *name*— The domain name
- *list* —The list that includes the domain name, administrator block list, or IronPort list

**Recommended Action** None required.

## 338303

**Error Message** %ASA-5-338303: Address *ipaddr (name)* timed out, Removing rule

**Explanation** An IP address that was discovered from the dynamic filter rule table was removed.

- *ipaddr*— The IP address from the DNS reply
- *name*— The domain name

**Recommended Action** None required.

## 338304

**Error Message** %ASA-6-338304: Successfully downloaded dynamic filter data file from updater server *url*

**Explanation** A new version of the data file has been downloaded.

- *url*—The URL of the updater server

**Recommended Action** None required.

## 338305

**Error Message** %ASA-3-338305: Failed to download dynamic filter data file from updater server *url*

**Explanation** The dynamic filter database has failed to download.

- *url*—The URL of the updater server

**Recommended Action** Make sure that you have a DNS configuration on the ASA so that the updater server URL can be resolved. If you cannot ping the server from the ASA, check with your network administrator for the correct network connection and routing configuration. If you are still having problems, contact the Cisco TAC.

## 338306

**Error Message** %ASA-3-338306: Failed to authenticate with dynamic filter updater server *url*

**Explanation** The ASA failed to authenticate with the dynamic filter updater server.

- *url*—The URL of the updater server

**Recommended Action** Contact the Cisco TAC.

## 338307

**Error Message** %ASA-3-338307: Failed to decrypt downloaded dynamic filter database file

**Explanation** The downloaded dynamic filter database file failed to decrypt.

**Recommended Action** Contact the Cisco TAC.

## 338308

**Error Message** %ASA-5-338308: Dynamic filter updater server dynamically changed from *old\_server\_host : old\_server\_port* to *new\_server\_host : new\_server\_port*

**Explanation** The ASA was directed to a new updater server host or port.

- *old\_server\_host :old\_server\_port*—The previous updater server host and port
- *new\_server\_host :new\_server\_port*—The new updater server host and port

**Recommended Action** None required.



## 338309

**Error Message** %ASA-3-338309: The license on this ASA does not support dynamic filter updater feature.

**Explanation** The dynamic filter updater is a licensed feature; however, the license on the ASA does not support this feature.

**Recommended Action** None required.

## 338310

**Error Message** %ASA-3-338310: Failed to update from dynamic filter updater server *url*, reason: *reason string*

**Explanation** The ASA failed to receive an update from the dynamic filter updater server.

- *url*— The URL of the updater server
- *reason string* —The reason for the failure, which can be one of the following:

- Failed to connect to updater server
- Received invalid server response
- Received invalid server manifest
- Error in stored update file information
- Script error
- Function call error
- Out of memory

**Recommended Action** Check the network connection to the server. Try to ping the server URL, which is shown in the output of the **show dynamic-filter updater-client** command. Make sure that the port is allowed through your network. If the network connection is not the problem, contact your network administrator.

## 339001

**Error Message** %ASA-3-339001: DNSCRYPT certificate update failed for <num\_tries> tries

**Explanation** The DNSCrypt failed to receive a certificate update.

- *num\_tries*— The number of times DNSCrypt failed to get a certificate update

**Recommended Action** Check for the following:

- If the route is setup for the Umbrella server.
- If the Umbrella server egress interface is up.
- If the correct Provider public key is used.

## 339002

**Error Message** %ASA-3-339002: Umbrella device registration failed with error code <err\_code>

**Explanation** The umbrella device registration failed.

- *err\_code*— The error code returned from the Umbrella Server.

**Recommended Action** If the error code is:

- 400 – There is a problem with the request format or content. The token is probably too short or corrupted. Verify if the token matches what is on the Umbrella Dashboard.
- 401 – The token is not authorized. If the token was refreshed on the Umbrella Dashboard, then the new token should be updated on ASA.
- 409 – The device id is conflicting with another organization. Contact the Umbrella Server Administrator.
- 500 – There is an internal server error. Contact the Umbrella Server Administrator.

## 339003

**Error Message** %ASA-3-339003: Umbrella device registration was successful

**Explanation** Successful message for the umbrella device registration.

**Recommended Action** None.

## 339004

**Error Message** %ASA-3-339004: Umbrella device registration failed due to missing token

**Explanation** Umbrella device registration failed due to missing token.

**Recommended Action** Make sure the token is configured under the global “umbrella” submode.

## 339005

**Error Message** %ASA-3-339005: Umbrella device registration failed after <num\_tries> retries

**Explanation** Umbrella device registration failed.

- *num\_tries*— The number of times the device failed to register with the Umbrella Server.

**Recommended Action** Locate the error code in the syslog 339002 message. Refer the workaround for the 339002 syslog message and fix.

## 339006

**Error Message** %ASA-3-339006: Umbrella resolver *current resolver ipv46* is reachable, resuming Umbrella redirect.

**Explanation** Umbrella had failed to open, and the resolver was unreachable. The resolver is now reachable and service is resumed.

**Recommended Action** None.

## 339007

**Error Message** %ASA-3-339007: Umbrella resolver *current resolver ipv46* is unreachable, moving to fail-open. Starting probe to resolver.

**Explanation** Umbrella fail-open has been configured and a resolver unreachability has been detected.

**Recommended Action** Check the network settings for reachability to the Umbrella resolvers.

## 339008

**Error Message** %ASA-3-339008: Umbrella resolver *current resolver ipv46* is unreachable, moving to fail-close.

**Explanation** Umbrella fail-open has NOT been configured and a resolver unreachability has been detected.

**Recommended Action** Check the network settings for reachability to the Umbrella resolvers.

## 340001

**Error Message** %ASA-3-340001: Loopback-proxy error: *error\_string* context id *context\_id* , context type = *version /request\_type /address\_type* client socket (internal)=  
*client\_address\_internal /client\_port\_internal* server socket (internal)=  
*server\_address\_internal /server\_port\_internal* server socket (external)=  
*server\_address\_external /server\_port\_external* remote socket (external)=  
*remote\_address\_external /remote\_port\_external*

**Explanation** Loopback proxy allows third-party applications running on the Secure Firewall ASA to access the network. The loopback proxy encountered an error.

- *context\_id*— A unique, 32-bit context ID that is generated for each loopback client proxy request
- *version* —The protocol version
- *request\_type* —The type of request, which can be one of the following: TC (TCP connection), TB (TCP bind), or UA (UDP association)
- *address\_type* —The types of addresses, which can be one of the following: IP4 (IPv4), IP6 (IPv6), or DNS (domain name service)
- *client\_address\_internal/server\_address\_internal*— The addresses that the loopback client and the loopback server used for communication
- *client\_port\_internal /server\_port\_internal*— The ports that the loopback client and the loopback server used for communication
- *server\_address\_external /remote\_address\_external* —The addresses that the loopback server and the remote host used for communication
- *server\_port\_external /remote\_port\_external* —The ports that the loopback server and the remote host used for communication
- *error\_string* —The error string that may help troubleshoot the problem

**Recommended Action** Copy the syslog message and contact the Cisco TAC.

## 340002

**Error Message** %ASA-6-340002: Loopback-proxy info: *error\_string* context id *context\_id* , context type = *version /request\_type /address\_type* client socket (internal)=

```

client_address_internal /client_port_internal server socket (internal)=
server_address_internal /server_port_internal server socket (external)=
server_address_external /server_port_external remote socket (external)=
remote_address_external /remote_port_external

```

**Explanation** Loopback proxy allows third-party applications running on the Secure Firewall ASA to access the network. The loopback proxy generated debugging information for use in troubleshooting.

- *context\_id*— A unique, 32-bit context ID that is generated for each loopback client proxy request
- *version* —The protocol version
- *request\_type* —The type of request, which can be one of the following: TC (TCP connection), TB (TCP bind), or UA (UDP association)
- *address\_type* —The types of addresses, which can be one of the following: IP4 (IPv4), IP6 (IPv6), or DNS (domain name service)
- *client\_address\_internal/server\_address\_internal*— The addresses that the loopback client and the loopback server used for communication
- *client\_port\_internal/server\_port\_internal*— The ports that the loopback client and the loopback server used for communication
- *server\_address\_external/remote\_address\_external* —The addresses that the loopback server and the remote host used for communication
- *server\_port\_external/remote\_port\_external* —The ports that the loopback server and the remote host used for communication
- *error\_string* —The error string that may help troubleshoot the problem

**Recommended Action** Copy the syslog message and contact the Cisco TAC.

## 341001

**Error Message** %ASA-6-341001: Policy Agent started successfully for VNMC *vnmc\_ip\_addr*

**Explanation** The policy agent processes (DME, ducatiAG, and commonAG) started successfully.

- *vnmc\_ip\_addr* —The IP address of the VNMC server

**Recommended Action** None.

## 341002

**Error Message** %ASA-6-341002: Policy Agent stopped successfully for VNMC *vnmc\_ip\_addr*

**Explanation** The policy agent processes (DME, ducatiAG, and commonAG) were stopped.

- *vnmc\_ip\_addr* —The IP address of the VNMC server

**Recommended Action** None.

## 341003

**Error Message** %ASA-3-341003: Policy Agent failed to start for VNMC *vnmc\_ip\_addr*

**Explanation** The policy agent failed to start.

- *vnmc\_ip\_addr* —The IP address of the VNMC server

**Recommended Action** Check for console history and the disk0:/pa/log/vnm\_pa\_error\_status for error messages. To retry starting the policy agent, issue the **registration host** command again.

## 341004

**Error Message** %ASA-3-341004: Storage device not available: Attempt to shutdown module %s failed.

**Explanation** All SSDs have failed or been removed with the system in Up state. The system has attempted to shut down the software module, but that attempt has failed.

- %s —The software module (for example, cxsc)

**Recommended Action** Replace the removed or failed drive and reload the Secure Firewall ASA.

## 341005

**Error Message** %ASA-3-341005: Storage device not available. Shutdown issued for module %s .

**Explanation** All SSDs have failed or been removed with the system in Up state. The system is shutting down the software module.

- %s —The software module (for example, cxsc)

**Recommended Action** Replace the removed or failed drive and reload the software module.

## 341006

**Error Message** %ASA-3-341006: Storage device not available. Failed to stop recovery of module %s .

**Explanation** All SSDs have failed or been removed with the system in recovery state. The system attempted to stop the recover, but that attempt failed.

- %s —The software module (for example, cxsc)

**Recommended Action** Replace the removed or failed drive and reload the Secure Firewall ASA.

## 341007

**Error Message** %ASA-3-341007: Storage device not available. Further recovery of module %s was stopped. This may take several minutes to complete.

**Explanation** All SSDs have failed or been removed with the system in recovery state. The system is stopping the recovery of the software module.

- %s —The software module (for example, cxsc)

**Recommended Action** Replace the removed or failed drive and reload the software module.

## 341008

**Error Message** %ASA-3-341008: Storage device not found. Auto-boot of module %s cancelled. Install drive and reload to try again.

**Explanation** After getting the system into Up state, all SSDs have failed or been removed before reloading the system. Because the default action during boot is to auto-boot the software module, that action is blocked because there is no storage device available.

**Recommended Action** Replace the removed or failed drive and reload the software module.

## 341010

**Error Message** %ASA-6-341010: Storage device with serial number *ser\_no* [inserted into | removed from] bay *bay\_no*

**Explanation** The Secure Firewall ASA has detected insertion or removal events and generates this syslog message immediately.

**Recommended Action** None required.

## 341011

**Error Message** %ASA-3-341011: Storage device with serial number *ser\_no* in bay *bay\_no* faulty.

**Explanation** The Secure Firewall ASA polls the hard disk drive (HDD) health status every 10 minutes and generates this syslog message if the HDD is in a failed state.

**Recommended Action** None required.

## 342001

**Error Message** %ASA-7-342001: REST API Agent started successfully.

**Explanation** The REST API Agent must be successfully started before a REST API Client can configure the ASA.

**Recommended Action** None.

## 342002

**Error Message** %ASA-3-342002: REST API Agent failed, reason: *reason*

**Explanation** The REST API Agent could fail to start or crash for various reasons, and the reason is specified.

- *reason* —The cause for the REST API failure

**Recommended Action** The actions taken to resolve the issue vary depending on the reason logged. For example, the REST API Agent crashes when the Java process runs out of memory. If this occurs, you need to restart the REST API Agent. If the restart is not successful, contact the Cisco TAC to identify the root cause fix.

## 342003

**Error Message** %ASA-3-342003: REST API Agent failure notification received. Agent will be restarted automatically.

**Explanation** A failure notification from the REST API Agent has been received and a restart of the Agent is being attempted.

**Recommended Action** None.

## 342004

**Error Message** %ASA-3-342004: Failed to automatically restart the REST API Agent after 5 unsuccessful attempts. Use the 'no rest-api agent' and 'rest-api agent' commands to manually restart the Agent.

**Explanation** The REST API Agent has failed to start after many attempts.

**Recommended Action** See syslog %ASA-3-342002 (if logged) to better understand the reason behind the failure. Try to disable the REST API Agent by entering the **no rest-api agent** command and re-enable the REST API Agent using the **rest-api agent** command.

## 342005

**Error Message** %ASA-7-342005: REST API image has been installed successfully.

**Explanation** The REST API image must be successfully installed before starting the REST API Agent.

**Recommended Action** None.

## 342006

**Error Message** %ASA-3-342006: Failed to install REST API image, reason: <reason>.

**Explanation** The REST API image installation may fail, for one of the following reasons: version check failed, image verification failed, image file not found, out of space on flash or mount failed.

**Recommended Action** The administrator should fix the failure and try to install the image again using 'rest-api image <image>'.  
'rest-api image <image>'.  
'rest-api image <image>'.

## 342007

**Error Message** %ASA-7-342007: REST API image has been uninstalled successfully.

**Explanation** The old REST API image must be successfully uninstalled before a new one can be installed.

**Recommended Action** None.

## 342008

**Error Message** %ASA-3-342008: Failed to uninstall REST API image, reason: <reason>.

**Explanation** The REST API image could not be uninstalled for the following reasons- unmount failed or REST Agent is enabled.

**Recommended Action** The administrator should disable the REST Agent, before trying to uninstall the REST API image.





## CHAPTER 4

# Syslog Messages 400000 to 450001

This chapter contains the following sections:

- [Messages 400000 to 409128, on page 187](#)
- [Messages 410001 to 450001, on page 217](#)

## Messages 400000 to 409128

This chapter includes messages from 400000 to 409128.

### 4000nn

**Error Message** %ASA-4-4000nn: IPS:*number string* from *IP\_address* to *IP\_address* on interface *interface\_name*

**Explanation** Messages 400000 through 400051 are Cisco Intrusion Prevention Service signature messages.

**Recommended Action** See the Cisco Intrusion Prevention Service User Guide on Cisco.com.

Not all signature messages are supported by the ASA in this release. IPS messages all start with 4-4000nn and have the following format:

<b>number</b>	The signature number. For more information, see the Cisco Intrusion Prevention Service User Guide on Cisco.com.
<b>string</b>	The signature message—approximately the same as the NetRanger signature message.
<b>IP_address</b>	The local to remote address to which the signature applies.
<b>interface_name</b>	The name of the interface on which the signature originated.

For example:

```
%ASA-4-400013 IPS:2003 ICMP redirect from 10.4.1.2 to 10.2.1.1 on interface dmz
%ASA-4-400032 IPS:4051 UDP Snork attack from 10.1.1.1 to 192.168.1.1 on interface outside
```

The following table lists the supported signature messages.

Table 46: IPS Syslog Messages

Message Number	Signature ID	Signature Title	Signature Type
400000	1000	IP options-Bad Option List	Informational
400001	1001	IP options-Record Packet Route	Informational
400002	1002	IP options-Timestamp	Informational
400003	1003	IP options-Security	Informational
400004	1004	IP options-Loose Source Route	Informational
400005	1005	IP options-SATNET ID	Informational
400006	1006	IP options-Strict Source Route	Informational
400007	1100	IP Fragment Attack	Attack
400008	1102	IP Impossible Packet	Attack
400009	1103	IP Fragments Overlap	Attack
400010	2000	ICMP Echo Reply	Informational
400011	2001	ICMP Host Unreachable	Informational
400012	2002	ICMP Source Quench	Informational
400013	2003	ICMP Redirect	Informational
400014	2004	ICMP Echo Request	Informational
400015	2005	ICMP Time Exceeded for a Datagram	Informational
400016	2006	ICMP Parameter Problem on Datagram	Informational
400017	2007	ICMP Timestamp Request	Informational
400018	2008	ICMP Timestamp Reply	Informational
400019	2009	ICMP Information Request	Informational
400020	2010	ICMP Information Reply	Informational
400021	2011	ICMP Address Mask Request	Informational
400022	2012	ICMP Address Mask Reply	Informational
400023	2150	Fragmented ICMP Traffic	Attack
400024	2151	Large ICMP Traffic	Attack
400025	2154	Ping of Death Attack	Attack
400026	3040	TCP NULL flags	Attack

Message Number	Signature ID	Signature Title	Signature Type
400027	3041	TCP SYN+FIN flags	Attack
400028	3042	TCP FIN only flags	Attack
400029	3153	FTP Improper Address Specified	Attack
400030	3154	FTP Improper Port Specified	Attack
400031	4050	UDP Bomb attack	Attack
400032	4051	UDP Snork attack	Attack
400033	4052	UDP Chargen DoS attack	Attack
400034	6050	DNS HINFO Request	Informational
400035	6051	DNS Zone Transfer	Informational
400036	6052	DNS Zone Transfer from High Port	Informational
400037	6053	DNS Request for All Records	Informational
400038	6100	RPC Port Registration	Informational
400039	6101	RPC Port Unregistration	Informational
400040	6102	RPC Dump	Informational
400041	6103	Proxied RPC Request	Attack
400042	6150	ypserv (YP server daemon) Portmap Request	Informational
400043	6151	ypbind (YP bind daemon) Portmap Request	Informational
400044	6152	yppasswdd (YP password daemon) Portmap Request	Informational
400045	6153	ypupdated (YP update daemon) Portmap Request	Informational
400046	6154	ypxfrd (YP transfer daemon) Portmap Request	Informational
400047	6155	mountd (mount daemon) Portmap Request	Informational
400048	6175	rexcd (remote execution daemon) Portmap Request	Informational
400049	6180	rexcd (remote execution daemon) Attempt	Informational
400050	6190	statd Buffer Overflow	Attack

## 401001

**Error Message** %ASA-4-401001: Shuns cleared

**Explanation** The **clear shun** command was entered to remove existing shuns from memory. An institution to keep a record of shunning activity was allowed.

**Recommended Action** None required.

## 401002

**Error Message** %ASA-4-401002: Shun added: *IP\_address IP\_address port port*

**Explanation** A **shun** command was entered, where the first IP address is the shunned host. The other addresses and ports are optional and are used to terminate the connection if available. An institution to keep a record of shunning activity was allowed.

**Recommended Action** None required.

## 401003

**Error Message** %ASA-4-401003: Shun deleted: *IP\_address*

**Explanation** A single shunned host was removed from the shun database. An institution to keep a record of shunning activity was allowed.

**Recommended Action** None required.

## 401004

**Error Message** %ASA-4-401004: Shunned packet: *IP\_address = IP\_address* on interface *interface\_name*

**Explanation** A packet was dropped because the host defined by IP SRC is a host in the shun database. A shunned host cannot pass traffic on the interface on which it is shunned. For example, an external host on the Internet can be shunned on the outside interface. A record of the activity of shunned hosts was provided. This message and message %ASA-4-401005 can be used to evaluate further risk concerning this host.

**Recommended Action** None required.

## 401005

**Error Message** %ASA-4-401005: Shun add failed: unable to allocate resources for *IP\_address IP\_address port port*

**Explanation** The Secure Firewall ASA is out of memory; a shun cannot be applied.

**Recommended Action** The Cisco IPS should continue to attempt to apply this rule. Try to reclaim memory and reapply a shun manually, or wait for the Cisco IPS to do this.

## 402114

**Error Message** %ASA-4-402114: IPSEC: Received an *protocol* packet (SPI=*spi* , sequence number=*seq\_num* ) from *remote\_IP* to *local\_IP* with an invalid SPI.

- >*protocol*— IPsec protocol
- >*spi*— IPsec Security Parameter Index

- `seq_num`>— IPsec sequence number
- `remote_IP`>— IP address of the remote endpoint of the tunnel
- `>username`— Username associated with the IPsec tunnel
- `local_IP`>— IP address of the local endpoint of the tunnel

**Explanation**An IPsec packet was received that specifies an SPI that does not exist in the SA database. This may be a temporary condition caused by slight differences in aging of SAs between the IPsec peers, or it may be because the local SAs have been cleared. It may also indicate incorrect packets sent by the IPsec peer, which may be part of an attack. This message is rate limited to no more than one message every five seconds.

**Recommended Action**The peer may not acknowledge that the local SAs have been cleared. If a new connection is established from the local router, the two peers may then reestablish connection successfully. Otherwise, if the problem occurs for more than a brief period, either attempt to establish a new connection or contact the peer administrator.

## 402115

**Error Message** %ASA-4-402115: IPSEC: Received a packet from `remote_IP` to `local_IP` containing `act_prot` data instead of `exp_prot` data.

**Explanation** An IPsec packet was received that is missing the expected ESP header. The peer is sending packets that do not match the negotiated security policy, which may indicate an attack. This message is rate limited to no more than one message every five seconds.

- `remote_IP`>— IP address of the remote endpoint of the tunnel
- `local_IP`>— IP address of the local endpoint of the tunnel
- `>act_prot`— Received IPsec protocol
- `>exp_prot`— Expected IPsec protocol

**Recommended Action** Contact the administrator of the peer.

## 402116

**Error Message** %ASA-4-402116: IPSEC: Received an `protocol` packet (SPI=`spi` , sequence number=`seq_num` ) from `remote_IP` (`username` ) to `local_IP` . The decapsulated inner packet doesn't match the negotiated policy in the SA. The packet specifies its destination as `pkt_daddr` , its source as `pkt_saddr` , and its protocol as `pkt_prot` . The SA specifies its local proxy as `id_daddr /id_dmask /id_dprot /id_dport` and its remote proxy as `id_saddr /id_smask /id_sprot /id_sport` .

**Explanation**A decapsulated IPsec packet does not match the negotiated identity. The peer is sending other traffic through this security association, which may be caused by a security association selection error by the peer, or it may be part of an attack. This message is rate limited to no more than one message every five seconds.

- `>protocol`— IPsec protocol
- `>spi`— IPsec Security Parameter Index
- `seq_num`>— IPsec sequence number
- `remote_IP`>— IP address of the remote endpoint of the tunnel
- `>username`— Username associated with the IPsec tunnel
- `local_IP`>— IP address of the local endpoint of the tunnel
- `pkt_daddr`>— Destination address from the decapsulated packet

- `pkt_saddr`>— Source address from the decapsulated packet
- `pkt_prot`>— Transport protocol from the decapsulated packet
- `id_daddr`>— Local proxy IP address
- `id_dmask`>— Local proxy IP subnet mask
- `id_dprot`>— Local proxy transport protocol
- `id_dport`>— Local proxy port
- `id_saddr`>— Remote proxy IP address
- `id_smask`>— Remote proxy IP subnet mask
- `id_sprot`>— Remote proxy transport protocol
- `id_sport`>— Remote proxy port

**Recommended Action**Contact the administrator of the peer and compare policy settings.

## 402117

**Error Message** %ASA-4-402117: IPSEC: Received a non-IPsec (*protocol*) packet from *remote\_IP* to *local\_IP*.

**Explanation**The received packet matched the crypto map ACL, but it is not IPsec-encapsulated. The IPsec peer is sending unencapsulated packets. This error can occur because of a policy setup error on the peer. For example, the firewall may be configured to only accept encrypted Telnet traffic to the outside interface port 23. If you attempt to use Telnet without IPsec encryption to access the outside interface on port 23, this message appears, but not with Telnet or traffic to the outside interface on ports other than 23. This error can also indicate an attack. This message is not generated except under these conditions (for example, it is not generated for traffic to the Secure Firewall ASA interfaces themselves). See messages 710001, 710002, and 710003, which track TCP and UDP requests. This message is rate limited to no more than one message every five seconds.

- `>protocol`— IPsec protocol
- `remote_IP`>— IP address of the remote endpoint of the tunnel
- `local_IP`>— IP address of the local endpoint of the tunnel

**Recommended Action**Contact the administrator of the peer to compare policy settings.

## 402118

**Error Message** %ASA-4-402118: IPSEC: Received an *protocol* packet (*SPI=spi*, sequence number *seq\_num*) from *remote\_IP* (*username*) to *local\_IP* containing an illegal IP fragment of length *frag\_len* with offset *frag\_offset*.

**Explanation**A decapsulated IPsec packet included an IP fragment with an offset less than or equal to 128 bytes. The latest version of the security architecture for IP RFC recommends 128 bytes as the minimum IP fragment offset to prevent reassembly attacks. This may be part of an attack. This message is rate limited to no more than one message every five seconds.

- `>protocol`— IPsec protocol
- `>spi`— IPsec Security Parameter Index
- `seq_num`>— IPsec sequence number
- `remote_IP`>— IP address of the remote endpoint of the tunnel
- `>username`— Username associated with the IPsec tunnel
- `local_IP`>— IP address of the local endpoint of the tunnel

- frag\_len>— IP fragment length
- frag\_offset>— IP fragment offset in bytes

**Recommended Action** Contact the administrator of the remote peer to compare policy settings.

## 402119

**Error Message** %ASA-4-402119: IPSEC: Received an *protocol* packet (SPI=*spi* , sequence number=*seq\_num* ) from *remote\_IP* (*username* ) to *local\_IP* that failed anti-replay checking.

**Explanation** An IPsec packet was received with an invalid sequence number. The peer is sending packets including sequence numbers that may have been previously used. This message indicates that an IPsec packet has been received with a sequence number outside of the acceptable window. This packet will be dropped by IPsec as part of a possible attack. This message is rate limited to no more than one message every five seconds.

- >*protocol*— IPsec protocol
- >*spi*— IPsec Security Parameter Index
- seq\_num>— IPsec sequence number
- remote\_IP>— IP address of the remote endpoint of the tunnel
- >*username*— Username associated with the IPsec tunnel
- local\_IP>— IP address of the local endpoint of the tunnel

**Recommended Action** Contact the administrator of the peer.

## 402120

**Error Message** %ASA-4-402120: IPSEC: Received an *protocol* packet (SPI=*spi* , sequence number=*seq\_num* ) from *remote\_IP* (*username* ) to *local\_IP* that failed authentication.

**Explanation** An IPsec packet was received and failed authentication. The packet is dropped. The packet may have been corrupted in transit, or the peer may be sending invalid IPsec packets, which may indicate an attack if many of these packets were received from the same peer. This message is rate limited to no more than one message every five seconds.

- >*protocol*— IPsec protocol
- >*spi*— IPsec Security Parameter Index
- seq\_num>— IPsec sequence number
- remote\_IP>— IP address of the remote endpoint of the tunnel
- >*username*— Username associated with the IPsec tunnel
- local\_IP>— IP address of the local endpoint of the tunnel

**Recommended Action** Contact the administrator of the remote peer if many failed packets were received.

## 402121

**Error Message** %ASA-4-402121: IPSEC: Received an *protocol* packet (SPI=*spi* , sequence number=*seq\_num* ) from *peer\_addr* (*username* ) to *lcl\_addr* that was dropped by IPsec (*drop\_reason* ).

**Explanation** An IPsec packet to be decapsulated was received and subsequently dropped by the IPsec subsystem. This may indicate a problem with the Secure Firewall ASA configuration or with the Secure Firewall ASA itself.

- *>protocol*— IPsec protocol
- *>spi*— IPsec Security Parameter Index
- *seq\_num*>— IPsec sequence number
- *peer\_addr*>— IP address of the remote endpoint of the tunnel
- *>username*— Username associated with the IPsec tunnel
- *lcl\_addr*>— IP address of the local endpoint of the tunnel
- *drop\_reason*>— Reason that the packet was dropped

**Recommended Action** If the problem persists, contact the Cisco TAC.

## 402122

**Error Message** %ASA-4-402122: Received a cleartext packet from *src\_addr* to *dest\_addr* that was to be encapsulated in IPsec that was dropped by IPsec (*drop\_reason*).

**Explanation** A packet to be encapsulated in IPsec was received and subsequently dropped by the IPsec subsystem. This may indicate a problem with the Secure Firewall ASA configuration or with the Secure Firewall ASA itself.

- *src\_addr* >— Source IP address
- *dest\_addr* >— Destination> IP address
- *drop\_reason*>— Reason that the packet was dropped

**Recommended Action** If the problem persists, contact the Cisco TAC.

## 402123

**Error Message** %ASA-4-402123: CRYPTO: The *accel\_type* hardware accelerator encountered an error (*code=error\_string*) while executing *crypto* command *command*.

**Explanation** An error was detected while running a *crypto* command with a hardware accelerator, which may indicate a problem with the accelerator. This type of error may occur for a variety of reasons, and this message supplements the *crypto* accelerator counters to help determine the cause.

- *accel\_type*—Hardware accelerator type
- *>error\_string*— Code indicating the type of error
- *command*—Crypto command that generated the error

**Recommended Action** If the problem persists, contact the Cisco TAC.

## 402124

**Error Message** %ASA-4-402124: CRYPTO: The ASA hardware accelerator encountered an error (Hardware error address, Core, Hardware error code, IstatReg, PciErrReg, CoreErrStat, CoreErrAddr, Doorbell Size, DoorBell Outstanding, SWReset).

**Explanation** The *crypto* hardware chip has reported a fatal error, indicating that the chip is inoperable. The information from this message captures the details to allow further analysis of the problem. The *crypto* chip is reset when this condition is detected to unobtrusively allow the Secure Firewall ASA to continue functioning. Also, the *crypto* environment at the time this issue is detected is written to a *crypto* archive directory on flash to provide further debugging information. Various parameters related to the *crypto* hardware are included in this message, as follows:



- HWErrAddr>— Hardware address (set by crypto chip)
- Core>— Crypto core experiencing the error
- HwErrCode>— Hardware error code (set by crypto chip)
- IstatReg>— Interrupt status register (set by crypto chip)
- PciErrReg>— PCI error register (set by crypto chip)
- CoreErrStat>— Core error status (set by crypto chip)
- CoreErrAddr>— Core error address (set by crypto chip)
- Doorbell Size>— Maximum crypto commands allowed
- DoorBell Outstanding>— Crypto commands outstanding
- SWReset>— Number of crypto chip resets since boot



**Note** The %ASA-vpn-4-402124: CRYPTO: The ASA hardware accelerator encountered an error (HWErrAddr= 0x40EE9800, Core= 0, HwErrCode= 23, IstatReg= 0x8, PciErrReg= 0x0, CoreErrStat= 0x41, CoreErrAddr= 0x844E9800, Doorbell Size[0]= 2048, DoorBell Outstanding[0]= 0, Doorbell Size[1]= 0, DoorBell Outstanding[1]= 0, SWReset= 99) error message indicates a AnyConnect problem and the workaround for this to upgrade to AnyConnect 3.1.x.

**Recommended Action** Forward the message information to the Cisco TAC for further analysis.

## 402125

**Error Message** %ASA-4-402125: The ASA hardware accelerator *ring* timed out (*parameters*).

**Explanation** The crypto driver has detected that either the IPSEC descriptor ring or SSL/Admin descriptor ring is no longer progressing, meaning the crypto chip no longer appears to be functioning. The crypto chip is reset when this condition is detected to unobtrusively allow the Secure Firewall ASA to continue functioning. Also, the crypto environment at the time this issue was detected was written to a crypto archive directory on flash to provide further debugging information.

- >*ring*— IPSEC or Admin ring
- *parameters* >— Include the following:
  - Desc>— Descriptor address
  - CtrlStat>— Control/status value
  - ResultP>— Success pointer
  - ResultVal>— Success value
  - Cmd>— Crypto command
  - CmdSize>— Command size
  - Param>— Command parameters
  - Dlen>— Data length
  - DataP>— Data pointer
  - CtxtP>— VPN context pointer
  - SWReset>— Number of crypto chip resets since boot

**Recommended Action** Forward the message information to the Cisco TAC for further analysis.

## 402126

**Error Message** %ASA-4-402126: CRYPTO: The ASA created Crypto Archive File *Archive Filename* as a Soft Reset was necessary. Please forward this archived information to Cisco.

**Explanation** A functional problem with the hardware crypto chip was detected (see syslog messages 402124 and 402125). To further debug the crypto problem, a crypto archive file was generated that included the current crypto hardware environment (hardware registers and crypto description entries). At boot time, a `crypto_archive` directory was automatically created on the flash file system (if it did not exist previously). A maximum of two crypto archive files are allowed to exist in this directory.

- *>Archive Filename*— The name of the crypto archive file name. The crypto archive file names are of the form, `crypto_arch_x.bin`, where `x = (1 or 2)`.

**Recommended Action** Forward the crypto archive files to the Cisco TAC for further analysis.

## 402127

**Error Message** %ASA-4-402127: CRYPTO: The ASA is skipping the writing of latest Crypto Archive File as the maximum # of files, *max\_number*, allowed have been written to *archive\_directory*. Please archive & remove files from *Archive Directory* if you want more Crypto Archive Files saved.

**Explanation** A functional problem with the hardware crypto chip was detected (see messages 4402124 and 4402125). This message indicates a crypto archive file was not written, because the maximum number of crypto archive files already existed.

- *max\_number* >— Maximum number of files allowed in the archive directory; currently set to two
- *>archive\_directory*— Name of the archive directory

**Recommended Action** Forward previously generated crypto archive files to the Cisco TAC. Remove the previously generated archive file(s) so that more can be written (if deemed necessary).

## 402128

**Error Message** %ASA-5-402128: CRYPTO: An attempt to allocate a large memory block failed, size: *size*, limit: *limit*

**Explanation** An SSL connection is attempting to use more memory than allowed. The request has been denied.

- *size* —The size of the memory block being allocated
- *limit* —The maximum size of allocated memory permitted

**Recommended Action** If this message persists, an SSL denial of service attack may be in progress. Contact the remote peer administrator or upstream provider.

## 402129

**Error Message** %ASA-6-402129: CRYPTO: An attempt to release a DMA memory block failed, location: *address*

**Explanation** An internal software error has occurred.

- *address* —The address being freed

**Recommended Action** Contact the Cisco TAC for assistance.

## 402130

**Error Message** %ASA-6-402130: CRYPTO: Received an ESP packet (SPI = xxxxxxxxxx, sequence number=xxxx) from 172.16.0.1 (user=user) to 192.168.0.2 with incorrect IPsec padding.

**Explanation** The Secure Firewall ASA crypto hardware accelerator detected an IPsec packet with invalid padding. The ATT VPN client sometimes pads IPsec packets incorrectly.

- *SPI* —The SPI associated with the packet
- *sequence number* —The sequence number associated with the packet
- *user* —Username string
- *padding* —Padding data from the packet

**Recommended Action** While this message is None required and does not indicate a problem with the Secure Firewall ASA, customers using the ATT VPN client may wish to upgrade their VPN client software.

## 402131

**Error Message** %ASA-4-402131: CRYPTO: *status* changing the *accel\_instance* hardware accelerator's configuration bias from *old\_config\_bias* to *new\_config\_bias* .

**Explanation** The hardware accelerator configuration has been changed on the Secure Firewall ASA. Some Secure Firewall ASA platforms have multiple hardware accelerators. One syslog message is generated for each hardware accelerator change.

- *status* —Indicates success or failure
- *accel\_instance* —The instance of the hardware accelerator
- *old\_config\_bias* —The old configuration
- *new\_config\_bias* —The new configuration

**Recommended Action** If any of the accelerators fails when attempting to change its configuration, collect logging information and contact the Cisco TAC. If a failure occurs, the software will retry the configuration change multiple times. The software will fall back to the original configuration bias if the retry attempts fail. If multiple attempts to reconfigure the hardware accelerator fail, it may indicate a hardware failure.

## 402140

**Error Message** %ASA-3-402140: CRYPTO: RSA key generation error: modulus len *len*

**Explanation** An error occurred during an RSA public key pair generation.

- *len* —The prime modulus length in bits

**Recommended Action** Contact the Cisco TAC for assistance.

## 402141

**Error Message** %ASA-3-402141: CRYPTO: Key zeroization error: key set *type* , reason *reason*

**Explanation** An error occurred during an RSA public key pair generation.

- *type* —The key set type, which can be any of the following: DH, RSA, DSA, or unknown
- *reason* —The unexpected crypto session type

**Recommended Action** Contact the Cisco TAC for assistance.

## 402142

**Error Message** %ASA-3-402142: CRYPTO: Bulk data *op* error: algorithm *alg* , mode *mode*

**Explanation** An error occurred during a symmetric key operation.

- *op* —The operation, which can be either encryption or decryption
- *alg* —The encryption algorithm, which can be any of the following: DES, 3DES, AES, or RC4
- *mode* —The mode, which can be any of the following: CBC, CTR, CFB, ECB, stateful-RC4, or stateless-RC4

**Recommended Action** Contact the Cisco TAC for assistance.

## 402143

**Error Message** %ASA-3-402143: CRYPTO: *alg type* key *op*

**Explanation** An error occurred during an asymmetric key operation.

- *alg* —The encryption algorithm, which can be either RSA or DSA
- *type* —The key type, which can be either public or private
- *op* —The operation, which can be either encryption or decryption

**Recommended Action** Contact the Cisco TAC for assistance.

## 402144

**Error Message** %ASA-3-402144: CRYPTO: Digital signature error: signature algorithm *sig* , hash algorithm *hash*

**Explanation** An error occurred during digital signature generation.

- *sig* —The signature algorithm, which can be either RSA or DSA
- *hash* —The hash algorithm, which can be any of the following: MD5, SHA1, SHA256, SHA384, or SHA512

**Recommended Action** Contact the Cisco TAC for assistance.

## 402145

**Error Message** %ASA-3-402145: CRYPTO: Hash generation error: algorithm *hash*

**Explanation** A hash generation error occurred.

- *hash* —The hash algorithm, which can be any of the following: MD5, SHA1, SHA256, SHA384, or SHA512

**Recommended Action** Contact the Cisco TAC for assistance.

## 402146

**Error Message** %ASA-3-402146: CRYPTO: Keyed hash generation error: algorithm *hash* , key *len*

**Explanation** A keyed hash generation error occurred.

- *hash* —The hash algorithm, which can be any of the following: MD5, SHA1, SHA256, SHA384, or SHA512
- *len* —The key length in bits

**Recommended Action** Contact the Cisco TAC for assistance.

## 402147

**Error Message** %ASA-3-402147: CRYPTO: HMAC generation error: algorithm *alg*

**Explanation** An HMAC generation error occurred.

- *alg* —The HMAC algorithm, which can be any of the following: HMAC-MD5, HMAC-SHA1, HMAC-SHA2, or AES-XCBC

**Recommended Action** Contact the Cisco TAC for assistance.

## 402148

**Error Message** %ASA-3-402148: CRYPTO: Random Number Generator error

**Explanation** A random number generator error occurred.

**Recommended Action** Contact the Cisco TAC for assistance.

## 402149

**Error Message** %ASA-3-402149: CRYPTO: weak *encryption type (length)* . Operation disallowed. Not FIPS 140-2 compliant

**Explanation** The Secure Firewall ASA tried to use an RSA key that is less than 2048 bits or DH groups 1, 2, or 5.

- *encryption type* —The encryption type
- *length* —The RSA key length or DH group number

**Recommended Action** Configure the Secure Firewall ASA or external application to use an RSA key that is at least 2048 bits, or to configure a DH group that is not 1, 2, or 5.

## 402150

**Error Message** %ASA-3-402150: CRYPTO: Deprecated hash algorithm used for RSA operation (*hash alg*). Operation disallowed. Not FIPS 140-2 compliant

**Explanation** An unacceptable hashing algorithm has been used for digital certificate signing or verification for FIPS 140-2 certification.

- *operation* —Sign or verify
- *hash alg* —The name of the unacceptable hashing algorithm

**Recommended Action** Make sure that you use the minimum acceptable hashing algorithm for digital certificate signing or verification for FIPS 140-2 certification. These include SHA-256, SHA-384, and SHA-512.

## 403101

**Error Message** %ASA-4-403101: PPTP session state not established, but received an XGRE packet, tunnel\_id=*number* , session\_id=*number*

**Explanation** The ASA received a PPTP XGRE packet without a corresponding control connection session.

**Recommended Action** If the problem persists, contact the Cisco TAC.

## 403102

**Error Message** %ASA-4-403102: PPP virtual interface *interface\_name* rcvd pkt with invalid protocol: *protocol* , reason: *reason* .

**Explanation** The module received an XGRE encapsulated PPP packet with an invalid protocol field.

**Recommended Action** If the problem persists, contact the Cisco TAC.

## 403103

**Error Message** %ASA-4-403103: PPP virtual interface max connections reached.

**Explanation** The module cannot accept additional PPTP connections. Connections are allocated as soon as they are available.

**Recommended Action** None required.

## 403104

**Error Message** %ASA-4-403104: PPP virtual interface *interface\_name* requires mschap for MPPE.

**Explanation** The MPPE was configured, but MS-CHAP authentication was not.

**Recommended Action** Add MS-CHAP authentication with the **vpdn group *group\_name* ppp authentication** command.

## 403106

**Error Message** %ASA-4-403106: PPP virtual interface *interface\_name* requires RADIUS for MPPE.

**Explanation** The MPPE was configured, but RADIUS authentication was not.

**Recommended Action** Add RADIUS authentication with the **vpdn group group\_name ppp authentication** command.

## 403107

**Error Message** %ASA-4-403107: PPP virtual interface *interface\_name* missing aaa server group info

**Explanation** The AAA server configuration information cannot be found.

**Recommended Action** Add the AAA server information with the **vpdn group group\_name client authentication aaa aaa\_server\_group** command.

## 403108

**Error Message** %ASA-4-403108: PPP virtual interface *interface\_name* missing client ip address option

**Explanation** The client IP address pool information is missing.

**Recommended Action** Add IP address pool information with the **vpdn group group\_name client configuration address local address\_pool\_name** command.

## 403109

**Error Message** %ASA-4-403109: Rec'd packet not an PPTP packet. (ip ) dest\_address=*dest\_address*, src\_addr= *source\_address*, data: string.

**Explanation** The module received a spoofed PPTP packet, which may indicate a hostile event.

**Recommended Action** Contact the administrator of the peer to check the PPTP configuration settings.

## 403110

**Error Message** %ASA-4-403110: PPP virtual interface *interface\_name* , user: *user* missing MPPE key from aaa server.

**Explanation** The AAA server was not returning the MPPE key attributes required to set up the MPPE encryption policy.

**Recommended Action** Check the AAA server configuration. If the AAA server cannot return MPPE key attributes, use local authentication instead by entering the **vpdn group group\_name client authentication local** command.

## 403500

**Error Message** %ASA-6-403500: PPPoE - Service name 'any' not received in PADO.  
Intf:*interface\_name* AC:*ac\_name* .

**Explanation** The Secure Firewall ASA requested the PPPoE service *any* from the access controller at the Internet service provider. The response from the service provider includes other services, but does not include

the service *any* . This is a discrepancy in the implementation of the protocol. The PADO packet is processed normally, and connection negotiations continue.

**Recommended Action** None required.

## 403501

**Error Message** %ASA-3-403501: PPPoE - Bad host-unique in PADO - packet dropped.  
 Intf: *interface\_name* AC: *ac\_name*

**Explanation** The Secure Firewall ASA sent an identifier called the host-unique value to the access controller. The access controller responded with a different host-unique value. The Secure Firewall ASA was unable to identify the corresponding connection request for this response. The packet was dropped, and connection negotiations were discontinued.

**Recommended Action** Contact the Internet service provider. Either the access controller at the service provider is mishandling the host-unique value, or the PADO packet is being forged.

## 403502

**Error Message** %ASA-3-403502: PPPoE - Bad host-unique in PADS - dropping packet.  
 Intf: *interface\_name* AC: *ac\_name*

**Explanation** The Secure Firewall ASA sent an identifier called the host-unique value to the access controller. The access controller responded with a different host-unique value. The Secure Firewall ASA was unable to identify the corresponding connection request for this response. The packet was dropped, and connection negotiations were discontinued.

**Recommended Action** Contact the Internet service provider. Either the access controller at the service provider is mishandling the host-unique value, or the PADO packet is being forged.

## 403503

**Error Message** %ASA-3-403503: PPPoE:PPP link down: *reason*

**Explanation** The PPP link has gone down. There are many reasons why this can happen. The first format will display a reason if PPP provides one.

**Recommended Action** Check the network link to ensure that the link is connected. The access concentrator may be down. Make sure that your authentication protocol matches the access concentrator and that your name and password are correct. Verify this information with your ISP or network support person.

## 403504

**Error Message** %ASA-3-403504: PPPoE:No 'vpdn group *group\_name* ' for PPPoE is created

**Explanation** PPPoE requires a dial-out configuration before starting a PPPoE session. In general, the configuration should specify a dialing policy, the PPP authentication, the username, and a password. The following example configures the Secure Firewall ASA for PPPoE dialout. The *my-username* and *my-password* commands are used to authenticate the access concentrator, using PAP if necessary.

For example:



```
ciscoasa# vpdn group my-pppoe request dialout pppoe
ciscoasa# vpdn group my-pppoe ppp authentication pap
ciscoasa# vpdn group my-pppoe localname my-username
ciscoasa# vpdn username my-username password my-password
ciscoasa# ip address outside pppoe setroute
```

**Recommended Action** Configure a VPDN group for PPPoE.

## 403505

**Error Message** %ASA-4-403505: PPPoE:PPP - Unable to set default route to *IP\_address* at *interface\_name*

**Explanation** This message is usually followed by the message, default route already exists.

**Recommended Action** Remove the current default route or remove the *setroute* parameter so that there is no conflict between PPPoE and the manually configured route.

## 403506

**Error Message** %ASA-4-403506: PPPoE:failed to assign PPP *IP\_address* netmask *netmask* at *interface\_name*

**Explanation** This message is followed by one of the followings messages: subnet is the same as interface, or on failover channel.

**Recommended Action** In the first case, change the address causing the conflict. In the second case, configure the PPPoE on an interface other than the failover interface.

## 403507

**Error Message** %ASA-3-403507: PPPoE:PPPoE client on interface *interface* failed to locate PPPoE vpdn group *group\_name*

**Explanation** You can configure the PPPoE client on an interface to use a particular VPDN group by entering the **pppoe client vpdn group *group\_name*** command. If a PPPoE VPDN group of the configured name was not located during system startup, this message is generated.

- *interface* —The interface on which the PPPoE client failed
- *group\_name* —The VPDN group name of the PPPoe client on the interface

**Recommended Action** Perform the following steps:

1. Add the required VPDN group by entering the **vpdn group *group\_name*** command. Request dialout PPPoE in global configuration mode, and add all the group properties.
2. Remove the **pppoe client vpdn group *group\_name*** command from the interface indicated. In this case, the PPPoE client will attempt to use the first PPPoE VPDN group defined.



**Note** All changes take effect only after the PPPoE client on the interface is restarted by entering the **ip address pppoe** command.

## 405001

**Error Message** %ASA-4-405001: Received ARP {request | response} collision from *IP\_address* /*MAC\_address* on interface *interface\_name* with existing ARP entry *IP\_address* /*MAC\_address*

**Explanation** The Secure Firewall ASA received an ARP packet, and the MAC address in the packet differs from the ARP cache entry.

**Recommended Action** This traffic might be legitimate, or it might indicate that an ARP poisoning attack is in progress. Check the source MAC address to determine where the packets are coming from and to see if they belong to a valid host.

## 405002

**Error Message** %ASA-4-405002: Received mac mismatch collision from *IP\_address* /*MAC\_address* for authenticated host

**Explanation** This packet appears for one of the following conditions:

- The Secure Firewall ASA received a packet with the same IP address, but a different MAC address from one of its uauth entries.
- You configured the **vpncient mac-exempt** command on the Secure Firewall ASA, and the Secure Firewall ASA received a packet with an exempt MAC address, but a different IP address from the corresponding uauth entry.

**Recommended Action** This traffic might be legitimate, or it might indicate that a spoofing attack is in progress. Check the source MAC address and IP address to determine where the packets are coming from and if they belong to a valid host.

## 405003

**Error Message** %ASA-4-405003: IP address collision detected between host *IP\_address* at *MAC\_address* and interface *interface\_name* , *MAC\_address* .

**Explanation** A client IP address in the network is the same as the Secure Firewall ASA interface IP address.

**Recommended Action** Change the IP address of the client.

## 405101

**Error Message** %ASA-4-405101: Unable to Pre-allocate H225 Call Signalling Connection for *foreign\_address* *outside\_address* [/*outside\_port* ] to local\_address *inside\_address* [/*inside\_port* ]

**Explanation** The module failed to allocate RAM system memory while starting a connection or has no more address translation slots available.

**Recommended Action** If this message occurs periodically, it can be ignored. You can check the size of the global pool compared to the number of inside network clients. A PAT address may be necessary. Alternatively, shorten the timeout interval of translates and connections. This error message may also be caused by insufficient memory; try reducing the amount of memory usage, or purchasing additional memory. If the problem persists, contact the Cisco TAC.

## 405102

**Error Message** %ASA-4-405102: Unable to Pre-allocate H245 Connection for foreign\_address outside\_address [/outside\_port ] to local\_address inside\_address [/inside\_port ]

**Explanation** The Secure Firewall ASA failed to allocate RAM system memory while starting a connection or has no more address translation slots available.

**Recommended Action** Check the size of the global pool compared to the number of inside network clients. A PAT address may be necessary. Alternatively, shorten the timeout interval of translations and connections. In addition, reduce the amount of memory usage, or purchase additional memory. If this message occurs periodically, it can be ignored. If the problem persists, contact the Cisco TAC.

## 405103

**Error Message** %ASA-4-405103: H225 message from source\_address/source\_port to dest\_address /dest\_port contains bad protocol discriminator hex

**Explanation** The Secure Firewall ASA is expecting the protocol discriminator, 0x08, but it received something other than 0x08. The endpoint may be sending a bad packet, or received a message segment other than the first segment. The packet is allowed through.

**Recommended Action** None required.

## 405104

**Error Message** %ASA-4-405104: H225 message received from outside\_address /outside\_port to inside\_address /inside\_port before SETUP

**Explanation** An H.225 message was received out of order, before the initial SETUP message, which is not allowed. The Secure Firewall ASA must receive an initial SETUP message for that H.225 call signalling channel before accepting any other H.225 messages.

**Recommended Action** None required.

## 405105

**Error Message** %ASA-4-405105: H323 RAS message AdmissionConfirm received from source\_address /source\_port to dest\_address /dest\_port without an AdmissionRequest

**Explanation** A gatekeeper has sent an ACF, but the Secure Firewall ASA did not send an ARQ to the gatekeeper.

**Recommended Action** Check the gatekeeper with the specified **source\_address** to determine why it sent an ACF without receiving an ARQ from the Secure Firewall ASA.

## 405106

**Error Message** %ASA-4-405106: H323 num channel is not created from %I/%d to %I/%d %s

**Explanation** The ASA tried to create a match condition on the H.323 media-type channel. See the **match media-type** command for more information.

**Recommended Action** None required.

## 405107

**Error Message** %ASA-4-405107: H245 Tunnel is detected and connection dropped from %I/%d to %I/%d %s

**Explanation** An H.323 connection has been dropped because of an attempted H.245 tunnel control during call setup. See the **h245-tunnel-block** command for more information.

**Recommended Action** None required.

## 405201

**Error Message** %ASA-4-405201: ILS *ILS\_message\_type* from *inside\_interface:source\_IP\_address* to *outside\_interface:/destination\_IP\_address* has wrong embedded address *embedded\_IP\_address*

**Explanation** The embedded address in the ILS packet payload was not the same as the source IP address of the IP packet header.

**Recommended Action** Check the host specified with the **source\_IP\_address** to determine why it sent an ILS packet with an incorrect embedded IP address.

## 405300

**Error Message** %ASA-4-405300: Radius Accounting Request received from *from\_addr* is not allowed

**Explanation** The accounting request came from a host that was not configured in the policy map. The message is logged and processing stops.

- *from\_addr* —The IP address of the host sending the request

**Recommended Action** If the host was configured to send RADIUS accounting messages to the ASA, make sure that it was configured in the correct policy map that was applied to the service policy. If the host was not configured to send RADIUS accounting messages to the ASA, then check to see why the messages are being sent. If the messages are illegitimate, then create the proper ACLs to drop the packets.

## 405301

**Error Message** %ASA-4-405301: Attribute *attribute\_number* does not match for user *user\_ip*

**Explanation** When the **validate-attribute** command was entered, the attribute values stored in the accounting request start received do not match those stored in the entry, if it exists.

- *attribute\_number* —The RADIUS attribute to be validated with RADIUS accounting. Values range from 1 to 191. Vendor-specific attributes are not supported.
- *user\_ip* —The IP address (framed IP attribute) of the user.

**Recommended Action** None required.

## 406001

**Error Message** %ASA-4-406001: FTP port command low port: *IP\_address /port* to *IP\_address* on interface *interface\_name*

**Explanation** A client entered an FTP port command and supplied a port less than 1024 (in the well-known port range usually devoted to server ports). This is indicative of an attempt to avert the site security policy. The Secure Firewall ASA drops the packet, terminates the connection, and logs the event.

**Recommended Action** None required.

## 406002

**Error Message** %ASA-4-406002: FTP port command different address: IP\_address(*IP\_address*) to *IP\_address* on interface *interface\_name*

**Explanation** A client entered an FTP port command and supplied an address other than the address used in the connection. An attempt to avert the site security policy occurred. For example, an attacker might attempt to hijack an FTP session by changing the packet on the way, and putting different source information instead of the correct source information. The Secure Firewall ASA drops the packet, terminates the connection, and logs the event. The address in parentheses is the address from the port command.

**Recommended Action** None required.

## 407001

**Error Message** %ASA-4-407001: Deny traffic for local-host *interface\_name* :*inside\_address* , license limit of *number* exceeded

**Explanation** The host limit was exceeded. An inside host is counted toward the limit when one of the following conditions is true:

- The inside host has forwarded traffic through the Secure Firewall ASA within the last five minutes.
- The inside host has reserved an xlate connection or user authentication at the Secure Firewall ASA.

**Recommended Action** The host limit is enforced on the low-end platforms. Use the **show version** command to view the host limit. Use the **show local-host** command to view the current active hosts and the inside users that have sessions at the Secure Firewall ASA. To forcefully disconnect one or more users, use the **clear local-host** command. To expire the inside users more quickly from the limit, set the xlate, connection, and uauth timeouts to the recommended values or lower as given in the table below:

**Table 47: Timeouts and Recommended Values**

Timeout	Recommended Value
xlate	00:05:00 (five minutes)
conn	00:01:00 (one hour)
uauth	00:05:00 (five minutes)

## 407002

**Error Message** %ASA-4-407002: Embryonic limit *nconns* /*elimit* for through connections exceeded.*outside\_address* /*outside\_port* to *global\_address* (*inside\_address*) /*inside\_port* on interface *interface\_name*

**Explanation** The number of connections from a specified foreign address over a specified global address to the specified local address exceeded the maximum embryonic limit for that static. The Secure Firewall ASA tries to accept the connection if it can allocate memory for that connection. It proxies on behalf of the local host and sends a SYN\_ACK packet to the foreign host. The Secure Firewall ASA retains pertinent state information, drops the packet, and waits for the acknowledgment from the client. The message might indicate legitimate traffic or that a DoS attack is in progress.

**Recommended Action** Check the source address to determine where the packets are coming from and whether or not a valid host is sending them.

## 407003

**Error Message** %ASA-4-407003: Established limit for RPC services exceeded number

**Explanation** The Secure Firewall ASA tried to open a new hole for a pair of RPC servers or services that have already been configured after the maximum number of holes has been met.

**Recommended Action** Wait for other holes to be closed (through associated timeout expiration), or limit the number of active pairs of servers or services.

## 408001

**Error Message** %ASA-4-408001: IP route counter negative - reason , IP\_address Attempt: number

**Explanation** An attempt to decrement the IP route counter into a negative value failed.

**Recommended Action** Enter the **clear ip route** command to reset the route counter. If the problem persists, contact the Cisco TAC.

## 408002

**Error Message** %ASA-4-408002: ospf process id route type update address1 netmask1  
[distance1/metric1 ] via source IP :interface1 address2 netmask2 [distance2 /metric2 ]  
interface2

**Explanation** A network update was received from a different interface with the same distance and a better metric than the existing route. The new route overrides the existing route that was installed through another interface. The new route is for redundancy purposes only and means that a path has shifted in the network. This change must be controlled through topology and redistribution. Any existing connections affected by this change are probably disabled and will time out. This path shift only occurs if the network topology has been specifically designed to support path redundancy, in which case it is expected.

**Recommended Action** None required.

## 408003

**Error Message** %ASA-4-408003: can't track this type of object hex

**Explanation** A component of the tracking system has encountered an object type that is not supported by the component. A STATE object was expected.

- *hex* —A hexadecimal value(s) depicting variable value(s) or addresses in memory

**Recommended Action** Reconfigure the track object to make it a STATE object.

## 408101

**Error Message** %ASA-4-408101: KEYMAN : Type *encription\_type* encryption unknown. Interpreting keystring as literal.

**Explanation** The format type was not recognized by the system. A keystring format type value of 0 (unencrypted keystring) or 7 (hidden keystring), followed by a space, can precede the actual keystring to indicate its format. An unknown type value will be accepted, but the system will consider the keystring as being unencrypted.

**Recommended Action** Use the correct format for the value type or remove the space following the value type.

## 408102

**Error Message** %ASA-4-408102: KEYMAN : Bad encrypted keystring for key id *key\_id*.

**Explanation** The system could not successfully decrypt an encrypted keystring. The keystring may have been corrupted during system configuration.

**Recommended Action** Re-enter the key-string command, and reconfigure the key string.

## 409001

**Error Message** %ASA-4-409001: Database scanner: external LSA *IP\_address netmask* is lost, reinstalls

**Explanation** The software detected an unexpected condition. The router will take corrective action and continue.

**Recommended Action** None required.

## 409002

**Error Message** %ASA-4-409002: db\_free: external LSA *IP\_address netmask*

**Explanation** An internal software error occurred.

**Recommended Action** None required.

## 409003

**Error Message** %ASA-4-409003: Received invalid packet: *reason* from *IP\_address* , *interface\_name*

**Explanation** An invalid OSPF packet was received. Details are included in the error message. The cause might be an incorrect OSPF configuration or an internal error in the sender.

**Recommended Action** Check the OSPF configuration of the receiver and the sender configuration for inconsistency.

## 409004

**Error Message** %ASA-4-409004: Received reason from unknown neighbor *IP\_address*

**Explanation** The OSPF hello, database description, or database request packet was received, but the router cannot identify the sender.

**Recommended Action** None required.

## 409005

**Error Message** %ASA-4-409005: Invalid length number in OSPF packet from *IP\_address* (ID *IP\_address* ), *interface\_name*

**Explanation** The Secure Firewall ASA received an OSPF packet with a field length of less than normal header size or that was inconsistent with the size of the IP packet in which it arrived. This indicates a configuration error in the sender of the packet.

**Recommended Action** From a neighboring address, locate the problem router and reboot it.

## 409006

**Error Message** %ASA-4-409006: Invalid lsa: *reason* Type number , LSID *IP\_address* from *IP\_address* , *IP\_address* , *interface\_name*

**Explanation** The router received an LSA with an invalid LSA type. The cause is either memory corruption or unexpected behavior on a router.

**Recommended Action** From a neighboring address, locate the problem router and reboot it. If the problem persists, contact the Cisco TAC.

## 409007

**Error Message** %ASA-4-409007: Found LSA with the same host bit set but using different mask  
LSA ID *IP\_address netmask* New: Destination *IP\_address netmask*

**Explanation** An internal software error occurred.

**Recommended Action** Copy the message exactly as it appears, and report it to the Cisco TAC.

## 409008

**Error Message** %ASA-4-409008: Found generating default LSA with non-zero mask LSA type: *number*  
Mask: *netmask* metric: *number* area: *string*

**Explanation** The router tried to generate a default LSA with an incorrect mask and possibly incorrect metric because an internal software error occurred.

**Recommended Action** Copy the message exactly as it appears, and report it to the Cisco TAC.

## 409009

**Error Message** %ASA-4-409009: OSPF process number cannot start. There must be at least one up IP interface, for OSPF to use as router ID

**Explanation** OSPF failed while attempting to allocate a router ID from the IP address of one of its interfaces.



**Recommended Action** Make sure that there is at least one interface that is up and has a valid IP address. If there are multiple OSPF processes running on the router, each requires a unique router ID. You must have enough interfaces up so that each of them can obtain a router ID.

## 409010

**Error Message** %ASA-4-409010: Virtual link information found in non-backbone area: *string*

**Explanation** An internal error occurred.

**Recommended Action** Copy the message exactly as it appears, and report it to the Cisco TAC.

## 409011

**Error Message** %ASA-4-409011: OSPF detected duplicate router-id *IP\_address* from *IP\_address* on interface *interface\_name*

**Explanation** OSPF received a hello packet from a neighbor that has the same router ID as this routing process. A full adjacency cannot be established.

**Recommended Action** The OSPF router ID should be unique. Change the neighbor router ID.

## 409012

**Error Message** %ASA-4-409012: Detected router with duplicate router ID *IP\_address* in area *string*

**Explanation** OSPF received a hello packet from a neighbor that has the same router ID as this routing process. A full adjacency cannot be established.

**Recommended Action** The OSPF router ID should be unique. Change the neighbor router ID.

## 409013

**Error Message** %ASA-4-409013: Detected router with duplicate router ID *IP\_address* in Type-4 LSA advertised by *IP\_address*

**Explanation** OSPF received a hello packet from a neighbor that has the same router ID as this routing process. A full adjacency cannot be established.

**Recommended Action** The OSPF router ID should be unique. Change the neighbor router ID.

## 409014

**Error Message** %ASA-4-409014: No valid authentication *send* key is available on interface *nameif*.

**Explanation** The authentication key configured on the interface is not valid.

**Recommended Action** Configure a new key.

## 409015

**Error Message** %ASA-4-409015: Key ID *key-id* received on interface *nameif*.

**Explanation** The ID is not found in the configured key chain.

**Recommended Action** Configure a new security association with the Key ID.

## 409016

**Error Message** %ASA-4-409016: Key chain name *key-chain-name* on *nameif* is invalid.

**Explanation** The key-chain name configured under OSPF interface does not match global key chain configuration.

**Recommended Action** Fix configuration. Either remove OSPF authentication command or configure key chain in global configuration mode.

## 409017

**Error Message** %ASA-4-409017: Key ID *key-id* in key chain *key-chain-name* is invalid.

**Explanation** The Key ID configured in the key chain is out of range for OSPF. This may happen because the key chain allows Key ID values of the range which is not acceptable for OSPF.

**Recommended Action** Configure a new security association with a Key ID that is in the range 1-255.

## 409023

**Error Message** %ASA-4-409023: Attempting AAA Fallback method *method\_name* for *request\_type* request for user *user* :Auth-server group *server\_tag* unreachable

**Explanation** An authentication or authorization attempt to an external server has failed and will be performed using the local user database.

- **aaa\_operation**—Either authentication or authorization
- **username**—The user associated with the connection
- **server\_group**—The name of the AAA server whose servers were unreachable

**Recommended Action** Investigate any connectivity problems with the AAA servers configured in the first method. Ping the authentication servers from the Secure Firewall ASA. Make sure that the daemons are running on the AAA server.

## 409101

**Error Message** %ASA-4-409101: Received invalid packet: *s* from *P* , *s*

**Explanation** An invalid OSPF packet was received. Details are included in the error message. The cause might be a misconfigured OSPF or an internal error in the sender.

**Recommended Action** Check the OSPF configuration of the receiver and the sender for inconsistencies.

## 409102

**Error Message** %ASA-4-409102: Received packet with incorrect area from P , s , area AREA\_ID\_STR , packet area AREA\_ID\_STR

**Explanation** An OSPF packet was received with an area ID in its header that does not match the area of this interface.

**Recommended Action** Check the OSPF configuration of the receiver and the sender for inconsistencies.

## 409103

**Error Message** %ASA-4-409103: Received s from unknown neighbor i

**Explanation** An OSPF hello, database description, or database request packet was received, but the router could not identify the sender.

**Recommended Action** None required.

## 409104

**Error Message** %ASA-4-409104: Invalid length d in OSPF packet type d from P (ID i ) , s

**Explanation** The system received an OSPF packet with a length field of less than normal header size or inconsistent with the size of the IP packet in which it arrived. An error in the sender of the packet has occurred.

**Recommended Action** None required.

## 409105

**Error Message** %ASA-4-409105: Invalid lsa: s : Type 0x x , Length 0x x , LSID u from i

**Explanation** The router received an LSA with invalid data. The LSA includes an invalid LSA type, incorrect checksum, or incorrect length, which is caused by either memory corruption or unexpected behavior on a router.

**Recommended Action** From a neighboring address, locate the problem router and do the following:

- Collect a running configuration of the router by entering the **show running-config** command.
- Enter the **show ipv6 ospf database** command to gather data that may help identify the nature of the error.
- Enter the **show ipv6 ospf database link-state-id** command. The *link-state-id* argument is the IP address of the invalid LSA.
- Enter the **show logging** command to gather data that may help identify the nature of the error.
- Reboot the router.

If you cannot determine the nature of the error from the collected information, contact the Cisco TAC and provide the gathered information.

## 409106

**Error Message** %ASA-4-409106: Found generating default LSA with non-zero mask LSA type: 0x x Mask: i metric: lu area: AREA\_ID\_STR

**Explanation** The router tried to generate the default LSA with the incorrect mask and possibly an incorrect metric because of an internal software error.

**Recommended Action** None required.

## 409107

**Error Message** %ASA-4-409107: OSPFv3 process *d* could not pick a router-id, please configure manually

**Explanation** OSPFv3 failed while attempting to allocate a router ID from the IP address of one of its interfaces.

**Recommended Action** Make sure that there is at least one interface that is up and has a valid IP address. If there are multiple OSPF processes running on the router, each requires a unique router ID. You must have enough up interfaces so that each of them can obtain a router ID.

## 409108

**Error Message** %ASA-4-409108: Virtual link information found in non-backbone area: *AREA\_ID\_STR*

**Explanation** An internal error has occurred.

**Recommended Action** None required.

## 409109

**Error Message** %ASA-4-409109: OSPF detected duplicate router-id *i* from *P* on interface *IF\_NAME*

**Explanation** OSPF received a hello packet from a neighbor that has the same router ID as this routing process. A full adjacency cannot be established. The OSPF router ID should be unique.

**Recommended Action** Change the neighbor router ID.

## 409110

**Error Message** %ASA-4-409110: Detected router with duplicate router ID *i* in area *AREA\_ID\_STR*

**Explanation** OSPF received a hello packet from a neighbor that has the same router ID as this routing process. A full adjacency cannot be established. The OSPF router ID should be unique.

**Recommended Action** Change the neighbor router ID.

## 409111

**Error Message** %ASA-4-409111: Multiple interfaces (*IF\_NAME* / *IF\_NAME* ) on a single link detected.

**Explanation** OSPFv3 enabled on multiple interfaces that are on the same link is not supported.

**Recommended Action** OSPFv3 should be disabled or made passive on all except one of the interfaces.

## 409112

**Error Message** %ASA-4-409112: Packet not written to the output queue

**Explanation** An internal error has occurred.

**Recommended Action** None required.

## 409113

**Error Message** %ASA-4-409113: Doubly linked list linkage is NULL

**Explanation** An internal error has occurred.

**Recommended Action** None required.

## 409114

**Error Message** %ASA-4-409114: Doubly linked list prev linkage is NULL x

**Explanation** An internal error has occurred.

**Recommended Action** None required.

## 409115

**Error Message** %ASA-4-409115: Unrecognized timer *d* in OSPF *s*

**Explanation** An internal error has occurred.

**Recommended Action** None required.

## 409116

**Error Message** %ASA-4-409116: Error for timer *d* in OSPF process *s*

**Explanation** An internal error has occurred.

**Recommended Action** None required.

## 409117

**Error Message** %ASA-4-409117: Can't find LSA database type *x* , area *AREA\_ID\_STR* , interface *x*

**Explanation**An internal error has occurred.

**Recommended Action** None required.

## 409118

**Error Message** %ASA-4-409118: Could not allocate DBD packet

**Explanation**An internal error has occurred.

**Recommended Action** None required.

## 409119

**Error Message** %ASA-4-409119: Invalid build flag x for LSA i , type 0x x

**Explanation** An internal error has occurred.

**Recommended Action** None required.

## 409120

**Error Message** %ASA-4-409120: Router-ID i is in use by ospf process d

**Explanation** The Secure Firewall ASA attempted to assign a router ID that is in use by another process.

**Recommended Action** Configure another router ID for one of the processes.

## 409121

**Error Message** %ASA-4-409121: Router is currently an ASBR while having only one area which is a stub area

**Explanation** An ASBR must be attached to an area that can carry AS External or NSSA LSAs.

**Recommended Action** Make the area to which the router is attached into an NSSA or regular area.

## 409122

**Error Message** %ASA-4-409122: Could not select a global IPv6 address. Virtual links require at least one global IPv6 address.

**Explanation** A virtual link was configured. For the virtual link to function, a global IPv6 address must be available. However, no global IPv6 address could be found on the router.

**Recommended Action** Configure a global IPv6 address on an interface on this router.

## 409123

**Error Message** %ASA-4-409123: Neighbor command allowed only on NBMA networks

**Explanation** The **neighbor** command is allowed only on NBMA networks.

**Recommended Action** Check the configuration options for the **neighbor** command, and correct the options or the network type for the neighbor interface.

## 409125

**Error Message** %ASA-4-409125: Can not use configured neighbor: poll and priority options are allowed only for a NBMA network

**Explanation** The configured neighbor was found on a point-to-multipoint network and either the poll or priority option was configured. These options are only allowed on NBMA type networks.

**Recommended Action** Check the configuration options for the **neighbor** command, and correct the options or the network type for the neighbor interface.

## 409128

**Error Message** %ASA-4-409128: OSPFv3-d Area *AREA\_ID\_STR* : Router *i* originating invalid type *0x x* LSA, ID *u* , Metric *d* on Link ID *d* Link Type *d*

**Explanation** The router indicated in this message has originated an LSA with an invalid metric. If this is a router LSA and the link metric is zero, a risk of routing loops and traffic loss exists in the network.

**Recommended Action** Configure a valid metric for the given LSA type and link type on the router that originated the reported LSA.

## Messages 410001 to 450001

This chapter includes messages from 410001 to 450001.

### 410001

**Error Message** %ASA-4-410001: UDP DNS request from *source\_interface* :*source\_address* /*source\_port* to *dest\_interface* :*dest\_address* /*dest\_port* ; (label length | domain-name length)*number* bytes exceeds remaining packet length of 63 bytes.

**Explanation** The label length exceeds bytes in a UDP DNS packet. See RFC 1035, section 2.3.4 for more information. .

**Recommended Action** Create the policy-map and add a custom DNS class-map to match traffic and exclude it from inspection to allow packets exceeding the label length.

### 410002

**Error Message** %ASA-2-410002: Dropped *num* DNS responses with mis-matched id in the past *sec* second(s): from *src\_ifc* :*sip* /*sport* to *dest\_ifc* :*dip* /*dport*

**Explanation** The ASA detects an excess number of DNS responses with a mismatched DNS identifier. A high rate of mismatched DNS identifiers might indicate an attack on the cache. The threshold is set by the **id-mismatch** DNS policy-map parameter submode command.

- *num* —The number of ID mismatch instances as configured by the **id-mismatch** command
- *sec* —The duration in seconds as configured by the **id-mismatch** command
- *src\_ifc* —The source interface name at which the DNS message is received with a mismatched DNS identifier
- *sip* —The source IP address
- *sport* —The source port
- *dest\_ifc* —The destination interface name
- *dip* —The destination IP address
- *dport* —The destination port

**Recommended Action** Check the IP address and port in the message to trace the source of the attack. You can configure ACLs to block traffic permanently from the source.

## 410003

**Error Message** %ASA-4-410003: *action\_class* : *action* DNS *query\_response* from *src\_ifc* :*sip* /*sport* to *dest\_ifc* :*dip* /*dport* ; *further\_info*

**Explanation** A DNS classification was performed on a DNS message and the specified criteria were satisfied. As a result, the configured action occurs.

- *action\_class* —The DNS Classification action class
- *action* —The action taken: Dropped, Dropped (no TSIG), or Masked header flags for
- *query\_response* —Either query or response
- *src\_ifc* —The source interface name
- *sip* —The source IP address
- *sport* —The source port
- *dest\_ifc* —The destination interface name
- *dip* —The destination IP address
- *dport* —The destination port
- *further\_info* —One of the following: matched Class id: *class\_name* , matched Class id: *match\_command* (for a standalone **match** command), or TSIG resource record not present (for messages generated by the **tsig enforced** command)

**Recommended Action** None required.

## 410004

**Error Message** %ASA-6-410004: *action\_class* : *action* DNS *query\_response* from *src\_ifc* :*sip* /*sport* to *dest\_ifc* :*dip* /*dport* ; *further\_info*

**Explanation** A DNS classification was performed on a DNS message and the specified criteria were satisfied.

- *action\_class* —The DNS Classification action class
- *action* —The action taken: Received or Received (no TSIG)
- *query\_response* —Either query or response
- *src\_ifc* —The source interface name
- *sip* —The source IP address
- *sport* —The source port
- *dest\_ifc* —The destination interface name
- *dip* —The destination IP address
- *dport* —The destination port
- *further\_info* —One of the following: matched Class id: *class\_name* , matched Class id: *match\_command* (for a standalone **match** command), or TSIG resource record not present (for messages generated by the **tsig enforced** command)

**Recommended Action** None required.

## 411001

**Error Message** %ASA-4-411001: Line protocol on interface *interface\_name* changed state to up

**Explanation** The status of the line protocol has changed from down to up . If **interface\_name** is a logical interface name such as inside and outside, this message indicates that the logical interface line protocol has



changed from down to up . If **interface\_name** is a physical interface name such as Ethernet0 and GigabitEthernet0/1, this message indicates that the physical interface line protocol has changed from down to up .

**Recommended Action** None required.

## 411002

**Error Message** %ASA-4-411002:Line protocol on interface *interface\_name* changed state to down

**Explanation** The status of the line protocol has changed from up to down. If **interface\_name** is a logical interface name such as inside and outside, this message indicates that the logical interface line protocol has changed from up to down. In this case, the physical interface line protocol status is not affected. If **interface\_name** is a physical interface name such as Ethernet0 and GigabitEthernet0/1, this message indicates that the physical interface line protocol has changed from up to down.

**Recommended Action** If this is an unexpected event on the interface, check the physical line.

## 411003

**Error Message** %ASA-4-411003: Configuration status on interface *interface\_name* changed state to downup

**Explanation** The configuration status of the interface has changed from down to up.

**Recommended Action** If this is an unexpected event, check the physical line.

## 411004

**Error Message** %ASA-4-411004: Configuration status on interface *interface\_name* changed state to up

**Explanation** The configuration status of the interface has changed from down to up.

**Recommended Action** None required.

## 411005

**Error Message** %ASA-4-411005: Interface *variable 1* experienced a hardware transmit hang. The interface has been reset.

**Explanation** The interface experienced a hardware transmit freeze that required a reset of the Ethernet controller to restore the interface to full operation.

- *variable 1* —The interface name, such as GigabitEthernet0/0

**Recommended Action** None required.

## 412001

**Error Message** %ASA-4-412001:MAC *MAC\_address* moved from *interface\_1* to *interface\_2*

**Explanation** A host move was detected from one module interface to another. In a transparent Secure Firewall ASA, mapping between the host (MAC) and Secure Firewall ASA port is maintained in a Layer 2 forwarding

table. The table dynamically binds packet source MAC addresses to an Secure Firewall ASA port. In this process, whenever movement of a host from one interface to another interface is detected, this message is generated.

**Recommended Action** The host move might be valid or might be an attempt to spoof host MACs on other interfaces. If it is a MAC spoof attempt, you can either locate vulnerable hosts on your network and remove them or configure static MAC entries, which will not allow MAC address and port binding to change. If it is a genuine host move, no action is required.

## 412002

**Error Message** %ASA-4-412002: Detected bridge table full while inserting MAC *MAC\_address* on interface *interface* . Number of entries = *num*

**Explanation** The bridge table was full and an attempt was made to add one more entry. The Secure Firewall ASA maintains a separate Layer 2 forwarding table per context and the message is generated whenever a context exceeds its size limit. The MAC address will be added, but it will replace the oldest existing dynamic entry (if available) in the table. This might be an attempted attack.

**Recommended Action** Make sure that the new bridge table entries are valid. In case of attack, use EtherType ACLs to control access to vulnerable hosts.

## 413001

**Error Message** %ASA-4-413001: Module *module\_id* is not able to shut down. Module Error: *errnum message*

**Explanation** The module identified by *module\_id* was not able to comply with a request from the Secure Firewall ASA system module to shut down. It may be performing a task that cannot be interrupted, such as a software upgrade. The **errnum** and **message** text describes the reason why the module cannot shut down, and the recommended corrective action.

**Recommended Action** Wait for the task on the module to complete before shutting down the module, or use the **session** command to access the CLI on the module, and stop the task that is preventing the module from shutting down.

## 413002

**Error Message** %ASA-4-413002: Module *module\_id* is not able to reload. Module Error: *errnum message*

**Explanation** The module identified by *module\_id* was not able to comply with a request from the Secure Firewall ASA module to reload. It may be performing a task that cannot be interrupted, such as a software upgrade. The **errnum** and **message** text describes the reason why the module cannot reload, and the recommended corrective action.

**Recommended Action** Wait for the task on the module to complete before reloading the module, or use the **session** command to access the CLI on the module and stop the task that is preventing the module from reloading.

## 413003

**Error Message** %ASA-4-413003: Module *string one* is not a recognized type

**Explanation** A module was detected that is not recognized as a valid module type.

**Recommended Action** Upgrade to a version of Secure Firewall ASA software that supports the module type installed.

## 413004

**Error Message** %ASA-4-413004: Module *string one* failed to write software *newver* (currently *ver* ), *reason* . Trying again.

**Explanation** The module failed to accept a software version, and will be transitioned to an UNRESPONSIVE state. Another attempt will be made to update the module software.

- *>string one*— The text string that specifies the module
- *>newver* —The new version number of software that was not successfully written to the module (for example, 1.0(1)0)
- *>ver* —The current version number of the software on the module (for example, 1.0(1)0)
- *>reason* —The reason the new version cannot be written to the module. The possible values for *>reason* include the following:

- write failure

- failed to create a thread to write the image

**Recommended Action** None required. Subsequent attempts will either generate a message indicating a successful update or failure. You may verify the module transitions to UP after a subsequent update attempt by using the **show module** command.

## 413005

**Error Message** %ASA-4-413005: Module *module\_id* , application is not supported *app\_name* version *app\_vers* type *app\_type*

**Error Message** %ASA-4-413005: Module *prod\_id* in slot *slot\_num* , application is not supported *app\_name* version *app\_vers* type *app\_type*

**Explanation** The module installed in slot *slot\_num* was running an unsupported application version or type.

- *module\_id*— The name of the software services module
- *prod\_id* —Product ID string
- *slot\_num* —The slot number in which the module is installed. Slot 0 indicates the system main board, and slot 1 indicates the module installed in the expansion slot.
- *app\_name* —Application name (string)
- *app\_vers* —Application version (string)
- *app\_type* —Application type (decimal)

**Recommended Action** If the problem persists, contact the Cisco TAC.

## 413006

**Error Message** %ASA-4-413006: *prod-id* Module software version mismatch; slot *slot* is *prod-id* version *running-vers* . Slot *slot* *prod-id* requires *required-vers* .

**Explanation** The version of software running on the module in slot *slot* was not the version required by another module.

- *slot*—Slot 0 indicates the system main board. Slot 1 indicates the module installed in the expansion slot.
- *prod\_id*—Product ID string for the device installed in slot *slot*
- *running\_vers*—Version of software currently running on the module installed in slot *slot*
- *required\_vers*—Version of software required by the module in slot *slot*

**Recommended Action** If the problem persists, contact the Cisco TAC.

## 413007

**Error Message** %ASA-1-413007: An unsupported ASA and IPS configuration is installed. *mpc\_description* with *ips\_description* is not supported.

**Explanation** An unsupported Secure Firewall ASA and IPS configuration has been detected during IPS SSP setup for slot 1. The Secure Firewall ASA should continue to function normally with an unsupported configuration.

- *mpc\_description*—A description string for the ASA model, which can be one of the following: ASA5585-SSP-10, ASA5585-SSP-20, ASA5585-SSP-40, ASA5585-SSP-60, ASA5585-SSP-10-K7, ASA5585-SSP-20-K7, ASA5585-SSP-40-K7, ASA5585-SSP-60-K7.
- *ips\_description*—A description string for the IPS SSP model, which can be one of the following: ASA5585-SSP-IPS10, ASA5585-SSP-IPS20, ASA5585-SSP-IPS40, ASA5585-SSP-IPS60, ASA5585-SSP-P10K7, ASA5585-SSP-P20K7, ASA5585-SSP-P40K7, ASA5585-SSP-P60K7.

**Recommended Action** None required.

## 413008

**Error Message** %ASA-1-413008: An unsupported combination of the power supply module and the fan module is detected. Two power supply modules are recommended when using ASA 10G and IPS 10G SSPs simultaneously

**Explanation** Only one power supply and one fan module are inserted when an ASA 10G SSP and IPS 10G SSP are present.

**Recommended Action** When using an ASA 10G SSP and IPS 10G SSP, insert two power supplies instead of one fan module and one power supply module.

## 414001

**Error Message** %ASA-3-414001: Failed to save logging buffer using file name *filename* to FTP server *ftp\_server\_address* on interface *interface\_name* : [*fail\_reason* ]

**Explanation** The logging module failed to save the logging buffer to an external FTP server.

**Recommended Action** Take applicable actions based on the failed reason:

- Protocol error—Make sure no connectivity issue exists between the FTP server and Secure Firewall ASA, and that the FTP sever can accept the FTP port command and PUT requests.
- Invalid username or password—Make sure that the configured FTP client username and password are correct.
- All other errors—If the problem persists, contact the Cisco TAC.

## 414002

**Error Message** %ASA-3-414002: Failed to save logging buffer to flash:/syslog directory using file name: *filename* : [*fail\_reason* ]

**Explanation** The logging module failed to save the logging buffer to system flash.

**Recommended Action** If the failed reason is caused by insufficient space, check the flash free space, and make sure that the configured limits of the **logging flash-size** command are set correctly. If the error is a flash file system I/O error, then contact the Cisco TAC for assistance.

## 414003

**Error Message** %ASA-3-414003: TCP Syslog Server *intf* : *IP\_Address* /*port* not responding. New connections are [permitted|denied] based on logging permit-hostdown policy.

**Explanation** The TCP syslog server for remote host logging was successful, is connected to the server, and new connections are permitted or denied based on the logging permit-hostdown policy. If the logging permit-hostdown policy is configured, a new connection is permitted. If not configured, a new connection is denied.

- *intf*—Interface of the Secure Firewall ASA to which the server is connected
- *IP\_Address* —IP address of the remote TCP syslog server
- *port* —Port of the remote TCP syslog server

**Recommended Action** Validate that the configured TCP syslog server is up. To permit new connections, configure the logging permit-hostdown policy. To deny new connections, do not configure the logging permit-hostdown policy.

## 414004

**Error Message** %ASA-6-414004: TCP Syslog Server *intf* : *IP\_Address* /*port* - Connection restored

**Explanation** The TCP syslog setup involves 4 channels connecting to the server. This message is generated only when one of the TCP syslog server channels become unreachable and the server is restored. This message is the first to reach the syslog server after a successful connection. This message is generated only on TCP syslog server.




---

**Note** This message does not appear every time when the TCP syslog server is restored. It appears only when the server is restored after one of its channels became unreachable.

---

- *intf*—Interface of the ASA to which the server is connected
- *IP\_Address* —IP address of the remote TCP syslog server

- *port* —Port of the remote TCP syslog server

**Recommended Action** None required.

## 414005

**Error Message** %ASA-3-414005: TCP Syslog Server *intf* : *IP\_Address* /*port* connected, New connections are permitted based on logging permit-hostdown policy

**Explanation** The TCP syslog server for remote host logging was successful, is connected to the server, and new connections are permitted based on the logging permit-hostdown policy. If the logging permit-hostdown policy is configured, a new connection is permitted.

- *intf* —Interface of the Secure Firewall ASA to which the server is connected
- *IP\_Address* —IP address of the remote TCP syslog server
- *port* —Port of the remote TCP syslog server

**Recommended Action** None required.

## 414006

**Error Message** %ASA-3-414006: TCP Syslog Server configured and logging queue is full. New connections denied based on logging permit-hostdown policy.

**Explanation** The logging queue is close to reaching the configured limit, so there is a risk that syslog messages will be discarded.

**Recommended Action** See the "Configuring the Logging Queue" section in the CLI configuration guide for information about how to tune the queue size to avoid this situation. If you want to deny new connections in this case, use the **no logging permit-hostdown** command. If you want to allow new connections in this case, use the **logging permit-hostdown** command.

## 414007

**Error Message** %ASA-6-414007: TCP Syslog Server connection restored. New connections are allowed.

**Explanation** The TCP syslog server for remote host logging was successfully connected and new connections are permitted.

**Recommended Action** None required.

## 414008

**Error Message** %ASA-6-414008: New connections are now allowed due to change of logging permit-hostdown policy.

**Explanation** An administrator changed the logging permit-hostdown policy by entering the **logging permit-hostdown** command at a time when new connections are being denied. Due to this change of policy, new connections will be allowed.

**Recommended Action** None required.

## 415001

**Error Message** %ASA-6-415001: HTTP - matched *matched\_string* in policy-map *map\_name* , header field count exceeded *connection\_action* from *int\_type* :*IP\_address* /*port\_num* to *int\_type* :*IP\_address* /*port\_num*

**Explanation** This message is generated when one of the following occurs:

- The total number of fields in the HTTP header exceeds the user-configured number of header fields. The relevant command is: **match {request | response} header count num.**
- The appearance of a specified field in the HTTP header exceeds the user-configured number for this header field. The relevant command is: **match {request | response} header header-name count num.**
- **matched\_string**—The matched string is one of the following:

- The class map ID, followed by the name of the class map. This string appears when the class map is user configured.

- The actual **match** command that initiated the message. This string appears when the class map is internal.

- *map\_name* —The name of the policy map
- *connection\_action* —Dropping the connection or resetting the connection
- *interface\_type* —The type of interface (for example, DMZ or outside)
- *IP\_address* —The IP address of the interface
- *port\_num* —The port number

**Recommended Action** Enter the **match {request | response} header** command to reconfigure the HTTP header field value.

## 415002

**Error Message** %ASA-6-415002: HTTP - matched *matched\_string* in policy-map *map\_name* , header field length exceeded *connection\_action* from *int\_type* :*IP\_address* /*port\_num* to *int\_type* :*IP\_address* /*port\_num*

**Explanation** The specified HTTP header field length exceeded the user-configured length.

- **matched\_string**—The matched string is one of the following:

- The class map ID, followed by the name of the class map. This string appears when the class map is user configured.

- The actual **match** command that initiated the message. This string appears when the class map is internal.

- *map\_name* —The name of the policy map
- *connection\_action* —Dropping connection or Resetting connection
- *interface\_type* —The type of interface (for example, DMZ or outside)
- *IP\_address* —The IP address of the interface
- *port\_num* —The port number

**Recommended Action** Enter the **match {request | response} header header\_name length gt num** command to change the HTTP header field length.

## 415003

**Error Message** %ASA-6-415003: HTTP - matched *matched\_string* in policy-map *map\_name* , body length exceeded *connection\_action* from *int\_type* :*IP\_address* /*port\_num* to *int\_type* :*IP\_address* /*port\_num*

**Explanation** The length of the message body exceeded the user-configured length.

- **matched\_string**—The matched string is one of the following:

- The class map ID, followed by the name of the class map. This string appears when the class map is user configured.

- The actual **match** command that initiated the message. This string appears when the class map is internal.

- *map\_name* —The name of the policy map
- *connection\_action* —Dropping the connection or resetting the connection
- *interface\_type* —The type of interface (for example, DMZ or outside)
- *IP\_address* —The IP address of the interface
- *port\_num* —The port number

**Recommended Action** Enter the **match {request | response} body length gt num** command to change the length of the message body.

## 415004

**Error Message** %ASA-5-415004: HTTP - matched *matched\_string* in policy-map *map\_name* , content-type verification failed *connection\_action* from *int\_type* :*IP\_address* /*port\_num* to *int\_type* :*IP\_address* /*port\_num*

**Explanation** The magic number in the body of the HTTP message is not the correct magic number for the MIME-type specified in the content-type field in the HTTP message header.

- **matched\_string**—The matched string is one of the following:

- The class map ID, followed by the name of the class map. This string appears when the class map is user configured.

- The actual **match** command that initiated the message. This string appears when the class map is internal.

- *map\_name* —The name of the policy map
- *connection\_action* —Dropping the connection or resetting the connection
- *interface\_type* —The type of interface (for example, DMZ or outside)
- *IP\_address* —The IP address of the interface
- *port\_num* —The port number

**Recommended Action** Enter the **match {request | response} header content-type violation** command to correct the error.

## 415005

**Error Message** %ASA-5-415005: HTTP - matched *matched\_string* in policy-map *map\_name* , URI length exceeded *connection\_action* from *int\_type* :*IP\_address* /*port\_num* to *int\_type* :*IP\_address* /*port\_num*



**Explanation** The length of the URI exceeded the user-configured length.

- **matched\_string**—The matched string is one of the following:

- The class map ID, followed by the name of the class map. This string appears when the class map is user configured.
- The actual **match** command that initiated the message. This string appears when the class map is internal.
  - *map\_name* —The name of the policy map
  - *connection\_action* —Dropping the connection or resetting the connection
  - *interface\_type* —The type of interface (for example, DMZ or outside)
  - *IP\_address* —The IP address of the interface
  - *port\_num* —The port number

**Recommended Action** Enter the **match request uri length gt num** command to change the length of the URI.

## 415006

**Error Message** %ASA-5-415006: HTTP - matched *matched\_string* in policy-map *map\_name* , URI matched *connection\_action* from *int\_type* :*IP\_address* /*port\_num* to *int\_type* :*IP\_address* /*port\_num*

**Explanation** The URI matched the regular expression that the user configured. See the **match request uri regex {regex-name | class class-name}** command for more information.

- **matched\_string**—The matched string is one of the following:

- The class map ID, followed by the name of the class map. This string appears when the class map is user configured.
- The actual **match** command that initiated the message. This string appears when the class map is internal.
  - *map\_name* —The name of the policy map
  - *connection\_action* —Dropping the connection or resetting the connection
  - *interface\_type* —The type of interface (for example, DMZ or outside)
  - *IP\_address* —The IP address of the interface
  - *port\_num* —The port number

**Recommended Action** None required.

## 415007

**Error Message** %ASA-5-415007: HTTP - matched *matched\_string* in policy-map *map\_name* , Body matched *connection\_action* from *int\_type* :*IP\_address* /*port\_num* to *int\_type* :*IP\_address* /*port\_num*

**Explanation** The message body matched the regular expression that the user configured. See the **match {request | response} body regex {regex-name | class class-name}** command for more information.

- **matched\_string**—The matched string is one of the following:

- The class map ID, followed by the name of the class map. This string appears when the class map is user configured.
- The actual **match** command that initiated the message. This string appears when the class map is internal.

- *map\_name* —The name of the policy map
- *connection\_action* —Dropping the connection or resetting the connection
- *interface\_type* —The type of interface (for example, DMZ or outside)
- *IP\_address* —The IP address of the interface
- *port\_num* —The port number

**Recommended Action** None required.

## 415008

**Error Message** %ASA-5-415008: HTTP - matched *matched\_string* in policy-map *map\_name* , header matched *connection\_action* from *int\_type* :*IP\_address* /*port\_num* to *int\_type* :*IP\_address* /*port\_num*

**Explanation** A value in a user-specified field in the message header matched the regular expression that the user configured. See the **match {request | response } header header-field-name {regex-name | class class-name}** command for more information.

- **matched\_string**—The matched string is one of the following:
  - The class map ID, followed by the name of the class map. This string appears when the class map is user configured.
  - The actual **match** command that initiated the message. This string appears when the class map is internal.
    - *map\_name* —The name of the policy map
    - *connection\_action* —Dropping the connection or resetting the connection
    - *interface\_type* —The type of interface (for example, DMZ or outside)
    - *IP\_address* —The IP address of the interface
    - *port\_num* —The port number

**Recommended Action** None required.

## 415009

**Error Message** %ASA-5-415009: HTTP - matched *matched\_string* in policy-map *map\_name* , method matched *connection\_action* from *int\_type* :*IP\_address* /*port\_num* to *int\_type* :*IP\_address* /*port\_num*

**Explanation** The HTTP method matched the user-configured regular expression. See the **match request method {regex-name | class class-name}** command for more information.

- **matched\_string**—The matched string is one of the following:
  - The class map ID, followed by the name of the class map. This string appears when the class map is user configured.
  - The actual **match** command that initiated the message. This string appears when the class map is internal.
    - *map\_name* —The name of the policy map
    - *connection\_action* —Dropping the connection or resetting the connection
    - *interface\_type* —The type of interface (for example, DMZ or outside)
    - *IP\_address* —The IP address of the interface
    - *port\_num* —The port number

**Recommended Action** None required.

## 415010

**Error Message** %ASA-5-415010: matched *matched\_string* in policy-map *map\_name* , transfer encoding matched *connection\_action* from *int\_type* :*IP\_address* /*port\_num* to *int\_type* :*IP\_address* /*port\_num*

**Explanation** The value in the transfer encoding field matched the user-configured regular expression or keyword. See the **match {request | response} header transfer-encoding {{regex-name | class class-name} | keyword}** command for more information.

- **matched\_string**—The matched string is one of the following:

- The class map ID, followed by the name of the class map. This string appears when the class map is user configured.

- The actual **match** command that initiated the message. This string appears when the class map is internal.

- *map\_name* —The name of the policy map
- *connection\_action* —Dropping the connection or resetting the connection
- *interface\_type* —The type of interface (for example, DMZ or outside)
- *IP\_address* —The IP address of the interface
- *port\_num* —The port number

**Recommended Action** None required.

## 415011

**Error Message** %ASA-5-415011: HTTP - policy-map *map\_name* :Protocol violation *connection\_action* from *int\_type* :*IP\_address* /*port\_num* to *int\_type* :*IP\_address* /*port\_num*

**Explanation** The HTTP parser cannot detect a valid HTTP message in the first few bytes of an HTTP message.

- *map\_name* —The name of the policy map
- *connection\_action* —Dropping the connection or resetting the connection
- *interface\_type* —The type of interface (for example, DMZ or outside)
- *IP\_address* —The IP address of the interface
- *port\_num* —The port number

**Recommended Action** Enter the **protocol-violation action {drop | reset} log** command to correct the problem.

## 415012

**Error Message** %ASA-5-415012: HTTP - matched *matched\_string* in policy-map *map\_name* , Unknown mime-type *connection\_action* from *int\_type* :*IP\_address* /*port\_num* to *int\_type* :*IP\_address* /*port\_num*

**Explanation** The content-type field did not contain a MIME type that matches a built-in MIME type.

- **matched\_string**—The matched string is one of the following:

- The class map ID, followed by the name of the class map. This string appears when the class map is user configured.
- The actual **match** command that initiated the message. This string appears when the class map is internal.
  - *map\_name* —The name of the policy map
  - *connection\_action* —Dropping the connection or resetting the connection
  - *interface\_type* —The type of interface (for example, DMZ or outside)
  - *IP\_address* —The IP address of the interface
  - *port\_num* —The port number

**Recommended Action** Enter the **match {request | response} header content-type unknown** command to correct the problem.

## 415013

**Error Message** %ASA-5-415013: HTTP - policy-map *map-name* :Malformed chunked encoding *connection\_action* from *int\_type* :*IP\_address* /*port\_num* to *int\_type* :*IP\_address* /*port\_num*

**Explanation** A chunked encoding was malformed, and the HTTP message cannot be parsed. In addition, logging for the **protocol-violation** command was configured.

- **map-name**— The name of the policy map
- *connection\_action* —Dropping the connection or resetting the connection
- *interface\_type* —The type of interface (for example, DMZ or outside)
- *IP\_address* —The IP address of the interface
- *port\_num* —The port number

**Recommended Action** Enter the **protocol-violation action {drop | reset} log** command to correct the problem.

## 415014

**Error Message** %ASA-5-415014: HTTP - matched *matched\_string* in policy-map *map\_name* , Mime-type in response wasn't found in the accept-types of the request *connection\_action* from *int\_type* :*IP\_address* /*port\_num* to *int\_type* :*IP\_address* /*port\_num*

**Explanation** The MIME type in an HTTP response was not in the accept field of the request.

- **matched\_string**—The matched string is one of the following:

- The class map ID, followed by the name of the class map. This string appears when the class map is user configured.
- The actual **match** command that initiated the message. This string appears when the class map is internal.
  - *map\_name* —The name of the policy map
  - *connection\_action* —Dropping the connection or resetting the connection
  - *interface\_type* —The type of interface (for example, DMZ or outside)
  - *IP\_address* —The IP address of the interface
  - *port\_num* —The port number

**Recommended Action** Enter the **match req-resp content-type mismatch** command to correct the problem.

## 415015

**Error Message** %ASA-5-415015: HTTP - matched *matched\_string* in policy-map *map\_name* , transfer-encoding unknown *connection\_action* from *int\_type* :*IP\_address* /*port\_num* to *int\_type* :*IP\_address* /*port\_num*

**Explanation** An empty transfer encoding occurred.

- **matched\_string**—The matched string is one of the following:

- The class map ID, followed by the name of the class map. This string appears when the class map is user configured.

- The actual **match** command that initiated the message. This string appears when the class map is internal.

- *map\_name* —The name of the policy map
- *connection\_action* —Dropping the connection or resetting the connection
- *interface\_type* —The type of interface (for example, DMZ or outside)
- *IP\_address* —The IP address of the interface
- *port\_num* —The port number

**Recommended Action** Enter the **match {request | response} header transfer-encoding empty** command to correct the problem.

## 415016

**Error Message** %ASA-4-415016: policy-map *map\_name* :Maximum number of unanswered HTTP requests exceeded *connection\_action* from *int\_type* :*IP\_address* /*port\_num* to *int\_type* :*IP\_address* /*port\_num*

**Explanation** The number of unanswered HTTP requests exceeded the internal number of requests allowed.

- *map\_name* —The name of the policy map
- *connection\_action* —Dropping the connection or resetting the connection
- *interface\_type* —The type of interface (for example, DMZ or outside)
- *IP\_address* —The IP address of the interface
- *port\_num* —The port number

**Recommended Action** Enter the **protocol-violation action {drop | reset} log** command to correct the problem.

## 415017

**Error Message** %ASA-6-415017: HTTP - *matched\_string* in policy-map *map\_name* , arguments matched *connection\_action* from *int\_type* :*IP\_address* /*port\_num* to *int\_type* :*IP\_address* /*port\_num*

**Explanation** A pattern in the arguments matches the user-configured regular expression or keyword. See the **match request args regex {regex-name | class class-name}** command for more information.

- **matched\_string**—The matched string is one of the following:

- The class map ID, followed by the name of the class map. This string appears when the class map is user configured.

- The actual **match** command that initiated the message. This string appears when the class map is internal.

- *map\_name* —The name of the policy map
- *connection\_action* —Dropping the connection or resetting the connection
- *interface\_type* —The type of interface (for example, DMZ or outside)
- *IP\_address* —The IP address of the interface
- *port\_num* —The port number

**Recommended Action** None required.

## 415018

**Error Message** %ASA-5-415018: HTTP - matched *matched\_string* in policy-map *map\_name* , Header length exceeded *connection\_action* from *int\_type* :*IP\_address* /*port\_num* to *int\_type* :*IP\_address* /*port\_num*

**Explanation** The total header length exceeded the user-configured length for the header.

- **matched\_string**—The matched string is one of the following:
  - The class map ID, followed by the name of the class map. This string appears when the class map is user configured.
  - The actual **match** command that initiated the message. This string appears when the class map is internal.
    - *map\_name* —The name of the policy map
    - *connection\_action* —Dropping the connection or resetting the connection
    - *interface\_type* —The type of interface (for example, DMZ or outside)
    - *IP\_address* —The IP address of the interface
    - *port\_num* —The port number

**Recommended Action** Enter the **match {request | response} header length gt num** command to reduce the length of the header.

## 415019

**Error Message** %ASA-5-415019: HTTP - matched *matched\_string* in policy-map *map\_name* , status line matched *connection\_action* from *int\_type* :*IP\_address* /*port\_num* to *int\_type* :*IP\_address* /*port\_num*

**Explanation** The status line in a response matched a user-configured regular expression. See the **match response status-line regex {regex-name | class class-name }** command for more information.

- **matched\_string**—The matched string is one of the following:
  - The class map ID, followed by the name of the class map. This string appears when the class map is user configured.
  - The actual **match** command that initiated the message. This string appears when the class map is internal.
    - *map\_name* —The name of the policy map
    - *connection\_action* —Dropping the connection or resetting the connection
    - *interface\_type* —The type of interface (for example, DMZ or outside)
    - *IP\_address* —The IP address of the interface
    - *port\_num* —The port number

**Recommended Action** None required.

## 415020

**Error Message** %ASA-5-415020: HTTP - matched *matched\_string* in policy-map *map\_name* , a non-ASCII character was matched *connection\_action* from *int\_type* :*IP\_address* /*port\_num* to *int\_type* :*IP\_address* /*port\_num*

**Explanation** A non-ASCII character was found.

- **matched\_string**—The matched string is one of the following:

- The class map ID, followed by the name of the class map. This string appears when the class map is user configured.

- The actual **match** command that initiated the message. This string appears when the class map is internal.

- *map\_name* —The name of the policy map
- *connection\_action* —Dropping the connection or resetting the connection
- *interface\_type* —The type of interface (for example, DMZ or outside)
- *IP\_address* —The IP address of the interface
- *port\_num* —The port number

**Recommended Action** Enter the **match {request | response} header non-ascii** command to correct the problem.

## 416001

**Error Message** %ASA-4-416001: Dropped UDP SNMP packet from *source\_interface* :*source\_IP* /*source\_port* to *dest\_interface* :*dest\_address* /*dest\_port* ; version (*prot\_version* ) is not allowed through the firewall

**Explanation** An SNMP packet was denied passage through the ASA because of a bad packet format or because the **prot\_version** is not allowed through the ASA. The **prot\_version** parameter can be one of the following values: 1, 2, 2c, or 3.

**Recommended Action** Change the settings for SNMP inspection using the **snmp-map** command, which allows the user to permit or deny specific protocol versions.

## 417001

**Error Message** %ASA-4-417001: Unexpected event received: *number*

**Explanation** A process received a signal, but no handler was found for the event.

**Recommended Action** If the problem persists, contact the Cisco TAC.

## 417004

**Error Message** %ASA-4-417004: Filter violation error: conn *number* (*string* :*string* ) in *string*

**Explanation** A client tried to modify a route attribute that the client does not own.

**Recommended Action** If the problem persists, contact the Cisco TAC.

## 417006

**Error Message** %ASA-4-417006: No memory for *string* ) in *string* . Handling: *string*

**Explanation** An operation failed because of low memory, but will be handled with another mechanism.

**Recommended Action** If the problem persists, contact the Cisco TAC.

## 418001

**Error Message** %ASA-4-418001: Through-the-device packet to/from management-only network is denied: *protocol\_string* from *interface\_name* *IP\_address* (port) [(*idfw\_user* |*FQDN\_string* ), *sg\_info* )] to *interface\_name* *IP\_address* (port) [(*idfw\_user* |*FQDN\_string* ), *sg\_info* ]

**Explanation** A packet from the specified source to the destination was dropped because it is traversing the Secure Firewall ASA to and from the management-only network.

- **protocol\_string**—TCP, UDP, ICMP, or protocol ID as a number in decimal
- **interface\_name**— Interface name
- **IP\_address**—IP address
- **port**—Port number
- **sg\_info** —Security group name or tag for the specified IP address

**Recommended Action** Determine who is generating this packet and why.

## 418018

**Error Message** %ASA-3-418018: neighbor *IP\_Address* Down User reset OR %ASA-3-418018: neighbor *IP\_Address* IPv4 Unicast topology base removed from session User reset OR %ASA-3-418018: neighbor *IP\_Address* Up OR %ASA-3-418018: neighbor *IP\_Address* IPv4 Unicast topology base removed from session BGP Notification sent

**Explanation** The different states of BGP peering and notification of changes on the topology DB as a result of the peering state transitions.

**Recommended Action** None required.

## 418019

**Error Message** %ASA-3-418019: sent to neighbor *IP\_Address*, Reason: *reason*, Bytes: *count*

**Explanation** An indication of why BGP peering was terminated.

- **Reason**—Reason for termination. The reason could be invalid or corrupt AS path, or expiry of hold time, and so on.
- **Bytes**—Number of bytes transmitted

**Recommended Action** None required.

## 418040

**Error Message** %ASA-3-418040: unsupported or mal-formatted message received from *IP\_Address*



**Explanation** Indication of unsupported or mal-formed messages received during the BGP handshake, not necessarily only related to Graceful restart specifically.

**Recommended Action** None required.

## 419001

**Error Message** %ASA-4-419001: Dropping TCP packet from *src\_ifc* :*src\_IP* /*src\_port* to *dest\_ifc* :*dest\_IP* /*dest\_port* , *reason* : MSS exceeded, MSS size , data size

**Explanation** The length of the TCP packet exceeded the MSS advertised in the three-way handshake.

- >*src\_ifc*— Input interface name
- >*src\_IP*— The source IP address of the packet
- >*src\_port*— The source port of the packet
- >*dest\_ifc*— The output interface name
- >*dest\_IP*— The destination IP address of the packet
- >*dest\_port*— The destination port of the packet

**Recommended Action** If there is a need to allow packets that exceed the MSS, create a TCP map using the **exceed-mss** command, as in the following example:

```
ciscoasa# access-list http-list permit tcp any host server_ip eq 80
ciscoasa# class-map http
ciscoasa# match access-list http-list
ciscoasa# tcp-map tmap
ciscoasa# exceed-mss allow
ciscoasa# policy-map global_policy
ciscoasa# class http
ciscoasa# set connection advanced-options tmap
```

## 419002

**Error Message** %ASA-4-419002: Received duplicate TCP SYN from *in\_interface* :*src\_address* /*src\_port* to *out\_interface* :*dest\_address* /*dest\_port* with different initial sequence number.

**Explanation** A duplicate TCP SYN was received during the three-way-handshake that has a different initial sequence number from the SYN that opened the embryonic connection. This may indicate that SYNs are being spoofed. This message occurs in Release 7.0.4.1 and later.

- **in\_interface**—The input interface
- **src\_address**—The source IP address of the packet
- **src\_port**—The source port of the packet
- **out\_interface**—The output interface
- **dest\_address**—The destination IP address of the packet
- **dest\_port**—The destination port of the packet

**Recommended Action** None required.

## 419003

**Error Message** %ASA-4-419003: Cleared TCP urgent flag from *out\_ifc* :*src\_ip* /*src\_port* to *in\_ifc* :*dest\_ip* /*dest\_port*.

**Explanation** A duplicate TCP SYN was received during the three-way-handshake that has a different initial sequence number from the SYN that opened the embryonic connection. This may indicate that SYNs are being spoofed. This message occurs in Release 7.0.4.1 and later.

- **in\_ifc**—The input interface
- **src\_ip**—The source IP address of the packet
- **src\_port**—The source port of the packet
- **out\_ifc**—The output interface
- **dest\_ip**—The destination IP address of the packet
- **dest\_port**—The destination port of the packet

**Recommended Action** If you need to keep the urgent flag in TCP headers, use the **urgent-flag allow** command in TCP map configuration mode.

**Error Message** %ASA-7-419003: Cleared TCP urgent flag.

**Explanation** This syslog is displayed when urgent flag or urgent pointer of tcp packet is cleared. This could be due to user configuration (tcp-map) or having some value for the urgent pointer in a tcp packet but the urgent flag is not set.

**Recommended Action** Verify if the tcp-map configurations whether the urget flag is set to clear.

## 419004

**Error Message** %ASA-6-419004: TCP connection *ID* from *src\_ifc:src\_ip/src\_port* to *dst\_ifc:dst\_ip/dst\_port* is probed by DCD

### Explanation

A TCP connection was probed by Dead Connection Detection (DCD) to determine if connection was still valid.

**Recommended Action** None.

## 419005

**Error Message** %ASA-6-419005: TCP connection *ID* from *src\_ifc:src\_ip/src\_port* duration *hh:mm:ss* data *bytes*, is kept open by DCD as valid connection

### Explanation

A TCP connection was kept open by Dead Connection Detection (DCD) as a valid connection.

**Recommended Action** None.

## 419006

**Error Message** %ASA-6-419006:TCP connection *ID* from *src\_ifc:src\_ip/src\_port* to *dst\_ifc:dst\_ip/dst\_port* duration*hh:mm:ss* data *bytes*, DCD probe was not responded from *client/server* interface *ifc\_name*

### Explanation

A TCP connection was closed by Dead Connection Detection (DCD) as it is no longer required.

**Recommended Action** None.

## 420001

**Error Message** %ASA-3-420001: IPS card not up and fail-close mode used, dropping ICMP packet *ifc\_in* :*SIP* to *ifc\_out* :*DIP* (type *ICMP\_TYPE* , code *ICMP\_CODE* )

For example:

```
%ASA-3-420001: IPS card not up and fail-close mode used, dropping TCP packet from >ifc_in
:>SIP
/>SPORT
  to >ifc_out
:>DIP
/>DPORT
%ASA-3-420001: IPS card not up and fail-close mode used, dropping UDP packet from >ifc_in
:>SIP
/>SPORT
  to >ifc_out
:>DIP
/>DPORT
%ASA-3-420001: IPS card not up and fail-close mode used, dropping protocol >protocol
packet from >ifc_in
:>SIP
  to >ifc_out
:>DIP
```

**Explanation** Packets are dropped when the IPS fail-close mode is used, and the IPS card is not up. This message is rate limited.

- *ifc\_in* —Input interface name
- *ifc\_out* —Output interface name
- *SIP* —Source IP of the packet
- *SPORT* —Source port of the packet
- *DIP* —Destination IP of the packet
- *DPORT* —Destination port of the packet
- *ICMP\_TYPE* —Type of the ICMP packet
- *ICMP\_CODE* —Code of the ICMP packet

**Recommended Action** Bring up the IPS card.

## 420002

**Error Message** %ASA-4-420002: IPS requested to drop ICMP packets *ifc\_in* :*SIP* to *ifc\_out* :*DIP* (type *ICMP\_TYPE* , code *ICMP\_CODE* )

For example:

```
%ASA-4-420002: IPS requested to drop TCP packet from ifc_in:SIP/SPORT to ifc_out:DIP/DPORT
%ASA-4-420002: IPS requested to drop UDP packet from ifc_in:SIP/SPORT to ifc_out:DIP/DPORT
%ASA-4-420002: IPS requested to drop protocol packet from ifc_in:SIP to ifc_out:DIP
```

**Explanation** IPS requested that the packet be dropped.

- *ifc\_in* —Input interface name
- *ifc\_out* —Output interface name
- *SIP* —Source IP of the packet
- *SPORT* —Source port of the packet

- *DIP* —Destination IP of the packet
- *DPORT* —Destination port of the packet
- *ICMP\_TYPE* —Type of the ICMP packet
- *ICMP\_CODE* —Code of the ICMP packet

**Recommended Action** None required.

## 420003

**Error Message** %ASA-4-420003: IPS requested to reset TCP connection from *ifc\_in* :*SIP* /*SPORT* to *ifc\_out* :*DIP* /*DPORT*

**Explanation** IPS requested a reset of a TCP connection.

- *ifc\_in* —Input interface name
- *ifc\_out* —Output interface name
- *SIP* —Source IP of the packet
- *SPORT* —Source port of the packet
- *DIP* —Destination IP of the packet
- *DPORT* —Destination port of the packet

**Recommended Action** None required.

## 420004

**Error Message** %ASA-6-420004: Virtual Sensor *sensor\_name* was added on the AIP SSM

**Explanation** A virtual sensor was added on the AIP SSM card.

- *n* —Card number

**Recommended Action** None required.

## 420005

**Error Message** %ASA-6-420005: Virtual Sensor *sensor\_name* was deleted from the AIP SSM

**Explanation** A virtual sensor was deleted from the AIP SSM card.

- *n* —Card number

**Recommended Action** None required.

## 420006

**Error Message** %ASA-3-420006: Virtual Sensor not present and fail-close mode used, dropping *protocol* packet from *ifc\_in*:*SIP*/*SPORT* to *ifc\_out*:*DIP*/*DPORT*

**Explanation** Packets are dropped when the IPS fail-close mode is used, and the virtual sensor used for the packet is not present.

- *protocol*— Protocol used to send the packet
- *ifc\_in* —Input interface name

- *ifc\_out* —Output interface name
- *SIP* —Source IP address of the packet
- *SPORT* —Source port of the packet
- *DIP* —Destination IP address of the packet
- *DPORT* —Destination port of the packet

**Recommended Action** Add the virtual sensor.

## 420007

**Error Message** %ASA-4-420007: *application-string* cannot be enabled for the module in slot *slot\_id*. The module's current software version does not support this feature. Please upgrade the software on the module in slot *slot\_id* to support this feature. Received backplane header version *version\_number*, required backplane header version *version\_number* or higher.

**Explanation** This message is generated by any new feature in the ASA that needs a corresponding software version in the SSM or SSC hardware module. The message is sent each time that the ASA module manager detects state changes in the SSM or SSC hardware module.

- *application-string* —The name of the application (for example, Promiscuous IDS)
- *slot\_id* —The module identifier, which is 1 for the current ASA
- *version\_number* —The version number of the message header between the ASA and the IPS application

**Recommended Action** Load the SSM or SSC hardware module with the correct software images that support the designated application.

## 420008

**Error Message** %ASA-3-420008: IPS module license disabled and fail-close mode used, dropping packet.

**Explanation** The IPS module license has been disabled and when the fail-close mode is configured, all traffic destined for the IPS module will be dropped. You can check the status of the license by using the **show activation-key** command.

**Recommended Action** Use the **activation-key** command to apply an activation key that has the IPS license enabled.

## 421001

**Error Message** %ASA-3-421001: TCP|UDP flow from *interface\_name* :*IP\_address*/*port* to *interface\_name* :*IP\_address* /*port* is dropped because *application* has failed.

**Explanation** A packet was dropped because the CSC SSM application failed. By default, this message is rate limited to 1 message every 10 seconds.

- **interface\_name**—The interface name
- **IP\_address**—The IP address
- **port**—The port number
- **application**—The CSC SSM is the only application supported in the current release

**Recommended Action** Determine the problem with the service module.

## 421002

**Error Message** %ASA-6-421002: TCP|UDP flow from *interface\_name* :*IP\_address* /*port* to *interface\_name* :*IP\_address* /*port* bypassed *application* checking because the protocol is not supported.

**Explanation** The connection bypassed service module security checking because the protocol that it is using cannot be scanned by the service module. For example, the CSC SSM is not capable of scanning Telnet traffic. If the user configures Telnet traffic to be scanned, the traffic will bypass the scanning service. By default, this message is rate limited to 1 message every 10 seconds.

- **IP\_address**—The IP address
- **port**—The port number
- **interface\_name**—The name of the interface on which the policy is applied
- **application**—The CSC SSM is the only application supported in the current release

**Recommended Action** The configuration should be modified to only include protocols that are supported by the service module.

## 421003

**Error Message** %ASA-3-421003: Invalid data plane encapsulation.

**Explanation** A packet injected by the service module did not have the correct data plane header. Packets exchanged on the data backplane adhere to a Cisco proprietary protocol called ASDP. Any packet that does not have the proper ASDP header is dropped.

**Recommended Action** Use the **capture name type asp-drop [ssm-asdp-invalid-encap]** command to capture the offending packets and contact the Cisco TAC.

## 421004

**Error Message** %ASA-7-421004: Failed to inject {TCP|UDP} packet from *IP\_address* /*port* to *IP\_address* /*port*

**Explanation** The ASA has failed to inject a packet as instructed by the service module. This may happen if the ASA tries to inject a packet into a flow that has already been released or when the ASA maintains its connection table independently from the service module. Normally it will not cause any problem.

- **IP\_address**—The IP address
- **port**—The port number

**Recommended Action** If ASA performance is affected, or if the problem persists, contact the Cisco TAC.

## 421005

**Error Message** %ASA-6-421005: *interface\_name* :*IP\_address* is counted as a user of *application*

**Explanation** A host has been counted toward the license limit. The specified host was counted as a user of **application**. The total number of users in 24 hours is calculated at midnight for license validation.

- **interface\_name**—The interface name
- **IP\_address**—The IP address

- **application**—The CSC SSM

**Recommended Action** None required. However, if the overall count exceeds the user license that you have purchased, contact the Cisco TAC to upgrade your license.

## 421006

**Error Message** %ASA-6-421006: There are *number* users of *application* accounted during the past 24 hours.

**Explanation** The total number of users who have used an application for the past 24 hours have been identified. This message is generated every 24 hours to give the total number of hosts that have used services provided by the service module.

- **application**—The CSC SSM

**Recommended Action** None required. However, if the overall count exceeds the user license that you have purchased, contact the Cisco TAC to upgrade your license.

## 421007

**Error Message** %ASA-3-421007: TCP|UDP flow from *interface\_name* :*IP\_address* /*port* to *interface\_name* :*IP\_address* /*port* is skipped because *application* has failed.

**Explanation** A flow was skipped because the service module application has failed. By default, this message is rate limited to 1 message every 10 seconds.

- **IP\_address**—The IP address
- **port**—The port number
- **interface\_name**—The name of the interface on which the policy is applied
- **application**—The CSC SSM

**Recommended Action** Determine the problem with the service module.

## 422004

**Error Message** %ASA-4-422004: IP SLA Monitor *number0* : Duplicate event received. Event number *number1*

**Explanation** The IP SLA monitor process has received a duplicate event. Currently, this message applies to destroy events. Only one destroy request will be applied. This is only a warning message.

- *number0* —The SLA operation number
- *number1* —The SLA operation event ID

**Recommended Action** If this recurs, enter the **show sla monitor configuration SLA\_operation\_id** command and copy the output of the command. Copy the message as it appears on the console or in the system log. Then contact the Cisco TAC and provide the representative with the information that you have, along with information about the application that is configuring and polling the SLA probes.

## 422005

**Error Message** %ASA-4-422005: IP SLA Monitor Probe(s) could not be scheduled because clock is not set.

**Explanation** One or more IP SLA monitor probes cannot be scheduled because the system clock was not set.

**Recommended Action** Make sure that the system clock is functional by using NTP or another mechanism.

## 422006

**Error Message** %ASA-4-422006: IP SLA Monitor Probe *number* : *string*

**Explanation** The IP SLA monitor probe cannot be scheduled. Either the configured starting time has already occurred or the starting time is invalid.

- *number* —The SLA operation ID
- *string* —A string describing the error

**Recommended Action** Reschedule the failed probe with a valid start time.

## 423001

**Error Message** %ASA-4-423001: {Allowed | Dropped} invalid NBNS *pkt\_type\_name* with *error\_reason\_str* from *ifc\_name* :*ip\_address* /*port* to *ifc\_name* :*ip\_address* /*port* .

**Explanation** The NBNS packet format is incorrect.

**Recommended Action** None required.

## 423002

**Error Message** %ASA-4-423002: {Allowed | Dropped} mismatched NBNS *pkt\_type\_name* with *error\_reason\_str* from *ifc\_name* :*ip\_address* /*port* to *ifc\_name* :*ip\_address* /*port* .

**Explanation** An NBNS ID mismatch occurred.

**Recommended Action** None required.

## 423003

**Error Message** %ASA-4-423003: {Allowed | Dropped} invalid NBDGM *pkt\_type\_name* with *error\_reason\_str* from *ifc\_name* :*ip\_address* /*port* to *ifc\_name* :*ip\_address* /*port* .

**Explanation** The NBDGM packet format is incorrect.

**Recommended Action** None required.

## 423004

**Error Message** %ASA-4-423004: {Allowed | Dropped} mismatched NBDGM *pkt\_type\_name* with *error\_reason\_str* from *ifc\_name* :*ip\_address* /*port* to *ifc\_name* :*ip\_address* /*port* .



**Explanation** An NBDGM ID mismatch occurred.

**Recommended Action** None required.

## 423005

**Error Message** %ASA-4-423005: {Allowed | Dropped} NBDGM *pkt\_type\_name* fragment with *error\_reason\_str* from *ifc\_name :ip\_address /port* to *ifc\_name :ip\_address /port* .

**Explanation** The NBDGM fragment format is incorrect.

**Recommended Action** None required.

## 424001

**Error Message** %ASA-4-424001: Packet denied *protocol\_string* *intf\_in :src\_ip /src\_port* [[*idfw\_user* | *FQDN\_string* ], *sg\_info* )] *intf\_out :dst\_ip /dst\_port* [[*idfw\_user* | *FQDN\_string* ], *sg\_info* )]. [Ingress|Egress] interface is in a backup state.

**Explanation** A packet was dropped because it was traversing the Secure Firewall ASA to or from a redundant interface. Interface functionality is limited on low-end platforms. The interface specified by the **backup interface** command can only be a backup for the primary interface configured. If the default route to the primary interface is up, any traffic through the Secure Firewall ASA from the backup interface will be denied. Conversely, if the default route to the primary interface is down, traffic through the Secure Firewall ASA from the primary interface will be denied.

- *protocol\_string* —The protocol string; for example, TCP or protocol ID (a decimal number)
- *intf\_in* —The input interface name
- *src\_ip* —The source IP address of the packet
- *src\_port* —The source port of the packet
- *intf\_out* —The output interface name
- *dst\_ip* —The destination IP address of the packet
- *dst\_port* —The destination port of the packet
- *sg\_info* —The security group name or tag for the specified IP address

**Recommended Action** Determine the source of the denied packet.

## 424002

**Error Message** %ASA-4-424002: Connection to the backup interface is denied: *protocol\_string* *intf :src\_ip /src\_port* *intf :dst\_ip /dst\_port*

**Explanation** A connection was dropped because it is in a backup state. Interface functionality is limited on low-end platforms. The backup interface can only be a backup for the primary interface specified by the **backup interface** command. If the default route to the primary interface is up, any connection to the Secure Firewall ASA through the backup interface will be denied. Conversely, if the default route to the primary interface is down, connections to the Secure Firewall ASA through the primary interface will be denied.

- *protocol\_string* —The protocol string; for example, TCP or protocol ID (a decimal number)
- *intf\_in* —The input interface name
- *src\_ip* —The source IP address of the packet
- *src\_port* —The source port of the packet

- *intf\_out* —The output interface name
- *dst\_ip* —The destination IP address of the packet
- *dst\_port* —The destination port of the packet

**Recommended Action** Determine the source of the denied packet.

## 425001

**Error Message** %ASA-6-425001 Redundant interface *redundant \_interface\_name* created.

**Explanation** The specified redundant interface was created in the configuration.

- *redundant\_interface\_name* —Redundant interface name

**Recommended Action** None required.

## 425002

**Error Message** %ASA-6-425002 Redundant interface *redundant \_interface\_name* removed.

**Explanation** The specified redundant interface was removed from the configuration.

- *redundant\_interface\_name* —Redundant interface name

**Recommended Action** None required.

## 425003

**Error Message** %ASA-6-425003 Interface *interface\_name* added into redundant interface *redundant \_interface\_name* .

**Explanation** The specified physical interface was added to the specified redundant interface as a member interface.

- *interface\_name* —An interface name
- *redundant\_interface\_name* —Redundant interface name

**Recommended Action** None required.

## 425004

**Error Message** %ASA-6-425004 Interface *interface\_name* removed from redundant interface *redundant \_interface\_name* .

**Explanation** The specified redundant interface was removed from the specified redundant interface.

- *interface\_name* —An interface name
- *redundant\_interface\_name* —Redundant interface name

**Recommended Action** None required.

## 425005

**Error Message** %ASA-5-425005 Interface *interface\_name* become active in redundant interface *redundant\_interface\_name*

**Explanation** Within a redundant interface, one member interface is the active member. Traffic only passes through the active member interface. The specified physical interface became the active member of the specified redundant interface. Member interface switchover occurs when one of the following is true:

- The **redundant-interface interface-name active-member interface-name** command was executed.
  - The active member interface is down, while the standby member interface is up.
  - The standby member interface comes up (from down), while the active member interface remains down.
- *interface\_name* —An interface name
  - *redundant\_interface\_name* —Redundant interface name

**Recommended Action** Check the status of the member interfaces.

## 425006

**Error Message** %ASA-3-425006 Redundant interface *redundant\_interface\_name* switch active member to *interface\_name* failed.

**Explanation** An error occurred when member interface switchover was attempted.

- *redundant\_interface\_name* —Redundant interface name
- *interface\_name* —An interface name

**Recommended Action** If the problem persists, contact the Cisco TAC.

## 426001

**Error Message** %ASA-6-426001: PORT-CHANNEL:Interface *ifc\_name* bundled into EtherChannel interface Port-channel *num*

**Explanation** The **interface port-channel *num*** or the **channel-group *num* mode *mode*** command has been used on a nonexistent port channel.

- *ifc\_name* —The EtherChannel interface name
- *num* —The port channel number

**Recommended Action** None required.

## 426002

**Error Message** %ASA-6-426002: PORT-CHANNEL:Interface *ifc\_name* unbundled from EtherChannel interface Port-channel *num*

**Explanation** The **no interface port-channel *num*** command has been used.

- *ifc\_name* —The EtherChannel interface name
- *num*— The port channel number

**Recommended Action** None required.

## 426003

**Error Message** %ASA-6-426003: PORT-CHANNEL:Interface *ifc\_name1* has become standby in EtherChannel interface Port-channel *num*

**Explanation** The **channel-group** *num mode mode* command has been used.

- *ifc\_name1* —The EtherChannel interface name
- *num* —The port channel number

**Recommended Action** None required.

## 426004

**Error Message** %ASA-4-426004: PORT-CHANNEL: Interface *ifc\_name1* is not compatible with *ifc\_name* and will be suspended (speed of *ifc\_name1* is X Mbps, Y is 1000 Mbps).

**Error Message** %ASA-4-426004: Interface *ifc\_name1* is not compatible with *ifc\_name1* and will be suspended (*ifc\_name1* is Full-duplex, *ifc\_name1* is Half-duplex)

**Explanation** The **channel-group** *num mode mode* command is executed on a physical interface and there is a speed or duplex mismatch of this physical interface with that of the port channel.

- *ifc\_name* —The interface that is being added to the port channel
- *ifc\_name1* —The interface that is already in the port channel and in a bundled state

**Recommended Action** Do one of the following:

- Change the speed of the physical interface to that of the port channel and execute the **channel-group** *num mode mode* command again.
- Leave the member interface in a suspended state. When the last active member is removed, then that member will try to reestablish LACP on the suspended member.

## 426101

**Error Message** %ASA-6-426101: PORT-CHANNEL:Interface *ifc\_name* is allowed to bundle into EtherChannel interface *port-channel id* by CLACP

**Explanation** A port has been bundled in a span-cluster channel group.

**Recommended Action** None required.

## 426102

**Error Message** %ASA-6-426102: PORT-CHANNEL:Interface *ifc\_name* is moved to standby in EtherChannel interface *port-channel id* by CLACP

**Explanation** A port has been moved to hot-standby state in a span-cluster channel group.

**Recommended Action** None required.

## 426103

**Error Message** %ASA-6-426103: PORT-CHANNEL:Interface *ifc\_name* is selected to move from standby to bundle in EtherChannel interface *port-channel id* by CLACP

**Explanation** A standby port has been selected to move to bundled state in a span-cluster channel group.

**Recommended Action** None required.

## 426104

**Error Message** %ASA-6-426104: PORT-CHANNEL:Interface *ifc\_name* is unselected in EtherChannel interface *port-channel id* by CLACP

**Explanation** A bundled port has been unbundled in a span-cluster channel group to obtain space for other ports to be bundled.

**Recommended Action** None required.

## 428002

**Error Message** %ASA-6-428002: WAAS confirmed from *in\_interface :src\_ip\_addr/src\_port* to *out\_interface :dest\_ip\_addr/dest\_port* , inspection services bypassed on this connection.

**Explanation** WAAS optimization was detected on a connection. All layer 7 inspection services, including IPS, are bypassed on WAAS-optimized connections.

**Recommended Action** No action is required if the network includes WAE devices; otherwise, the network administrator should investigate the use of the WAAS option on this connection.

## 429001

**Error Message** %ASA-3-429001: CXSC card not up and fail-close mode used. Dropping *protocol* packet from *interface\_name :ip\_address /port* to *interface\_name :ip\_address /port*

**Explanation** Data has been dropped because an SSP is down and a fail-close policy exists.

**Recommended Action** Check the status of the service module and contact the Cisco TAC for assistance, if necessary.

## 429002

**Error Message** %ASA-4-429002: CXSC service card requested to drop *protocol* packet from *interface\_name :ip\_address /port* to *interface\_name :ip\_address /port*

**Explanation** The CXSC SSP requested that the ASA drop a packet of a connection.

**Recommended Action** None.

## 429003

**Error Message** %ASA-4-429003: CXSC service card requested to reset TCP connection from *interface\_name :ip\_addr /port* to *interface\_name :ip\_addr /port*

**Explanation** The CXSC SSP requested that the ASA reset a TCP connection.

**Recommended Action** None required.

## 429004

**Error Message** %ASA-3-429004: Unable to set up authentication-proxy rule for the cx action on interface *interface\_name* for *policy\_type* service-policy.

**Explanation** The ASA could not set up to-the-box rules for authentication proxy with the CXSC action because of some internal errors, such as insufficient memory.

**Recommended Action** This error should not occur. Contact the Cisco TAC for assistance.

## 429005

**Error Message** %ASA-6-429005: Set up authentication-proxy *protocol\_type* rule for the CXSC action on interface *interface\_name* for traffic destined to *ip\_address* /*port* for *policy\_type* service-policy.

**Explanation** The ASA successfully set up to-the-box rules for authentication proxy with the CXSC action.

**Recommended Action** None.

## 429006

**Error Message** %ASA-6-429006: Cleaned up authentication-proxy rule for the CXSC action on interface *interface\_name* for traffic destined to *ip\_address* for *policy\_type* service-policy.

**Explanation** The ASA successfully cleaned up to-the-box rules for authentication proxy with the CXSC action.

**Recommended Action** None.

## 429007

**Error Message** %ASA-4-429007: CXSC redirect will override Scansafe redirect for flow from *interface\_name* :*ip\_address* /*port* to *interface\_name* :*ip\_address* /*port* with *username*

**Explanation** A flow matches both CXSC and Scansafe redirects. The message indicates that the CXSC redirect overrides the Scansafe redirect for the displayed flow.

**Recommended Action** If this is unwanted behavior, then reconfigure the policy to ensure that no overlap of CXSC and Scansafe redirection occurs for the same flow.

## 429008

**Error Message** %ASA-4-429008: Unable to respond to VPN query from CX for session 0x%x . Reason %s

**Explanation** The CX sent a VPN session query to the Secure Firewall ASA, but it did not respond either because of an invalid session ID or another reason. Valid reasons can be any of the following:

- TLV length is invalid

- TLV memory allocation failed
- VPN session query message enqueue failed
- VPN session ID is invalid

**Recommended Action** None required.

## 431001

**Error Message** %ASA-4-431001: RTP conformance: Dropping RTP packet from *in\_ifc :src\_ip /src\_port* to *out\_ifc :dest\_ip /dest\_port* , Drop reason: *drop\_reason value*

**Explanation** The RTP packet was dropped.

- **in\_ifc**—The input interface
- **src\_ip**—The source IP address of the packet
- **src\_port**—The source port of the packet
- **out\_ifc**—The output interface
- **dest\_ip**—The destination IP address of the packet
- **dest\_port**—The destination port of the packet
- **drop\_reason**—One of the following drop reasons:

- Incorrect version *value* —The version number from the packet is incorrect.
- Invalid payload-type *value* —The payload type from the packet is invalid.
- Incorrect SSRC *value* —The SSRC from the packet is incorrect.
- Out-of-range sequence number *value* sequence number from the packet.
- Out of sequence in packet in probation *value* sequence number from the packet.

**Recommended Action** Examine the dropped RTP packets to determine which field the RTP source is setting incorrectly. Also examine the source to verify that it is legitimate and not an attacker trying to misuse an opening in the ASA.

## 431002

**Error Message** %ASA-4-431002: RTCP conformance: Dropping RTCP packet from *in\_ifc :src\_ip /src\_port* to *out\_ifc :dest\_ip /dest\_port* , Drop reason: *drop\_reason value*

**Explanation** The RTCP packet was dropped.

- **in\_ifc**—The input interface
- **src\_ip**—The source IP address of the packet
- **src\_port**—The source port of the packet
- **out\_ifc**—The output interface
- **dest\_ip**—The destination IP address of the packet
- **dest\_port**—The destination port of the packet
- **drop\_reason**—One of the following drop reasons:

- Incorrect version **value**—The version number from the packet is incorrect.
- Invalid payload-type **value**—The payload type from the packet is incorrect.

**Recommended Action** Examine the dropped RTP packets to determine which field the RTP source is setting incorrectly. Also examine the source to verify that it is legitimate and not an attacker trying to misuse an opening in the ASA.

## 434001

**Error Message** %ASA-4-434001: SFR card not up and fail-close mode used, dropping *protocol* packet from *ingress interface:source IP address /source port* to *egress interface :destination IP address /destination port*

**Explanation** A packet has been dropped because of a fail-close configuration for the module. Your loss of connectivity for all the flows is caused by redirecting them to the module, because the fail-close configuration is designed to drop all the flows if the module is down.

**Recommended Action** Try to understand the reason for failure and restore services. Alternatively, you can use the fail-open option even if the card does not recover immediately. Note that in the fail-open configuration, all packets to the module are bypassed if the card status is down.

## 434002

**Error Message** %ASA-4-434002: SFR requested to drop *protocol* packet from *ingress interface :source IP address /source port* to *egress interface :destination IP address /destination port*

**Explanation** A packet has been denied by the module. Your connection is not successful for a certain flow has been redirected to the module.

**Recommended Action** Try to identify the module policy that caused this flow or packet to be denied.

## 434003

**Error Message** %ASA-4-434003: SFR requested to reset TCP connection from *ingress interface :source IP address /source port* to *egress interface :destination IP address /destination port*

**Explanation** A TCP flow has been reset by the ASA, as requested by the module. Your TCP connection is not successful for a certain flow because it was redirected to the module.

**Recommended Action** Try to identify the module policy that caused this flow or packet to be denied.

## 434004

**Error Message** %ASA-5-434004: SFR requested ASA to bypass further packet redirection and process flow from %s:%A/%d to %s:%A/%d locally

**Explanation** SourceFire (SFR) has determined not to inspect more traffic of a flow and requests the Secure Firewall ASA to stop redirecting the flow of traffic to SFR.

**Recommended Action** None Required.



## 434007

**Error Message** %ASA-4-434007: SFR redirect will override Scansafe redirect for flow from *ingress interface :source IP address /source port* to *egress interface :destination IP address /destination port (user )*

**Explanation** A flow that was inspected by Scansafe is now inspected by SourceFire (SFR) only. Scansafe and SFR cannot inspect a flow simultaneously.

**Recommended Action** Reconfigure the ASA inspect policy that caused this flow or packet to be inspected by either Scansafe or SFR.

## 444004

**Error Message** %ASA-2-444004: Temporary license key *key* has expired. Applying permanent license key *permkey*

**Explanation** The temporary license that was installed has expired. The features that the license provided are no longer available.

- *key* —The temporary activation key
- *permkey* —The permanent activation key

**Recommended Action** A permanent license should be purchased and installed.

## 444005

**Error Message** %ASA-4-444005: Timebased activation key *activation -key* will expire in *num* days

**Explanation** This message is generated every 24 hours, indicating that the temporary license will expire in the number of days specified. After that date, the features that the license provided will no longer be available.

- *activation-key* —The temporary activation key
- *num* —The number of days left until expiration

**Recommended Action** If the amount of time remaining is less than 30 days, you should purchase another time-based activation key before the temporary license runs out.

## 444007

**Error Message** %ASA-2-444007: Timebased activation key *activation -key* has expired. Reverting to [permanent | timebased] license key. The following features will be affected: *feature , feature*

**Explanation** The time-based activation key has expired. The specified features that the license provided are no longer available.

- *activation-key* —The temporary activation key
- *feature* —The name of the licensed feature being affected

**Recommended Action** You must purchase another time-based activation key as soon as possible to prevent service disruption for the features specified.

## 444008

**Error Message** %ASA-4-444008: %s license has expired, and the system is scheduled to reload in x days. Apply a new activation key to enable %s license and prevent the automatic reload.

**Explanation** The specific license has expired, which will cause the system to reload in x days. Apply a new activation key to enable the specific license and prevent automatic reload.

**Recommended Action** Apply a new activation key to enable the specific license and prevent automatic reload.

## 444009

**Error Message** %ASA-2-444009: %s license has expired 30 days ago. The system will now reload.

**Explanation** The specific license expired 30 days ago. The system will reload.

**Recommended Action** None required.

## 444100

**Error Message** %ASA-5-444100: Shared *request* request failed. Reason: *reason*

**Explanation** A shared license client request was unsuccessfully sent or processed by the server.

• *request* —Valid requests are:

- get AnyConnect Premium
- release AnyConnect Premium
- transfer AnyConnect Premium

• *reason* —The reason that the request failed. Valid reasons are:

- connection failed to server
- version not supported by server
- message signature invalid
- client ID unknown by server
- server is not active
- license capacity reached

**Recommended Action** None required.

## 444101

**Error Message** %ASA-5-444101: Shared license service is active. License server address: *address*

**Explanation** The shared license server has become active.

• *address* —The license server IPv4 or IPv6 address

**Recommended Action** None required.

## 444102

**Error Message** %ASA-2-444102: Shared license service inactive. License server is not responding.

**Explanation** The shared license service was inactive because the license server was not responding. The ASA failed to register with the shared license server.

**Recommended Action** Verify that the license server address, secret, and port are configured correctly.

## 444103

**Error Message** %ASA-6-444103: Shared *licensetype* license usage is over 90% capacity.

**Explanation** The shared license usage on the network is over 90 percent capacity.

- *licensetype* —AnyConnect Premium

**Recommended Action** None required.

## 444104

**Error Message** %ASA-6-444104: Shared *licensetype* license availability: *value* .

**Explanation** The shared license availability on the network appeared.

- *licensetype* —AnyConnect Premium
- *value* —The license availability

**Recommended Action** None required.

## 444105

**Error Message** %ASA-2-444105: Released *value* shared *licensetype* license(s). License server has been unreachable for 24 hours.

**Explanation** The shared license server has been unreachable for 24 hours, and all shared licenses that have been acquired by the ASA have been released. The ASA failed to register with the license server.

- *licensetype* —AnyConnect Premium
- *value* —The license availability

**Recommended Action** Verify the connectivity to the license server, and that the configuration has not been changed on the license server.

## 444106

**Error Message** %ASA-4-444106: Shared license backup server *address* is not available.

**Explanation** The shared license backup server is not reachable. License server information is not synchronized with the backup device.

- *address* —The IPv4 or IPv6 address of the backup license server

**Recommended Action** None required.

## 444107

**Error Message** %ASA-6-444107: Shared license service *status* on interface *ifname* .

**Explanation** The shared license service has been enabled or disabled on the specified interface.

- *ifname* —The interface name.
- *status* —The status of the license server. Valid values are enabled or disabled.

**Recommended Action** None required.

## 444108

**Error Message** %ASA-6-444108: Shared license *state* client id *id* .

**Explanation** The multi-site license client ID has registered or expired with the server.

- *id* —The ID of the client
- *state* —The state of the license server. Valid values are registered or expired.

**Recommended Action** None required.

## 444109

**Error Message** %ASA-4-444109: Shared license backup server role changed to *state* .

**Explanation** The shared backup license server role has changed.

- *state* —The state of the license server. Valid values are active or inactive.

**Recommended Action** None required.

## 444110

**Error Message** %ASA-4-444110: Shared license server *backup* has *days* remaining as active license server.

**Explanation** The shared backup license server is in an active role and remains active for a specified number of days. The ASA failed to register with the license server, and needs to register with the primary license server soon.

- *days* —The number of days left as the active license server

**Recommended Action** Verify that the license server is online and reachable by the ASA.

## 444111

**Error Message** %ASA-2-444111: Shared license backup service has been terminated due to the primary license server *address* being unavailable for more than *days* days. The license server needs to be brought back online to continue using shared licensing.

**Explanation** The shared backup license server active time has expired. The primary server needs to go online in order for the shared license service to continue.

- *address* —The IPv4 or IPv6 address of the license server

- *days* —The number of days that the license server has been unavailable

**Recommended Action** Register with the primary license server in order to continue using the shared license service.

## 444302

**Error Message** %ASA-2-444302: %SMART\_LIC-2-PLATFORM\_ERROR: Platform error.

**Explanation** Smart Licensing Agent has encountered a platform problem. This indicates that the platform team did not properly implement smart licensing on the device.

**Recommended Action** The platform team needs to address this problem before release.

## 444303

**Error Message** %ASA-3-444303: %SMART\_LIC-3-AGENT\_REG\_FAILED: Smart Agent for licensing registration with Cisco licensing cloud failed.

**Explanation** Smart Licensing registration failed. This may have been caused due to an invalid ID token used during the registration or network connection failure to cisco.com.

**Recommended Action** Please check the Smart Agent syslog messages for additional information. Turn on the smart agent debug mode (CLI command: 'debug license agent all') and retry for more detailed information. Check your Smart Call Home configuration, your network connection with Cisco, and if the Identity token you used for registration is valid.

**Error Message** %ASA-3-444303: %SMART\_LIC-3-AGENT\_DEREG\_FAILED: Smart Agent for licensing deregistration with CSSM failed.

**Explanation** Smart Licensing deregistration failed. This may have been caused due to a network connection failure to CSSM. The local registration information has been removed from the device.

**Recommended Action** Please check the Smart Agent syslog messages for additional information. Turn on the smart agent debug mode (CLI command: 'debug license agent all') and retry for more detailed information. Check your Smart Call Home configuration and your network connection with CSSM.

**Error Message** %ASA-3-444303: %SMART\_LIC-3-OUT\_OF\_COMPLIANCE: One or more entitlements are out of compliance.

**Explanation** One or more requested entitlements from the customer are out of compliance.

**Recommended Action** Customer needs to go to the smart licensing portal to view their entitlements to understand the non-compliance.

**Error Message** %ASA-3-444303: %SMART\_LIC-3-EVAL\_EXPIRED: Evaluation period expired.

**Explanation** Your evaluation period has expired. Please obtain a new identity token from the smart agent portal and re-register the device.

**Recommended Action** Customer needs to obtain a new identity token from the smart agent portal and re-register the device with the Cisco licensing service.

**Error Message** %ASA-3-444303: %SMART\_LIC-3-BAD\_MODE: An unknown mode was specified.

**Explanation** An invalid entitlement enforcement mode was received by the smart agent in the process of logging a syslog message.

**Recommended Action** This is a smart call home internal error. Please report this to Cisco.

**Error Message** %ASA-3-444303: %SMART\_LIC-3-BAD\_NOTIF: A bad notification type was specified.

**Explanation** An invalid notification type was received by the smart agent in the process of logging a syslog message.

**Recommended Action** This is a smart call home internal error. Please report this to Cisco.

**Error Message** %ASA-3-444303: %SMART\_LIC-3-ID\_CERT\_EXPIRED: Identity certificate expired. Agent will transition to the unidentified (not registered) state.

**Explanation** The device has not communicated with Cisco for an extended period of time and the device has not automatically renewed the device registration with Cisco.

**Recommended Action** Please check the smart call home settings and network connectivity to cisco.com.

**Error Message** %ASA-3-444303: %SMART\_LIC-3-ID\_CERT\_RENEW\_NOT\_STARTED: Identity certificate start date not reached yet.

**Explanation** The device registration failed. The Identity certificate start date is later than the device current time.

**Recommended Action** Please adjust your device clock to be up-to-date and retry the registration again.

**Error Message** %ASA-3-444303: %SMART\_LIC-3-ID\_CERT\_RENEW\_FAILED: Identity certificate renewal failed.

**Explanation** The device has not communicated with Cisco for an extended period of time and the device has failed to automatically renew the device registration with Cisco.

**Recommended Action** Please check the smart call home settings and network connectivity to cisco.com.

**Error Message** %ASA-3-444303: %SMART\_LIC-3-ENTITLEMENT\_RENEW\_FAILED: Entitlement authorization with Cisco licensing cloud failed.

**Explanation** The device has failed to communicate with Cisco to renew the entitlement authorization.

**Recommended Action** Please check the smart agent syslog messages for further information. Additionally, check for smart call home settings and network connectivity to cisco.com.

**Error Message** %ASA-3-444303: %SMART\_LIC-3-COMM\_FAILED: Communications failure with Cisco licensing cloud.

**Explanation** The device communication with the Cisco licensing service failed.

**Recommended Action** Please check the smart call home settings and network connectivity to cisco.com.

**Error Message** %ASA-3-444303: %SMART\_LIC-3-CERTIFICATE\_VALIDATION: Certificate validation failed by smart agent.

**Explanation** The identity certificate validation failed.

**Recommended Action** Please check the smart agent syslog file for more information. Turn on the smart agent debug mode (CLI command: license smart debug enable) and retry again for additional information. Additionally, check if the identity certificate expiration date has been reached.

**Error Message** %ASA-3-444303: %SMART\_LIC-3-AUTH\_RENEW\_FAILED: Authorization renewal with Cisco licensing cloud failed.

**Explanation** The authorization renew request failed. This may have been caused due to wrong smart call home settings or network connectivity failure to cisco.com.

**Recommended Action** Please check the smart agent syslog file for more information. Turn on the smart agent debug mode and retry again for additional information. Additionally, check the smart call home settings and network connectivity to cisco.com.

**Error Message** %ASA-3-444303: %SMART\_LIC-3-INVALID\_TAG: The entitlement tag is invalid.

**Explanation** The tag is not defined in the Cisco Smart Software Manager.

**Recommended Action** Report this error to Cisco.

**Error Message** %ASA-3-444303: %SMART\_LIC-3-INVALID\_ROLE\_STATE: The current role is not allowed to move to the new role.

**Explanation** From the last role event, we can only move to certain roles. The device has moved to a role to which the smart agent cannot follow.

**Recommended Action** Please check the smart agent syslog file for more information. Turn on the smart agent debug mode and retry again for additional information.

**Error Message** %ASA-3-444303: %SMART\_LIC-3-EVAL\_WILL\_EXPIRE\_WARNING: Evaluation period will expire in time.

**Explanation** The device is using the evaluation period which will expire in the specified time.

**Recommended Action** Use the 'license smart register ID token' CLI to register this device before the evaluation period expires.

**Error Message** %ASA-3-444303: %SMART\_LIC-3-EVAL\_EXPIRED\_WARNING: Evaluation period expired on time.

**Explanation** The device evaluation period has expired.

**Recommended Action** Use the 'license smart register ID token' CLI to register this device.

**Error Message** %ASA-3-444303: %SMART\_LIC-3-ID\_CERT\_EXPIRED\_WARNING: This device's registration will expire in time.

**Explanation** The registration for this device will expire at the specified time. This usually indicates a communications failure with the Cisco licensing authority.

**Recommended Action** Please check the smart call home settings and network connectivity to cisco.com. Additionally, check if the identity certificate need to be renewed.

**Error Message** %ASA-3-444303: %SMART\_LIC-3-CONFIG\_OUT\_OF\_SYNC: Trusted Store Enable flag not in sync with System Configuration, TS flag Config flag.

**Explanation** Smart licensing configuration does not match the value of the enable flag in persistent storage. This can happen if a configuration is copied onto the system and a reload occurs. If the new configuration does not contain the Smart Licensing Enable command, the value in persistent storage will not match.

**Recommended Action** Apply the desired Smart Licensing Configuration Command and persist the configuration.

**Error Message** %ASA-3-444303: %SMART\_LIC-3-REG\_EXPIRED\_CLOCK\_CHANGE: Smart Licensing registration has expired because the system time was changed outside the validity period of the registration period. The agent will transition to the un-registered state in 60 minutes.

**Explanation** The system clock has been changed so that it is now outside the valid registration period. If the clock is reset to a value inside the registration validity period within one hour smart licensing will continue function normally. If the clock is not reset the device will become un-registered and a new identity token will

need to be obtained to re-register the device. The registration validity period is defined by the start and end date in the identity certificate. Use 'show tech license' to get the id certificate information.

**Error Message** %ASA-3-444303: %SMART\_LIC-3-ROOT\_CERT\_MISMATCH\_PROD: Certificate type mismatch.

**Explanation** Smart Agent received incorrect certificate for validation. Please contact your product support team.

**Error Message** %ASA-3-444303: %SMART\_LIC-3-HOT\_STANDBY\_OUT\_OF\_SYNC: Smart Licensing agent on hot standby is out of sync with active Smart Licensing agent.

**Explanation** Smart Licensing Agent on the hot standby failed to process the data necessary to stay in sync with the active agent. If a switchover occurs the new active agent will not be in the same state as the current active agent configuration does not match the value of the enable flag in persistent storage. This can happen if a configuration is copied onto the system and a reload occurs. If the new configuration does not contain the Smart Licensing Enable command, the value in persistent storage will not match.

## 444304

**Error Message** %ASA-4-444304: %SMART\_LIC-4-IN\_OVERAGE: One or more entitlements are in overage.

**Explanation** This is for information only. The customer is still in compliance and within the overage amount as specified in their contract.

**Error Message** %ASA-4-444304: %SMART\_LIC-4-CONFIG\_NOT\_SAVED: Smart Licensing configuration has not been saved.

This is for information only. The customer remains in IN/OUT\_OF compliance state.

**Recommended Action** None.

## 444305

**Error Message** %ASA-5-444305: %SMART\_LIC-5-SYSTEM\_CLOCK\_CHANGED: Smart Agent for Licensing System clock has been changed.

**Explanation** System clock was manually reset.

**Error Message** %ASA-5-444305: %SMART\_LIC-5-IN\_COMPLIANCE: All entitlements are authorized.

**Explanation** All customer requested entitlements are authorized by Cisco licensing service.

**Error Message** %ASA-5-444305: %SMART\_LIC-5-EVAL\_START: Entering evaluation period.

**Explanation** Either customer allocate entitlement prior to registration or customer registration has expired. The device is now de-registered and is in evaluation mode.

**Error Message** %ASA-5-444305: %SMART\_LIC-5-AUTHORIZATION\_EXPIRED: Authorization expired.

**Explanation** The device has not communicated with Cisco for an extended period of time and the device has not automatically renewed the entitlement authorizations.

**Error Message** %ASA-5-444305: %SMART\_LIC-5-COMM\_RESTORED: Communications with Cisco licensing cloud restored.

**Explanation** Smart Agent communication with the Cisco licensing service is restored.

**Error Message** %ASA-5-444305: %SMART\_LIC-5-COMM\_INIT\_FAILED: Failed to initialize communications with the Cisco Licensing Cloud.



**Explanation** Smart Agent could not initialize communication with the Cisco licensing service.

**Recommended Action** None.

## 444306

**Error Message** %ASA-6-444306: %SMART\_LIC-6-AGENT\_READY: Smart Agent for Licensing is initialized.

**Explanation** Smart Agent is initialized and ready for use.

**Error Message** %ASA-6-444306: %SMART\_LIC-6-AGENT\_ENABLED: Smart Agent for Licensing is enabled.

**Explanation** Smart Agent is enabled and ready for use.

**Error Message** %ASA-6-444306: %SMART\_LIC-6-AGENT\_REG\_SUCCESS: Smart Agent for Licensing Registration with Cisco licensing cloud successful.

**Explanation** Smart Licensing registration was successful.

**Error Message** %ASA-6-444306: %SMART\_LIC-6-AGENT\_DEREG\_SUCCESS: Smart Agent for Licensing De-registration with Cisco licensing cloud successful.

**Explanation** Smart Licensing deregistration was successful.

**Error Message** %ASA-6-444306: %SMART\_LIC-6-DISABLED: Smart Agent for Licensing disabled.

**Explanation** Smart Agent has been disabled.

**Error Message** %ASA-6-444306: %SMART\_LIC-6-ID\_CERT\_RENEW\_SUCCESS: Identity certificate renewal successful.

**Explanation** Customer identity certificate has been renewed successfully and can continue to use the device.

**Error Message** %ASA-6-444306: %SMART\_LIC-6-ENTITLEMENT\_RENEW\_SUCCESS: Entitlement authorization renewal with Cisco licensing cloud successful.

**Explanation** Authorization renewal request is successful.

**Error Message** %ASA-6-444306: %SMART\_LIC-6-AUTH\_RENEW\_SUCCESS: Authorization renewal with Cisco licensing cloud successful.

**Explanation** Authorization of customer requested entitlements are successfully renewed.

**Error Message** %ASA-6-444306: %SMART\_LIC-6-HA\_ROLE\_CHANGED: Smart Agent HA role changed to role.

**Explanation** Smart Agent role on HA RP has been changed to either active or standby.

**Error Message** %ASA-6-444306: %SMART\_LIC-6-HA\_CHASSIS\_ROLE\_CHANGED: Smart Agent HA chassis role changed to role.

**Explanation** Smart Agent chassis role on HA has been changed to either active or standby.

**Error Message** %ASA-6-444306: %SMART\_LIC-6-AGENT\_ALREADY\_REGISTER: Smart Agent is already registered with the Cisco licensing cloud.

**Explanation** Smart Licensing has already registered with Cisco. Use the force option to register again.

**Error Message** %ASA-6-444306: %SMART\_LIC-6-AGENT\_ALREADY\_DEREGISTER: Smart Agent is already Deregistered with the CSSM.

**Explanation** Smart Licensing has already de-registered with Cisco, use the force option to register again.

**Error Message** %ASA-6-444306: %SMART\_LIC-6-EXPORT\_CONTROLLED: Usage of export controlled features is status.

**Explanation** Notification of whether the usage of export controlled features is allowed or not allowed. This message is generated following the registration with Cisco licensing cloud.

**Recommended Action** None.

## 444307

**Error Message** %ASA-7-444307: %SMART\_LIC-7-DAILY\_JOB\_TIMER\_RESET: Daily job timer reset.

**Explanation** This message is only used for testing purposes and does not indicate an error.

**Recommended Action** None.

## 446001

**Error Message** %ASA-4-446001: Maximum TLS Proxy session limit of *max\_sess* reached.

**Explanation** A configured maximum session limit for TLS proxy was reached. New sessions beyond the limit were denied.

- *max\_sess* —The currently effective maximum session limit

**Recommended Action** If more TLS sessions are needed, use the **tls-proxy maximum-sessions max\_sess** command to increase the limit. Alternatively, you can use the **tls-proxy proxy\_name** and **tls-proxy maximum-sessions max\_sess** commands, and then reboot for the commands to take effect.

## 446003

**Error Message** %ASA-4-446003: Denied TLS Proxy session from *src\_int* :*src\_ip* /*src\_port* to *dst\_int* :*dst\_ip* /*dst\_port* , UC-IME license is disabled.

**Explanation** The UC-IME license is either on or off. Once enabled, UC-IME can use any number of available TLS sessions, according to the Secure Firewall ASA limit and the K8 export limit.

- *src\_int* —The source interface name (inside or outside)
- *src\_ip* —The source IP address
- *src\_port* —The source port
- *dst\_int* —The destination interface name (inside or outside)
- *dst\_ip* —The destination IP address
- *dst\_port* —The destination port

**Recommended Action** Check to see if UC-IME is disabled. If so, activate it.

## 447001

**Error Message** %ASA-4-447001: ASP DP to CP *queue\_name* was full. Queue length *length* , limit *limit*

**Explanation** This message indicates a particular data path (DP) to control point (CP) event queue is full, and one or more multiple enqueue actions have failed. If the event contains a packet block, such as for CP application inspection, the packet will be dropped by the DP, and a counter from the **show asp drop** command will increment. If the event is for punt to CP, a typical counter is the Punt no memory ASP-drop counter.

- *queue* —The name of the DP-CP event queue.
- *length* —The current number of events on the queue.
- *limit* —The maximum number of events that are allowed on the queue.

**Recommended Action** The queue-full condition reflects the fact that the load on the CP has exceeded the CP processing ability, which may or may not be a temporary condition. You should consider reducing the feature load on the CP if this message appears repeatedly. Use the **show asp event dp-cp** command to identify the features that contribute the most load on the event queue.

## 448001

**Error Message** %ASA-4-448001: Denied SRTP crypto session setup on flow from *src\_int* :*src\_ip* /*src\_port* to *dst\_int* :*dst\_ip* /*dst\_port* , licensed K8 SRTP crypto session of *limit* exceeded

**Explanation** For a K8 platform, the limit of 250 SRTP crypto sessions is enforced. Each pair of SRTP encrypt or decrypt sessions is counted as one SRTP crypto session. A call is counted toward this limit only when encryption or decryption is required for a medium, which means that if the pass-through is set for the call, even if both legs use SRTP, they are not counted toward this limit.

- *src\_int* —The source interface name (inside or outside)
- *src\_ip* —The source IP address
- *src\_port* —The source port
- *dst\_int* —The destination interface name (inside or outside)
- *dst\_ip* —The destination IP address
- *dst\_port* —The destination port
- *limit* —The K8 limit of SRTP crypto sessions (250)

**Recommended Action** None required. You can set up new SRTP crypto sessions only when existing SRTP crypto sessions have been released.

## 450001

**Error Message** ASA-4-450001: Deny traffic for protocol *protocol\_id* src *interface\_name* :*IP\_address* /*port* dst *interface\_name* :*IP\_address* /*port* , licensed host limit of *num* exceeded.

**Explanation** The licensed host limit was exceeded. This message applies to the ASA 5505 ASA only.

- *protocol\_id* —The protocol ID number
- *interface\_name* —The interface associated with the sender or receiver of the packet
- *IP\_address* —The IP address of the sender/receiver of the packet
- *port* —The port number of the packet transmitted
- *num* —The maximum host limit value

**Recommended Action** None required.





## CHAPTER 5

# Syslog Messages 500001 to 520025

This chapter contains the following sections:

- [Messages 500001 to 504002, on page 263](#)
- [Messages 505001 to 520025, on page 267](#)

## Messages 500001 to 504002

This chapter includes messages from 500001 to 504002.

### 500001

**Error Message** %ASA-5-500001: ActiveX content in java script is modified: src *src ip* dest *dest ip* on interface *interface name*

**Explanation** Ensure the blocking of Java/ActiveX content present in Java script when the policy (filter Java (or) filter ActiveX) is enabled on the Secure Firewall ASA.

**Recommended Action** None required.

### 500002

**Error Message** %ASA-5-500002: Java content in java script is modified: src *src ip* dest *dest ip* on interface *interface name*

**Explanation** Ensure the blocking of Java/ActiveX content present in Java script when the policy (filter Java (or) filter ActiveX) is enabled on the Secure Firewall ASA.

**Recommended Action** None required.

### 500003

**Error Message** %ASA-5-500003: Bad TCP hdr length (hdrlen=*bytes* , pktlen=*bytes* ) from *source\_address /source\_port* to *dest\_address /dest\_port* , flags: *tcp\_flags* , on interface *interface\_name*

**Explanation** A header length in TCP was incorrect. Some operating systems do not handle TCP resets (RSTs) correctly when responding to a connection request to a disabled socket. If a client tries to connect to an FTP

server outside the Secure Firewall ASA and the FTP server is not listening, then it sends an RST. Some operating systems send incorrect TCP header lengths, which causes this problem. UDP uses ICMP port unreachable messages.

The TCP header length may indicate that it is larger than the packet length, which results in a negative number of bytes being transferred. A negative number appears by a message as an unsigned number, which makes it appear much larger than it would be normally; for example, it may show 4 GB transferred in one second. This message should occur infrequently.

**Recommended Action** None required.

## 500004

**Error Message** %ASA-4-500004: Invalid transport field for protocol=*protocol* , from *source\_address /source\_port* to *dest\_address /dest\_port*

**Explanation** An invalid transport number was used, in which the source or destination port number for a protocol is zero. The **protocol** value is 6 for TCP and 17 for UDP.

**Recommended Action** If these messages persist, contact the administrator of the peer.

## 500005

**Error Message** %ASA-3-500005: connection terminated for *protocol* from *in\_ifc\_name :src\_address /src\_port* to *out\_ifc\_name :dest\_address /dest\_port* due to invalid combination of inspections on same flow. Inspect *inspect\_name* is not compatible with filter *filter\_name* .

**Explanation** A connection matched with single or multiple inspection and/or single or multiple filter features that are not allowed to be applied to the same connection.

- *protocol*— The protocol that the connection was using
- *in\_ifc\_name* —The input interface name
- *src\_address* —The source IP address of the connection
- *src\_port* —The source port of the connection
- *out\_ifc\_name* —The output interface name
- *dest\_address* —The destination IP address of the connection
- *dest\_port* —The destination port of the packet
- *inspect\_name* —The inspect or filter feature name
- *filter\_name* —The filter feature name

**Recommended Action** Review the **class-map**, **policy-map**, **service-policy**, and/or **filter** command configurations that are causing the referenced inspection and/or filter features that are matched for the connection. The rules for inspection and filter feature combinations for a connection are as follows:

- The **inspect http [http-policy-map]** and/or **filter url** and/or **filter java** and/or **filter activex** commands are valid.
- The **inspect ftp [ftp-policy-map]** and/or **filter ftp** commands are valid.
- The **filter https** command with any other **inspect** command or **filter** command is not valid.

Besides these listed combinations, any other inspection and/or filter feature combinations are not valid.

## 501101

**Error Message** %ASA-5-501101: User transitioning priv level

**Explanation** The privilege level of a command was changed.

**Recommended Action** None required.

## 502101

**Error Message** %ASA-5-502101: New user added to local dbase: Uname: *user* Priv: *privilege\_level*  
Encpass: *string*

**Explanation** A new username record was created, which included the username, privilege level, and encrypted password.

**Recommended Action** None required.

## 502102

**Error Message** %ASA-5-502102: User deleted from local dbase: Uname: *user* Priv: *privilege\_level*  
Encpass: *string*

**Explanation** A username record was deleted, which included the username, privilege level, and encrypted password.

**Recommended Action** None required.

## 502103

**Error Message** %ASA-5-502103: User priv level changed: Uname: *user* From: *privilege\_level* To:  
*privilege\_level*

**Explanation** The privilege level of a user changed.

**Recommended Action** None required.

## 502111

**Error Message** %ASA-5-502111: New group policy added: name: *policy\_name* Type: *policy\_type*

**Explanation** A group policy was configured using the **group-policy** CLI command.

- **policy\_name**—The name of the group policy
- **policy\_type**—Either internal or external

**Recommended Action** None required.

## 502112

**Error Message** %ASA-5-502112: Group policy deleted: name: *policy\_name* Type: *policy\_type*

**Explanation** A group policy has been removed using the **group-policy** CLI command.

- **policy\_name**—The name of the group policy
- **policy\_type**—Either internal or external

**Recommended Action** None required.

## 503001

**Error Message** %ASA-5-503001: Process number, Nbr IP\_address on interface\_name from string to string , reason

**Explanation** An OSPFv2 neighbor has changed its state. The message describes the change and the reason for it. This message appears only if the **log-adjacency-changes** command is configured for the OSPF process.

**Recommended Action** Copy the message exactly as it appears, and report it to the Cisco TAC.

## 503002

**Error Message** %ASA-5-503002: The last key has expired for interface nameif, packets sent using last valid key.

**Explanation** None of the security associations have a lifetime that include the current system time.

**Recommended Action** Configure a new security association or alter the lifetime of a current security association.

## 503003

**Error Message** %ASA-5-503003: Packet sent | received on interface nameif with expired Key ID key-id.

**Explanation** The Key ID configured on the interface expired.

**Recommended Action** Configure a new key.

## 503004

**Error Message** %ASA-5-503004: Key ID key-id in key chain key-chain-name does not have a key.

**Explanation** OSPF has been configured to use cryptographic authentication, however a key or password has not been configured.

**Recommended Action** Configure a new security association or alter the lifetime of a current security association.

## 503005

**Error Message** %ASA-5-503005: Key ID key-id in key chain key-chain-name does not have a cryptographic algorithm.

**Explanation** OSPF has been configured to use cryptographic authentication, however an algorithm has not been configured.

**Recommended Action** Configure a cryptographic-algorithm for the security association.



## 503101

**Error Message** %ASA-5-503101: Process *d*, Nbr *i* on *s* from *s* to *s*, *s*

**Explanation** An OSPFv3 neighbor has changed its state. The message describes the change and the reason for it. This message appears only if the **log-adjacency-changes** command is configured for the OSPF process.

**Recommended Action** None required.

## 504001

**Error Message** %ASA-5-504001: Security context *context\_name* was added to the system

**Explanation** A security context was successfully added to the Secure Firewall ASA.

**Recommended Action** None required.

## 504002

**Error Message** %ASA-5-504002: Security context *context\_name* was removed from the system

**Explanation** A security context was successfully removed from the Secure Firewall ASA.

**Recommended Action** None required.

## Messages 505001 to 520025

This chapter includes messages from 505001 to 520025.

## 505001

**Error Message** %ASA-5-505001: Module *string one* is shutting down. Please wait...

**Explanation** A module is being shut down.

**Recommended Action** None required.

## 505002

**Error Message** %ASA-5-505002: Module *ips* is reloading. Please wait...

**Explanation** An IPS module is being reloaded.

**Recommended Action** None required.

## 505003

**Error Message** %ASA-5-505003: Module *string one* is resetting. Please wait...

**Explanation** A module is being reset.

**Recommended Action** None required.

**505004**

**Error Message** %ASA-5-505004: Module *string one* shutdown is complete.

**Explanation** A module has been shut down.

**Recommended Action** None required.

**505005**

**Error Message** %ASA-5-505005: Module *module\_name* is initializing control communication. Please wait...

**Explanation** A module has been detected, and the Secure Firewall ASA is initializing control channel communication with it.

**Recommended Action** None required.

**505006**

**Error Message** %ASA-5-505006: Module *string one* is Up.

**Explanation** A module has completed control channel initialization and is in the UP state.

**Recommended Action** None required.

**505007**

**Error Message** %ASA-5-505007: Module *module\_id* is recovering. Please wait...

**Error Message** %ASA-5-505007: Module *prod\_id* in slot *slot\_num* is recovering. Please wait...

**Explanation** A software module is being recovered with the **sw-module module service-module-name recover boot** command, or a hardware module is being recovered with the **hw-module module slotnum recover boot** command.

- **module\_id**—The name of the software services module.
- **prod\_id**—The product ID string.
- **slot\_num**—The slot in which the hardware services module is installed. Slot 0 indicates the system main board, and slot 1 indicates the module installed in the expansion slot.

**Recommended Action** None required.

**505008**

**Error Message** %ASA-5-505008: Module *module\_id* software is being updated to *newver* (currently *ver* )

**Error Message** %ASA-5-505008: Module *module\_id* in slot *slot\_num* software is being updated to *newver* (currently *ver* )

**Explanation** The services module software is being upgraded. The update is proceeding normally.

- **module\_id**—The name of the software services module
- **slot\_num**—The slot number that contains the hardware services module

- *>newver*—The new version number of software that was not successfully written to the module (for example, 1.0(1)0)
- *>ver*—The current version number of the software on the module (for example, 1.0(1)0)

**Recommended Action** None required.

## 505009

**Error Message** %ASA-5-505009: Module *string one* software was updated to *newver*

**Explanation** The 4GE SSM module software was successfully upgraded.

- *string one*—The text string that specifies the module
- *newver*—The new version number of software that was not successfully written to the module (for example, 1.0(1)0)
- *ver*—The current version number of the software on the module (for example, 1.0(1)0)

**Recommended Action** None required.

## 505010

**Error Message** %ASA-5-505010: Module in slot *slot* removed.

**Explanation** An SSM was removed from the Secure Firewall ASA chassis.

- *slot*—The slot from which the SSM was removed

**Recommended Action** None required.

## 505011

**Error Message** %ASA-1-505011: Module *ips* , data channel communication is UP.

**Explanation** The data channel communication recovered from a DOWN state.

**Recommended Action** None required.

## 505012

**Error Message** %ASA-5-505012: Module *module\_id* , application stopped *application* , version *version*

**Error Message** %ASA-5-505012: Module *prod\_id* in slot *slot\_num* , application stopped *application* , version *version*

**Explanation** An application was stopped or removed from a services module. This may occur when the services module upgraded an application or when an application on the services module was stopped or uninstalled.

- **module\_id**—The name of the software services module
- *prod\_id*—The product ID string for the device installed in the hardware services module
- *slot\_num*—The slot in which the application was stopped
- **application**—The name of the application stopped
- **version**—The application version stopped

**Recommended Action** If an upgrade was not occurring on the 4GE SSM or the application was not intentionally stopped or uninstalled, review the logs from the 4GE SSM to determine why the application stopped.

## 505013

**Error Message** %ASA-5-505013: Module *module\_id* application changed from: *application* version *version* to: *newapplication* version *newversion* .

**Error Message** %ASA-5-505013: Module *prod\_id* in slot *slot\_num* application changed from: *application* version *version* to: *newapplication* version *newversion* .

**Explanation** An application version changed, such as after an upgrade. A software update for the application on the services module is complete.

- **module\_id**—The name of the software services module
- **application**—The name of the application that was upgraded
- **version**—The application version that was upgraded
- **prod\_id**—The product ID string for the device installed in the hardware services module
- **slot\_num**—The slot in which the application was upgraded
- **application**—The name of the application that was upgraded
- **version**—The application version that was upgraded
- **newapplication**—The new application name
- **newversion**—The new application version

**Recommended Action** Verify that the upgrade was expected and that the new version is correct.

## 505014

**Error Message** %ASA-1-505014: Module *module\_id* , application *down name* , version *version* *reason*

**Error Message** %ASA-1-505014: Module *prod\_id* in slot *slot\_num* , application *down name* , version *version* *reason*

**Explanation** The application running on the module is disabled.

- **module\_id**—The name of the software services module
- **prod\_id**—The product ID string for the device installed in the hardware services module
- **slot\_num**—The slot in which the application was disabled. Slot 0 indicates the system main board, and slot 1 indicates the module installed in the expansion slot.
- **name**—Application name (string)
- **application**—The name of the application that was upgraded
- **version**—The application version (string)
- **reason**—Failure reason (string)

**Recommended Action** If the problem persists, contact the Cisco TAC.

## 505015

**Error Message** %ASA-1-505015: Module *module\_id* , application *up application* , version *version*

**Error Message** %ASA-1-505015: Module *prod\_id* in slot *slot\_num* , application up *application* , version *version*

**Explanation** The application running on the SSM in slot *slot\_num* is up and running.

- **module\_id**—The name of the software services module
- **prod\_id**—The product ID string for the device installed in the hardware services module
- **slot\_num**—The slot in which the application is running. Slot 0 indicates the system main board, and slot 1 indicates the module installed in the expansion slot.
- **application**—The application name (string)
- **version**—The application version (string)

**Recommended Action** None required.

## 505016

**Error Message** %ASA-3-505016: Module *module\_id* application changed from: *name* version *version* state *state* to: *name* version *version* state *state* .

**Error Message** %ASA-3-505016: Module *prod\_id* in slot *slot\_num* application changed from: *name* version *version* state *state* to: *name* version *version* state *state* .

**Explanation** The application version or a name change was detected.

- **module\_id**—The name of the software services module
- **prod\_id**—The product ID string for the device installed in the hardware services module
- **slot\_num**—The slot in which the application changed. Slot 0 indicates the system main board, and slot 1 indicates the module installed in the expansion slot.
- **name**—Application name (string)
- **version**—The application version (string)
- **state**—Application state (string)
- **application**—The name of the application that changed

**Recommended Action** Verify that the change was expected and that the new version is correct.

## 506001

**Error Message** %ASA-5-506001: *event\_source\_string* *event\_string*

**Explanation** The status of a file system has changed. The event and the source of the event that caused a file system to become available or unavailable appear. Examples of sources and events that can cause a file system status change are as follows:

- External CompactFlash removed
- External CompactFlash inserted
- External CompactFlash unknown event

**Recommended Action** None required.

## 507001

**Error Message** %ASA-5-507001: Terminating TCP-Proxy connection from *interface\_inside:source\_address/source\_port* to *interface\_outside :dest\_address /dest\_port* - reassembly limit of *limit* bytes exceeded

**Explanation** The assembly buffer limit was exceeded during TCP segment reassembly.

- **source\_address/source\_port**—The source IP address and the source port of the packet initiating the connection
- **dest\_address/dest\_port**—The destination IP address and the destination port of the packet initiating the connection
- **interface\_inside**—The name of the interface on which the packet which initiated the connection arrives
- **interface\_outside**—The name of the interface on which the packet which initiated the connection exits
- **limit**—The configured embryonic connection limit for the traffic class

**Recommended Action** None required.

## 507002

**Error Message** %ASA-4-507002: Data copy in proxy-mode exceeded the buffer limit

**Explanation** An operational error occurred during processing of a fragmented TCP message.

**Recommended Action** None required.

## 507003

**Error Message** %ASA-3-507003: The flow of type *protocol* from the originating interface: *src\_ip /src\_port* to *dest\_if :dest\_ip /dest\_port* terminated by inspection engine, *reason-*

**Explanation** The TCP proxy or session API terminated a connection for various reasons, which are provided in the message.

- **protocol**—The protocol for the flow
- **src\_ip**—The source IP address for the flow
- *src\_port* —The name of the source port for the flow
- *dest\_if*—The destination interface for the flow
- *dest\_ip* —The destination IP address for the flow
- *dest\_port* —The destination port for the flow
- *reason* —The description of why the flow is being terminated by the inspection engine. Valid reasons include:
  - Failed to create flow
  - Failed to initialize session API
  - Filter rules installed/matched are incompatible
  - Failed to consolidate new buffer data with original
  - Reset unconditionally
  - Reset based on “service reset inbound” configuration
  - Disconnected, dropped packet

- Packet length changed
- Reset reflected back to sender
- Proxy inspector reset unconditionally
- Proxy inspector drop reset
- Proxy inspector received data after FIN
- Proxy inspector disconnected, dropped packet
- Inspector reset unconditionally
- Inspector drop reset
- Inspector received data after FIN
- Inspector disconnected, dropped packet
- Could not buffer unprocessed data
- Session API proxy forward failed
- Conversion of inspect data to session data failed
- SSL channel for TLS proxy is closed
- The number of unprocessed segments are more than the threshold value

**Recommended Action** None required.

## 508001

**Error Message** %ASA-5-508001: DCERPC *message\_type* non-standard *version\_type* *version* *version\_number* from *src\_if* :*src\_ip* /*src\_port* to *dest\_if* :*dest\_ip* /*dest\_port* , terminating connection.

**Explanation** During DCERPC inspection, a message header included a nonstandard major or minor version.

- **message\_type**—The DCERPC message type
- **version\_type**—The version type, which can be major or minor
- **version\_number**—The nonstandard version in the message header

**Recommended Action** If this is a valid version, and the problem persists, contact the Cisco TAC.

## 508002

**Error Message** %ASA-5-508002: DCERPC response has low endpoint port *port\_number* from *src\_if* :*src\_ip* /*src\_port* to *dest\_if* :*dest\_ip* /*dest\_port* , terminating connection.

**Explanation** During DCERPC inspection, a response message included an endpoint port number less than 1024 (in the range of well-known server ports).

**Recommended Action** None required.

## 509001

**Error Message** %ASA-5-509001: Connection attempt from *src\_intf* :*src\_ip* /*src\_port* [(*idfw\_user* | *FQDN\_string* ), *sg\_info* ] to *dst\_intf* :*dst\_ip* /*dst\_port* [(*idfw\_user* | *FQDN\_string* ), *sg\_info* ] was prevented by "no forward" command.

**Explanation** The **no forward interface** command was entered to block traffic from the source interface to the destination interface given in the message. This command is required on low-end platforms to allow the creation of interfaces beyond the licensed limit.

- **src\_intf**—The name of the source interface to which the **no forward interface** command restriction applies
- **dst\_intf**—The name of the destination interface to which the **no forward interface** command restriction applies
- **sg\_info**—The security group name or tag for the specified IP address

**Recommended Action** Upgrade the license to remove the requirement of this command on low-end platforms, then remove the command from the configuration.

## 520001

**Error Message** %ASA-3-520001: *error\_string*

**Explanation** A malloc failure occurred in ID Manager. The error string can be either of the following:

- Malloc failure—*id\_reserve*
- Malloc failure—*id\_get*

**Recommended Action** Contact the Cisco TAC.

## 520002

**Error Message** %ASA-3-520002: bad new ID table size

**Explanation** A bad new table request to the ID Manager occurred.

**Recommended Action** Contact the Cisco TAC.

## 520003

**Error Message** %ASA-3-520003: bad id in *error\_string* (id: *0xid\_num*)

**Explanation** An ID Manager error occurred. The error string may be any of the following:

- *id\_create\_new\_table* (no more entries allowed)
- *id\_destroy\_table* (bad table ID)
- *id\_reserve*
- *id\_reserve* (bad ID)
- *id\_reserve*: ID out of range
- *id\_reserve* (unassigned table ID)
- *id\_get* (bad table ID)
- *id\_get* (unassigned table ID)
- *id\_get* (out of IDs!)



- `id_to_ptr`
- `id_to_ptr` (bad ID)
- `id_to_ptr` (bad table ID)
- `id_get_next_id_ptr` (bad table ID)
- `id_delete`
- `id_delete` (bad ID)
- `id_delete` (bad table key)

**Recommended Action** Contact the Cisco TAC.

## 520004

**Error Message** %ASA-3-520004: *error\_string*

**Explanation** An `id_get` was attempted at the interrupt level.

**Recommended Action** Contact the Cisco TAC.

## 520005

**Error Message** %ASA-3-520005: *error\_string*

**Explanation** An internal error occurred with the ID Manager.

**Recommended Action** Contact the Cisco TAC.

## 520010

**Error Message** %ASA-3-520010: Bad queue elem - *qelem\_ptr* : *flink flink\_ptr* , *blink blink\_ptr*  
 , *flink-blink flink\_blink\_ptr* , *blink-flink blink\_flink\_ptr*

**Explanation** An internal software error occurred, which can be any of the following:

- *qelem\_ptr* —A pointer to the queue data structure
- *flink\_ptr* —A pointer to the forward element of the queue data structure
- *blink\_ptr* —A pointer to the backward element of the queue data structure
- *flink\_blink\_ptr* —A pointer to the forward element's backward pointer of the queue data structure
- *blink\_flink\_ptr* —A pointer to the backward element's forward pointer of the queue data structure

**Recommended Action** Contact the Cisco TAC.

## 520011

**Error Message** %ASA-3-520011: Null queue elem

**Explanation** An internal software error occurred.

**Recommended Action** Contact the Cisco TAC.

## 520013

**Error Message** %ASA-3-520013: Regular expression access check with bad list `acl_ID`

**Explanation** A pointer to an access list is invalid.

**Recommended Action** The event that caused this message to be issued should not have occurred. It can mean that one or more data structures have been overwritten. If this message recurs, and you decide to report it to your TAC representative, you should copy the text of the message exactly as it appears and include the associated stack trace. Because access list corruption may have occurred, a TAC representative should verify that access lists are functioning correctly.

## 520020

**Error Message** %ASA-3-520020: No memory available

**Explanation** The system is out of memory.

**Recommended Action** Try one of the following actions to correct the problem:

- Reduce the number of routes accepted by this router.
- Upgrade hardware.
- Use a smaller subset image on run-from-RAM platforms.

## 520021

**Error Message** %ASA-3-520021: Error deleting trie entry, *error\_message*

**Explanation** A software programming error occurred. The error message can be any of the following:

- Inconsistent annotation
- Couldn't find our annotation
- Couldn't find deletion target

**Recommended Action** Copy the error message exactly as it appears, and report it to Cisco TAC.

## 520022

**Error Message** %ASA-3-520022: Error adding mask entry, *error\_message*

**Explanation** A software or hardware error occurred. The error message can be any of the following:

- Mask already in tree
- Mask for route not entered
- Non-unique normal route, mask not entered

**Recommended Action** Copy the error message exactly as it appears, and report it to Cisco TAC.

## 520023

**Error Message** %ASA-3-520023: Invalid pointer to head of tree, 0x *radix\_node\_ptr*

**Explanation** A software programming error occurred.

**Recommended Action** Copy the error message exactly as it appears, and report it to Cisco TAC.

## 520024

**Error Message** %ASA-3-520024: Orphaned mask #radix\_mask\_ptr, refcount= radix\_mask\_ptr's ref count at #radix\_node\_address, next= #radix\_node\_nxt

**Explanation** A software programming error occurred.

**Recommended Action** Copy the error message exactly as it appears, and report it to Cisco TAC.

## 520025

**Error Message** %ASA-3-520025: No memory for radix initialization: err\_msg

**Explanation** The system ran out of memory during initialization. This should only occur if an image is too large for the existing dynamic memory. The error message can be either of the following: Initializing leaf nodesMask housekeeping

**Recommended Action** Use a smaller subset image or upgrade hardware.





## CHAPTER 6

# Syslog Messages 602101 to 622102

This chapter contains the following sections:

- [Messages 602101 to 609002, on page 279](#)
- [Messages 610001 to 622102, on page 292](#)

## Messages 602101 to 609002

This section includes messages from 602101 to 609002.

### 602101

**Error Message** %ASA-6-602101: PMTU-D packet *number* bytes greater than effective mtu *number*  
dest\_addr=*dest\_address* , src\_addr=*source\_address* , prot=*protocol*

**Explanation** The Secure Firewall ASA sent an ICMP destination unreachable message and fragmentation is needed.

**Recommended Action** Make sure that the data is sent correctly.

### 602103

**Error Message** %ASA-6-602103: IPSEC: Received an ICMP Destination Unreachable from src\_addr with suggested PMTU of rcvd\_mtu; PMTU updated for SA with peer peer\_addr, SPI spi, tunnel name username, old PMTU old\_mtu, new PMTU new\_mtu.

**Explanation** The MTU of an SA was changed. When a packet is received for an IPsec tunnel, the corresponding SA is located and the MTU is updated based on the MTU suggested in the ICMP packet. If the suggested MTU is greater than 0 but less than 256, then the new MTU is set to 256. If the suggested MTU is 0, the old MTU is reduced by 256 or it is set to 256—whichever value is greater. If the suggested MTU is greater than 256, then the new MTU is set to the suggested value.

- src\_addr—IP address of the PMTU sender
- rcvd\_mtu—Suggested MTU received in the PMTU message
- peer\_addr—IP address of the IPsec peer
- spi—IPsec Security Parameter Index
- username—Username associated with the IPsec tunnel
- old\_mtu—Previous MTU associated with the IPsec tunnel

- *new\_mtu*—New MTU associated with the IPsec tunnel

**Recommended Action** None required.

## 602104

**Error Message** %ASA-6-602104: IPSEC: Received an ICMP Destination Unreachable from *src\_addr* , PMTU is unchanged because suggested PMTU of *rcvd\_mtu* is equal to or greater than the current PMTU of *curr\_mtu* , for SA with peer *peer\_addr* , SPI *spi* , tunnel name *username* .

**Explanation** An ICMP message was received indicating that a packet sent over an IPsec tunnel exceeded the path MTU, and the suggested MTU was greater than or equal to the current MTU. Because the MTU value is already correct, no MTU adjustment is made. This may happen when multiple PMTU messages are received from different intermediate stations, and the MTU is adjusted before the current PMTU message is processed.

- *src\_addr*—IP address of the PMTU sender
- *rcvd\_mtu*—Suggested MTU received in the PMTU message
- *curr\_mtu*—Current MTU associated with the IPsec tunnel
- *peer\_addr*—IP address of the IPsec peer
- *spi*—IPsec Security Parameter Index
- *username* —Username associated with the IPsec tunnel

**Recommended Action** None required.

## 602303

**Error Message** %ASA-6-602303: IPSEC: An *direction tunnel\_type* SA (SPI=*spi* ) between *local\_IP* and *remote\_IP* (*username* ) has been created.

**Explanation** A new SA was created.

- *direction*—SA direction (inbound or outbound)
- *tunnel\_type*—SA type (remote access or L2L)
- *spi*—IPsec Security Parameter Index
- *local\_IP*—IP address of the tunnel local endpoint
- *remote\_IP*—IP address of the tunnel remote endpoint
- *>username* —Username associated with the IPsec tunnel

**Recommended Action** None required.

## 602304

**Error Message** %ASA-6-602304: IPSEC: An *direction tunnel\_type* SA (SPI=*spi* ) between *local\_IP* and *remote\_IP* (*username* ) has been deleted.

**Explanation** An SA was deleted.

- *direction*—SA direction (inbound or outbound)
- *tunnel\_type*—SA type (remote access or L2L)
- *spi*—IPsec Security Parameter Index
- *local\_IP*—IP address of the tunnel local endpoint
- *remote\_IP*—IP address of the tunnel remote endpoint

- *>username* —Username associated with the IPsec tunnel

**Recommended Action** None required.

## 602305

**Error Message** %ASA-3-602305: IPSEC: SA creation error, source *source address* , destination *destination address* , reason *error string*

**Explanation** An error has occurred while creating an IPsec security association.

**Recommended Action** This is typically a transient error condition. If this message occurs consistently, contact the Cisco TAC.

## 602306

**Error Message** %ASA-3-602306: IPSEC: SA change peer IP error, SPI: *IPsec SPI*, (src {*original src IP address* | *original src port*}, dest {*original dest IP address*| *original dest port*} => src {*new src IP address* | *new src port*}, dest: {*new dest IP address* | *new dest port*}), reason *failure reason*

**Explanation** An error has occurred while updating an IPsec tunnel's peer address for Mobile IKE and the peer address could not be changed.

**Recommended Action** This is typically a transient error condition. If this message occurs consistently, contact the Cisco TAC.

## 603101

**Error Message** %ASA-6-603101: PPTP received out of seq or duplicate pkt, tnl\_id=*number* , sess\_id=*number* , seq=*number* .

**Explanation** The ASA received a PPTP packet that was out of sequence or duplicated.

**Recommended Action** If the packet count is high, contact the peer administrator to check the client PPTP configuration.

## 603102

**Error Message** %ASA-6-603102: PPP virtual interface *interface\_name* - user: *user aaa* authentication started.

**Explanation** The ASA sent an authentication request to the AAA server.

**Recommended Action** None required.

## 603103

**Error Message** %ASA-6-603103: PPP virtual interface *interface\_name* - user: *user aaa* authentication *status*

**Explanation** The ASA received an authentication response from the AAA server.

**Recommended Action** None required.

## 603104

**Error Message** %ASA-6-603104: PPTP Tunnel created, tunnel\_id is *number* , remote\_peer\_ip is *remote\_address* , ppp\_virtual\_interface\_id is *number* , client\_dynamic\_ip is *IP\_address* , username is *user* , MPPE\_key\_strength is *string*

**Explanation** A PPTP tunnel was created.

**Recommended Action** None required.

## 603105

**Error Message** %ASA-6-603105: PPTP Tunnel deleted, tunnel\_id = *number* , remote\_peer\_ip = *remote\_address*

**Explanation** A PPTP tunnel was deleted.

**Recommended Action** None required.

## 603106

**Error Message** %ASA-6-603106: L2TP Tunnel created, tunnel\_id is *number* , remote\_peer\_ip is *remote\_address* , ppp\_virtual\_interface\_id is *number* , client\_dynamic\_ip is *IP\_address* , username is *user*

**Explanation** An L2TP tunnel was created. The username is hidden when invalid or unknown, but appears when valid or the **no logging hide username** command has been configured.

**Recommended Action** None required.

## 603107

**Error Message** %ASA-6-603107: L2TP Tunnel deleted, tunnel\_id = *number* , remote\_peer\_ip = *remote\_address*

**Explanation** An L2TP tunnel was deleted.

**Recommended Action** None required.

## 603108

**Error Message** %ASA-6-603108: Built PPTP Tunnel at *interface\_name* , tunnel-id = *number* , remote-peer = *IP\_address* , virtual-interface = *number* , client-dynamic-ip = *IP\_address* , username = *user* , MPPE-key-strength = *number*

**Explanation** A new PPPoE tunnel was created.

**Recommended Action** None required.

## 603109

**Error Message** %ASA-6-603109: Teardown PPPOE Tunnel at *interface\_name* , tunnel-id = *number* , remote-peer = *IP\_address*



**Explanation** A new PPPoE tunnel was deleted.

**Recommended Action** None required.

## 603110

**Error Message** %ASA-4-603110: Failed to establish L2TP session, tunnel\_id = *tunnel\_id* , remote\_peer\_ip = *peer\_ip* , user = *username* . Multiple sessions per tunnel are not supported

**Explanation** An attempt to establish a second session was detected and denied. Cisco does not support multiple L2TP sessions per tunnel.

- *tunnel\_id* —The L2TP tunnel ID
- *peer\_ip* —The peer IP address
- *username* —The name of the authenticated user

**Recommended Action** None required.

## 604101

**Error Message** %ASA-6-604101: DHCP client interface *interface\_name* : Allocated ip = *IP\_address* , mask = *netmask* , gw = *gateway\_address*

**Explanation** The Secure Firewall ASA DHCP client successfully obtained an IP address from a DHCP server. The dhcpc command statement allows the Secure Firewall ASA to obtain an IP address and network mask for a network interface from a DHCP server, as well as a default route. The default route statement uses the gateway address as the address of the default router.

**Recommended Action** None required.

## 604102

**Error Message** %ASA-6-604102: DHCP client interface *interface\_name* : address released

**Explanation** The Secure Firewall ASA DHCP client released an allocated IP address back to the DHCP server.

**Recommended Action** None required.

## 604103

**Error Message** %ASA-6-604103: DHCP daemon interface *interface\_name* : address granted *MAC\_address* (*IP\_address* )

**Explanation** The Secure Firewall ASA DHCP server granted an IP address to an external client.

**Recommended Action** None required.

## 604104

**Error Message** %ASA-6-604104: DHCP daemon interface *interface\_name* : address released *build\_number* (*IP\_address* )

**Explanation** An external client released an IP address back to the Secure Firewall ASA DHCP server.

**Recommended Action** None required.

## 604105

**Error Message** %ASA-4-604105: DHCPD: Unable to send DHCP reply to client *hardware\_address* on interface *interface\_name* . Reply exceeds options field size (*options\_field\_size* ) by *number\_of\_octets* octets.

**Explanation** An administrator can configure the DHCP options to return to the DHCP client. Depending on the options that the DHCP client requests, the DHCP options for the offer could exceed the message length limits. A DHCP offer cannot be sent, because it will not fit within the message limits.

- *hardware\_address*—The hardware address of the requesting client.
- *interface\_name*— The interface to which server messages are being sent and received
- *options\_field\_size*—The maximum options field length. The default is 312 octets, which includes 4 octets to terminate.
- *number\_of\_octets*—The number of exceeded octets.

**Recommended Action** Reduce the size or number of configured DHCP options.

## 604201

**Error Message** %ASA-6-604201: DHCPv6 PD client on interface <pd-client-iface> received delegated prefix <prefix> from DHCPv6 PD server <server-address> with preferred lifetime <in-seconds> seconds and valid lifetime <in-seconds> seconds.

**Explanation** This syslog is displayed whenever DHCPv6 PD client is received with delegated prefix from PD server as part of initial 4-way exchange. In the case of multiple prefixes, the syslog is displayed for each prefix.

- *pd-client-iface*—The interface name on which the DHCPv6 PD client is enabled.
- *prefix*—Prefix received from DHCPv6 PD server.
- *server-address*—DHCPv6 PD server address.
- *in-seconds*—Associated preferred and valid lifetime in seconds for delegated prefixes.

**Recommended Action** None.

## 604202

**Error Message** %ASA-6-604202: DHCPv6 PD client on interface <pd-client-iface> releasing delegated prefix <prefix> received from DHCPv6 PD server <server-address>.

**Explanation** This syslog is displayed whenever DHCPv6 PD Client is releasing delegated prefix(s) received from PD Server upon no configuration. In the case of multiple prefixes, the syslog is displayed for each prefix.

- *pd-client-iface*—The interface name on which the DHCPv6 PD client is enabled.
- *prefix*—Prefix received from DHCPv6 PD server.
- *server-address*—DHCPv6 PD server address.

**Recommended Action** None.

## 604203

**Error Message** %ASA-6-604203: DHCPv6 PD client on interface <pd-client-iface> renewed delegated prefix <prefix> from DHCPv6 PD server <server-address> with preferred lifetime <in-seconds> seconds and valid lifetime <in-seconds> seconds.

**Explanation** This syslog is displayed whenever DHCPv6 PD Client initiate renewal of previously allocated delegated prefix from PD Server and upon successful. In the case of multiple prefixes, the syslog is displayed for each prefix.

- *pd-client-iface*—The interface name on which the DHCPv6 PD client is enabled.
- *prefix*—Prefix received from DHCPv6 PD server.
- *server-address*—DHCPv6 PD server address.
- *in-seconds*—Associated preferred and valid lifetime in seconds for delegated prefixes.

**Recommended Action** None.

## 604204

**Error Message** %ASA-6-604204: DHCPv6 delegated prefix <delegated prefix> got expired on interface <pd-client-iface>, received from DHCPv6 PD server <server-address>.

**Explanation** This syslog is displayed whenever DHCPv6 PD Client received delegated prefix is getting expired.

- *pd-client-iface*—The interface name on which the DHCPv6 PD client is enabled.
- *prefix*—Prefix received from DHCPv6 PD server.
- *delegated prefix*—The delegated prefix received from DHCPv6 PD server.

**Recommended Action** None.

## 604205

**Error Message** %ASA-6-604205: DHCPv6 client on interface <client-iface> allocated address <ipv6-address> from DHCPv6 server <server-address> with preferred lifetime <in-seconds> seconds and valid lifetime <in-seconds> seconds

**Explanation** This syslog is displayed whenever DHCPv6 Client address is received from DHCPv6 Server as part of initial 4-way exchange and is valid. In the case of multiple addresses, the syslog is displayed for each received address.

- *client-iface*—The interface name on which the DHCPv6 client address is enabled.
- *ipv6-address*—IPv6 Address received from DHCPv6 server.
- *server-address*—DHCPv6 server address.
- *in-seconds*—Associated preferred and valid lifetime in seconds for client address.

**Recommended Action** None.

## 604206

**Error Message** %ASA-6-604206: DHCPv6 client on interface <client-iface> releasing address <ipv6-address> received from DHCPv6 server <server-address>.

**Explanation** DHCPv6 Client is releasing received client address whenever no configuration of DHCPv6 client address is performed. In the case of multiple addresses release, the syslog is displayed for each address.

- *client-iface*—The interface name on which the DHCPv6 client address is enabled.
- *ipv6-address*—IPv6 address received from DHCPv6 server.
- *server-address*—DHCPv6 server address.

**Recommended Action** None.

## 604207

**Error Message** %ASA-6-604207: DHCPv6 client on interface <client-iface> renewed address <ipv6-address> from DHCPv6 server <server-address> with preferred lifetime <in-seconds> seconds and valid lifetime <in-seconds> seconds.

**Explanation** This syslog is displayed whenever DHCPv6 client initiates renewal of previously allocated address from DHCPv6 server. In the case of multiple addresses, the syslog is displayed for each renewed address.

- *client-iface*—The interface name on which the DHCPv6 client address is enabled.
- *ipv6-address*—IPv6 Address received from DHCPv6 server.
- *server-address*—DHCPv6 server address.
- *in-seconds*—Associated preferred and valid lifetime in seconds for client address.

**Recommended Action** None.

## 604208

**Error Message** %ASA-6-604208: DHCPv6 client address <ipv6-address> got expired on interface <client-iface>, received from DHCPv6 server <server-address>

**Explanation** This syslog is displayed whenever DHCPv6 client received address is getting expired.

- *client-iface*—The interface name on which the DHCPv6 client address is enabled.
- *ipv6-address*—IPv6 Address received from DHCPv6 server.
- *server-address*—DHCPv6 server address.

**Recommended Action** None.

## 605004

**Error Message** %ASA-6-605004: Login denied from *source-address/source-port* to *interface:destination/service* for user "username "

**Explanation** The following form of the message appears when the user attempts to log in to the console:

```
Login denied from serial to console for user "username"
```

An incorrect login attempt or a failed login to the Secure Firewall ASA occurred. For all logins, three attempts are allowed per session, and the session is terminated after three incorrect attempts. For SSH and Telnet logins, this message is generated after the third failed attempt or if the TCP session is terminated after one or more failed attempts. For other types of management sessions, this message is generated after every failed attempt.

The username is hidden when invalid or unknown, but appears when valid or the **no logging hide username** command has been configured.

- *source-address*— Source address of the login attempt
- *source-port*— Source port of the login attempt
- *interface*— Destination management interface
- *destination*— Destination IP address
- *service*— Destination service
- *username* — Destination management interface

**Recommended Action** If this message appears infrequently, no action is required. If this message appears frequently, it may indicate an attack. Communicate with the user to verify the username and password.

## 605005

**Error Message** %ASA-6-605005: Login permitted from *source-address /source-port* to *interface:destination /service* for user "username "

The following form of the message appears when the user logs in to the console:

```
Login permitted from serial to console for user "username"
```

**Explanation** A user was authenticated successfully, and a management session started.

- *source-address*— Source address of the login attempt
- *source-port*— Source port of the login attempt
- *interface*— Destination management interface
- *destination*— Destination IP address
- *service*— Destination service
- *username*— Destination management interface

**Recommended Action** None required.

## 606001

**Error Message** %ASA-6-606001: ASDM session number *number* from *IP\_address* started

**Explanation** An administrator has been authenticated successfully, and an ASDM session started.

**Recommended Action** None required.

## 606002

**Error Message** %ASA-6-606002: ASDM session number *number* from *IP\_address* ended

**Explanation** An ASDM session ended.

**Recommended Action** None required.

## 606003

**Error Message** %ASA-6-606003: ASDM logging session number *id* from *IP\_address* started *id* session ID assigned

**Explanation** An ASDM logging connection was started by a remote management client.

- **IP\_address**—IP address of the remote management client

**Recommended Action** None required.

## 606004

**Error Message** %ASA-6-606004: ASDM logging session number *id* from *IP\_address* ended

**Explanation** An ASDM logging connection was terminated.

- **id**—Session ID assigned
- **IP\_address**—IP address of remote management client

**Recommended Action** None required.

## 607001

**Error Message** %ASA-6-607001: Pre-allocate SIP *connection\_type* secondary channel for *interface\_name:IP\_address/port* to *interface\_name:IP\_address* from *string* message

**Explanation** The **fixup sip** command preallocated a SIP connection after inspecting a SIP message . The **connection\_type** is one of the following strings:

- SIGNALLING UDP
- SIGNALLING TCP
- SUBSCRIBE UDP
- SUBSCRIBE TCP
- Via UDP
- Route
- RTP
- RTCP

**Recommended Action** None required.

## 607002

**Error Message** %ASA-4-607002: *action\_class* : *action* SIP *req\_resp req\_resp\_info* from *src\_ifc* :*sip /sport* to *dest\_ifc* :*dip /dport* ; *further\_info*

**Explanation** A SIP classification was performed on a SIP message, and the specified criteria were satisfied. As a result, the configured action occurs.

- **action\_class** —The class of the action: SIP Classification for SIP match commands or SIP Parameter for parameter commands
- **action** —The action taken: Dropped, Dropped connection for, Reset connection for, or Masked header flags for

- *req\_resp* —Request or Response
- *req\_resp\_info* —The SIP method name if the type is Request: INVITE or CANCEL. The SIP response code if the type is Response: 100, 183, 200.
- *src\_ifc* —The source interface name
- *sip* —The source IP address
- *sport* —The source port
- *dest\_ifc* —The destination interface name
- *dip* —The destination IP address
- *dport* —The destination port
- *further\_info* —More information appears for SIP match and SIP parameter commands, as follows:

For SIP match commands:

matched Class **id: class-name**

For example:

```
matched Class 1234: my_class
```

For SIP parameter commands:

**parameter-command: descriptive-message**

For example:

```
strict-header-validation: Mandatory header field Via is missing
state-checking: Message CANCEL is not permitted to create a Dialog.
```

**Recommended Action** None required.

## 607003

**Error Message** %ASA-6-607003: *action\_class* : Received SIP *req\_resp req\_resp\_info* from *src\_ifc* :*sip* /*sport* to *dest\_ifc* :*dip* /*dport* ; *further\_info*

**Explanation** A SIP classification was performed on a SIP message, and the specified criteria were satisfied. As a result, the standalone log action occurs.

- *action\_class* —SIP classification for SIP match commands or SIP parameter for parameter commands
- *req\_resp* —Request or Response
- *req\_resp\_info* —The SIP method name if the type is Request: INVITE or CANCEL. The SIP response code if the type is Response: 100, 183, 200.
- *src\_ifc* —The source interface name
- *sip* —The source IP address
- *sport* —The source port
- *dest\_ifc* —The destination interface name
- *dip* —The destination IP address.
- *dport* —The destination port.
- *further\_info* —More information appears for SIP match and SIP parameter commands, as follows:

For SIP match commands:

matched Class **id: class-name**

For example:

```
matched Class 1234: my_class
```

For SIP parameter commands:

**parameter-command: descriptive-message**

For example:

```
strict-header-validation: Mandatory header field Via is missing
state-checking: Message CANCEL is not permitted to create a Dialog.
```

**Recommended Action** None required.

## 607004

**Error Message** %ASA-4-607004: Phone Proxy: Dropping SIP message from *src\_if:src\_ip /src\_port* to *dest\_if :dest\_ip /dest\_port* with source MAC *mac\_address* due to secure phone database mismatch.

**Explanation** The MAC address in the SIP message is compared with the secure database entries in addition to the IP address and interface. If they do not match, then the particular message is dropped.

**Recommended Action** None required.

## 608001

**Error Message** %ASA-6-608001: Pre-allocate Skinny *connection\_type* secondary channel for *interface\_name:IP\_address* to *interface\_name:IP\_address* from *string* message

**Explanation** The **inspect skinny** command preallocated a Skinny connection after inspecting a Skinny message. The **connection\_type** is one of the following strings:

- SIGNALLING UDP
- SIGNALLING TCP
- SUBSCRIBE UDP
- SUBSCRIBE TCP
- Via UDP
- Route
- RTP
- RTCP

**Recommended Action** None required.

## 608002

**Error Message** %ASA-4-608002: Dropping Skinny message for *in\_ifc :src\_ip /src\_port* to *out\_ifc :dest\_ip /dest\_port*, SCCP Prefix length value too small

**Explanation** A Skinny (SCCP) message was received with an SCCP prefix length less than the minimum length configured.

- *in\_ifc* —The input interface



- *src\_ip* —The source IP address of the packet
- *src\_port* —The source port of the packet
- *out\_ifc* —The output interface
- *dest\_ip* —The destination IP address of the packet
- *dest\_port* —The destination port of the packet
- *value* —The SCCP prefix length of the packet

**Recommended Action** If the SCCP message is valid, then customize the Skinny policy map to increase the minimum length value of the SCCP prefix.

## 608003

**Error Message** %ASA-4-608003: Dropping Skinny message for *in\_ifc :src\_ip /src\_port* to *out\_ifc :dest\_ip /dest\_port* , SCCP Prefix length *value* too large

**Explanation** A Skinny (SCCP) message was received with an SCCP prefix length greater than the maximum length configured.

- *in\_ifc* —The input interface
- *src\_ip* —The source IP address of the packet
- *src\_port* —The source port of the packet
- *out\_ifc* —The output interface
- *dest\_ip* —The destination IP address of the packet
- *dest\_port* —The destination port of the packet
- *value* —The SCCP prefix length of the packet

**Recommended Action** If the SCCP message is valid, then customize the Skinny policy map to increase the maximum length value of the SCCP prefix.

## 608004

**Error Message** %ASA-4-608004: Dropping Skinny message for *in\_ifc :src\_ip /src\_port* to *out\_ifc :dest\_ip /dest\_port* , message id *value* not allowed

**Explanation** This SCCP message ID is not allowed.

- *in\_ifc* —The input interface
- *src\_ip* —The source IP address of the packet
- *src\_port* —The source port of the packet
- *out\_ifc* —The output interface
- *dest\_ip* —The destination IP address of the packet
- *dest\_port* —The destination port of the packet
- *value* —The SCCP prefix length of the packet

**Recommended Action** If the SCCP messages should be allowed, then customize the Skinny policy map to allow them.

## 608005

**Error Message** %ASA-4-608005: Dropping Skinny message for *in\_ifc :src\_ip /src\_port* to *out\_ifc :dest\_ip /dest\_port* , message id *value* registration not complete

**Explanation** This SCCP message ID is not allowed, because the endpoint did not complete registration.

- *in\_ifc* —The input interface
- *src\_ip* —The source IP address of the packet
- *src\_port* —The source port of the packet
- *out\_ifc* —The output interface
- *dest\_ip* —The destination IP address of the packet
- *dest\_port* —The destination port of the packet
- *value* —The SCCP prefix length of the packet

**Recommended Action** If the SCCP messages that are being dropped are valid, then customize the Skinny policy map to disable registration enforcement.

## 609001

**Error Message** %ASA-7-609001: Built local-host *zone-name/\** :*ip-address*

**Explanation** A network state container was reserved for host **ip-address** connected to zone *zone-name* . The *zone-name/\** parameter is used if the interface on which the host is created is part of a zone. The asterisk symbolizes all interfaces because hosts do not belong to any one interface.

**Recommended Action** None required.

## 609002

**Error Message** %ASA-7-609002: Teardown local-host *zone-name/\** :*ip-address* duration *time*

**Explanation** A network state container for host **ip-address** connected to zone **zone-name** was removed. The *zone-name/\** parameter is used if the interface on which the host is created is part of a zone. The asterisk symbolizes all interfaces because hosts do not belong to any one interface.

**Recommended Action** None required.

# Messages 610001 to 622102

This section includes messages from 610001 to 622102.

## 610001

**Error Message** %ASA-3-610001: NTP daemon interface *interface\_name* : Packet denied from *IP\_address*

**Explanation** An NTP packet was received from a host that does not match one of the configured NTP servers. The ASA is only an NTP client; it is not a time server and does not respond to NTP requests.

**Recommended Action** None required.

## 610002

**Error Message** %ASA-3-610002: NTP daemon interface *interface\_name* : Authentication failed for packet from *IP\_address*

**Explanation** The received NTP packet failed the authentication check.

**Recommended Action** Make sure that both the ASA and the NTP server are set to use authentication, and the same key number and value.

## 610101

**Error Message** %ASA-6-610101: Authorization failed: Cmd: *command* Cmdtype: *command\_modifier*

**Explanation** Command authorization failed for the specified command. The **command\_modifier** is one of the following strings:

- **cmd** (this string means the command has no modifier)
- **clear**
- **no**
- **show**

If the ASA encounters any other value other than the four command types listed, the message “ unknown command type ” appears.

**Recommended Action** None required.

## 611101

**Error Message** %ASA-6-611101: User authentication succeeded: IP, *IP address* : Uname: *user*

**Explanation** User authentication succeeded when accessing the Secure Firewall ASA. The username is hidden when invalid or unknown, but appears when valid or the **no logging hide username** command has been configured.

- *IP address* —The IP address of the client that succeeded user authentication
- *user* —The user that authenticated

**Recommended Action** None required.

## 611102

**Error Message** %ASA-6-611102: User authentication failed: IP = *IP address*, Uname: *user*

**Explanation** User authentication failed when attempting to access the Secure Firewall ASA. The username is hidden when invalid or unknown, but appears when valid or the **no logging hide username** command has been configured.

- *IP address* —The IP address of the client that failed user authentication
- *user* —The user that authenticated

**Recommended Action** None required.

## 611103

**Error Message** %ASA-5-611103: User logged out: Uname: *user*

**Explanation** The specified user logged out.

**Recommended Action** None required.

## 611104

**Error Message** %ASA-5-611104: Serial console idle timeout exceeded

**Explanation** The configured idle timeout for the Secure Firewall ASA serial console was exceeded because of no user activity.

**Recommended Action** None required.

## 611301

**Error Message** %ASA-6-611301: VPNClient: NAT configured for Client Mode with no split tunneling: NAT address: *mapped\_address*

**Explanation** The VPN client policy for client mode with no split tunneling was installed.

**Recommended Action** None required.

## 611302

**Error Message** %ASA-6-611302: VPNClient: NAT exemption configured for Network Extension Mode with no split tunneling

**Explanation** The VPN client policy for network extension mode with no split tunneling was installed.

**Recommended Action** None required.

## 611303

**Error Message** %ASA-6-611303: VPNClient: NAT configured for Client Mode with split tunneling: NAT address: *mapped\_address* Split Tunnel Networks: *IP\_address/netmask IP\_address/netmask*

**Explanation** The VPN client policy for client mode with split tunneling was installed.

**Recommended Action** None required.

## 611304

**Error Message** %ASA-6-611304: VPNClient: NAT exemption configured for Network Extension Mode with split tunneling: Split Tunnel Networks: *IP\_address/netmask IP\_address/netmask*

**Explanation** The VPN client policy for network extension mode with split tunneling was installed.

**Recommended Action** None required.

## 611305

**Error Message** %ASA-6-611305: VPNClient: DHCP Policy installed: Primary DNS: *IP\_address* Secondary DNS: *IP\_address* Primary WINS: *IP\_address* Secondary WINS: *IP\_address*

**Explanation** The VPN client policy for DHCP was installed.

**Recommended Action** None required.

## 611306

**Error Message** %ASA-6-611306: VPNClient: Perfect Forward Secrecy Policy installed

**Explanation** Perfect forward secrecy was configured as part of the VPN client download policy.

**Recommended Action** None required.

## 611307

**Error Message** %ASA-6-611307: VPNClient: Head end: *IP\_address*

**Explanation** The VPN client is connected to the specified headend.

**Recommended Action** None required.

## 611308

**Error Message** %ASA-6-611308: VPNClient: Split DNS Policy installed: List of domains: *string string*

**Explanation** A split DNS policy was installed as part of the VPN client downloaded policy.

**Recommended Action** None required.

## 611309

**Error Message** %ASA-6-611309: VPNClient: Disconnecting from head end and uninstalling previously downloaded policy: Head End: *IP\_address*

**Explanation** A VPN client is disconnecting and uninstalling a previously installed policy.

**Recommended Action** None required.

## 611310

**Error Message** %ASA-6-611310: VPNClient: XAUTH Succeeded: Peer: *IP\_address*

**Explanation** The VPN client Xauth succeeded with the specified headend.

**Recommended Action** None required.

## 611311

**Error Message** %ASA-6-611311: VPNClient: XAUTH Failed: Peer: *IP\_address*

**Explanation** The VPN client Xauth failed with the specified headend.

**Recommended Action** None required.

## 611312

**Error Message** %ASA-6-611312: VPNClient: Backup Server List: *reason*

**Explanation** When the Secure Firewall ASA is an Easy VPN remote device, the Easy VPN server downloaded a list of backup servers to the Secure Firewall ASA. This list overrides any backup servers that you have configured locally. If the downloaded list is empty, then the Secure Firewall ASA uses no backup servers. The **reason** is one of the following messages:

- A list of backup server IP addresses
- Received NULL list. Deleting current backup servers

**Recommended Action** None required.

## 611313

**Error Message** %ASA-3-611313: VPNClient: Backup Server List Error: *reason*

**Explanation** When the Secure Firewall ASA is an Easy VPN remote device, and the Easy VPN server downloads a backup server list to the Secure Firewall ASA, the list includes an invalid IP address or a hostname. The Secure Firewall ASA does not support DNS, and therefore does not support hostnames for servers, unless you manually map a name to an IP address using the **name** command.

**Recommended Action** On the Easy VPN server, make sure that the server IP addresses are correct, and configure the servers as IP addresses instead of hostnames. If you must use hostnames on the server, use the **name** command on the Easy VPN remote device to map the IP addresses to names.

## 611314

**Error Message** %ASA-6-611314: VPNClient: Load Balancing Cluster with Virtual IP: *IP\_address* has redirected the to server *IP\_address*

**Explanation** When the Secure Firewall ASA is an Easy VPN remote device, the director server of the load balancing group redirected the Secure Firewall ASA to connect to a particular server.

**Recommended Action** None required.

## 611315

**Error Message** %ASA-6-611315: VPNClient: Disconnecting from Load Balancing Cluster member *IP\_address*

**Explanation** When the Secure Firewall ASA is an Easy VPN remote device, it disconnected from a load balancing cluster server.

**Recommended Action** None required.

## 611316

**Error Message** %ASA-6-611316: VPNClient: Secure Unit Authentication Enabled

**Explanation** When the Secure Firewall ASA is an Easy VPN remote device, the downloaded VPN policy enabled SUA.

**Recommended Action** None required.

## 611317

**Error Message** %ASA-6-611317: VPNClient: Secure Unit Authentication Disabled

**Explanation** When the Secure Firewall ASA is an Easy VPN remote device, the downloaded VPN policy disabled SUA.

**Recommended Action** None required.

## 611318

**Error Message** %ASA-6-611318: VPNClient: User Authentication Enabled: Auth Server IP: *IP\_address* Auth Server Port: *port* Idle Timeout: *time*

**Explanation** When the Secure Firewall ASA is an Easy VPN remote device, the downloaded VPN policy enabled IUA for users on the Secure Firewall ASA inside network.

- **IP\_address**—The server IP address to which the Secure Firewall ASA sends authentication requests.
- **port**—The server port to which the Secure Firewall ASA sends authentication requests
- **time**—The idle timeout value for authentication credentials

**Recommended Action** None required.

## 611319

**Error Message** %ASA-6-611319: VPNClient: User Authentication Disabled

**Explanation** When the Secure Firewall ASA is an Easy VPN remote device, the downloaded VPN policy disabled IUA for users on the Secure Firewall ASA inside network.

**Recommended Action** None required.

## 611320

**Error Message** %ASA-6-611320: VPNClient: Device Pass Thru Enabled

**Explanation** When the Secure Firewall ASA is an Easy VPN remote device, the downloaded VPN policy enabled device pass-through. The device pass-through feature allows devices that cannot perform authentication (such as an IP phone) to be exempt from authentication when IUA is enabled. If the Easy VPN server enabled this feature, you can specify the devices that should be exempt from authentication (IUA) using the **vpnclient mac-exempt** command on the Secure Firewall ASA.

**Recommended Action** None required.

## 611321

**Error Message** %ASA-6-611321: VPNClient: Device Pass Thru Disabled

**Explanation** When the Secure Firewall ASA is an Easy VPN remote device, the downloaded VPN policy disabled device pass-through.

**Recommended Action** None required.

## 611322

**Error Message** %ASA-6-611322: VPNClient: Extended XAUTH conversation initiated when SUA disabled

**Explanation** When the Secure Firewall ASA is an Easy VPN remote device and the downloaded VPN policy disabled SUA, the Easy VPN server uses two-factor/SecurID/cryptocard-based authentication mechanisms to authenticate the Secure Firewall ASA using XAUTH.

**Recommended Action** If you want the Easy VPN remote device to be authenticated using two-factor/SecureID/cryptocard-based authentication mechanisms, enable SUA on the server.

## 611323

**Error Message** %ASA-6-611323: VPNClient: Duplicate split nw entry

**Explanation** When the Secure Firewall ASA is an Easy VPN remote device, the downloaded VPN policy included duplicate split network entries. An entry is considered a duplicate if it matches both the network address and the network mask.

**Recommended Action** Remove duplicate split network entries from the VPN policy on the Easy VPN server.

## 612001

**Error Message** %ASA-5-612001: Auto Update succeeded:filename , version:number

**Explanation** An update from an Auto Update server was successful. The **filename** variable is image, ASDM file, or configuration. The **version number** variable is the version number of the update.

**Recommended Action** None required.

## 612002

**Error Message** %ASA-4-612002: Auto Update failed:filename , version:number , reason:reason

**Explanation** An update from an Auto Update server failed.

- **filename**—Either an image file, an ASDM file, or a configuration file.
- **number**—The version number of the update.
- **reason**—The failure reason, which may be one of the following:
  - Failover module failed to open stream buffer
  - Failover module failed to write data to stream buffer
  - Failover module failed to perform control operation on stream buffer
  - Failover module failed to open flash file
  - Failover module failed to write data to flash
  - Failover module operation timeout
  - Failover command link is down



- Failover resource is not available
- Invalid failover state on mate
- Failover module encountered file transfer data corruption
- Failover active state change
- Failover command EXEC failed
- The image cannot run on current system
- Unsupported file type

**Recommended Action** Check the configuration of the Auto Update server. Check to see if the standby unit is in the failed state. If the Auto Update server is configured correctly, and the standby unit is not in the failed state, contact the Cisco TAC.

## 612003

**Error Message** %ASA-4-612003:Auto Update failed to contact:url , reason:reason

**Explanation** The Auto Update daemon was unable to contact the specified URL **url**, which can be the URL of the Auto Update server or one of the file server URLs returned by the Auto Update server. The **reason** field describes why the contact failed. Possible reasons for the failure include no response from the server, authentication failed, or a file was not found.

**Recommended Action** Check the configuration of the Auto Update server.

## 613001

**Error Message** %ASA-6-613001: Checksum Failure in database in area *string* Link State Id  
*IP\_address* Old Checksum *number* New Checksum *number*

**Explanation** OSPF has detected a checksum error in the database because of memory corruption.

**Recommended Action** Restart the OSPF process.

## 613002

**Error Message** %ASA-6-613002: interface *interface\_name* has zero bandwidth

**Explanation** The interface reported its bandwidth as zero.

**Recommended Action** Copy the message exactly as it appears, and report it to the Cisco TAC.

## 613003

**Error Message** %ASA-6-613003: *IP\_address netmask* changed from area *string* to area *string*

**Explanation** An OSPF configuration change has caused a network range to change areas.

**Recommended Action** Reconfigure OSPF with the correct network range.

## 613004

**Error Message** %ASA-3-613004: Internal error: memory allocation failure

**Explanation** An internal software error occurred.

**Recommended Action** Copy the error message exactly as it appears, and report it to Cisco TAC.

## 613005

**Error Message** %ASA-3-613005: Flagged as being an ABR without a backbone area

**Explanation** The router was flagged as an Area Border Router (ABR) without a backbone area in the router.

**Recommended Action** Restart the OSPF process.

## 613006

**Error Message** %ASA-3-613006: Reached unknown state in neighbor state machine

**Explanation** An internal software error in this router has resulted in an invalid neighbor state during database exchange.

**Recommended Action** Copy the error message, the configuration and any details about the events leading up to this error and submit them to Cisco TAC.

## 613007

**Error Message** %ASA-3-613007: area string lsid IP\_address mask netmask type number

**Explanation** OSPF is trying to add an existing LSA to the database.

**Recommended Action** Copy the error message, the configuration and any details about the events leading up to this error and submit them to Cisco TAC.

## 613008

**Error Message** %ASA-3-613008: if inside if\_state number

**Explanation** An internal error occurred.

**Recommended Action** Copy the error message, the configuration and any details about the events leading up to this error and submit them to Cisco TAC.

## 613011

**Error Message** %ASA-3-613011: OSPF process number is changing router-id. Reconfigure virtual link neighbors with our new router-id

**Explanation** An OSPF process is being reset, and it is going to select a new router ID. This action brings down all virtual links. To make them work again, the virtual link configuration needs to be changed on all virtual link neighbors.

**Recommended Action** Change the virtual link configuration on all the virtual link neighbors to reflect the new router ID.

## 613013

**Error Message** %ASA-3-613013: OSPF LSID IP\_address adv IP\_address type number gateway IP\_address metric number forwarding addr route IP\_address/mask type number has no corresponding LSA

**Explanation** OSPF found inconsistency between its database and the IP routing table.

**Recommended Action** Copy the error message, the configuration and any details about the events leading up to this error, and submit them to Cisco TAC.

## 613014

**Error Message** %ASA-6-613014: Base topology enabled on interface string attached to MTR compatible mode area string

**Explanation** OSPF interfaces attached to MTR-compatible OSPF areas require the base topology to be enabled.

**Recommended Action** None.

## 613015

**Error Message** %ASA-4-613015: Process 1 flushes LSA ID IP\_address type-number adv-rtr IP\_address in area mask

**Explanation** A router is extensively re-originating or flushing the LSA reported by this error message.

**Recommended Action** If this router is flushing the network LSA, it means the router received a network LSA whose LSA ID conflicts with the IP address of one of the router's interfaces and flushed the LSA out of the network. For OSPF to function correctly, the IP addresses of transit networks must be unique. Conflicting routers are the router reporting this error message and the router with the OSPF router ID reported as adv-rtr in this message. If this router is re-originating an LSA, it is highly probable that some other router is flushing this LSA out of the network. Find that router and avoid the conflict. The conflict for a Type-2 LSA may be due to a duplicate LSA ID. For a Type-5 LSA, it may be a duplicate router ID on the router reporting this error message and on the routers connected to a different area. In an unstable network, this message may also warn of extensive re-origination of the LSA for some other reason. Contact Cisco TAC to investigate this type of case.

## 613016

**Error Message** %ASA-3-613016: Area string router-LSA of length number bytes plus update overhead bytes is too large to flood.

**Explanation** The router tried to build a router-LSA that is larger than the huge system buffer size or the OSPF protocol imposed maximum.

**Recommended Action** If the reported total length (LSA size plus overhead) is larger than the huge system buffer size but less than 65535 bytes (the OSPF protocol imposed maximum), you may increase the huge

system buffer size. If the reported total length is greater than 65535, you need to decrease the number of OSPF interfaces in the reported area.

## 613017

**Error Message** %ASA-4-613017: Bad LSA mask: Type number, LSID IP\_address Mask mask from IP\_address

**Explanation** The router received an LSA with an invalid LSA mask because of an incorrect configuration from the LSA originator. As a result, this route is not installed in the routing table.

**Recommended Action** Find the originating router of the LSA with the bad mask, then correct any misconfiguration of this LSA's network. For further debugging, call Cisco TAC for assistance.

## 613018

**Error Message** %ASA-4-613018: Maximum number of non self-generated LSA has been exceeded "OSPF number" - number LSAs

**Explanation** The maximum number of non self-generated LSAs has been exceeded.

**Recommended Action** Check whether or not a router in the network is generating a large number of LSAs as a result of a misconfiguration.

## 613019

**Error Message** %ASA-4-613019: Threshold for maximum number of non self-generated LSA has been reached "OSPF number" - number LSAs

**Explanation** The threshold for the maximum number of non self-generated LSAs has been reached.

**Recommended Action** Check whether or not a router in the network is generating a large number of LSAs as a result of a misconfiguration.

## 613021

**Error Message** %ASA-4-613021: Packet not written to the output queue

**Explanation** An internal error occurred.

**Recommended Action** Copy the error message, the configuration and any details about the events leading up to this error, and submit them to Cisco TAC.

## 613022

**Error Message** %ASA-4-613022: Doubly linked list linkage is NULL

**Explanation** An internal error occurred.

**Recommended Action** Copy the error message, the configuration and any details about the events leading up to this error, and submit them to Cisco TAC.

## 613023

**Error Message** %ASA-4-613023: Doubly linked list prev linkage is NULL number

**Explanation** An internal error occurred.

**Recommended Action** Copy the error message, the configuration and any details about the events leading up to this error, and submit them to Cisco TAC.

## 613024

**Error Message** %ASA-4-613024: Unrecognized timer number in OSPF string

**Explanation** An internal error occurred.

**Recommended Action** Copy the error message, the configuration and any details about the events leading up to this error, and submit them to Cisco TAC.

## 613025

**Error Message** %ASA-4-613025: Invalid build flag number for LSA IP\_address, type number

**Explanation** An internal error occurred.

**Recommended Action** Copy the error message, the configuration and any details about the events leading up to this error, and submit them to Cisco TAC.

## 613026

**Error Message** %ASA-4-613026: Can not allocate memory for area structure

**Explanation** An internal error occurred.

**Recommended Action** Copy the error message, the configuration and any details about the events leading up to this error, and submit them to Cisco TAC.

## 613027

**Error Message** %ASA-6-613027: OSPF process number removed from interface interface\_name

**Explanation** The OSPF process was removed from the interface because of an IP VRF.

**Recommended Action** None.

## 613028

**Error Message** %ASA-6-613028: Unrecognized virtual interface inteface\_name. Treat it as loopback stub route

**Explanation** The virtual interface type was not recognized by OSPF, so it is treated as a loopback interface stub route.

**Recommended Action** None.

## 613029

**Error Message** %ASA-3-613029: Router-ID IP\_address is in use by ospf process number

**Explanation** The Secure Firewall ASA attempted to assign a router ID that is in use by another process.

**Recommended Action** Configure another router ID for one of the processes.

## 613030

**Error Message** %ASA-4-613030: Router is currently an ASBR while having only one area which is a stub area

**Explanation** An ASBR must be attached to an area that can carry AS external or NSSA LSAs.

**Recommended Action** Make the area to which the router is attached into an NSSA or regular area.

## 613031

**Error Message** %ASA-4-613031: No IP address for interface inside

**Explanation** The interface is not point-to-point and is unnumbered.

**Recommended Action** Change the interface type or give the interface an IP address.

## 613032

**Error Message** %ASA-3-613032: Init failed for interface inside, area is being deleted. Try again.

**Explanation** The interface initialization failed. The possible reasons include the following:

- The area to which the interface is being attached is being deleted.
- It was not possible to create a neighbor datablock for the local router.

**Recommended Action** Remove the configuration command that covers the interface and then try it again.

## 613033

**Error Message** %ASA-3-613033: Interface inside is attached to more than one area

**Explanation** The interface is on the interface list for an area other than the one to which the interface links.

**Recommended Action** Copy the error message, the configuration and any details about the events leading up to this error, and submit them to Cisco TAC.

## 613034

**Error Message** %ASA-3-613034: Neighbor IP\_address not configured

**Explanation** The configured neighbor options are not valid.

**Recommended Action** Check the configuration options for the **neighbor** command and correct the options or the network type for the neighbor's interface.

## 613035

**Error Message** %ASA-3-613035: Could not allocate or find neighbor IP\_address

**Explanation** An internal error occurred.

**Recommended Action** Copy the error message exactly as it appears, and report it to Cisco TAC.

## 613036

**Error Message** %ASA-4-613036: Can not use configured neighbor: cost and database-filter options are allowed only for a point-to-multipoint network

**Explanation** The configured neighbor was found on an NBMA network and either the cost or database-filter option was configured. These options are only allowed on point-to-multipoint type networks.

**Recommended Action** Check the configuration options for the **neighbor** command and correct the options or the network type for the neighbor's interface.

## 613037

**Error Message** %ASA-4-613037: Can not use configured neighbor: poll and priority options are allowed only for a NBMA network

**Explanation** The configured neighbor was found on a point-to-multipoint network and either the poll or priority option was configured. These options are only allowed on NBMA-type networks.

**Recommended Action** Check the configuration options for the **neighbor** command and correct the options or the network type for the neighbor's interface.

## 613038

**Error Message** %ASA-4-613038: Can not use configured neighbor: cost or database-filter option is required for point-to-multipoint broadcast network

**Explanation** The configured neighbor was found on a point-to-multipoint broadcast network. Either the **cost** or **database-filter** option needs to be configured.

**Recommended Action** Check the configuration options for the **neighbor** command and correct the options or the network type for the neighbor's interface.

## 613039

**Error Message** %ASA-4-613039: Can not use configured neighbor: neighbor command is allowed only on NBMA and point-to-multipoint networks

**Explanation** The configured neighbor was found on a network for which the network type was neither NBMA nor point-to-multipoint.

**Recommended Action** None.

## 613040

**Error Message** %ASA-4-613040: OSPF-1 Area string: Router IP\_address originating invalid type number LSA, ID IP\_address, Metric number on Link ID IP\_address Link Type number

**Explanation** The router indicated in this message has originated an LSA with an invalid metric. If this is a router LSA and the link metric is zero, a risk of routing loops and traffic loss in the network exists.

**Recommended Action** Configure a valid metric for the given LSA type and link type on the router originating on the reported LSA.

## 613041

**Error Message** %ASA-6-613041: OSPF-100 Areav string: LSA ID IP\_address, Type number, Adv-rtr IP\_address, LSA counter DoNotAge

**Explanation** An internal error has corrected itself. There is no operational effect related to this error message.

**Recommended Action** Check the system memory. If memory is low, then the timer wheel functionality did not initialize. Try to reenter the commands when memory is available. If there is sufficient memory, then contact the Cisco TAC and provide output from the **show memory**, **show processes**, and **show tech-support ospf** commands.

## 613042

**Error Message** %ASA-4-613042: OSPF process number lacks forwarding address for type 7 LSA IP\_address in NSSA string - P-bit cleared

**Explanation** There is no viable forwarding address in the NSSA area. As a result, the P-bit must be cleared and the Type 7 LSA is not translated into a Type 5 LSA by the NSSA translator. See RFC 3101.

**Recommended Action** Configure at least one interface in the NSSA with an advertised IP address. A loopback is preferable because an advertisement does not depend on the underlying layer 2 state.

## 613043

**Error Message** %ASA-6-613043:

**Explanation** A negative database reference count occurred.

**Recommended Action** Check the system memory. If memory is low, then the timer wheel functionality did not initialize. Try to reenter the commands when memory is available. If there is sufficient memory, then contact the Cisco TAC and provide output from the **show memory**, **show processes**, and **show tech-support ospf** commands.

## 613101

**Error Message** %ASA-6-613101: Checksum Failure in database in area s Link State Id i Old Checksum #x New Checksum #x

**Explanation** OSPF has detected a checksum error in the database because of memory corruption.

**Recommended Action** Restart the OSPF process.



## 613102

**Error Message** %ASA-6-613102: interface *s* has zero bandwidth

**Explanation** The interface reports its bandwidth as zero.

**Recommended Action** None required.

## 613103

**Error Message** %ASA-6-613103: *i m* changed from area *AREA\_ID\_STR* to area *AREA\_ID\_STR*

**Explanation** An OSPF configuration change has caused a network range to change areas.

**Recommended Action** None required.

## 613104

**Error Message** %ASA-6-613104: Unrecognized virtual interface *IF\_NAME* .

**Explanation** The virtual interface type was not recognized by OSPFv3, so it is treated as a loopback interface stub route.

**Recommended Action** None required.

## 614001

**Error Message** %ASA-6-614001: Split DNS: request patched from server: *IP\_address* to server: *IP\_address*

**Explanation** Split DNS is redirecting DNS queries from the original destination server to the primary enterprise DNS server.

**Recommended Action** None required.

## 614002

**Error Message** %ASA-6-614002: Split DNS: reply from server:*IP\_address* reverse patched back to original server:*IP\_address*

**Explanation** Split DNS is redirecting DNS queries from the enterprise DNS server to the original destination server.

**Recommended Action** None required.

## 615001

**Error Message** %ASA-6-615001: vlan number not available for firewall interface

**Explanation** The switch removed the VLAN from the Secure Firewall ASA.

**Recommended Action** None required.

## 615002

**Error Message** %ASA-6-615002: vlan number available for firewall interface

**Explanation** The switch added the VLAN to the Secure Firewall ASA.

**Recommended Action** None required.

## 616001

**Error Message** %ASA-6-616001:Pre-allocate MGCP *data\_channel* connection for *inside\_interface* :*inside\_address* to *outside\_interface* :*outside\_address* /*port* from *message\_type* *message*

**Explanation** An MGCP data channel connection, RTP, or RTCP was preallocated. The message text also specifies which message has triggered the connection preallocation.

**Recommended Action** None required.

## 617001

**Error Message** %ASA-6-617001: GTPv version *msg\_type* from *source\_interface* :*source\_address* /*source\_port* not accepted by *source\_interface* :*dest\_address* /*dest\_port*

**Explanation** A request was not accepted by the peer, which is usually seen with a Create PDP Context request.

**Recommended Action** None required.

## 617002

**Error Message** %ASA-6-617002: Removing vl PDP Context with TID *tid* from GGSN *IP\_address* and SGSN *IP\_address* , Reason: *reason* or Removing vl *primary* |*secondary* PDP Context with TID *tid* from GGSN *IP\_address* and SGSN *IP\_address* , Reason: *reason*

**Explanation** A PDP context was removed from the database either because it expired, a Delete PDP Context Request/Response was exchanged, or a user removed it using the CLI.

**Recommended Action** None required.

## 617003

**Error Message** %ASA-6-617003: GTP Tunnel created from *source\_interface* :*source\_address* /*source\_port* to *source\_interface* :*dest\_address* /*dest\_port*

**Explanation** A GTP tunnel was created after receiving a Create PDP Context Response that accepted the request.

**Recommended Action** None required.

## 617004

**Error Message** %ASA-6-617004: GTP connection created for response from *source\_interface* :*source\_address* /*0* to *source\_interface* :*dest\_address* /*dest\_port*

**Explanation** The SGSN or GGSN signaling address in the Create PDP Context Request or Response, respectively, was different from the SGSN/GGSN sending it.

**Recommended Action** None required.

## 617100

**Error Message** ASA-6-617100: Teardown *num\_conns* connection(s) for user *user\_ip*

**Explanation** The connections for this user were torn down because either a RADIUS accounting stop or RADIUS accounting start was received, which includes attributes that were configured in the policy map for a match. The attributes did not match those stored for the user entry, if the user entry exists.

- **num\_conns**—The number of connections torn down
- **user\_ip**—The IP address (framed IP attribute) of the user

**Recommended Action** None required.

## 618001

**Error Message** ASA-6-618001: Denied STUN packet <msg\_type> from <ingress\_ifc>:<source\_addr>/<source\_port> to <egress\_ifc>:<destination\_addr>/<destination\_port> for connection <conn\_id>, <drop\_reason>

**Explanation** This syslog is modeled after 4313009. This message is rate limited to 25 logs per second.

- **msg\_type**—The STUN message type value.
- **ingress\_ifc**—The interface on which the packet arrived.
- **source\_addr**—The IP address of the host which sent the packet.
- **source\_port**—The port number of the host which sent the packet.
- **egress\_ifc**—The interface on which the packet will leave.
- **destination\_addr**—The IP address of the host which will receive the packet
- **destination\_port**—The port number of the host which will receive the packet.
- **conn\_id**—The unique connection ID
- **drop\_reason**—The reason why the STUN packet was dropped.

**Recommended Action** None required.

## 620001

**Error Message** %ASA-6-620001: Pre-allocate CTIQBE {RTP | RTCP} secondary channel for *interface\_name* :*outside\_address* [/*outside\_port* ] to *interface\_name* :*inside\_address* [/*inside\_port* ] from *CTIQBE\_message\_name* message

**Explanation** The ASA preallocated a connection object for the specified CTIQBE media traffic. This message is rate limited to one message every 10 seconds.

**Recommended Action** None required.

## 620002

**Error Message** %ASA-4-620002: Unsupported CTIQBE version: **hex**: from *interface\_name* :*IP\_address* /*port* to *interface\_name* :*IP\_address* /*port*

**Explanation** The ASA received a CTIQBE message with an unsupported version number, and dropped the packet. This message is rate limited to one message every 10 seconds.

**Recommended Action** If the version number captured in the log message is unreasonably large (greater than 10), the packet may be malformed, a non-CTIQBE packet, or corrupted before it arrives at the ASA. We recommend that you determine the source of the packets. If the version number is reasonably small (less than or equal to 10), then contact the Cisco TAC to see if a new ASA image that supports this CTIQBE version is available.

## 621001

**Error Message** %ASA-6-621001: Interface *interface\_name* does not support multicast, not enabled

**Explanation** An attempt was made to enable PIM on an interface that does not support multicast.

**Recommended Action** If the problem persists, contact the Cisco TAC.

## 621002

**Error Message** %ASA-6-621002: Interface *interface\_name* does not support multicast, not enabled

**Explanation** An attempt was made to enable IGMP on an interface that does not support multicast.

**Recommended Action** If the problem persists, contact the Cisco TAC.

## 621003

**Error Message** %ASA-6-621003: The event queue size has exceeded *number*

**Explanation** The number of event managers created has exceeded the expected amount.

**Recommended Action** If the problem persists, contact the Cisco TAC.

## 621006

**Error Message** %ASA-6-621006: Mrib disconnected, (*IP\_address* ,*IP\_address* ) event cancelled

**Explanation** A packet triggering a data-driven event was received, but the connection to the MRIB was down. The notification was canceled.

**Recommended Action** If the problem persists, contact the Cisco TAC.

## 621007

**Error Message** %ASA-6-621007: Bad register from *interface\_name* :*IP\_address* to *IP\_address* for (*IP\_address* , *IP\_address* )

**Explanation** A PIM router configured as a rendezvous point or with NAT has received a PIM register packet from another PIM router. The data encapsulated in this packet is invalid.

**Recommended Action** The sending router is erroneously sending non-RFC registers. Upgrade the sending router.

## 622001

**Error Message** %ASA-6-622001: *string* tracked route *network mask address* , distance *number* , table *string* , on interface *interface-name*

**Explanation** A tracked route has been added to or removed from a routing table, which means that the state of the tracked object has changed from up or down.

- *string* —Adding or Removing
- *network* —The network address
- *mask* —The network mask
- *address* —The gateway address
- *number* —The route administrative distance
- *string* —The routing table name
- *interface-name* —The interface name as specified by the **nameif** command

**Recommended Action** None required.

## 622101

**Error Message** %ASA-6-622101: Starting regex table compilation for *match\_command* ; table entries = *regex\_num* entries

**Explanation** Information on the background activities of regex compilation appear.

- *match\_command* —The match command to which the regex table is associated
- *regex\_num* —The number of regex entries to be compiled

**Recommended Action** None required.

## 622102

**Error Message** %ASA-6-622102: Completed regex table compilation for *match\_command* ; table size = *num* bytes

**Explanation** Information on the background activities of the regex compilation appear.

- *match\_command* —The match command to which the regex table is associated
- *num* —The size, in bytes, of the compiled table

**Recommended Action** None required.





## CHAPTER 7

# Syslog Messages 701001 to 714011

This chapter contains the following sections:

- [Messages 701001 to 713109, on page 313](#)
- [Messages 713112 to 714011, on page 332](#)

## Messages 701001 to 713109

This section includes messages from 701001 to 713109.

### 701001

**Error Message** %ASA-7-701001: alloc\_user() out of Tcp\_user objects

**Explanation** A AAA message that appears if the user authentication rate is too high for the module to handle new AAA requests.

**Recommended Action** Enable Flood Defender with the floodguard enable command.

### 701002

**Error Message** %ASA-7-701002: alloc\_user() out of Tcp\_proxy objects

**Explanation** A AAA message that appears if the user authentication rate is too high for the module to handle new AAA requests.

**Recommended Action** Enable Flood Defender with the floodguard enable command.

### 702305

**Error Message** %ASA-3-702305: IPSEC: An *direction tunnel\_type* SA (SPI=*spi*) between *local\_IP* and *remote\_IP (username)* is rekeying due to sequence number rollover.

**Explanation** More than four billion packets have been received in the IPsec tunnel, and a new tunnel is being negotiated.

- *direction*—SA direction (inbound or outbound)
- *tunnel\_type*—SA type (remote access or L2L)

- spi—IPsec Security Parameter Index
- local\_IP—IP address of the tunnel local endpoint
- remote\_IP—IP address of the tunnel remote endpoint
- >username —Username associated with the IPsec tunnel

**Recommended Action** Contact the peer administrator to compare the SA lifetime setting.

## 702307

**Error Message** %ASA-7-702307: IPSEC: An *direction tunnel\_type* SA (SPI=*spi* ) between *local\_IP* and *remote\_IP* (*username* ) is rekeying due to data rollover.

**Explanation** An SA data life span expired. An IPsec SA is rekeying as a result of the amount of data transmitted with that SA. This information is useful for debugging rekeying issues.

- direction—SA direction (inbound or outbound)
- tunnel\_type—SA type (remote access or L2L)
- spi—IPsec Security Parameter Index
- local\_IP—IP address of the tunnel local endpoint
- remote\_IP—IP address of the tunnel remote endpoint
- >username —Username associated with the IPsec tunnel

**Recommended Action** None required.

## 703001

**Error Message** %ASA-7-703001: H.225 message received from *interface\_name* :*IP\_address* /*port* to *interface\_name* :*IP\_address* /*port* is using an unsupported version *number*

**Explanation** The Secure Firewall ASA received an H.323 packet with an unsupported version number. The Secure Firewall ASA might reencode the protocol version field of the packet to the highest supported version.

**Recommended Action** Use the version of H.323 that the Secure Firewall ASA supports in the VoIP network.

## 703002

**Error Message** %ASA-7-703002: Received H.225 Release Complete with newConnectionNeeded for *interface\_name* :*IP\_address* to *interface\_name* :*IP\_address* /*port*

**Explanation** The Secure Firewall ASA received the specified H.225 message, and the Secure Firewall ASA opened a new signaling connection object for the two specified H.323 endpoints.

**Recommended Action** None required.

## 703008

**Error Message** %ASA-7-703008: Allowing early-message: %s before SETUP from %s:%Q/%d to %s:%Q/%d

**Explanation** This message indicates that an outside endpoint requested an incoming call to an inside host and wants the inside host to send FACILITY message before SETUP message towards Gatekeeper and wants to follow H.460.18.



**Recommended Action** Ensure that the setup indeed intends to allow early FACILITY message before SETUP message for incoming H323 calls as described in H.640.18.

## 709001, 709002

**Error Message** %ASA-7-709001: FO replication failed: cmd=*command* returned=*code*

**Error Message** %ASA-7-709002: FO unreplicable: cmd=*command*

**Explanation** Failover messages that only appear during the development debugging and testing phases.

**Recommended Action** None required.

## 709003

**Error Message** %ASA-1-709003: (Primary) Beginning configuration replication: Sending to mate.

**Explanation** A failover message that appears when the active unit starts replicating its configuration to the standby unit. Primary can also be listed as Secondary for the secondary unit.

**Recommended Action** None required.

## 709004

**Error Message** %ASA-1-709004: (Primary) End Configuration Replication (ACT)

**Explanation** A failover message that appears when the active unit completes replication of its configuration on the standby unit. Primary can also be listed as Secondary for the secondary unit.

**Recommended Action** None required.

## 709005

**Error Message** %ASA-1-709005: (Primary) Beginning configuration replication: Receiving from mate.

**Explanation** The standby Secure Firewall ASA received the first part of the configuration replication from the active Secure Firewall ASA. Primary can also be listed as Secondary for the secondary unit.

**Recommended Action** None required.

## 709006

**Error Message** %ASA-1-709006: (Primary) End Configuration Replication (STB)

**Explanation** A failover message that appears when the standby unit completes replication of a configuration sent by the active unit. Primary can also be listed as Secondary for the secondary unit.

**Recommended Action** None required.

## 709007

**Error Message** %ASA-2-709007: Configuration replication failed for command

**Explanation** A failover message that appears when the standby unit is unable to complete replication of a configuration sent by the active unit. The command that caused the failure appears at the end of the message.

**Recommended Action** If the problem persists, contact the Cisco TAC.

## 709008

**Error Message** %ASA-4-709008: (Primary | Secondary) Configuration sync in progress. Command: '*command*' executed from (terminal/http) will not be replicated to or executed by the standby unit.

**Explanation** A command was issued during the configuration sync, which triggered an interactive prompt to indicate that this command would not be issued on the standby unit. To continue, note that the command will be issued on the active unit only and will not be replicated on the standby unit.

- Primary | Secondary—The device is either primary or secondary
- *command*—The command issued while the configuration sync is in progress
- terminal/http—Issued from the terminal or via HTTP.

**Recommended Action** None.

## 709009

**Error Message** %ASA-6-709009: (unit-role) Configuration on Active and Standby is matching. No config sync. Time elapsed *time-elapsed* ms

**Explanation** This message is generated when the hash computed on both the active and joining unit matches. It also displays the time elapsed, from the time of sending the hash request to the time of getting and comparing the hash response..

**Recommended Action** None.

## 709010

**Error Message** %ASA-6-709010: Configuration between units doesn't match. Going for config sync. Time elapsed *time-elapsed* ms.

**Explanation** This syslog message is generated when the hash that is computed on both the active and joining unit does not match. It also displays the time elapsed, from the time of sending the hash request to the time of getting and comparing the hash response.

**Recommended Action** None.

## 709011

**Error Message** %ASA-6-709011: Total time to sync the config *time* ms.

**Explanation** This message displays the time taken to synchronize the config, in the case of hash not matching, and therefore going for a full configuration sync process.

**Recommended Action** None.

## 709012

**Error Message** %ASA-6-709012: Skip configuration replication from mate as configuration on Active and Standby is matching.

**Explanation** This message is generated when the configuration replication is skipped because, the configuration between active and joining unit matches.

**Recommended Action** None.

## 709013

**Error Message** %ASA-4-709013: Failover configuration replication hash comparison timeout expired.

**Explanation** This syslog message is generated when the hash computation, transfer, and comparison has timed out. Due to the timeout, the full configuration sync operation is triggered. The timeout value is 60 secs and you cannot modify this value.

**Recommended Action** None.

## 710001

**Error Message** %ASA-7-710001: TCP access requested from *source\_address /source\_port* to *interface\_name :dest\_address /service*

**Explanation** The first TCP packet destined to the Secure Firewall ASA requests to establish a TCP session. This packet is the first SYN packet of the three-way handshake. This message appears when the respective (Telnet, HTTP, or SSH) has permitted the packet. However, the SYN cookie verification is not yet completed and no state is reserved.

**Recommended Action** None required.

## 710002

**Error Message** %ASA-7-710002: {TCP|UDP} access permitted from *source\_address /source\_port* to *interface\_name :dest\_address /service*

**Explanation** For a TCP connection, the second TCP packet destined for the Secure Firewall ASA requested to establish a TCP session. This packet is the final ACK of the three-way handshake. The respective (Telnet, HTTP, or SSH) has permitted the packet. Also, the SYN cookie verification was successful and the state is reserved for the TCP session.

For a UDP connection, the connection was permitted. For example, the module received an SNMP request from an authorized SNMP management station, and the request has been processed. This message is rate limited to one message every 10 seconds.

**Recommended Action** None required.

## 710003

**Error Message** %ASA-3-710003: {TCP|UDP} access denied by ACL from *source\_IP/source\_port* to *interface\_name :dest\_IP/service*

**Explanation** The Secure Firewall ASA denied an attempt to connect to the interface service. For example, the Secure Firewall ASA received an SNMP request from an unauthorized SNMP management station. If this message appears frequently, it can indicate an attack.

For example:

```
%ASA-3-710003: UDP access denied by ACL from 95.1.1.14/5000 to outside:95.1.1.13/1005
```

**Recommended Action** Use the **show run http**, **show run ssh**, or **show run telnet** commands to verify that the Secure Firewall ASA is configured to permit the service access from the host or network.

## 710004

**Error Message** %ASA-7-710004: TCP connection limit exceeded from *Src\_ip /Src\_port* to *In\_name :Dest\_ip /Dest\_port* (current connections/connection limit = *Curr\_conn/Conn\_lmt*)

**Explanation** The maximum number of Secure Firewall ASA management connections for the service was exceeded. The Secure Firewall ASA permits at most five concurrent management connections per management service. Alternatively, an error may have occurred in the to-the-box connection counter.

- *Src\_ip* —The source IP address of the packet
- *Src\_port* —The source port of the packet
- *In\_ifc* —The input interface
- *Dest\_ip* —The destination IP address of the packet
- *Dest\_port* —The destination port of the packet
- *Curr\_conn* —The number of current to-the-box admin connections
- *Conn\_lmt* —The connection limit

**Recommended Action** From the console, use the **kill** command to release the unwanted session. If the message was generated because of an error in the to-the-box counter, run the **show conn all** command to display connection details.

## 710005

**Error Message** %ASA-7-710005: {TCP|UDP|SCTP} request discarded from *source\_address /source\_port* to *interface\_name :dest\_address /service*

**Explanation** The Secure Firewall ASA does not have a UDP server that services the UDP request. Also, a TCP packet that does not belong to any session on the Secure Firewall ASA may have been discarded. In addition, this message appears (with the SNMP service) when the Secure Firewall ASA receives an SNMP request with an empty payload, even if it is from an authorized host. When the service is SNMP, this message occurs a maximum of once every 10 seconds so that the log receiver is not overwhelmed. This message is also applicable for SCTP packets.

**Recommended Action** In networks that use broadcasting services such as DHCP, RIP, or NetBIOS extensively, the frequency of this message can be high. If this message appears in excessive numbers, it may indicate an attack.

## 710006

**Error Message** %ASA-7-710006: *protocol request discarded from source\_address to interface\_name :dest\_address*

**Explanation** The Secure Firewall ASA does not have an IP server that services the IP protocol request; for example, the Secure Firewall ASA receives IP packets that are not TCP or UDP, and the Secure Firewall ASA cannot service the request.

**Recommended Action** In networks that use broadcasting services such as DHCP, RIP, or NetBIOS extensively, the frequency of this message can be high. If this message appears in excessive numbers, it may indicate an attack.

## 710007

**Error Message** %ASA-7-710007: NAT-T keepalive received from 86.1.161.1/1028 to outside:86:1.129.1/4500

**Explanation** The Secure Firewall ASA received NAT-T keepalive messages.

**Recommended Action** None required.

## 711001

**Error Message** %ASA-7-711001: *debug\_trace\_msg*

**Explanation** You have entered the **logging debug-trace** command for the logging feature. When the **logging debug-trace** command is enabled, all debugging messages will be redirected to the message for processing. For security reasons, the message output must be encrypted or sent over a secure out-of-band network.

**Recommended Action** None required.

## 711002

**Error Message** %ASA-4-711002: Task ran for *elapsed\_time* msecs, process = *process\_name* , PC = *PC* Traceback = *traceback*

**Explanation** A process used the CPU for more than 100 milliseconds. This message is used for debugging CPU purposes, and can appear once every five seconds for each offending process.

- **PC**—Instruction pointer of the CPU hogging process
- **traceback**—Stack trace of the CPU hogging process, which can include up to 12 addresses

**Recommended Action** None required.

## 711003

**Error Message** %ASA-7-711003: Unknown/Invalid interface identifier(*vpifnum*) detected.

**Explanation** An internal inconsistency that should not occur during normal operation has occurred. However, this message is not harmful if it rarely occurs. If it occurs frequently, it might be worthwhile debugging.

- *vpifnum* —The 32-bit value corresponding to the interface

**Recommended Action** If the problem persists, contact the Cisco TAC.

## 711004

**Error Message** %ASA-4-711004: Task ran for msec msec, Process = process\_name , PC = pc , Call stack = call\_stack

**Explanation** A process used the CPU for more than 100 milliseconds. This message is used for debugging CPU purposes, and can appear once every five seconds for each offending process.

- msec—Length of the detected CPU hog in milliseconds
- process\_name —Name of the hogging process
- pc—Instruction pointer of the CPU hogging process
- call\_stack—Stack trace of the CPU hogging process, which can include up to 12 addresses

**Recommended Action** None required.

## 711005

**Error Message** %ASA-5-711005: Traceback: call\_stack

**Explanation** An internal software error that should not occur has occurred. The device can usually recover from this error, and no harmful effect to the device results.

- call\_stack —The EIPs of the call stack

**Recommended Action** Contact the Cisco TAC.

## 711006

**Error Message** %ASA-7-711006: CPU profiling has started for n-samples samples. Reason: reason-string .

**Explanation** CPU profiling has started.

- n-samples —The specified number of CPU profiling samples
- reason-string —The possible values are:

“CPU utilization passed cpu-utilization %”

“Process process-name CPU utilization passed cpu-utilization %”

**Recommended Action** “None specified”

**Recommended Action** Collect CPU profiling results and provide them to Cisco TAC.

## 713004

**Error Message** %ASA-3-713004: device scheduled for reboot or shutdown, IKE key acquire message on interface interface\_num , for Peer IP\_address ignored

**Explanation** The Secure Firewall ASA has received an IKE packet from a remote entity trying to initiate a tunnel. Because the Secure Firewall ASA is scheduled for a reboot or shutdown, it does not allow any more tunnels to be established. The IKE packet is ignored and dropped.

**Recommended Action** None required.

## 713201

**Error Message** %ASA-5-713201: Duplicate Phase *Phase* packet detected. *Action*

**Explanation** The Secure Firewall ASA has received a duplicate of a previous Phase 1 or Phase 2 packet, and will transmit the last message. A network performance or connectivity issue may have occurred, in which the peer is not receiving sent packets in a timely manner.

- **Phase**—Phase 1 or 2
- **Action**—Retransmitting last packet, or No last packet to transmit.

**Recommended Action** Verify network performance or connectivity.

## 713202

**Error Message** %ASA-6-713202: Duplicate *IP\_addr* packet detected.

**Explanation** The Secure Firewall ASA has received a duplicate first packet for a tunnel that the Secure Firewall ASA is already aware of and negotiating, which indicates that the Secure Firewall ASA probably received a retransmission of a packet from the peer.

- **IP\_addr**—The IP address of the peer from which the duplicate first packet was received

**Recommended Action** None required, unless the connection attempt is failing. If this is the case, debug further and diagnose the problem.

## 713006

**Error Message** %ASA-5-713006: Failed to obtain state for message Id *message\_number* , Peer Address: *IP\_address*

**Explanation** The Secure Firewall ASA does not know about the received message ID. The message ID is used to identify a specific IKE Phase 2 negotiation. An error condition on the Secure Firewall ASA may have occurred, and may indicate that the two IKE peers are out-of-sync.

**Recommended Action** None required.

## 713008

**Error Message** %ASA-3-713008: Key ID in ID payload too big for pre-shared IKE tunnel

**Explanation** A key ID value was received in the ID payload, which was longer than the maximum allowed size of a group name for this IKE session using preshared keys authentication. This is an invalid value, and the session is rejected. Note that the key ID specified would never work because a group name of that size cannot be created in the Secure Firewall ASA.

**Recommended Action** Make sure that the client peer (most likely an Altiga remote access client) specifies a valid group name. Notify the user to change the incorrect group name on the client. The current maximum length for a group name is 32 characters.

## 713009

**Error Message** %ASA-3-713009: OU in DN in ID payload too big for Certs IKE tunnel

**Explanation** An OU value in the DN was received in the ID payload, which was longer than the maximum allowed size of a group name for this IKE session using Certs authentication. This OU is skipped, and another OU or other criteria may find a matching group.

**Recommended Action** For the client to be able to use an OU to find a group in the Secure Firewall ASA, the group name must be a valid length. The current maximum length of a group name is 32 characters.

## 713010

**Error Message** %ASA-5-713010: IKE area: failed to find centry for message Id *message\_number*

An attempt was made to locate a conn\_entry (IKE phase 2 structure that corresponds to an IPsec SA) using the unique message ID, which failed. The internal structure was not found, which may occur if a session was terminated in a nonstandard way, but it is more likely that an internal error occurred.

If this problem persists, investigate the peer.

## 713012

**Error Message** %ASA-3-713012: Unknown protocol (*protocol*). Not adding SA w/spi=SPI value

**Explanation** An illegal or unsupported IPsec protocol has been received from the peer.

**Recommended Action** Check the ISAKMP Phase 2 configuration on the peer(s) to make sure it is compatible with the Secure Firewall ASA.

## 713014

**Error Message** %ASA-3-713014: Unknown Domain of Interpretation (DOI): *DOI value*

**Explanation** The ISAKMP DOI received from the peer is unsupported.

**Recommended Action** Check the ISAKMP DOI configuration on the peer.

## 713016

**Error Message** %ASA-3-713016: Unknown identification type, Phase 1 or 2, Type *ID\_Type*

**Explanation** The ID received from the peer is unknown. The ID can be an unfamiliar valid ID or an invalid or corrupted ID.

**Recommended Action** Check the configuration on the headend and peer.

## 713017

**Error Message** %ASA-3-713017: Identification type not supported, Phase 1 or 2, Type *ID\_Type*

**Explanation** The Phase 1 or Phase 2 ID received from the peer is legal, but not supported.

**Recommended Action** Check the configuration on the headend and peer.



## 713018

**Error Message** %ASA-3-713018: Unknown ID type during find of group name for certs, Type *ID\_Type*

**Explanation** Tn internal software error has occurred.

**Recommended Action** If the problem persists, contact the Cisco TAC.

## 713020

**Error Message** %ASA-3-713020: No Group found by matching OU(s) from ID payload: *OU\_value*

**Explanation** Tn internal software error has occurred.

**Recommended Action** If the problem persists, contact the Cisco TAC.

## 713022

**Error Message** %ASA-3-713022: No Group found matching *peer\_ID* or *IP\_address* for Pre-shared key peer *IP\_address*

**Explanation** group exists in the group database with the same name as the value (key ID or IP address) specified by the peer.

**Recommended Action** Verify the configuration on the peer.

## 713024

**Error Message** %ASA-7-713024: Group *group* IP *ip* Received local Proxy Host data in ID Payload: Address *IP\_address* , Protocol *protocol* , Port *port*

**Explanation** The Secure Firewall ASA has received the Phase 2 local proxy ID payload from the remote peer.

**Recommended Action** None required.

## 713025

**Error Message** %ASA-7-713025: Received remote Proxy Host data in ID Payload: Address *IP\_address* , Protocol *protocol* , Port *port*

**Explanation** The Secure Firewall ASA has received the Phase 2 local proxy ID payload from the remote peer.

**Recommended Action** None required.

## 713028

**Error Message** %ASA-7-713028: Received local Proxy Range data in ID Payload: Addresses *IP\_address - IP\_address* , Protocol *protocol* , Port *port*

**Explanation** The Secure Firewall ASA has received the Phase 2 local proxy ID payload of the remote peer, which includes an IP address range.

**Recommended Action** None required.

## 713029

**Error Message** %ASA-7-713029: Received remote Proxy Range data in ID Payload: Addresses *IP\_address - IP\_address* , Protocol *protocol* , Port *port*

**Explanation** The Secure Firewall ASA has received the Phase 2 local proxy ID payload of the remote peer, which includes an IP address range.

**Recommended Action** None required.

## 713032

**Error Message** %ASA-3-713032: Received invalid local Proxy Range *IP\_address - IP\_address*

**Explanation** The local ID payload included the range ID type, and the specified low address was not less than the high address. A configuration problem may exist.

**Recommended Action** Check the configuration of ISAKMP Phase 2 parameters.

## 713033

**Error Message** %ASA-3-713033: Received invalid remote Proxy Range *IP\_address - IP\_address*

**Explanation** The remote ID payload included the range ID type, and the specified low address was not less than the high address. A configuration problem may exist.

**Recommended Action** Check the configuration of ISAKMP Phase 2 parameters.

## 713034

**Error Message** %ASA-7-713034: Received local IP Proxy Subnet data in ID Payload: Address *IP\_address* , Mask *netmask* , Protocol *protocol* , Port *port*

**Explanation** The local IP proxy subnet data has been received in the Phase 2 ID payload.

**Recommended Action** None required.

## 713035

**Error Message** %ASA-7-713035: Group *group* IP *ip* Received remote IP Proxy Subnet data in ID Payload: Address *IP\_address* , Mask *netmask* , Protocol *protocol* , Port *port*

**Explanation** The remote IP proxy subnet data has been received in the Phase 2 ID payload.

**Recommended Action** None required.

## 713039

**Error Message** %ASA-7-713039: Send failure: Bytes (*number*), Peer: *IP\_address*

**Explanation** An internal software error has occurred, and the ISAKMP packet cannot be transmitted.

**Recommended Action** If the problem persists, contact the Cisco TAC.

## 713040

**Error Message** %ASA-7-713040: Could not find connection entry and can not encrypt: msgid *message\_number*

**Explanation** An internal software error has occurred, and a Phase 2 data structure cannot be found.

**Recommended Action** If the problem persists, contact the Cisco TAC.

## 713041

**Error Message** %ASA-5-713041: IKE Initiator: *new* or *rekey* Phase 1 or 2, Intf *interface\_number*, IKE Peer *IP\_address* local Proxy Address *IP\_address*, remote Proxy Address *IP\_address*, Crypto map (*crypto map tag*)

**Explanation** Secure Firewall ASA is negotiating a tunnel as the initiator.

**Recommended Action** None required.

## 713042

**Error Message** %ASA-3-713042: IKE Initiator unable to find policy: Intf *interface\_number*, Src: *source\_address*, Dst: *dest\_address*

**Explanation** The IPsec fast path processed a packet that triggered IKE, but the IKE policy lookup failed. This error may be timing related. The ACLs that triggered IKE might have been deleted before IKE processed the initiation request. This problem will most likely correct itself.

**Recommended Action** If the condition persists, check the L2L configuration, paying special attention to the type of ACL associated with crypto maps.

## 713043

**Error Message** %ASA-3-713043: Cookie/peer address *IP\_address* session already in progress

**Explanation** IKE has been triggered again while the original tunnel is in progress.

**Recommended Action** None required.

## 713048

**Error Message** %ASA-3-713048: Error processing payload: Payload ID: *id*

**Explanation** A packet has been received with a payload that cannot be processed.

**Recommended Action** If this problem persists, a misconfiguration may exist on the peer.

## 713049

**Error Message** %ASA-5-713049: Security negotiation complete for *tunnel\_type* type (*group\_name*) *Initiator /Responder* , Inbound SPI = *SPI* , Outbound SPI = *SPI*

**Explanation** An IPsec tunnel has been started.

**Recommended Action** None required.

## 713050

**Error Message** %ASA-5-713050: Connection terminated for peer *IP\_address* . Reason: termination reason Remote Proxy *IP\_address* , Local Proxy *IP\_address*

**Explanation** An IPsec tunnel has been terminated. Possible termination reasons include:

- IPsec SA Idle Timeout
- IPsec SA Max Time Exceeded
- Administrator Reset
- Administrator Reboot
- Administrator Shutdown
- Session Disconnected
- Session Error Terminated
- Peer Terminate

**Recommended Action** None required.

## 713052

**Error Message** %ASA-7-713052: User (*user*) authenticated.

**Explanation** remote access user was authenticated.

**Recommended Action** None required.

## 713056

**Error Message** %ASA-3-713056: Tunnel rejected: SA (*SA\_name*) not found for group (*group\_name*)!

**Explanation** The IPsec SA was not found.

**Recommended Action** If this is a remote access tunnel, check the group and user configuration, and verify that a tunnel group and group policy have been configured for the specific user group. For externally authenticated users and groups, check the returned authentication attributes.

## 713060

**Error Message** %ASA-3-713060: Tunnel Rejected: User (*user*) not member of group (*group\_name*), group-lock check failed.

**Explanation** The user is configured for a different group than what was sent in the IPsec negotiation.

**Recommended Action** If you are using the Cisco VPN client and preshared keys, make sure that the group configured on the client is the same as the group associated with the user on the Secure Firewall ASA. If you are using digital certificates, the group is dictated either by the OU field of the certificate, or the user automatically defaults to the remote access default group.

## 713061

**Error Message** %ASA-3-713061: Tunnel rejected: Crypto Map Policy not found for Src: *source\_address* , Dst: *dest\_address* !

**Explanation** The Secure Firewall ASA was not able to find security policy information for the private networks or hosts indicated in the message. These networks or hosts were sent by the initiator and do not match any crypto ACLs at the Secure Firewall ASA. This is most likely a misconfiguration.

**Recommended Action** Check the protected network configuration in the crypto ACLs on both sides and make sure that the local net on the initiator is the remote net on the responder and vice-versa. Pay special attention to wildcard masks, and host addresses versus network addresses. Non-Cisco implementations may have the private addresses labeled as proxy addresses or red networks.

## 713062

**Error Message** %ASA-3-713062: IKE Peer address same as our interface address *IP\_address*

**Explanation** The IP address configured as the IKE peer is the same as the IP address configured on one of the Secure Firewall ASA IP interfaces.

**Recommended Action** Check the L2L and IP interface configurations.

## 713063

**Error Message** %ASA-3-713063: IKE Peer address not configured for destination *IP\_address*

**Explanation** The IKE peer address is not configured for an L2L tunnel.

**Recommended Action** Check the L2L configuration.

## 713065

**Error Message** %ASA-3-713065: IKE Remote Peer did not negotiate the following: *proposal attribute*

**Explanation** An internal software error has occurred.

**Recommended Action** If the problem persists, contact the Cisco TAC.

## 713066

**Error Message** %ASA-7-713066: IKE Remote Peer configured for SA: *SA\_name*

**Explanation** The crypto policy settings of the peer have been configured.

**Recommended Action** None required.

## 713068

**Error Message** %ASA-5-713068: Received non-routine Notify message: notify\_type (notify\_value)

**Explanation** Notification messages that caused this event are not explicitly handled in the notify processing code.

**Recommended Action** Examine the specific reason to determine the action to take. Many notification messages indicate a configuration mismatch between the IKE peers.

## 713072

**Error Message** %ASA-3-713072: Password for user (user ) too long, truncating to number characters

**Explanation** The password of the user is too long.

**Recommended Action** Correct password lengths on the authentication server.

## 713073

**Error Message** %ASA-5-713073: Responder forcing change of Phase 1 /Phase 2 rekeying duration from larger\_value to smaller\_value seconds

**Explanation** Rekeying durations are always set to the lower of the values proposed by IKE peers. The value of the initiator is the lower one.

**Recommended Action** None required.

## 713074

**Error Message** %ASA-5-713074: Responder forcing change of IPsec rekeying duration from larger\_value to smaller\_value Kbs

**Explanation** Rekeying durations are always set to the lower of the values proposed by IKE peers. The value of the initiator is the lower one.

**Recommended Action** None required.

## 713075

**Error Message** %ASA-5-713075: Overriding Initiator's IPsec rekeying duration from larger\_value to smaller\_value seconds

**Explanation** Rekeying durations are always set to the lower of the values proposed by IKE peers. The value of the responder is the lower one.

**Recommended Action** None required.

## 713076

**Error Message** %ASA-5-713076: Overriding Initiator's IPsec rekeying duration from larger\_value to smaller\_value Kbs

**Explanation** Rekeying durations are always set to the lower of the values proposed by IKE peers. The value of the responder is the lower one.

**Recommended Action** None required.

## 713078

**Error Message** %ASA-2-713078: Temp buffer for building mode config attributes exceeded: bufsize *available\_size* , used *value*

**Explanation** An internal software error has occurred while processing modecfg attributes.

**Recommended Action** Disable any unnecessary tunnel group attributes, or shorten any text messages that are excessively long. If the problem persists, contact the Cisco TAC.

## 713081

**Error Message** %ASA-3-713081: Unsupported certificate encoding type *encoding\_type*

**Explanation** One of the loaded certificates is unreadable, and may be an unsupported encoding scheme.

**Recommended Action** Check the configuration of digital certificates and trustpoints.

## 713082

**Error Message** %ASA-3-713082: Failed to retrieve identity certificate

**Explanation** The identity certificate for this tunnel cannot be found.

**Recommended Action** Check the configuration of digital certificates and trustpoints.

## 713083

**Error Message** %ASA-3-713083: Invalid certificate handle

**Explanation** The identity certificate for this tunnel cannot be found.

**Recommended Action** Check the configuration of digital certificates and trustpoints.

## 713084

**Error Message** %ASA-3-713084: Received invalid phase 1 port value (*port*) in ID payload

**Explanation** The port value received in the IKE phase 1 ID payload was incorrect. Acceptable values are 0 or 500 (ISAKMP is also known as IKE).

**Recommended Action** Make sure that a peer conforms to the IKE standards to avoid a network problem resulting in corrupted packets.

## 713085

**Error Message** %ASA-3-713085: Received invalid phase 1 protocol (*protocol*) in ID payload

**Explanation** The protocol value received in the IKE phase 1 ID payload was incorrect. Acceptable values are 0 or 17 (UDP).

**Recommended Action** Make sure that a peer conforms to the IKE standards to avoid a network problem resulting in corrupted packets.

## 713086

**Error Message** %ASA-3-713086: Received unexpected Certificate payload Possible invalid Auth Method (Auth method (auth numerical value))

**Explanation** A certificate payload was received, but our internal certificate handle indicates that we do not have an identity certificate. The certificate handle was not obtained through a normal enrollment method. One likely reason this can happen is that the authentication method is not made through RSA or DSS signatures, although the IKE SA negotiation should fail if each side is misconfigured.

**Recommended Action** Check the trustpoint and ISAKMP configuration settings on the Secure Firewall ASA and its peer.

## 713088

**Error Message** %ASA-3-713088: Set Cert filehandle failure: no IPsec SA in group *group\_name*

**Explanation** The tunnel group cannot be found, based on the digital certificate information.

**Recommended Action** Verify that the tunnel group is set up correctly to handle the certificate information of the peer.

## 713092

**Error Message** %ASA-5-713092: Failure during phase 1 rekeying attempt due to collision

**Explanation** An internal software error has occurred. This is often a benign event.

**Recommended Action** If the problem persists, contact the Cisco TAC.

## 713094

**Error Message** %ASA-7-713094: Cert validation failure: handle invalid for *Main /Aggressive Mode Initiator /Responder* !

**Explanation** An internal software error has occurred.

**Recommended Action** You may have to reenroll the trustpoint. If the problem persists, contact the Cisco TAC.

## 713098

**Error Message** %ASA-3-713098: Aborting: No identity cert specified in IPsec SA (*SA\_name*) !

**Explanation** An attempt was made to establish a certificate-based IKE session, but no identity certificate has been specified in the crypto policy.

**Recommended Action** Specify the identity certificate or trustpoint that you want to transmit to peers.



## 713099

**Error Message** %ASA-7-713099: Tunnel Rejected: Received NONCE length *number* is out of range!

**Explanation** An internal software error has occurred.

**Recommended Action** If the problem persists, contact the Cisco TAC.

## 713102

**Error Message** %ASA-3-713102: Phase 1 ID Data length *number* too long - reject tunnel!

**Explanation** IKE has received an ID payload that includes an identification data field of 2 K or larger.

**Recommended Action** None required.

## 713103

**Error Message** %ASA-7-713103: Invalid (NULL) secret key detected while computing hash

**Explanation** An internal software error has occurred.

**Recommended Action** If the problem persists, contact the Cisco TAC.

## 713104

**Error Message** %ASA-7-713104: Attempt to get Phase 1 ID data failed while *hash computation*

**Explanation** An internal software error has occurred.

**Recommended Action** If the problem persists, contact the Cisco TAC.

## 713105

**Error Message** %ASA-3-713105: Zero length data in ID payload received during phase 1 or 2 processing

**Explanation** A peer sent an ID payload without including any ID data, which is invalid.

**Recommended Action** Check the configuration of the peer.

## 713107

**Error Message** %ASA-3-713107: IP\_Address request attempt failed!

**Explanation** An internal software error has occurred.

**Recommended Action** If the problem persists, contact the Cisco TAC.

## 713109

**Error Message** %ASA-3-713109: Unable to process the received peer certificate

**Explanation** The Secure Firewall ASA was unable to process the certificate received from the remote peer, which can occur if the certificate data was malformed (for example, if the public key size is larger than 4096 bits) or if the data in the certificate cannot be stored by the Secure Firewall ASA.

**Recommended Action** Try to reestablish the connection using a different certificate on the remote peer.

## Messages 713112 to 714011

This section includes messages from 713112 to 714011.

### 713112

**Error Message** %ASA-3-713112: Failed to process CONNECTED notify (SPI *SPI\_value* )!

**Explanation** The Secure Firewall ASA was unable to successfully process the notification payload that included the CONNECTED notify type. This may occur if the IKE phase 2 structure cannot be found using the SPI to locate it, or the commit bit had not been set in the received ISAKMP header. The latter case may indicate a nonconforming IKE peer.

**Recommended Action** If the problem persists, check the configuration of the peer and/or disable commit bit processing.

### 713113

**Error Message** %ASA-7-713113: Deleting IKE SA with associated IPsec connection entries. IKE peer: *IP\_address* , SA address: *internal\_SA\_address* , tunnel count: *count*

**Explanation** An IKE SA is being deleted with a nonzero tunnel count, which means that either the IKE SA tunnel count has lost synchronization with the associated connection entries or the associated connection cookie fields for the entries have lost synchronization with the cookie fields of the IKE SA to which the connection entry points. If this occurs, the IKE SA and its associated data structures will not be freed, so that the entries that may point to it will not have a stale pointer.

**Recommended Action** None required. Error recovery is built-in.

### 713114

**Error Message** %ASA-7-713114: Connection entry (conn entry internal address) points to IKE SA (*SA\_internal\_address* ) for peer *IP\_address* , but cookies don't match

**Explanation** An internal software error has occurred.

**Recommended Action** If the problem persists, contact the Cisco TAC.

### 713115

**Error Message** %ASA-5-713115: Client rejected NAT enabled IPsec request, falling back to standard IPsec

**Explanation** The client rejected an attempt by the Secure Firewall ASA to use IPsec over UDP. IPsec over UDP is used to allow multiple clients to establish simultaneous tunnels to the Secure Firewall ASA through

a NAT device. The client may have rejected the request, either because it does not support this feature or because it is configured not to use it.

**Recommended Action** Verify the configuration on the headend and peer.

## 713117

**Error Message** %ASA-7-713117: Received Invalid SPI notify (SPI *SPI\_Value* )!

**Explanation** The IPsec SA identified by the SPI value is no longer active on the remote peer, which might indicate that the remote peer has rebooted or been reset.

**Recommended Action** This problem should correct itself once DPDs recognize that the peer no longer has the appropriate SAs established. If DPD is not enabled, this may require you to manually reestablish the affected tunnel.

## 713118

**Error Message** %ASA-3-713118: Detected invalid Diffie-Hellman *group\_descriptor group\_number*, in IKE area

**Explanation** The **group\_descriptor** field included an unsupported value. Currently we support only groups 1, 2, 5, and 7. In the case of a centry, the **group\_descriptor** field may also be set to 0 to indicate that perfect forward secrecy is disabled.

**Recommended Action** Check the peer Diffie-Hellman configuration.

## 713119

**Error Message** %ASA-5-713119: Group *group* IP *ip* PHASE 1 COMPLETED

**Explanation** IKE Phase 1 has completed successfully.

**Recommended Action** None required.

## 713120

**Error Message** %ASA-5-713120: PHASE 2 COMPLETED (*msgid=msg\_id*)

**Explanation** IKE Phase 2 has completed successfully.

**Recommended Action** None required.

## 713121

**Error Message** %ASA-7-713121: Keep-alive type for this connection: *keepalive\_type*

**Explanation** The type of keepalive mechanism that is being used for this tunnel is specified.

**Recommended Action** None required.

## 713122

**Error Message** %ASA-3-713122: Keep-alives configured *keepalive\_type* but peer *IP\_address* support keep-alives (type = *keepalive\_type* )

**Explanation** Keepalives were configured on or off for this device, but the IKE peer does or does not support keepalives.

**Recommended Action** No action is required if this configuration is intentional. If it is not intentional, change the keepalive configuration on both devices.

## 713123

**Error Message** %ASA-3-713123: IKE lost contact with remote peer, deleting connection (keepalive type: *keepalive\_type* )

**Explanation** The remote IKE peer did not respond to keepalives within the expected window of time, so the connection to the IKE peer was terminated. The message includes the keepalive mechanism used.

**Recommended Action** None required.

## 713124

**Error Message** %ASA-3-713124: Received DPD sequence number *rcv\_sequence\_#* in *DPD Action*, *description expected seq #*

**Explanation** The remote IKE peer sent a DPD with a sequence number that did not match the expected sequence number. The packet is discarded. This might indicate a packet loss problem with the network.

**Recommended Action** None required.

## 713127

**Error Message** %ASA-3-713127: Xauth required but selected Proposal does not support xauth, Check priorities of ike xauth proposals in ike proposal list

**Explanation** The peer wanted to perform a XAUTH, but the Secure Firewall ASA did not choose the XAUTH IKE proposal.

**Recommended Action** Check the priorities of the IKE xauth proposals in the IKE proposal list.

## 713128

**Error Message** %ASA-6-713128: Connection attempt to VCPIP redirected to VCA peer *IP\_address* via load balancing

**Explanation** A connection attempt has been made to the VCPIP and has been redirected to a less loaded peer using load balancing.

**Recommended Action** None required.

## 713129

**Error Message** %ASA-3-713129: Received unexpected Transaction Exchange payload type: `payload_id`

**Explanation** An unexpected payload has been received during XAUTH or Mode Cfg, which may indicate that the two peers are out-of-sync, that the XAUTH or Mode Cfg versions do not match, or that the remote peer is not complying with the appropriate RFCs.

**Recommended Action** Verify the configuration between peers.

## 713130

**Error Message** %ASA-5-713130: Received unsupported transaction mode attribute: `attribute id`

**Explanation** The device received a request for a valid transaction mode attribute (XAUTH or Mode Cfg) that is currently not supported. This is generally a benign condition.

**Recommended Action** None required.

## 713131

**Error Message** %ASA-5-713131: Received unknown transaction mode attribute: `attribute_id`

**Explanation** The Secure Firewall ASA has received a request for a transaction mode attribute (XAUTH or Mode Cfg) that is outside the range of known attributes. The attribute may be valid but only supported in later versions of configuration mode, or the peer may be sending an illegal or proprietary value. This should not cause connectivity problems, but may affect the functionality of the peer.

**Recommended Action** None required.

## 713132

**Error Message** %ASA-3-713132: Cannot obtain an `IP_address` for remote peer

**Explanation** A request for an IP address for a remote access client from the internal utility that provides these addresses cannot be satisfied.

**Recommended Action** Check the configuration of IP address assignment methods.

## 713133

**Error Message** %ASA-3-713133: Mismatch: Overriding phase 2 DH Group(`DH group DH_group_id`) with phase 1 group(`DH group DH_group_number`)

**Explanation** The configured Phase 2 PFS Group differed from the DH group that was negotiated for Phase 1.

**Recommended Action** None required.

## 713134

**Error Message** %ASA-3-713134: Mismatch: P1 Authentication algorithm in the crypto map entry different from negotiated algorithm for the L2L connection

**Explanation** The configured LAN-to-LAN proposal is different from the one accepted for the LAN-to-LAN connection. Depending on which side is the initiator, different proposals will be used.

**Recommended Action** None required.

## 713135

**Error Message** %ASA-5-713135: message received, redirecting tunnel to *IP\_address* .

**Explanation** The tunnel is being redirected because of load balancing on the remote Secure Firewall ASA. A REDIRECT\_CONNECTION notify packet was received.

**Recommended Action** None required.

## 713136

**Error Message** %ASA-5-713136: IKE session establishment timed out [*IKE\_state\_name* ], aborting!

**Explanation** The Reaper has detected an Secure Firewall ASA stuck in an inactive state. The Reaper will try to remove the inactive Secure Firewall ASA.

**Recommended Action** None required.

## 713137

**Error Message** %ASA-5-713137: Reaper overriding refCnt [*ref\_count*] and tunnelCnt [*tunnel\_count*] -- deleting SA!

**Explanation** An internal software error has occurred.

**Recommended Action** If the problem persists, contact the Cisco TAC.

## 713138

**Error Message** %ASA-3-713138: Group *group\_name* not found and BASE GROUP default preshared key not configured

**Explanation** No group exists in the group database with the same name as the IP address of the peer. In Main Mode, the Secure Firewall ASA will fall back and try to use the default preshared key configured in one of the default groups. The default preshared key is not configured.

**Recommended Action** Verify the configuration of the preshared keys.

## 713139

**Error Message** %ASA-5-713139: *group\_name* not found, using BASE GROUP default preshared key

**Explanation** No tunnel group exists in the group database with the same name as the IP address of the peer. In Main Mode, the Secure Firewall ASA will fall back and use the default preshared key configured in the default group.

**Recommended Action** None required.

## 713140

**Error Message** %ASA-3-713140: Split Tunneling Policy requires network list but none configured

**Explanation** The split tunneling policy is set to either split tunneling or to allow local LAN access. A split tunneling ACL must be defined to represent the information required by the VPN client.

**Recommended Action** Check the configuration of the ACLs.

## 713141

**Error Message** %ASA-3-713141: Client-reported firewall does not match configured firewall: *action tunnel*. Received -- Vendor: *vendor(id)* , Product *product(id)* , Caps: *capability\_value* . Expected -- Vendor: *vendor(id)* , Product: *product(id)* , Caps: *capability\_value*

**Explanation** The Secure Firewall ASA installed on the client does not match the configured required Secure Firewall ASA. This message lists the actual and expected values, and whether the tunnel is terminated or allowed.

**Recommended Action** You may need to install a different personal Secure Firewall ASA on the client or change the configuration on the Secure Firewall ASA.

## 713142

**Error Message** %ASA-3-713142: Client did not report firewall in use, but there is a configured firewall: *action tunnel*. Expected -- Vendor: *vendor(id)* , Product *product(id)* , Caps: *capability\_value*

**Explanation** The client did not report an Secure Firewall ASA in use using ModeCf, but one is required. The event lists the expected values and whether the tunnel is terminated or allowed. Note that the number following the product string is a bitmask of all of the allowed products.

**Recommended Action** You may need to install a different personal Secure Firewall ASA on the client or change the configuration on the Secure Firewall ASA.

## 713143

**Error Message** %ASA-7-713143: Processing firewall record. Vendor: *vendor(id)* , Product: *product(id)* , Caps: *capability\_value* , Version Number: *version\_number* , Version String: *version\_text*

**Explanation** Debugging information about the Secure Firewall ASA installed on the client appears.

**Recommended Action** None required.

## 713144

**Error Message** %ASA-5-713144: Ignoring received malformed firewall record; reason - *error\_reason* TLV type *attribute\_value* correction

**Explanation** Bad Secure Firewall ASA information was received from the client.

**Recommended Action** Check the personal configuration on the client and the Secure Firewall ASA.

## 713145

**Error Message** %ASA-6-713145: Detected Hardware Client in network extension mode, adding static route for address: *IP\_address* , mask: *netmask*

**Explanation** A tunnel with a hardware client in network extension mode has been negotiated, and a static route is being added for the private network behind the hardware client. This configuration enables the Secure Firewall ASA to make the remote network known to all the routers on the private side of the headend.

**Recommended Action** None required.

## 713146

**Error Message** %ASA-3-713146: Could not add route for Hardware Client in network extension mode, address: *IP\_address* , mask: *netmask*

**Explanation** An internal software error has occurred. A tunnel with a hardware client in network extension mode has been negotiated, and an attempt to add the static route for the private network behind the hardware client failed. The routing table may be full, or a possible addressing error has occurred.

**Recommended Action** If the problem persists, contact the Cisco TAC.

## 713147

**Error Message** %ASA-6-713147: Terminating tunnel to Hardware Client in network extension mode, deleting static route for address: *IP\_address* , mask: *netmask*

**Explanation** A tunnel to a hardware client in network extension mode is being removed, and the static route for the private network is being deleted behind the hardware client.

**Recommended Action** None required.

## 713148

**Error Message** %ASA-5-713148: Terminating tunnel to Hardware Client in network extension mode, unable to delete static route for address: *IP\_address* , mask: *netmask*

**Explanation** While a tunnel to a hardware client in network extension mode was being removed, a route to the private network behind the hardware client cannot be deleted. This might indicate an addressing or software problem.

**Recommended Action** Check the routing table to ensure that the route is not there. If it is, it may have to be removed manually, but only if the tunnel to the hardware client has been completely removed.



## 713149

**Error Message** %ASA-3-713149: Hardware client security attribute *attribute\_name* was enabled but not requested.

**Explanation** The headend Secure Firewall ASA has the specified hardware client security attribute enabled, but the attribute was not requested by the VPN 3002 hardware client.

**Recommended Action** Check the configuration on the hardware client.

## 713152

**Error Message** %ASA-3-713152: Unable to obtain any rules from filter *ACL\_tag* to send to client for CPP, terminating connection.

**Explanation** The client is required to use CPP to provision its Secure Firewall ASA, but the headend device was unable to obtain any ACLs to send to the client. This is probably due to a misconfiguration.

**Recommended Action** Check the ACLs specified for CPP in the group policy for the client.

## 713154

**Error Message** %ASA-4-713154: DNS lookup for *peer\_description* Server [*server\_name*] failed!

**Explanation** This message appears when a DNS lookup for the specified server has not been resolved.

**Recommended Action** Check the DNS server configuration on the Secure Firewall ASA. Also check the DNS server to ensure that it is operational and has hostname to IP address mapping.

## 713155

**Error Message** %ASA-5-713155: DNS lookup for Primary VPN Server [*server\_name*] successfully resolved after a previous failure. Resetting any Backup Server init.

**Explanation** A previous DNS lookup failure for the primary server might have caused the Secure Firewall ASA to initialize a backup peer. This message indicates that a later DNS lookup on the primary server finally succeeded and is resetting any backup server initializations. A tunnel initiated after this point will be aimed at the primary server.

**Recommended Action** None required.

## 713156

**Error Message** %ASA-5-713156: Initializing Backup Server [*server\_name* or *IP\_address*]

**Explanation** The client is failing over to a backup server, or a failed DNS lookup for the primary server caused the Secure Firewall ASA to initialize a backup server. A tunnel initiated after this point will be aimed at the specified backup server.

**Recommended Action** None required.

## 713157

**Error Message** %ASA-4-713157: Timed out on initial contact to server [*server\_name* or *IP\_address* ] Tunnel could not be established.

**Explanation** The client tried to initiate a tunnel by sending out IKE MSG1, but did not receive a response from the Secure Firewall ASA on the other end. If backup servers are available, the client will attempt to connect to one of them.

**Recommended Action** Verify connectivity to the headend Secure Firewall ASA.

## 713158

**Error Message** %ASA-5-713158: Client rejected NAT enabled IPsec Over UDP request, falling back to IPsec Over TCP

**Explanation** The client is configured to use IPsec over TCP. The client rejected the attempt by the Secure Firewall ASA to use IPsec over UDP.

**Recommended Action** If TCP is desired, no action is required. Otherwise, check the client configuration.

## 713159

**Error Message** %ASA-3-713159: TCP Connection to Firewall Server has been lost, restricted tunnels are now allowed full network access

**Explanation** The TCP connection to the Secure Firewall ASA server was lost for a certain reason, such as the server has rebooted, a network problem has occurred, or an SSL mismatch has occurred.

**Recommended Action** If the server connection was lost after the initial connection was made, then the server and network connections must be checked. If the initial connection is lost immediately, this might indicate an SSL authentication problem.

## 713160

**Error Message** %ASA-7-713160: Remote user (session Id - *id* ) has been granted access by the Firewall Server

**Explanation** Normal authentication of the remote user to the Secure Firewall ASA server has occurred.

**Recommended Action** None required.

## 713161

**Error Message** %ASA-3-713161: Remote user (session Id - *id* ) network access has been restricted by the Firewall Server

**Explanation** The Secure Firewall ASA server has sent the Secure Firewall ASA a message indicating that this user must be restricted. There are several reasons for this, including Secure Firewall ASA software upgrades or changes in permissions. The Secure Firewall ASA server will transition the user back into full access mode as soon as the operation has been completed.

**Recommended Action** No action is required unless the user is never transitioned back into full access state. If this does not happen, refer to the Secure Firewall ASA server for more information on the operation that is being performed and the state of the Secure Firewall ASA software running on the remote machine.

## 713162

**Error Message** %ASA-3-713162: Remote user (session Id - *id* ) has been rejected by the Firewall Server

**Explanation** The Secure Firewall ASA server has rejected this user.

**Recommended Action** Check the policy information on the Secure Firewall ASA server to make sure that the user is configured correctly.

## 713163

**Error Message** %ASA-3-713163: Remote user (session Id - *id* ) has been terminated by the Firewall Server

**Explanation** The Secure Firewall ASA server has terminated this user session, which can occur if the integrity agent stops running on the client machine or if the security policy is modified by the remote user in any way.

**Recommended Action** Verify that the Secure Firewall ASA software on the client machine is still running and that the policy is correct.

## 713164

**Error Message** %ASA-7-713164: The Firewall Server has requested a list of active user sessions

**Explanation** The Secure Firewall ASA server will request the session information if it detects that it has stale data or if it loses the session data (because of a reboot).

**Recommended Action** None required.

## 713165

**Error Message** %ASA-3-713165: Client IKE Auth mode differs from the group's configured Auth mode

**Explanation** The client negotiated with preshared keys while its tunnel group points to a policy that is configured to use digital certificates.

**Recommended Action** Check the client configuration.

## 713166

**Error Message** %ASA-3-713166: Headend security gateway has failed our user authentication attempt - check configured username and password

**Explanation** The hardware client has failed extended authentication. This is most likely a username and password problem or an authentication server issue.

**Recommended Action** Verify that the configured username and password values on each side match. Also verify that the authentication server at the headend is operational.

## 713167

**Error Message** %ASA-3-713167: Remote peer has failed user authentication - check configured username and password

**Explanation** The remote user has failed to extend authentication. This is most likely a username or password problem, or an authentication server issue.

**Recommended Action** Verify that the configured username and password values on each side match. Also verify that the authentication server being used to authenticate the remote user is operational.

## 713168

**Error Message** %ASA-3-713168: Re-auth enabled, but tunnel must be authenticated interactively!

**Explanation** Reauthentication on rekeying has been enabled, but the tunnel authentication requires manual intervention.

**Recommended Action** If manual intervention is desired, no action is required. Otherwise, check the interactive authentication configuration.

## 713169

**Error Message** %ASA-7-713169: IKE Received delete for rekeyed SA IKE peer: *IP\_address* , SA address: *internal\_SA\_address* , tunnelCnt: *tunnel\_count*

**Explanation** IKE has received a delete message from the remote peer to delete its old IKE SA after a rekey has completed.

**Recommended Action** None required.

## 713170

**Error Message** %ASA-7-713170: Group *group* IP *ip* IKE Received delete for rekeyed centry IKE peer: *IP\_address* , centry address: *internal\_address* , msgid: *id*

**Explanation** IKE has received a delete message from the remote peer to delete its old centry after Phase 2 rekeying is completed.

**Recommended Action** None required.

## 713171

**Error Message** %ASA-7-713171: NAT-Traversal sending NAT-Original-Address payload

**Explanation** UDP-Encapsulated-Transport was either proposed or selected during Phase 2. Send this payload for NAT-Traversal in this case.

**Recommended Action** None required.

## 713172

**Error Message** %ASA-6-713172: Automatic NAT Detection Status: Remote end *is* |*is not* behind a NAT device This end *is* |*is not* behind a NAT device

**Explanation** NAT-Traversal auto-detected NAT.

**Recommended Action** None required.

## 713174

**Error Message** %ASA-3-713174: Hardware Client connection rejected! Network Extension Mode is not allowed for this group!

**Explanation** A hardware client is attempting to tunnel in using network extension mode, but network extension mode is not allowed.

**Recommended Action** Verify the configuration of the network extension mode versus PAT mode.

## 713176

**Error Message** %ASA-2-713176: *Device\_type* memory resources are critical, IKE key acquire message on interface *interface\_number* , for Peer *IP\_address* ignored

**Explanation** The Secure Firewall ASA is processing data intended to trigger an IPsec tunnel to the indicated peer. Because memory resources are at a critical state, it is not initiating any more tunnels. The data packet has been ignored and dropped.

**Recommended Action** If condition persists, verify that the Secure Firewall ASA is efficiently configured. An Secure Firewall ASA with increased memory may be required for this application.

## 713177

**Error Message** %ASA-6-713177: Received remote Proxy Host FQDN in ID Payload: Host Name: *host\_name* Address *IP\_address* , Protocol *protocol* , Port *port*

**Explanation** A Phase 2 ID payload containing an FQDN has been received from the peer.

**Recommended Action** None required.

## 713178

**Error Message** %ASA-5-713178: IKE Initiator received a packet from its peer without a Responder cookie

**Explanation** An internal software error has occurred.

**Recommended Action** If the problem persists, contact the Cisco TAC.

## 713179

**Error Message** %ASA-5-713179: IKE AM Initiator received a packet from its peer without a *payload\_type* payload

**Explanation** An internal software error has occurred.

**Recommended Action** If the problem persists, contact the Cisco TAC.

## 713182

**Error Message** %ASA-3-713182: IKE could not recognize the version of the client! IPsec Fragmentation Policy will be ignored for this connection!

**Explanation** An internal software error has occurred.

**Recommended Action** If the problem persists, contact the Cisco TAC.

## 713184

**Error Message** %ASA-6-713184: Client Type: *Client\_type* Client Application Version: *Application\_version\_string*

**Explanation** The client operating system and application version appear. If the information is not available, then N/A will be indicated.

**Recommended Action** None required.

## 713185

**Error Message** %ASA-3-713185: Error: Username too long - connection aborted

**Explanation** The client returned an invalid length username, and the tunnel was torn down.

**Recommended Action** Check the username and make changes, if necessary.

## 713186

**Error Message** %ASA-3-713186: Invalid secondary domain name list received from the authentication server. List Received: *list\_text* Character *index* (value) is illegal

**Explanation** An invalid secondary domain name list was received from an external RADIUS authentication server. When split tunnelling is used, this list identifies the domains that the client should resolve through the tunnel.

**Recommended Action** Correct the specification of the Secondary-Domain-Name-List attribute (vendor-specific attribute 29) on the RADIUS server. The list must be specified as a comma-delimited list of domain names. Domain names may include only alphanumeric characters, a hyphen, an underscore, and a period.

## 713187

**Error Message** %ASA-7-713187: Tunnel Rejected: IKE peer does not match remote peer as defined in L2L policy IKE peer address: *IP\_address* , Remote peer address: *IP\_address*

**Explanation** The IKE peer that is attempting to bring up this tunnel is not the one that is configured in the ISAKMP configuration that is bound to the received remote subnet.

**Recommended Action** Verify that L2L settings are correct on the headend and peer.

## 713189

**Error Message** %ASA-3-713189: Attempted to assign network or broadcast *IP\_address* , removing ( *IP\_address* ) from pool.

**Explanation** The IP address from the pool is either the network or broadcast address for this subnet. This address will be marked as unavailable.

**Recommended Action** This error is generally benign, but the IP address pool configuration should be checked.

## 713190

**Error Message** %ASA-7-713190: Got bad refCnt ( *ref\_count\_value* ) assigning *IP\_address* ( *IP\_address* )

**Explanation** The reference counter for this SA is invalid.

**Recommended Action** None required.

## 713191

**Error Message** %ASA-3-713191: Maximum concurrent IKE negotiations exceeded!

**Explanation** To minimize CPU-intensive cryptographic calculations, the Secure Firewall ASA limits the number of connection negotiations in progress. When a new negotiation is requested and the Secure Firewall ASA is already at its limit, the new negotiation is rejected. When an existing connection negotiation completes, new connection negotiation will again be permitted.

**Recommended Action** See the **crypto ikev1 limit max-in-negotiation-sa** command. Increasing the limit can degrade performance..

## 713193

**Error Message** %ASA-3-713193: Received packet with missing payload, Expected payload: *payload\_id*

**Explanation** The Secure Firewall ASA received an encrypted or unencrypted packet of the specified exchange type that had one or more missing payloads. This usually indicates a problem on the peer.

**Recommended Action** Verify that the peer is sending valid IKE messages.

## 713194

**Error Message** %ASA-3-713194: Sending *IKE |IPsec* Delete With Reason message: *termination\_reason*

**Explanation** A delete message with a termination reason code was received.

**Recommended Action** None required.

## 713195

**Error Message** %ASA-3-713195: Tunnel rejected: Originate-Only: Cannot accept incoming tunnel yet!

**Explanation** The originate-only peer can accept incoming connections only after it brings up the first P2 tunnel. At that point, data from either direction can initiate additional Phase 2 tunnels.

**Recommended Action** If a different behavior is desired, the originate-only configuration needs to be revised.

## 713196

**Error Message** %ASA-5-713196: Remote L2L Peer *IP\_address* initiated a tunnel with same outer and inner addresses. Peer could be Originate Only - Possible misconfiguration!

**Explanation** The remote L2L peer has initiated a public-public tunnel. The remote L2L peer expects a response from the peer at the other end, but does not receive one, because of a possible misconfiguration.

**Recommended Action** Check the L2L configuration on both sides.

## 713197

**Error Message** %ASA-5-713197: The configured Confidence Interval of *number* seconds is invalid for this *tunnel\_type* connection. Enforcing the second default.

**Explanation** The configured confidence interval in the group is outside of the valid range.

**Recommended Action** Check the confidence setting in the group to make sure it is within the valid range.

## 713198

**Error Message** %ASA-3-713198: User Authorization failed: user User authorization failed. Username could not be found in the certificate

**Explanation** A reason string that states that a username cannot be found in the certificate appears.

**Recommended Action** Check the group configuration and client authorization.

## 713199

**Error Message** %ASA-5-713199: Reaper corrected an SA that has not decremented the concurrent IKE negotiations counter ( *counter\_value* )!

**Explanation** The Reaper corrected an internal software error.

**Recommended Action** If the problem persists, contact the Cisco TAC.

## 713203

**Error Message** %ASA-3-713203: IKE Receiver: Error reading from socket.

**Explanation** An error occurred while reading a received IKE packet. This is generally an internal error and might indicate a software problem.



**Recommended Action** This problem is usually benign, and the system will correct itself. If the problem persists, contact the Cisco TAC.

## 713204

**Error Message** %ASA-7-713204: Adding static route for client address: *IP\_address*

**Explanation** This message indicates that a route to the peer-assigned address or to the networks protected by a hardware client was added to the routing table.

**Recommended Action** None required.

## 713205

**Error Message** %ASA-3-713205: Could not add static route for client address: *IP\_address*

**Explanation** An attempt to add a route to the client-assigned address or to the networks protected by a hardware client failed. This might indicate duplicate routes in the routing table or a corrupted network address. The duplicate routes might be caused by routes that were not cleaned up correctly or by having multiple clients sharing networks or addresses.

**Recommended Action** Check the IP local pool configuration as well as any other IP address-assigning mechanism being used (for example, DHCP or RADIUS). Make sure that routes are being cleared from the routing table. Also check the configuration of networks and/or addresses on the peer.

## 713206

**Error Message** %ASA-3-713206: Tunnel Rejected: Conflicting protocols specified by tunnel-group and group-policy

**Explanation** A tunnel was dropped because the allowed tunnel specified in the group policy was different from the allowed tunnel in the tunnel group configuration.

**Recommended Action** Check the tunnel group and group policy configuration.

## 713207

**Error Message** %ASA-4-713207: Terminating connection: IKE Initiator and tunnel group specifies L2TP Over IPsec

**Explanation** This syslog is displayed for ikev1 while terminating the connection if GW is an initiator and tunnel group type is L2TP over IPSEC.

**Recommended Action** None required.

## 713208

**Error Message** %ASA-3-713208: Cannot create dynamic rule for Backup L2L entry rule *rule\_id*

**Explanation** A failure occurred in creating the ACLs that trigger IKE and allow IPsec data to be processed properly. The failure was specific to the backup L2L configuration, which may indicate a configuration error, a capacity error, or an internal software error.

**Recommended Action** If the Secure Firewall ASA is running the maximum number of connections and VPN tunnels, there may be a memory issue. If not, check the backup L2L and crypto map configurations, specifically the ACLs associated with the crypto maps.

## 713209

**Error Message** %ASA-3-713209: Cannot delete dynamic rule for Backup L2L entry rule id

**Explanation** A failure occurred in deleting the ACLs that trigger IKE and allow IPsec data to be processed correctly. The failure was specific to the backup L2L configuration. This may indicate an internal software error.

**Recommended Action** If the problem persists, contact the Cisco TAC.

## 713210

**Error Message** %ASA-3-713210: Cannot create dynamic map for Backup L2L entry rule\_id

**Explanation** A failure occurred in creating a run-time instance of the dynamic crypto map associated with backup L2L configuration. This may indicate a configuration error, a capacity error, or an internal software error.

**Recommended Action** If the Secure Firewall ASA is running the maximum number of connections and VPN tunnels, there may be a memory issue. If not, check the backup L2L and crypto map configurations, and specifically the ACLs associated with the crypto maps.

## 713211

**Error Message** %ASA-6-713211: Adding static route for L2L peer coming in on a dynamic map.  
address: *IP\_address* , mask: *netmask*

**Explanation** The ASA is adding a route for the private address or networks of the peer. In this case, the peer is either a client or a L2L peer with an unknown address. Both of these cases use dynamic crypto maps to allow the tunnel.

**Recommended Action** None required.

## 713212

**Error Message** %ASA-3-713212: Could not add route for L2L peer coming in on a dynamic map. address:  
*IP\_address* , mask: *netmask*

**Explanation** The Secure Firewall ASA failed while attempting to add a route for the private address or networks of the peer. In this case, the peer is either a client or a L2L peer with an unknown address. Both of these cases use dynamic crypto maps to allow the tunnel. This might indicate duplicate routes, a full routing table, or a failure of the Secure Firewall ASA to remove previously used routes.

Check the routing table to make sure there is room for additional routes and that obsolete routes are not present. If the table is full or includes obsolete routes, remove the routes and try again. If the problem persists, contact the Cisco TAC.

## 713213

**Error Message** %ASA-6-713213: Deleting static route for L2L peer that came in on a dynamic map. address: *IP\_address* , mask: *netmask*

**Explanation** The Secure Firewall ASA is deleting a route for the private address or networks of the peer. In this case, the peer is either a client or a L2L peer with an unknown address. Both of these cases use dynamic crypto maps to allow the tunnel.

**Recommended Action** None required.

## 713214

**Error Message** %ASA-3-713214: Could not delete route for L2L peer that came in on a dynamic map. address: *IP\_address* , mask: *netmask*

**Explanation** The Secure Firewall ASA experienced a failure while deleting a route for the private address or networks of the peer. In this case, the peer is either a client or a L2L peer with an unknown address. Both of these cases use dynamic crypto maps to allow the tunnel. The route may have already been deleted, or an internal software error has occurred.

**Recommended Action** If the route has already been deleted, the condition is benign and the device will function normally. If the problem persists or can be linked to routing issues over VPN tunnels, then check the routing and addressing portions of the VPN L2L configuration. Check the reverse route injection and the ACLs associated with the appropriate crypto map. If the problem persists, contact the Cisco TAC.

## 713215

**Error Message** %ASA-6-713215: No match against Client Type and Version rules. Client: *type* version *is /is* not allowed by default

**Explanation** The client type and the version of a client did not match any of the rules configured on the Secure Firewall ASA. The default action appears.

**Recommended Action** Determine what the default action and deployment requirements are, and make the applicable changes.

## 713216

**Error Message** %ASA-5-713216: Rule: *action* [Client type]: *version* Client: *type* version allowed/not allowed

**Explanation** The client type and the version of a client have matched one of the rules. The results of the match and the rule are displayed.

**Recommended Action** Determine what the deployment requirements are, and make the appropriate changes.

## 713217

**Error Message** %ASA-3-713217: Skipping unrecognized rule: action: *action* client type: *client\_type* client version: *client\_version*

**Explanation** A malformed client type and version rule exist. The required format is action client type | client version action. Either permit or deny client type and client version are displayed under Session Management. Only one wildcard per parameter (\*) is supported.

**Recommended Action** Correct the rule.

## 713218

**Error Message** %ASA-3-713218: Tunnel Rejected: Client Type or Version not allowed.

The client was denied access according to the configured rules.

None required.

## 713219

**Error Message** %ASA-6-713219: Queuing KEY-ACQUIRE messages to be processed when P1 SA is complete.

**Explanation** Phase 2 messages are being enqueued after Phase 1 completes.

**Recommended Action** None required.

## 713220

**Error Message** %ASA-6-713220: De-queuing KEY-ACQUIRE messages that were left pending.

**Explanation** Queued Phase 2 messages are being processed.

**Recommended Action** None required.

## 713221

**Error Message** %ASA-7-713221: Static Crypto Map check, checking map = *crypto\_map\_tag* , seq = *seq\_number*...

**Explanation** The Secure Firewall ASA is iterating through the crypto maps looking for configuration information.

**Recommended Action** None required.

## 713222

**Error Message** %ASA-7-713222: Group *group* Username *username* IP *ip* Static Crypto Map check, map = *crypto\_map\_tag* , seq = *seq\_number* , ACL does not match proxy IDs src:*source\_address* dst:*dest\_address*

**Explanation** While iterating through the configured crypto maps, the Secure Firewall ASA cannot match any of the associated ACLs. This generally means that an ACL was misconfigured.

**Recommended Action** Check the ACLs associated with this tunnel peer, and make sure that they specify the appropriate private networks from both sides of the VPN tunnel.

## 713223

**Error Message** %ASA-7-713223: Static Crypto Map check, map = *crypto\_map\_tag* , seq = *seq\_number* , no ACL configured

**Explanation** The crypto map associated with this peer is not linked to an ACL.

**Recommended Action** Make sure an ACL associated with this crypto map exists, and that the ACL includes the appropriate private addresses or network from both sides of the VPN tunnel.

## 713224

**Error Message** %ASA-7-713224: Static Crypto Map Check by-passed: Crypto map entry incomplete!

**Explanation** The crypto map associated with this VPN tunnel is missing critical information.

**Recommended Action** Verify that the crypto map is configured correctly with both the VPN peer, a transform set, and an associated ACL.

## 713225

**Error Message** %ASA-7-713225: [IKEv1], Static Crypto Map check, map *map\_name* , seq = *sequence\_number* is a successful match

**Explanation** The Secure Firewall ASA found a valid matching crypto map for this VPN tunnel.

**Recommended Action** None required.

## 713226

**Error Message** %ASA-3-713226: Connection failed with peer *IP\_address* , no trust-point defined in tunnel-group *tunnel\_group*

**Explanation** When the device is configured to use digital certificates, a trustpoint must be specified in the configuration. When the trustpoint is missing from the configuration, this message is generated to flag an error.

- **IP\_address**—IP address of the peer
- **tunnel\_group**—Tunnel group for which the trustpoint was missing in the configuration

**Recommended Action** The administrator of the device has to specify a trustpoint in the configuration.

## 713227

**Error Message** %ASA-3-713227: Rejecting new IPsec SA negotiation for peer *Peer\_address* . A negotiation was already in progress for local Proxy *Local\_address /Local\_netmask* , remote Proxy *Remote\_address /Remote\_netmask*

**Explanation** When establishing a Phase SA, the Secure Firewall ASA will reject a new Phase 2 matching this proxy.

**Recommended Action** None required.

## 713228

**Error Message** %ASA-6-713228: Group = *group* , Username = *uname* , IP = *remote\_IP\_address*  
Assigned private IP address *assigned\_private\_IP* to remote user

**Explanation** IKE obtained a private IP address for the client from DHCP or from the address pool.

- *group*— The name of the group
- *uname* —The name of the user
- *remote\_IP\_address* —The IP address of the remote client
- *assigned\_private\_IP* —The client IP address assigned by DHCP or from the local address pool

**Recommended Action** None required.

## 713229

**Error Message** %ASA-5-713229: Auto Update - Notification to client *client\_ip* of update  
string: *message\_string* .

**Explanation** A VPN remote access client is notified that updated software is available for download. The remote client user is responsible for choosing to update the client access software.

- *client\_ip*—The IP address of the remote client
- *message\_string*—The message text sent to the remote client

**Recommended Action** None required.

## 713230

**Error Message** %ASA-3-713230 Internal Error, *ike\_lock* trying to lock bit that is already  
locked for type *type*

**Explanation** An internal error occurred, which is reporting that the IKE subsystem is attempting to lock memory that has already been locked. This indicates errors on semaphores that are used to protect memory violations for IKE SAs. This message does not indicate that anything is seriously wrong. However, an unexpected event has occurred, and steps are automatically being taken for recovery.

- *>type* —String that describes the type of semaphore that had a locking issue

**Recommended Action** If the problem persists, contact the Cisco TAC.

## 713231

**Error Message** %ASA-3-713231 Internal Error, *ike\_lock* trying to unlock bit that is not locked  
for type *type*

**Explanation** An internal error has occurred, which is reporting that the IKE subsystem is attempting to unlock memory that is not currently locked. This indicates errors on semaphores that are used to protect memory violations for IKE SAs. This message does not indicate that anything is seriously wrong. However, an unexpected event has occurred, and steps are automatically being taken for recovery.

- *type* —String that describes the type of semaphore that had a locking issue

**Recommended Action** If the problem persists, contact the Cisco TAC.

## 713232

**Error Message** %ASA-3-713232 SA lock refCnt = *value* , bitmask = *hexvalue* , pl\_decrypt\_cb = *value* , qm\_decrypt\_cb = *value* , qm\_hash\_cb = *value* , qm\_spi\_ok\_cb = *value* , qm\_dh\_cb = *value* , qm\_secret\_key\_cb = *value* , qm\_encrypt\_cb = *value*

**Explanation** All the IKE SA are locked, and a possible error has been detected. This message reports errors on semaphores that are used to protect memory violations for IKE SAs.

- >*value* —Decimal value
- >*hexvalue* —Hexadecimal value

**Recommended Action** If the problem persists, contact the Cisco TAC.

## 713233

**Error Message** %ASA-7-713233: (VPN-unit ) Remote network (*remote network* ) validated for network extension mode.

**Explanation** The remote network received during the Phase 2 negotiation was validated. The message indicates the results of the remote network check during Phase 2 negotiations for Network Extension Mode clients. This is part of an existing feature that prevents users from misconfiguring their hardware client network (for example, configuring overlapping networks or the same network on multiple clients).

- *remote network* —Subnet address and subnet mask from Phase 2 proxy

**Recommended Action** None required.

## 713234

**Error Message** %ASA-7-713234: (VPN-unit) Remote network (*remote network* ) from network extension mode client mismatches AAA configuration (*aaa network* ).

**Explanation** The remote network received during the Phase 2 negotiation does not match the framed-ip-address and framed-subnet-mask that were returned from the AAA server for this session.

- *remote network* —Subnet address and subnet mask from Phase 2 proxy
- *aaa network* —Subnet address and subnet mask configured through AAA

**Recommended Action** Do one of the following:

- Check the address assignment for this user and group, then check the network configuration on the HW client, and correct any inconsistencies.
- Disable address assignment for this user and group.

## 713235

**Error Message** %ASA-6-713235: Attempt to send an IKE packet from standby unit. Dropping the packet!

**Explanation** Normally, IKE packets should never be sent from the standby unit to the remote peer. If such an attempt is made, an internal logic error may have occurred. The packet never leaves the standby unit because of protective code. This message facilitates debugging.

**Recommended Action** None required.

## 713236

**Error Message** %ASA-7-713236: IKE\_DECODE tx/rx Message (msgid=msgid) with payloads:payload1 (payload1\_len) + payload2 (payload2\_len)...total length: tlen

**Explanation** IKE sent or received various messages.

The following example shows the output when IKE receives a message with an 8-byte hash payload, an 11-byte notify payload, and two 13-byte vendor-specific payloads:

```
%ASA-7-713236: IKE_DECODE RECEIVED Message msgid=0) with payloads: HDR + HASH (8) + NOTIFY (11) + VENDOR (13) + VENDOR (13) + NONE (0)
```

**Recommended Action** None required.

## 713237

**Error Message** %ASA-5-713237: ACL update (*access\_list* ) received during re-key re-authentication will not be applied to the tunnel.

**Explanation** The Phase 1 rekey of a remote access IPsec tunnel appears under the following conditions:

- The tunnel is configured to reauthenticate the user when the tunnel is rekeyed.
- The RADIUS server returns an access list or a reference to a locally configured access list that is different from the one that was returned when the tunnel was first established.

**Recommended Action** Under these conditions, the Secure Firewall ASA ignores the new access list and this message is generated.

- *>access\_list*—Name associated with the static or dynamic access list, as displayed in the output of the **show access-list** command

IPsec users must reconnect for new user-specific access lists to take effect.

## 713238

**Error Message** %ASA-3-713238: Invalid source proxy address: 0.0.0.0! Check private address on remote client

**Explanation** The private side address of a network extension mode client came across as 0.0.0.0. This usually indicates that no IP address was set on the private interface of the hardware client.

**Recommended Action** Verify the configuration of the remote client.

## 713239

**Error Message** %ASA-4-713239: *IP\_Address* : Tunnel Rejected: The maximum tunnel count allowed has been reached

**Explanation** An attempt to create a tunnel has occurred after the maximum number of tunnels allowed has been reached.

- *IP\_Address*—The IP address of the peer

**Recommended Action** None required.



## 713240

**Error Message** %ASA-4-713240: Received DH key with bad length: received length=*rlength* expected length=*elength*

**Explanation** A Diffie-Hellman key with the incorrect length was received from the peer.

- *rlength*—The length of the DH key that was received
- *elength*—The expected length (based on the DH key size)

**Recommended Action** None required.

## 713241

**Error Message** %ASA-4-713241: IE Browser Proxy Method setting\_number is Invalid

**Explanation** An invalid proxy setting was found during ModeCfg processing. P1 negotiation will fail.

**Recommended Action** Check the **msie-proxy method** command settings (a subcommand of the **group-policy** command), which should conform to one of the following: [**auto-detect** | **no-modify** | **no-proxy** | **use-server**] . Any other value or no value is incorrect. Try resetting the **msie-proxy method** command settings. If the problem persists, contact the Cisco TAC.

## 713242

**Error Message** %ASA-4-713242: Remote user is authenticated using Hybrid Authentication. Not starting IKE rekey.

**Explanation** The Secure Firewall ASA has detected a request to start an IKE rekey for a tunnel configured to use Hybrid Xauth, but the rekey was not started. The Secure Firewall ASA will wait for the client to detect and initiate an IKE rekey.

**Recommended Action** None required.

## 713243

**Error Message** %ASA-4-713243: *META-DATA* Unable to find the requested certificate

**Explanation** The IKE peer requested a certificate from the cert-req payload. However, no valid identity certificate issued by the requested DN was found.

**Recommended Action** Perform the following steps:

1. Check the identity certificates.
2. Enroll or import the desired certificate.
3. Enable certificate debugging for more details.

## 713244

**Error Message** %ASA-4-713244: *META-DATA* Received Legacy Authentication Method(LAM) type *type* is different from the last type received *type* .

**Explanation** The LAM attribute type received differs from the last type received. The type must be consistent throughout the user authentication process. The user authentication process cannot proceed, and the VPN connection will not be established.

- **type**—The LAM type

**Recommended Action** If the problem persists, contact the Cisco TAC.

## 713245

**Error Message** %ASA-4-713245: *META-DATA* Unknown Legacy Authentication Method(LAM) type *type* received.

**Explanation** An unsupported LAM type was received during the CRACK challenge or response user authentication process. The user authentication process cannot proceed, and the VPN connection will not be established.

- **type**—The LAM type

**Recommended Action** If the problem persists, contact the Cisco TAC.

## 713246

**Error Message** %ASA-4-713246: *META-DATA* Unknown Legacy Authentication Method(LAM) attribute *type type* received.

**Explanation** The Secure Firewall ASA received an unknown LAM attribute type, which should not cause connectivity problems, but might affect the functionality of the peer.

- **type**—The LAM attribute type

**Recommended Action** None required.

## 713247

**Error Message** %ASA-4-713247: *META-DATA* Unexpected error: in Next Card Code mode while not doing SDI.

**Explanation** An unexpected error occurred during state processing.

**Recommended Action** If the problem persists, contact the Cisco TAC.

## 713248

**Error Message** %ASA-5-713248: *META-DATA* Rekey initiation is being disabled during CRACK authentication.

**Explanation** When an IKE SA is negotiated using the CRACK authentication method, the Phase 1 SA rekey timer at the headend expired before a successful rekey. Because the remote client is always the initiator of the exchange when using the CRACK authentication method, the headend will not initiate the rekey. Unless the remote peer initiates a successful rekey before the IKE SA expires, the connection will come down upon IKE SA expiration.

**Recommended Action** None required.

## 713249

**Error Message** %ASA-4-713249: *META-DATA* Received unsupported authentication results: *result*

**Explanation** While negotiating an IKE SA using the CRACK authentication method, the IKE subsystem received a result that is not supported during CRACK authentication from the authentication subsystem. The user authentication fails, and the VPN connection is torn down.

- *result* —The result returned from the authentication subsystem

**Recommended Action** If the problem persists, contact the Cisco TAC.

## 713250

**Error Message** %ASA-5-713250: *META-DATA* Received unknown Internal Address attribute: *attribute*

**Explanation** The Secure Firewall ASA received a request for an internal address attribute that is not recognizable. The attribute might be valid, but not currently supported, or the peer might be sending an illegal value. This should not cause connectivity problems, but might affect the functionality of the peer.

**Recommended Action** None required.

## 713251

**Error Message** %ASA-4-713251: *META-DATA* Received authentication failure message

**Explanation** The Secure Firewall ASA received a notification message that indicated an authentication failure while an IKE SA is negotiated using the CRACK authentication method. The connection is torn down.

**Recommended Action** None required.

## 713252

**Error Message** %ASA-5-713252: Group = *group* , Username = *user* , IP = *ip* , Integrity Firewall Server is not available. VPN Tunnel creation rejected for client.

**Explanation** When the group policy is configured to require the client to authenticate with a Zonelab Integrity Server, the server might need to be connected to the concentrator depending on the failure policy configured. If the fail policy is to reject the client connection, this message is generated when a Zonelab Integrity Server is not connected to the Secure Firewall ASA at the time the client is connecting.

- *group* —The tunnel group to which the remote access user is connecting
- *user* —The remote access user
- *ip* —The IP address of the remote access user

**Recommended Action** Check that the configurations on the concentrator and the Zonelab Integrity Server match. Then verify that communication exists between the concentrator and the Zonelab Integrity Server.

## 713253

**Error Message** %ASA-5-713253: Group = *group* , Username = *user* , IP = *ip* , Integrity Firewall Server is not available. Entering ALLOW mode. VPN Tunnel created for client.

**Explanation** When the group policy is configured to require a client to authenticate with a Zonelab Integrity Server, the server might need to be connected to the concentrator, depending on the failure policy configured. If the failure policy is to accept the client connection, and provide unrestricted network access, this message is generated when a Zonelab Integrity Server is not connected to the Secure Firewall ASA at the time the client is connecting.

- *group* —The tunnel group to which the remote access user is connecting
- *user* —The remote access user
- *ip* —The IP address of the remote access user

**Recommended Action** Check that the configurations on the Secure Firewall ASA and the Zonelab Integrity Server match, and verify that communication exists between the Secure Firewall ASA and the Zonelab Integrity Server.

## 713254

**Error Message** %ASA-3-713254: Group = *groupname* , Username = *username* , IP = *peerip* , Invalid IPsec/UDP port = *portnum* , valid range is *minport* - *maxport* , except port 4500, which is reserved for IPsec/NAT-T

**Explanation** You cannot use UDP port 4500 for IPsec/UDP connections, because it is reserved for IPsec or NAT-T connections. The CLI does not allow this configuration for local groups. This message should only occur for externally defined groups.

- *groupname* —The name of the user group
- *username* —The name of the user
- *peerip* —The IP address of the client
- *portnum* —The IPsec/UDP port number on the external server
- *minport* —The minimum valid port number for a user-configurable port, which is 4001
- *maxport* —The maximum valid port number for a user-configurable port, which is 49151

**Recommended Action** Change the IPsec or UDP port number on the external server to another port number. Valid port numbers are 4001 to 49151.

## 713255

**Error Message** %ASA-4-713255: IP = *peer-IP* , Received ISAKMP Aggressive Mode message 1 with unknown tunnel group name *group-name*

**Explanation** An unknown tunnel group was specified in ISAKMP Aggressive Mode message 1.

- *peer-ip* —The address of the peer
- *group-name* —The group name specified by the peer

**Recommended Action** Check the tunnel group and client configurations to make sure that they are valid.

## 713256

**Error Message** %ASA-6-713256: IP = *peer-IP* , Sending spoofed ISAKMP Aggressive Mode message 2 due to receipt of unknown tunnel group. Aborting connection.

**Explanation** When the peer specifies an invalid tunnel group, the Secure Firewall ASA will still send message 2 to prevent the peer from gleaning tunnel group information.

- *peer-ip* —The address of the peer

**Recommended Action** None required.

## 713257

**Error Message** %ASA-5-713257: Phase *var1* failure: Mismatched attribute types for class *var2*  
: Rcv'd: *var3* Cfg'd: *var4*

**Explanation** An Secure Firewall ASA has acted as the responder in a LAN-to-LAN connection. It indicates that the Secure Firewall ASA crypto configuration does not match the configuration of the initiator. The message specifies during which phase the mismatch occurred, and which attributes both the responder and the initiator had that were different.

- *var1* —The phase during which the mismatch occurred
- *var2* —The class to which the attributes that do not match belong
- *var3* —The attribute received from the initiator
- *var4* —The attribute configured

**Recommended Action** Check the crypto configuration on both of the LAN-to-LAN devices for inconsistencies. In particular, if a mismatch between UDP-Tunnel (NAT-T) and something else is reported, check the crypto maps. If one configuration has NAT-T disabled on the matched crypto map and the other does not, this will cause a failure.

## 713258

**Error Message** %ASA-3-713258: IP = *var1* , Attempting to establish a phase2 tunnel on *var2* interface but phase1 tunnel is on *var3* interface. Tearing down old phase1 tunnel due to a potential routing change.

**Explanation** The Secure Firewall ASA tries to establish a Phase 2 tunnel on an interface, and a Phase 1 tunnel already exists on a different interface. The existing Phase 1 tunnel is torn down to allow the establishment of a new tunnel on the new interface.

- *var1* —The IP address of the peer
- *var2* —The interface on which the Secure Firewall ASA is trying to establish a Phase 2 tunnel
- *var3* —The interface on which the Phase 1 tunnel exists

**Recommended Action** Check whether or not the route of the peer has changed. If the route has not changed, a possible misconfiguration may exist.

## 713259

**Error Message** %ASA-5-713259: Group = *groupname* , Username = *username* , IP = *peerIP* , Session is being torn down. Reason: *reason*

**Explanation** The termination reason for the ISAKMP session appears, which occurs when the session is torn down through session management.

- *groupname* —The tunnel group of the session being terminated
- *username* —The username of the session being terminated
- *peerIP* —The peer address of the session being terminated
- *reason* —The RADIUS termination reason of the session being terminated. Reasons include the following:

- Port Preempted (simultaneous logins)
- Idle Timeout
- Max Time Exceeded
- Administrator Reset

**Recommended Action** None required.

## 713260

**Error Message** %ASA-3-713260: Output interface %d to peer was not found

**Explanation** When trying to create a Phase 1 SA, the interface database could not be found for the interface ID.

**Recommended Action** If the problem persists, contact the Cisco TAC.

## 713261

**Error Message** %ASA-3-713261: IPV6 address on output interface %d was not found

**Explanation** When trying to create a Phase 1 SA, no IPv6 address is specified on the local interface.

**Recommended Action** For information about how to set up an IPv6 address on a desired interface, see the “Configuring IPv6 Addressing” section in the CLI configuration guide.

## 713262

**Error Message** %ASA-3-713262: Rejecting new IPSec SA negotiation for peer *Peer\_address* . A negotiation was already in progress for local Proxy *Local\_address /Local\_prefix\_len* , remote Proxy *Remote\_address /Remote\_prefix\_len*

**Explanation** When establishing a Phase SA, the Secure Firewall ASA will reject a new Phase 2 SA matching this proxy.

- *Peer\_address* —The new address attempting to initiate Phase 2 with a proxy matching an existing negotiation
- *Local\_address* —The address of the previous local peer currently negotiating Phase 2
- *Local\_prefix\_len* —The length of the subnet prefix according to CIDR notation
- *Remote\_address* —The address of the proxy
- *Remote\_prefix\_len* —The length of the subnet prefix according to CIDR notation

**Recommended Action** None required.

## 713263

**Error Message** %ASA-7-713263: Received local IP Proxy Subnet data in ID Payload: Address *IP\_address* , Mask */prefix\_len* , Protocol *protocol* , Port *port*

**Explanation** The Secure Firewall ASA is adding a route for the private address or networks of the peer. In this case, the peer is either a client or a L2L peer with an unknown address. Both of these cases use dynamic crypto maps to allow the tunnel.

- *IP\_address* —The base IP address of the destination network of the peer
- *prefix\_len* —The length of the subnet prefix according to CIDR notation
- *protocol* — The proxy protocol
- *port* —The proxy port

**Recommended Action** None required.

## 713264

**Error Message** %ASA-7-713264: Received local IP Proxy Subnet data in ID Payload: Address *IP\_address* , Mask/*prefix\_len* , Protocol *protocol* , Port *port* ("Received remote IP Proxy Subnet data in ID Payload: Address %a , Mask/%d , Protocol %u , Port %u ")

**Explanation** The Secure Firewall ASA is adding a route for the private address or networks of the peer. In this case, the peer is either a client or a L2L peer with an unknown address. Both of these cases use dynamic crypto maps to allow the tunnel.

- *IP\_address* —The base IP address of the destination network of the peer
- *prefix\_len* —The length of the subnet prefix according to CIDR notation
- *protocol* — The proxy protocol
- *port* —The proxy port

**Recommended Action** None required.

## 713265

**Error Message** %ASA-6-713265: Adding static route for L2L peer coming in on a dynamic map. address: *IP\_address* , mask: /*prefix\_len*

**Explanation** The Secure Firewall ASA is adding a route for the private address or networks of the peer. In this case, the peer is either a client or a L2L peer with an unknown address. Both of these cases use dynamic crypto maps to allow the tunnel.

- *IP\_address* —The base IP address of the destination network of the peer
- *prefix\_len* —The length of the subnet prefix according to CIDR notation

**Recommended Action** None required.

## 713266

**Error Message** %ASA-3-713266: Could not add route for L2L peer coming in on a dynamic map. address: *IP\_address* , mask: /*prefix\_len*

**Explanation** The Secure Firewall ASA failed while attempting to add a route for the private address or networks of the peer. In this case, the peer is either a client or a L2L peer with an unknown address. Both of these cases use dynamic crypto maps to allow the tunnel. This might indicate duplicate routes, a full IPv6 routing table, or a failure of the Secure Firewall ASA to remove previously used routes.

- *IP\_address* —The base IP address of the destination network of the peer
- *prefix\_len* —The length of the subnet prefix according to CIDR notation

**Recommended Action** Check the IPv6 routing table to make sure there is room for additional routes, and that obsolete routes are not present. If the table is full or includes obsolete routes, remove the routes and try again. If the problem persists, contact the Cisco TAC.

## 713267

**Error Message** %ASA-6-713267: Deleting static route for L2L peer that came in on a dynamic map. address: *IP\_address* , mask: */prefix\_len*

**Explanation** The Secure Firewall ASA failed while attempting to add a route for the private address or networks of the peer. In this case, the peer is either a client or a L2L peer with an unknown address. Both of these cases use dynamic crypto maps to allow the tunnel.

- *IP\_address* —The base IP address of the destination network of the peer
- *prefix\_len* —The length of the subnet prefix according to CIDR notation

**Recommended Action** None required.

## 713268

**Error Message** %ASA-3-713268: Could not delete route for L2L peer that came in on a dynamic map. address: *IP\_address* , mask: */prefix\_len*

**Explanation** The Secure Firewall ASA experienced a failure while deleting a route for the private address or networks of the peer. In this case, the peer is either a client or a L2L peer with an unknown address. Both of these cases use dynamic crypto maps to allow the tunnel. The route may have already been deleted, or an internal software error has occurred.

- *IP\_address* —The base IP address of the destination network of the peer
- *prefix\_len* —The length of the subnet prefix according to CIDR notation

**Recommended Action** If the route has already been deleted, the condition is benign and the device will function normally. If the problem persists or can be linked to routing issues over VPN tunnels, then check the routing and addressing portions of the VPN L2L configuration. Also check the reverse route injection and the ACLs associated with the appropriate crypto map. If the problem persists, contact the Cisco TAC.

## 713269

**Error Message** %ASA-6-713269: Detected Hardware Client in network extension mode, adding static route for address: *IP\_address* , mask: */prefix\_len*

**Explanation** A tunnel with a hardware client in network extension mode has been negotiated, and a static route is being added for the private network behind the hardware client. This configuration enables the Secure Firewall ASA to make the remote network known to all the routers on the private side of the headend.

- *IP\_address* —The base IP address of the destination network of the peer
- *prefix\_len* —The length of the subnet prefix according to CIDR notation

**Recommended Action** None required.



## 713270

**Error Message** %ASA-3-713270: Could not add route for Hardware Client in network extension mode, address: *IP\_address* , mask: */prefix\_len*

**Explanation** An internal software error has occurred. A tunnel with a hardware client in network extension mode has been negotiated, and an attempt to add the static route for the private network behind the hardware client failed. The IPv6 routing table may be full, or a possible addressing error has occurred.

- *IP\_address* —The base IP address of the destination network of the peer
- *prefix\_len* —The length of the subnet prefix according to CIDR notation

**Recommended Action** If the problem persists, contact the Cisco TAC.

## 713271

**Error Message** %ASA-6-713271: Terminating tunnel to Hardware Client in network extension mode, deleting static route for address: *IP\_address* , mask:*/prefix\_len*

**Explanation** A tunnel to a hardware client in network extension mode is being removed, and the static route for the private network is being deleted behind the hardware client.

- *IP\_address* —The base IP address of the destination network of the peer
- *prefix\_len* —The length of the subnet prefix according to CIDR notation

**Recommended Action** None required.

## 713272

**Error Message** %ASA-3-713272: Terminating tunnel to Hardware Client in network extension mode, unable to delete static route for address: *IP\_address* , mask: */prefix\_len*

**Explanation** While a tunnel to a hardware client in network extension mode was being removed, a route to the private network behind the hardware client cannot be deleted. This might indicate an addressing or software problem.

- *IP\_address* —The base IP address of the destination network of the peer
- *prefix\_len* —The length of the subnet prefix according to CIDR notation

**Recommended Action** Check the IPv6 routing table to ensure that the route is not there. If it is, it may have to be removed manually, but only if the tunnel to the hardware client has been completely removed.

## 713273

**Error Message** %ASA-7-713273: Deleting static route for client address: *IP\_Address IP\_Address* address of client whose route is being removed

**Explanation** A route to the peer-assigned address or the networks protected by a hardware client were removed from the routing table.

**Recommended Action** None required.

## 713274

**Error Message** %ASA-3-713274: Could not delete static route for client address: *IP\_Address*  
*IP\_Address* address of client whose route is being removed

**Explanation** While a tunnel to an IPsec client was being removed, its entry in the routing table could not be removed. This condition may indicate a networking or software problem.

**Recommended Action** Check the routing table to make sure that the route does not exist. If it does, it may need to be removed manually, but only if the tunnel has been closed successfully.

## 713275

**Error Message** %ASA-3-713275: IKEv1 Unsupported certificate keytype %s found at trustpoint  
%s

**Explanation** This syslog is displayed for ikev1 when certificate key type is not of type ECDSA. Ensure that certificates of valid KEY type is installed on the GW.

**Recommended Action** None required.

## 713276

**Error Message** %ASA-3-713276: Dropping new negotiation - IKEv1 in-negotiation context limit  
of %u reached

**Explanation** This syslog message is displayed for ikev1 in multi context when maximum in negotiation limit is reached.

**Recommended Action** None required.

## 713900

**Error Message** %ASA-1-713900: *Descriptive\_event\_string*.

**Explanation** A serious event or failure has occurred. For example, the Secure Firewall ASA is trying to generate a Phase 2 deletion, but the SPI did not match any of the existing Phase 2 SAs.

**Recommended Action** In the example described, both peers are deleting Phase 2 SAs at the same time. In this case, it is a benign error and can be ignored. If the error is persistent and results in negative side effects such as dropped tunnels or device reboots, it may reflect a software failure. In this case, copy the error message exactly as it appears on the console or in the system log, and then contact the Cisco TAC for further assistance.

## 713901

**Error Message** %ASA-2-713901: *Descriptive\_event\_string* .

**Explanation** An error has occurred, which may be the result of a configuration error on the headend or remote access client. The event string provides details about the error that occurred.

**Recommended Action** You may need to troubleshoot the message to determine what caused the error. Check the ISAKMP and crypto map configuration on both peers.

## 713902

**Error Message** %ASA-3-713902: *Descriptive\_event\_string*.

**Explanation** An error has occurred, which may be the result of a configuration error either on the headend or remote access client.

**Recommended Action** It might be necessary to troubleshoot the configuration to determine the cause of the error. Check the ISAKMP and crypto map configuration on both peers.

## 713903

**Error Message** %ASA-4-713903: *IKE error message reason reason*.

**Explanation** This syslog ID is used for IKE warning messages which can display multiple other syslogs.

**Recommended Action** None required.

Examples:

```
%ASA-4-713903: Group = group policy , Username = user name , IP = remote IP , ERROR: Failed to install Redirect URL: redirect URL Redirect ACL: non_exist for assigned IP
```

```
%ASA-4-713903: IKE Receiver: Runt ISAKMP packet discarded on Port Port_Number from Source_URL
```

```
%ASA-4-713903: IP = IP address, Header invalid, missing SA payload! (next payload = x)
```

```
%ASA-4-713903: Group = DefaultRAGroup, IP = IP address, Error: Unable to remove PeerTblEntry
```

## 713904

**Error Message** %ASA-5-713904: *Descriptive\_event\_string* .

**Explanation** Notification status information appears, which is used to track events that have occurred.

**Recommended Action** None required.

## 713905

**Error Message** %ASA-6-713905: *Descriptive\_event\_string*.

**Explanation** Information status details appear, which are used to track events that have occurred.

Example

```
%ASA-6-713905: IKE successfully unreserved UDP port 27910 on interface outside
```

**Recommended Action** None required.

## 713906

**Error Message** %ASA-7-713906: *Descriptive\_event\_string* .

**Explanation** Debugging status information appears, which is used to track events that have occurred.

**Recommended Action** None required.

## 714001

**Error Message** %ASA-7-714001: *description\_of\_event\_or\_packet*

**Explanation** A description of an IKE protocol event or packet was provided.

**Recommended Action** None required.

## 714002

**Error Message** %ASA-7-714002: IKE Initiator starting QM: msg id = *message\_number*

**Explanation** The Secure Firewall ASA has sent the first packet of the Quick mode exchange as the Phase 2 initiator.

**Recommended Action** None required.

## 714003

**Error Message** %ASA-7-714003: IKE Responder starting QM: msg id = *message\_number*

**Explanation** The Secure Firewall ASA has received the first packet of the Quick mode exchange as the Phase 2 responder.

**Recommended Action** None required.

## 714004

**Error Message** %ASA-7-714004: IKE Initiator sending 1st QM pkt: msg id = *message\_number*

**Explanation** The protocol of the first Quick Mode packet was decoded.

**Recommended Action** None required.

## 714005

**Error Message** %ASA-7-714005: IKE Responder sending 2nd QM pkt: msg id = *message\_number*

**Explanation** The protocol of the second Quick Mode packet was decoded.

**Recommended Action** None required.

## 714006

**Error Message** %ASA-7-714006: IKE Initiator sending 3rd QM pkt: msg id = *message\_number*

**Explanation** The protocol of the third Quick Mode packet was decoded.

**Recommended Action** None required.

## 714007

**Error Message** %ASA-7-714007: IKE Initiator sending Initial Contact

**Explanation** The Secure Firewall ASA is building and sending the initial contact payload.

**Recommended Action** None required.

## 714011

**Error Message** %ASA-7-714011: *Description of received ID values*

**Explanation** The Secure Firewall ASA received the displayed ID information during the negotiation.

**Recommended Action** None required.





## CHAPTER 8

# Syslog Messages 715001 to 721019

---

This chapter contains the following sections:

- [Messages 715001 to 715080, on page 369](#)
- [Messages 716001 to 716603, on page 381](#)
- [Messages 717001 to 717064, on page 400](#)
- [Messages 718001 to 719026, on page 417](#)
- [Messages 720001 to 721019, on page 438](#)

## Messages 715001 to 715080

This section includes messages from 715001 to 715080.

### 715001

**Error Message** %ASA-7-715001: *Descriptive statement*

**Explanation** A description of an event or problem encountered by the Secure Firewall ASA appears.

**Recommended Action** The action depends on the description.

### 715004

**Error Message** %ASA-7-715004: subroutine *name* () Q Send failure: RetCode (*return\_code*)

**Explanation** An internal error occurred when attempting to put messages in a queue.

**Recommended Action** This is often a benign condition. If the problem persists, contact the Cisco TAC.

### 715005

**Error Message** %ASA-7-715005: subroutine **name** () Bad message code: Code (*message\_code*)

**Explanation** An internal subroutine received a bad message code.

**Recommended Action** This is often a benign condition. If the problem persists, contact the Cisco TAC.

## 715006

**Error Message** %ASA-7-715006: IKE got SPI from key engine: SPI = *SPI\_value*

**Explanation** The IKE subsystem received an SPI value from IPsec.

**Recommended Action** None required.

## 715007

**Error Message** %ASA-7-715007: IKE got a KEY\_ADD msg for SA: SPI = *SPI\_value*

**Explanation** IKE has completed tunnel negotiation and has successfully loaded the appropriate encryption and hashing keys for IPsec use.

**Recommended Action** None required.

## 715008

**Error Message** %ASA-7-715008: Could not delete SA *SA\_address*, refCnt = *number* , caller = *calling\_subroutine\_address*

**Explanation** The calling subroutine cannot delete the IPsec SA. This might indicate a reference count problem.

**Recommended Action** If the number of stale SAs grows as a result of this event, contact the Cisco TAC.

## 715009

**Error Message** %ASA-7-715009: IKE Deleting SA: Remote Proxy *IP\_address* , Local Proxy *IP\_address*

**Explanation** SA is being deleted with the listed proxy addresses.

**Recommended Action** None required.

## 715013

**Error Message** %ASA-7-715013: Tunnel negotiation in progress for destination *IP\_address* , discarding data

**Explanation** IKE is in the process of establishing a tunnel for this data. All packets to be protected by this tunnel will be dropped until the tunnel is fully established.

**Recommended Action** None required.

## 715018

**Error Message** %ASA-7-715018: IP Range type id was loaded: Direction %s, From: %a, Through: %a

**Explanation** This syslog message is generated while updating IPSEC SA details.

**Recommended Action** None required.



## 715019

**Error Message** %ASA-7-715019: Group *group* Username *username* IP *ip* IKEGetUserAttributes:  
Attribute name = *name*

**Explanation** The **modcfg** attribute name and value pair being processed by the Secure Firewall ASA appear.

**Recommended Action** None required.

## 715020

**Error Message** %ASA-7-715020: construct\_cfg\_set: Attribute name = *name*

**Explanation** The **modcfg** attribute name and value pair being transmitted by the Secure Firewall ASA appear.

**Recommended Action** None required.

## 715021

**Error Message** %ASA-7-715021: Delay Quick Mode processing, Cert/Trans Exch/RM DSID in progress

**Explanation** Quick mode processing is being delayed until all Phase 1 processing has been completed (for transaction mode).

**Recommended Action** None required.

## 715022

**Error Message** %ASA-7-715022: Resume Quick Mode processing, Cert/Trans Exch/RM DSID completed

**Explanation** Phase 1 processing has completed, and quick mode is being resumed.

**Recommended Action** None required.

## 715027

**Error Message** %ASA-7-715027: IPsec SA Proposal # *chosen\_proposal* , Transform #  
*chosen\_transform* acceptable Matches global IPsec SA entry # *crypto\_map\_index*

**Explanation** The indicated IPsec SA proposal and transform were selected from the payloads that the responder received. This data can be useful when attempting to debug IKE negotiation issues.

**Recommended Action** None required.

## 715028

**Error Message** %ASA-7-715028: IKE SA Proposal # 1, Transform # **chosen\_transform** acceptable  
Matches global IKE entry # *crypto\_map\_index*

**Explanation** The indicated IKE SA transform was selected from the payloads that the responder received. This data can be useful when attempting to debug IKE negotiation issues.

**Recommended Action** None required.

## 715031

**Error Message** %ASA-7-715031: Obtained IP addr (%s) prior to initiating Mode Cfg (XAuth %s)

**Explanation** This syslog is generated when the IP address is assigned by the IP util subsystem.

**Recommended Action** None required.

## 715032

**Error Message** %ASA-7-715032: Sending subnet mask (%s) to remote client

**Explanation** This syslog is generated when the IP address is assigned by the IP util subsystem.

**Recommended Action** None required.

## 715033

**Error Message** %ASA-7-715033: Processing CONNECTED notify (MsgId *message\_number* )

**Explanation** The Secure Firewall ASA is processing a message containing a notify payload with the notify type CONNECTED (16384). The CONNECTED notify type is used to complete the commit bit processing and should be included in the fourth overall quick mode packet, which is sent from the responder to the initiator.

**Recommended Action** None required.

## 715034

**Error Message** %ASA-7-715034: action IOS keep alive payload: proposal=*time 1* /*time 2* sec.

**Explanation** Processing for sending or receiving a keepalive payload message is being performed.

**Recommended Action** None required.

## 715035

**Error Message** %ASA-7-715035: Starting IOS keepalive monitor: *seconds* sec.

**Explanation** The keepalive timer will monitor for a variable number of seconds for keepalive messages.

**Recommended Action** None required.

## 715036

**Error Message** %ASA-7-715036: Sending keep-alive of type *notify\_type* (seq number *number* )

**Explanation** Processing for sending a keepalive notify message is being performed.

**Recommended Action** None required.

## 715037

**Error Message** %ASA-7-715037: Unknown IOS Vendor ID version: *major.minor.variance*

**Explanation** The capabilities of this version of the Cisco IOS are not known.

**Recommended Action** There may be interoperability issues with features such as IKE keepalives. If the problem persists, contact the Cisco TAC.

## 715038

**Error Message** %ASA-7-715038: *action Spoofing\_information* Vendor ID payload (version: *major.minor.variance* , capabilities: *value* )

**Explanation** Processing for the Cisco IOS vendor ID payload has been performed. The action being performed might be Altiga spoofing the Cisco IOS.

**Recommended Action** None required.

## 715039

**Error Message** %ASA-7-715039: Unexpected cleanup of tunnel table entry during SA delete.

**Explanation** An entry in the IKE tunnel table was never removed when the SA was freed. This indicates a defect in the state machine.

**Recommended Action** If the problem persists, contact the Cisco TAC.

## 715040

**Error Message** %ASA-7-715040: Deleting active auth handle during SA deletion: handle = *internal\_authentication\_handle*

**Error Message** The authentication handle was still active during SA deletion. This is part of cleanup recovery during the error condition.

**Recommended Action** None required.

## 715041

**Error Message** %ASA-7-715041: Received keep-alive of type *keepalive\_type* , not the negotiated type

**Explanation** A keepalive of the type indicated in the message was received unexpectedly.

**Recommended Action** Check the keepalive configuration on both peers.

## 715042

**Error Message** %ASA-7-715042: IKE received response of type *failure\_type* to a request from the *IP\_address* utility

**Explanation** A request for an IP address for a remote access client from the internal utility that provides these addresses cannot be satisfied. Variable text in the message string indicates more specifically what went wrong.

**Recommended Action** Check the IP address assignment configuration and adjust accordingly.

## 715044

**Error Message** %ASA-7-715044: Ignoring Keepalive payload from vendor not support KeepAlive capability

**Explanation** A Cisco IOS keepalive payload from a vendor was received without keepalive capabilities being set. The payload is ignored.

**Recommended Action** None required.

## 715045

**Error Message** %ASA-7-715045: ERROR: malformed Keepalive payload

**Explanation** A malformed keepalive payload has been received. The payload is ignored.

**Recommended Action** None required.

## 715046

**Error Message** %ASA-7-715046: Group = *groupname* , Username = *username* , IP = *IP\_address* , constructing *payload\_description* payload

**Explanation** An IP address from a remote client for a specific group and user shows details about the IKE payload being constructed.

**Recommended Action** None required.

## 715047

**Error Message** %ASA-7-715047: processing *payload\_description* payload

**Explanation** Details of the IKE payload received and being processed appear.

**Recommended Action** None required.

## 715048

**Error Message** %ASA-7-715048: Send *VID\_type* VID

**Explanation** The type of vendor ID payload being sent appears.

**Recommended Action** None required.

## 715049

**Error Message** %ASA-7-715049: Received *VID\_type* VID

**Explanation** The type of vendor ID payload received appears.

**Recommended Action** None required.

## 715050

**Error Message** %ASA-7-715050: Claims to be IOS but failed authentication

**Explanation** The vendor ID received looks like a Cisco IOS VID, but does not match **hmac\_sha**.

**Recommended Action** Check the vendor ID configuration on both peers. If this issue affects interoperability and the problem persists, contact the Cisco TAC.

## 715051

**Error Message** %ASA-7-715051: Received unexpected TLV type *TLV\_type* while processing FWTYPE ModeCfg Reply

**Explanation** An unknown TLV was received in an Secure Firewall ASA record while an FWTYPE ModeCfg Reply was being processed. The TLV will be discarded. This might occur either because of packet corruption or because the connecting client supports a later version of the Secure Firewall ASA protocol.

**Recommended Action** Check the personal FW installed on the Cisco VPN client and the personal firewall configuration on the Secure Firewall ASA. This may also indicate a version mismatch between the VPN client and the Secure Firewall ASA.

## 715052

**Error Message** %ASA-7-715052: Old P1 SA is being deleted but new SA is DEAD, cannot transition centries

**Explanation** The old P1 SA is being deleted, but has no new SA to transition to because it was marked for deletion as well. This generally indicates that the two IKE peers are out-of-sync with each other and may be using different rekey times. The problem should correct itself, but there may be some small amount of data loss until a fresh P1 SA is reestablished.

**Recommended Action** None required.

## 715053

**Error Message** %ASA-7-715053: MODE\_CFG: Received request for *attribute\_info* !

**Explanation** The Secure Firewall ASA received a mode configuration message requesting the specified attribute.

**Recommended Action** None required.

## 715054

**Error Message** %ASA-7-715054: MODE\_CFG: Received *attribute\_name* reply: *value*

**Explanation** The Secure Firewall ASA received a mode configuration reply message from the remote peer.

**Recommended Action** None required.

## 715055

**Error Message** %ASA-7-715055: Send *attribute\_name*

**Explanation** The Secure Firewall ASA sent a mode configuration message to the remote peer.

**Recommended Action** None required.

## 715056

**Error Message** %ASA-7-715056: Client is configured for *TCP\_transparency*

**Explanation** Because the remote end (client) is configured for IPsec over TCP, the headend Secure Firewall ASA must not negotiate IPsec over UDP or IPsec over NAT-T with the client.

**Recommended Action** The NAT transparency configuration may require adjustment of one of the peers if the tunnel does not come up.

## 715057

**Error Message** %ASA-7-715057: Auto-detected a NAT device with NAT-Traversal. Ignoring IPsec-over-UDP configuration.

**Explanation** IPsec-over-UDP mode configuration information will not be exchanged because NAT-Traversal was detected.

**Recommended Action** None required.

## 715058

**Error Message** %ASA-7-715058: NAT-Discovery payloads missing. Aborting NAT-Traversal.

**Explanation** The remote end did not provide NAT-Discovery payloads required for NAT-Traversal after exchanging NAT-Traversal VIDs. At least two NAT-Discovery payloads must be received.

**Recommended Action** This may indicate a nonconforming NAT-T implementation. If the offending peer is a Cisco product and the problem persists, contact the Cisco TAC. If the offending peer is not a Cisco product, then contact the manufacturer support team.

## 715059

**Error Message** %ASA-7-715059: Proposing/Selecting only UDP-Encapsulated-Tunnel and UDP-Encapsulated-Transport modes defined by NAT-Traversal

**Explanation** You need to use these modes instead of the usual transport and tunnel modes defined in the SA to successfully negotiate NAT-Traversal.

**Recommended Action** None required.

## 715060

**Error Message** %ASA-7-715060: Dropped received IKE fragment. Reason: *reason*

**Explanation** The reason for dropping the fragment appears.

**Recommended Action** The recommended action depends on the drop reason, but might indicate a problem with an intervening NAT device or a nonconforming peer.

## 715061

**Error Message** %ASA-7-715061: Rcv'd fragment from a new fragmentation set. Deleting any old fragments.

**Explanation** A resend of the same packet occurred, but fragmented to a different MTU, or another packet altogether.

**Recommended Action** None required.

## 715062

**Error Message** %ASA-7-715062: Error assembling fragments! Fragment numbers are non-continuous.

**Explanation** There is a gap in fragment numbers.

**Recommended Action** This might indicate a network problem. If the condition persists and results in dropped tunnels or prevents certain peers from negotiating with the Secure Firewall ASA, contact the Cisco TAC.

## 715063

**Error Message** %ASA-7-715063: Successfully assembled an encrypted pkt from rcv'd fragments!

**Explanation** Assembly for a fragmented packet that was received was successful.

**Recommended Action** None required.

## 715064

**Error Message** %ASA-7-715064 -- IKE Peer included IKE fragmentation capability flags: Main Mode: *true /false* Aggressive Mode: *true /false*

**Explanation** The peer supports IKE fragmentation based on the information provided in the message.

**Recommended Action** None required.

## 715065

**Error Message** %ASA-7-715065: IKE *state\_machine subtype* FSM error history (struct *data\_structure\_address* ) *state , event* : *state /event* pairs

**Explanation** A Phase 1 error occurred and the **state**, **event** history pairs will be displayed in reverse chronological order.

**Recommended Action** Most of these errors are benign. If the problem persists, contact the Cisco TAC.

## 715066

**Error Message** %ASA-7-715066: Can't load an IPsec SA! The corresponding IKE SA contains an invalid logical ID.

**Explanation** The logical ID in the IKE SA is NULL. The Phase II negotiation will be torn down.

**Recommended Action** An internal error has occurred. If the problem persists, contact the Cisco TAC.

## 715067

**Error Message** %ASA-7-715067: QM IsRekeyed: existing sa from different peer, rejecting new sa

**Explanation** The LAN-TO-LAN SA that is being established already exists, that is, an SA with the same remote network, but is sourced from a different peer. This new SA will be deleted, because this is not a legal configuration.

**Recommended Action** Check the LAN-TO-LAN configuration on all associated peers. Specifically, multiple peers should not be sharing private networks.

## 715068

**Error Message** %ASA-7-715068: QM IsRekeyed: duplicate sa found by address , deleting old sa

**Explanation** The remote access SA that is being established already exists, that is, an SA with the same remote network, but is sourced from a different peer. The old SA will be deleted, because the peer may have changed its IP address.

**Recommended Action** This may be a benign condition, especially if a client tunnel was terminated abruptly. If the problem persists, contact the Cisco TAC.

## 715069

**Error Message** %ASA-7-715069: Invalid ESP SPI size of *SPI\_size*

**Explanation** The Secure Firewall ASA received an IPsec SA proposal with an invalid ESP SPI size. This proposal will be skipped.

**Recommended Action** Generally, this is a benign condition but might indicate that a peer may be nonconforming. If the problem persists, contact the Cisco TAC.

## 715070

**Error Message** %ASA-7-715070: Invalid IPComp SPI size of *SPI\_size*

**Explanation** The Secure Firewall ASA received an IPsec SA proposal with an invalid IPComp SPI size. This proposal will be skipped.

**Recommended Action** Generally, this is a benign condition but might indicate that a peer is nonconforming. If the problem persists, contact the Cisco TAC.



## 715071

**Error Message** %ASA-7-715071: AH proposal not supported

**Explanation** The IPsec AH proposal is not supported. This proposal will be skipped.

**Recommended Action** None required.

## 715072

**Error Message** %ASA-7-715072: Received proposal with unknown protocol ID *protocol\_ID*

**Explanation** The Secure Firewall ASA received an IPsec SA proposal with an unknown protocol ID. This proposal will be skipped.

**Recommended Action** Generally, this is a benign condition, but might indicate that a peer is nonconforming. If the problem persists, contact the Cisco TAC.

## 715074

**Error Message** %ASA-7-715074: Could not retrieve authentication attributes for peer *IP\_address*

**Explanation** The Secure Firewall ASA cannot get authorization information for the remote user.

**Recommended Action** Make sure that authentication and authorization settings have been configured correctly. If the problem persists, contact the Cisco TAC.

## 715075

**Error Message** %ASA-7-715075: Group = *group\_name* , IP = *IP\_address* Received keep-alive of type *message\_type* (seq number *number* )

**Explanation** This message is paired with DPD R-U-THERE message 715036, which logs the DPD sending messages.

- **group\_name**—The VPN group name of the peer
- **IP\_address**—IP address of the VPN peer
- **message\_type**—The message type (DPD R-U-THERE or DPD R-U-THERE-ACK)
- **number**—The DPD sequence number

Two possible cases:

- Received peer sending DPD R-U-THERE message
- Received peer reply DPD R-U-THERE-ACK message

Be aware of the following:

- The DPD R-U-THERE message is received and its sequence number matches the outgoing DPD reply messages.

If the Secure Firewall ASA sends a DPD R-U-THERE-ACK message without first receiving a DPD R-U-THERE message from the peer, it is likely experiencing a security breach.

- The received DPD R-U-THERE-ACK message's sequence number is matched with previously sent DPD messages.

If the Secure Firewall ASA did not receive a DPD R-U-THERE-ACK message within a reasonable amount of time after sending a DPD R-U-THERE message to the peer, the tunnel is most likely down.

**Recommended Action** None required.

## 715076

**Error Message** %ASA-7-715076: Computing hash for ISAKMP

**Explanation** IKE computed various hash values.

This object will be prepended as follows:

Group = >groupname , Username = >username , IP = >ip\_address ...

**Recommended Action** None required.

## 715077

**Error Message** %ASA-7-715077: Pitcher: msg string , spi spi

**Explanation** Various messages have been sent to IKE.

*msg\_string* can be one of the following:

- Received a key acquire message
- Received SPI for nonexistent SA
- Received key delete msg
- Received KEY\_UPDATE
- Received KEY\_REKEY\_IB
- Received KEY\_REKEY\_OB
- Received KEY\_SA\_ACTIVE
- Could not find IKE SA to activate IPSEC (OB)
- Could not find IKE SA to rekey IPSEC (OB)
- KEY\_SA\_ACTIVE no centry found
- KEY\_ADD centry not found
- KEY\_UPDATE centry not found

This object will be prepended as follows:

Group = >groupname , Username = >username , IP = >ip\_address ,...

**Recommended Action** None required.

## 715078

**Error Message** %ASA-7-715078: Received %s LAM attribute

**Explanation** This syslog is generated during parsing of challenge/response payload.

**Recommended Action** None required.

## 715079

**Error Message** %ASA-7-715079: INTERNAL\_ADDRESS: Received request for %s

**Explanation** This syslog is generated during processing of internal address payload.

**Recommended Action** None required.

## 715080

**Error Message** %ASA-7-715080: VPN: Starting P2 rekey timer: 28800 seconds.

**Error Message** An IKE rekey timer has started.

**Recommended Action** None required.

## Messages 716001 to 716603

This section includes messages from 716001 to 716603.

### 716001

**Error Message** %ASA-6-716001: Group *group* User *user* IP *ip* WebVPN session started.

**Explanation** The WebVPN session has started for the user in this group at the specified IP address. When the user logs in via the WebVPN login page, the WebVPN session starts.

**Recommended Action** None required.

### 716002

**Error Message** %ASA-6-716002: Group *GroupPolicy* User *username* IP *ip* WebVPN session terminated: User requested.

**Explanation** The WebVPN session has been terminated by a user request. Possible reasons include:

- Lost carrier
- Lost service
- Idle timeout
- Max time exceeded
- Administrator reset
- Administrator reboot
- Administrator shutdown
- Port error
- NAS error
- NAS request
- NAS reboot
- Port unneeded

- Port preempted. This reason indicates that the allowed number of simultaneous (same user) logins has been exceeded. To resolve this problem, increase the number of simultaneous logins or have users only log in once with a given username and password.
- Port suspended
- Service unavailable
- Callback
- User error
- Host requested
- Bandwidth management error
- ACL parse error
- VPN simultaneous logins limit specified in the group policy
- Unknown

**Recommended Action** Unless the reason indicates a problem, then no action is required.

## 716003

**Error Message** %ASA-6-716003: Group *group* User *user* IP *ip* WebVPN access "GRANTED: *url* "

**Explanation** The WebVPN user in this group at the specified IP address has been granted access to this URL. The user access to various locations can be controlled using WebVPN-specific ACLs.

**Recommended Action** None required.

## 716004

**Error Message** %ASA-6-716004: Group *group* User *user* WebVPN access DENIED to specified location: *url*

**Explanation** The WebVPN user in this group has been denied access to this URL. The WebVPN user access to various locations can be controlled using WebVPN-specific ACLs. In this case, a particular entry is denying access to this URL.

**Recommended Action** None required.

## 716005

**Error Message** %ASA-6-716005: Group *group* User *user* WebVPN ACL Parse Error: *reason*

**Explanation** The ACL for the WebVPN user in the specified group failed to parse correctly.

**Recommended Action** Correct the WebVPN ACL.

## 716006

**Error Message** %ASA-6-716006: Group *name* User *user* WebVPN session terminated. Idle timeout.

**Explanation** The WebVPN session was not created for the user in the specified group because the VPN tunnel protocol is not set to WebVPN.

**Recommended Action** None required.

## 716007

**Error Message** %ASA-4-716007: Group *group* User *user* WebVPN Unable to create session.

**Explanation** The WebVPN session was not created for the user in the specified group because of resource issues. For example, the user may have reached the maximum login limit.

**Recommended Action** None required.

## 716008

**Error Message** %ASA-7-716008: WebVPN ACL: *action*

**Explanation** The WebVPN ACL has begun performing an action (for example, begin parsing).

**Recommended Action** None required.

## 716009

**Error Message** %ASA-6-716009: Group *group* User *user* WebVPN session not allowed. WebVPN ACL parse error.

**Explanation** The WebVPN session for the specified user in this group is not allowed because the associated ACL did not parse. The user will not be allowed to log in via WebVPN until this error has been corrected.

**Recommended Action** Correct the WebVPN ACL.

## 716010

**Error Message** %ASA-7-716010: Group *group* User *user* Browse network.

**Explanation** The WebVPN user in the specified group browsed the network.

**Recommended Action** None required.

## 716011

**Error Message** %ASA-7-716011: Group *group* User *user* Browse domain *domain* .

**Explanation** The WebVPN specified user in this group browsed the specified domain.

**Recommended Action** None required.

## 716012

**Error Message** %ASA-7-716012: Group *group* User *user* Browse directory *directory* .

**Explanation** The specified WebVPN user browsed the specified directory.

**Recommended Action** None required.

**716013**

**Error Message** %ASA-7-716013: Group *group* User *user* Close file *filename* .

**Explanation** The specified WebVPN user closed the specified file.

**Recommended Action** None required.

**716014**

**Error Message** %ASA-7-716014: Group *group* User *user* View file *filename* .

**Explanation** The specified WebVPN user viewed the specified file.

**Recommended Action** None required.

**716015**

**Error Message** %ASA-7-716015: Group *group* User *user* Remove file *filename* .

**Explanation** The WebVPN user in the specified group removed the specified file.

**Recommended Action** None required.

**716016**

**Error Message** %ASA-7-716016: Group *group* User *user* Rename file *old\_filename* to *new\_filename* .

**Explanation** The specified WebVPN user renamed the specified file.

**Recommended Action** None required.

**716017**

**Error Message** %ASA-7-716017: Group *group* User *user* Modify file *filename* .

**Explanation** The specified WebVPN user modified the specified file.

**Recommended Action** None required.

**716018**

**Error Message** %ASA-7-716018: Group *group* User *user* Create file *filename* .

**Explanation** The specified WebVPN user created the specified file.

**Recommended Action** None required.

**716019**

**Error Message** %ASA-7-716019: Group *group* User *user* Create directory *directory* .

**Explanation** The specified WebVPN user created the specified directory.

**Recommended Action** None required.

## 716020

**Error Message** %ASA-7-716020: Group *group* User *user* Remove directory *directory* .

**Explanation** The specified WebVPN user removed the specified directory.

**Recommended Action** None required.

## 716021

**Error Message** %ASA-7-716021: File access DENIED, *filename* .

**Explanation** The specified WebVPN user was denied access to the specified file.

**Recommended Action** None required.

## 716022

**Error Message** %ASA-4-716022: Unable to connect to proxy server *reason* .

**Explanation** The WebVPN HTTP/HTTPS redirect failed for the specified reason.

**Recommended Action** Check the HTTP/HTTPS proxy configuration.

## 716023

**Error Message** %ASA-4-716023: Group *name* User *user* Session could not be established: session limit of *maximum\_sessions* reached.

**Explanation** The user session cannot be established because the current number of sessions exceeds the maximum session load.

**Recommended Action** Increase the configured limit, if possible, to create a load-balanced cluster.

## 716024

**Error Message** %ASA-7-716024: Group *name* User *user* Unable to browse the network. Error: *description*

**Explanation** The user was unable to browse the Windows network using the CIFS protocol, as indicated by the description. For example, “Unable to contact necessary server” indicates that the remote server is unavailable or unreachable. This might be a transient condition or may require further troubleshooting.

**Recommended Action** Check the connectivity between the WebVPN device and the server being accessed by the CIFS protocol. Also check the NetBIOS name server configuration on the Secure Firewall ASA.

## 716025

**Error Message** %ASA-7-716025: Group *name* User *user* Unable to browse domain *domain* . Error: *description*

**Explanation** The user was unable to browse the remote domain using the CIFS protocol.

**Recommended Action** Check the connectivity between the WebVPN device and the server being accessed by the CIFS protocol. Check the NetBIOS name server configuration on the Secure Firewall ASA.

## 716026

**Error Message** %ASA-7-716026: Group name User user Unable to browse directory *directory* .  
Error: *description*

**Explanation** The user was unable to browse the remote directory using the CIFS protocol.

**Recommended Action** Check the connectivity between the WebVPN device and the server being accessed by the CIFS protocol. Also check the NetBIOS name server configuration on the Secure Firewall ASA.

## 716027

**Error Message** %ASA-7-716027: Group name User user Unable to view file *filename* . Error:  
*description*

**Explanation** The user was unable to view the remote file using the CIFS protocol.

**Recommended Action** Check the connectivity between the WebVPN device and the server being accessed by the CIFS protocol. Also check the NetBIOS name server configuration on the Secure Firewall ASA.

## 716028

**Error Message** %ASA-7-716028: Group name User user Unable to remove file *filename* . Error:  
*description*

**Explanation** The user was unable to remove the remote file using the CIFS protocol, probably caused by a lack of file permissions.

**Recommended Action** Check the connectivity between the WebVPN device and the server being accessed by the CIFS protocol. Also check the NetBIOS name server configuration on the Secure Firewall ASA and the file permissions.

## 716029

**Error Message** %ASA-7-716029: Group name User user Unable to rename file *filename* . Error:  
*description*

**Explanation** The user was unable to rename the remote file using the CIFS protocol, probably caused by lack of file permissions.

**Recommended Action** Check the connectivity between the WebVPN device and the server being accessed by the CIFS protocol. Also check the NetBIOS name server configuration on the Secure Firewall ASA and the file permissions.

## 716030

**Error Message** %ASA-7-716030: Group name User user Unable to modify file *filename* . Error:  
*description*



**Explanation** A problem occurred when a user attempted to modify an existing file using the CIFS protocol, probably caused by a lack of file permissions.

**Recommended Action** Check the connectivity between the WebVPN device and the server being accessed by the CIFS protocol. Also check the NetBIOS name server configuration on the Secure Firewall ASA and the file permissions.

## 716031

**Error Message** %ASA-7-716031: Group *name* User *user* Unable to create file *filename* . Error: *description*

**Explanation** A problem occurred when a user attempted to create a file using the CIFS protocol, probably caused by a file permissions problem.

**Recommended Action** Check the connectivity between the WebVPN device and the server being accessed by the CIFS protocol. Also check the NetBIOS name server configuration on the Secure Firewall ASA and the file permissions.

## 716032

**Error Message** %ASA-7-716032: Group *name* User *user* Unable to create folder *folder* . Error: *description*

**Explanation** A problem occurred when a user attempted to create a folder using the CIFS protocol, probably caused by a file permissions problem.

**Recommended Action** Check the connectivity between the WebVPN device and the server being accessed by the CIFS protocol. Also check the NetBIOS name server configuration on the Secure Firewall ASA and the file permissions.

## 716033

**Error Message** %ASA-7-716033: Group *name* User *user* Unable to remove folder *folder* . Error: *description*

**Explanation** A problem occurred when a user of the CIFS protocol attempted to remove a folder, which probably occurred because of a permissions problem or a problem communicating with the server on which the file resides.

**Recommended Action** Check the connectivity between the WebVPN device and the server being accessed by the CIFS protocol. Also check the NetBIOS name server configuration on the Secure Firewall ASA.

## 716034

**Error Message** %ASA-7-716034: Group *name* User *user* Unable to write to file *filename* .

**Explanation** A problem occurred when a user attempted to write to a file using the CIFS protocol, probably caused by a permissions problem or a problem communicating with the server on which the file resides.

**Recommended Action** None required.

## 716035

**Error Message** %ASA-7-716035: Group *name* User *user* Unable to read file *filename* .

**Explanation** A problem occurred when a user of the CIFS protocol tried to read a file, probably caused by a file permissions problem.

**Recommended Action** Check the file permissions.

## 716036

**Error Message** %ASA-7-716036: Group *name* User *user* File Access: User *user* logged into the *server* *server*.

**Explanation** A user successfully logged into the server using the CIFS protocol

**Recommended Action** None required.

## 716037

**Error Message** %ASA-7-716037: Group *name* User *user* File Access: User *user* failed to login into the *server* *server*.

**Explanation** A user attempted to log in to a server using the CIFS protocol, but was unsuccessful.

**Recommended Action** Verify that the user entered the correct username and password.

## 716038

**Error Message** %ASA-6-716038: Group *group* User *user* IP *ip* Authentication: successful, Session Type: WebVPN.

**Explanation** Before a WebVPN session can start, the user must be authenticated successfully by a local or remote server (for example, RADIUS or TACACS+).

**Recommended Action** None required.

## 716039

**Error Message** %ASA-6-716039: Authentication: rejected, group = *name* user = *user* , Session Type: %s

**Explanation** Before a WebVPN session starts, the user must be authenticated successfully by a local or remote server (for example, RADIUS or TACACS+). In this case, the user credentials (username and password) either did not match, or the user does not have permission to start a WebVPN session. The username is hidden when invalid or unknown, but appears when valid or the **no logging hide username** command has been configured.

- %s—The session type, which can be either WebVPN or admin

**Recommended Action** Verify the user credentials on the local or remote server and that WebVPN is configured for the user.

## 716040

**Error Message** %ASA-6-716040: Reboot pending, new sessions disabled. Denied user login.

**Explanation** A user was unable to log in to WebVPN because the Secure Firewall ASA is in the process of rebooting.

- **user**—The session user

**Recommended Action** None required.

## 716041

**Error Message** %ASA-6-716041: access-list *acl\_ID* *action* *url* *url* *hit\_cnt* *count*

**Explanation** The WebVPN URL named **acl\_ID** has been hit **count** times for location **url**, whose **action** is permitted or denied.

- **acl\_ID**—The WebVPN URL ACL
- *count* —The number of times the URL was accessed
- *url* —The URL that was accessed
- *action* —The user action

**Recommended Action** None required.

## 716042

**Error Message** %ASA-6-716042: access-list *acl\_ID* *action* *tcp* *source\_interface* /*source\_address* (*source\_port* ) - *dest\_interface* /*dest\_address* (*dest\_port* ) hit-cnt *count*

**Explanation** The WebVPN TCP named **acl\_ID** has been hit **count** times for packet received on the source interface **source\_interface/source\_address** and source port **source\_port** forwarded to **dest\_interface/dest\_address** destination **dest\_port**, whose **action** is permitted or denied.

- *count* —The number of times the ACL was accessed
- *source\_interface* —The source interface
- *source\_address* —The source IP address
- *source\_port* —The source port
- *dest\_interface* —The destination interface
- *dest\_address* —The destination IP address
- *action* —The user action

**Recommended Action** None required.

## 716043

**Error Message** %ASA-6-716043 Group *group-name* , User *user-name* , IP *IP\_address* : WebVPN Port Forwarding Java applet started. Created new hosts file mappings.

**Explanation** The user has launched a TCP port-forwarding applet from a WebVPN session.

- **group-name**—Group name associated with the session
- **user-name**—Username associated with the session

- **IP\_address**—Source IP address associated with the session

**Recommended Action** None required.

## 716044

**Error Message** %ASA-4-716044: Group *group-name* User *user-name* IP *IP\_address* AAA parameter *param-name* value *param-value* out of range.

**Explanation** The given parameter has a bad value.

- **group-name**—The name of the group
- **user-name**—The name of the user
- **IP\_address**—The IP address
- **param-name**—The name of the parameter
- **param-value**—The value of the parameter

**Recommended Action** Modify the configuration to correct the indicated parameter. If the parameter is `vlan` or `nac-settings`, verify that it is correctly configured on the AAA server and the Secure Firewall ASA.

## 716045

**Error Message** %ASA-4-716045: Group *group-name* User *user-name* IP *IP\_address* AAA parameter *param-name* value invalid.

**Explanation** The given parameter has a bad value. The value is not shown because it might be very long.

- **group-name**—The name of the group
- **user-name**—The name of the user
- **IP\_address**—The IP address
- **param-name**—The name of the parameter

**Recommended Action** Modify the configuration to correct the indicated parameter.

## 716046

**Error Message** %ASA-4-716046: Group *group-name* User *user-name* IP *IP\_address* User ACL *access-list-name* from AAA doesn't exist on the device, terminating connection.

**Explanation** The specified ACL was not found on the Secure Firewall ASA.

- **group-name**—The name of the group
- **user-name**—The name of the user
- **IP\_address**—The IP address
- **access-list-name**—The name of the ACL

**Recommended Action** Modify the configuration to add the specified ACL or to correct the ACL name.

## 716047

**Error Message** %ASA-4-716047: Group *group-name* User *user-name* IP *IP\_address* User ACL *access-list-name* from AAA ignored, AV-PAIR ACL used instead.

**Explanation** The specified ACL was not used because a Cisco AV-PAIR ACL was used.

- **group-name**—The name of the group
- **user-name**—The name of the user
- **IP\_address**—The IP address
- **access-list-name**—The name of the ACL

**Recommended Action** Determine the correct ACL to use and correct the configuration.

## 716048

**Error Message** %ASA-4-716048: Group *group-name* User *user-name* IP *IP\_address* No memory to parse ACL.

**Explanation** There was not enough memory to parse the ACL.

- **group-name**—The name of the group
- **user-name**—The name of the user
- **IP\_address**—The IP address

**Recommended Action** Purchase more memory, upgrade the Secure Firewall ASA, or reduce the load on it.

## 716049

**Error Message** %ASA-6-716049: Group *group-name* User *user-name* IP *IP\_address* Empty SVC ACL.

**Explanation** The ACL to be used by the client was empty.

- **group-name**—The name of the group
- **user-name**—The name of the user
- **IP\_address**—The IP address

**Recommended Action** Determine the correct ACL to use and modify the configuration.

## 716050

**Error Message** %ASA-6-716050: Error adding to ACL: *ace\_command\_line*

**Explanation** The ACL entry had a syntax error.

- **ace\_command\_line**—The ACL entry that is causing the error

**Recommended Action** Correct the downloadable ACL configuration.

## 716051

**Error Message** %ASA-6-716051: Group *group-name* User *user-name* IP *IP\_address* Error adding dynamic ACL for user.

**Explanation** There is not enough memory to perform the action.

- **group-name**—The name of the group
- **user-name**—The name of the user
- **IP\_address**—The IP address

**Recommended Action** Purchase more memory, upgrade the Secure Firewall ASA, or reduce the load on it.

## 716052

**Error Message** %ASA-4-716052: Group *group-name* User *user-name* IP *IP\_address* Pending session terminated.

**Explanation** A user did not complete login and the pending session was terminated. This may be due to an SVC that was unable to connect.

- **group-name**—The name of the group
- **user-name**—The name of the user
- **IP\_address**—The IP address

**Recommended Action** Check the user PC for SVC compatibility.

## 716053

**Error Message** %ASA-5-716053: SAML Server added: name: *name* Type: SP

**Explanation** A SAML IDP server entry has been added to the webvpn configuration.

- **name**—The entityID of the SAML IDP

**Recommended Action** None required.

## 716054

**Error Message** %ASA-5-716054: SAML Server deleted: name: *name* Type: SP

**Explanation** A SAML IDP server entry has been removed from the webvpn configuration. .

- **name**—The entityID of the SAML IDP

**Recommended Action** None required.

## 716057

**Error Message** %ASA-3-716057: Group *group* User *user* IP *ip* Session terminated, no *type* license available.

**Explanation** A user has attempted to connect to the Secure Firewall ASA using a client that is not licensed. This message may also occur if a temporary license has expired.

- *group* —The group policy that the user logged in with
- *user* —The name of the user
- *IP* —The IP address of the user
- *type* —The type of license requested, which can be one of the following:

- AnyConnect Mobile
- LinkSys Phone
- The type of license requested by the client (if other than the AnyConnect Mobile or LinkSys Phone)
- Unknown

**Recommended Action** A permanent license with the appropriate feature should be purchased and installed.

## 716058

**Error Message** %ASA-6-716058: Group *group* User *user* IP *ip* AnyConnect session lost connection. Waiting to resume.

**Explanation** The SSL tunnel was dropped and the AnyConnect session enters the inactive state, which can be caused by a hibernating host, a standby host, or a loss of network connectivity.

- *group* —The tunnel group name associated with the AnyConnect session
- *user* —The name of the user associated with the session
- *ip* —The source IP address of the session

**Recommended Action** None required.

## 716059

**Error Message** %ASA-6-716059: Group *group* User *user* IP *ip* AnyConnect session resumed. Connection from *ip2* .

**Explanation** An AnyConnect session resumed from the inactive state.

- *group* —The tunnel group name associated with the AnyConnect session
- *user* —The name of the user associated with the session
- *ip* —The source IP address of the session
- *ip2* —The source IP address of the host on which the session is resumed

**Recommended Action** None required.

## 716060

**Error Message** %ASA-6-716060: Group *group* User *user* IP *ip* Terminated AnyConnect session in inactive state to accept a new connection. License limit reached.

**Explanation** An AnyConnect session in the inactive state was logged out to allow a new incoming SSL VPN (AnyConnect or clientless) connection.

- *group* —The tunnel group name associated with the AnyConnect session
- *user* —The name of the user associated with the session
- *ip* —The source IP address of the session

**Recommended Action** None required.

## 716061

**Error Message** %ASA-3-716061: Group *DfltGrpPolicy* User *user* IP *ip* *addr* IPv6 User Filter *tempipv6* configured for AnyConnect. This setting has been deprecated, terminating connection

**Explanation** The IPv6 VPN filter has been deprecated and if it is configured instead of a unified filter for IPv6 traffic access control, the connection will be terminated.

**Recommended Action** Configure a unified filter with IPv6 entries to control IPv6 traffic for the user.

## 716158

**Error Message** %ASA-3-716158: Failed to create SAML logout request, initiated by SP. Reason: *reason*

**Explanation** The device was unable to inform the SAML IDP of a user logout because it encountered an error while creating the SAML Logout request. The reasons could be *profile is empty, could not create logout object*, and so on.

**Recommended Action** None

## 716159

**Error Message** %ASA-3-716159: Failed to process SAML logout request, initiated by SP. Reason: *reason*

**Explanation** The device encountered an error while processing a SAML logout request initiated by the IDP. The reasons could be *NameID is invalid, could not create logout object*, and so on.

**Recommended Action** None

## 716160

**Error Message** %ASA-3-716160: Failed to create SAML authentication request. Reason: *reason*

**Explanation** The device was unable to authenticate a user with the SAML IDP because it encountered an error while creating the SAML authn request. The reasons could be *NameIDPolicy is invalid, could not create new login instance*, and so on.

**Recommended Action** None

## 716162

**Error Message** %ASA-3-716162: Failed to consume SAML assertion. Reason: *reason*

**Explanation** The device encountered an error while processing an authentication response from a SAML IDP. The reasons could be *response or assertion is empty, could not create new login instance, assertion is expired or not valid, assertion is empty, issuer is empty, subject is empty, issuer content is empty, name\_id or content is empty*, and so on.

**Recommended Action** None

## 716165

**Error Message** %ASA-4-716165: SAML assertion cannot be replay protected because it does not contain time constraints.

**Explanation** SAML assertions need to contain time constraints in order for the firewall device to be able to guarantee replay detection. SAML assertions that do not contain time constraints are still accepted and cached for 10 minutes (default) or for the time specified by the `timeout assertion` CLI in the `config-webvpn-saml-idp` submode. After the assertion is removed from the cache, the assertion will again become valid when it is received again.

**Recommended Action** None. This needs to be addressed within the IDP product.



## 716500

**Error Message** %ASA-2-716500: internal error in: *function* : Fiber library cannot locate AK47 instance

**Explanation** The fiber library cannot locate the application kernel layer 4 to 7 instance.

**Recommended Action** To determine the cause of the problem, contact the Cisco TAC.

## 716501

**Error Message** %ASA-2-716501: internal error in: *function* : Fiber library cannot attach AK47 instance

**Explanation** The fiber library cannot attach the application kernel layer 4 to 7 instance.

**Recommended Action** To determine the cause of the problem, contact the Cisco TAC.

## 716502

**Error Message** %ASA-2-716502: internal error in: *function* : Fiber library cannot allocate default arena

**Explanation** The fiber library cannot allocate the default arena.

**Recommended Action** To determine the cause of the problem, contact the Cisco TAC.

## 716503

**Error Message** %ASA-2-716503: internal error in: *function* : Fiber library cannot allocate fiber descriptors pool

**Explanation** The fiber library cannot allocate the fiber descriptors pool.

**Recommended Action** To determine the cause of the problem, contact the Cisco TAC.

## 716504

**Error Message** %ASA-2-716504: internal error in: *function* : Fiber library cannot allocate fiber stacks pool

**Explanation** The fiber library cannot allocate the fiber stack pool.

**Recommended Action** To determine the cause of the problem, contact the Cisco TAC.

## 716505

**Error Message** %ASA-2-716505: internal error in: *function* : Fiber has joined fiber in unfinished state

**Explanation** The fiber has joined fiber in an unfinished state.

**Recommended Action** To determine the cause of the problem, contact the Cisco TAC.

## 716506

**Error Message** %ASA-2-716506: UNICORN\_SYSLOGID\_JOINED\_UNEXPECTED\_FIBER

**Explanation** An internal fiber library was generated.

**Recommended Action** Contact the Cisco TAC.

## 716507

**Error Message** %ASA-1-716507: Fiber scheduler has reached unreachable code. Cannot continue, terminating.

**Explanation** The Secure Firewall ASA has experienced an unexpected error and has recovered.

**Recommended Action** Check for high CPU usage or CPU hogs, and potential memory leaks. If the problem persists, contact the Cisco TAC.

## 716508

**Error Message** %ASA-1-716508: internal error in: *function* : Fiber scheduler is scheduling rotten fiber. Cannot continuing terminating

**Explanation** The fiber scheduler is scheduling rotten fiber, so it cannot continue terminating.

**Recommended Action** To determine the cause of the problem, contact the Cisco TAC.

## 716509

**Error Message** %ASA-1-716509:internal error in: *function* : Fiber scheduler is scheduling alien fiber. Cannot continue terminating

**Explanation** The fiber scheduler is scheduling alien fiber, so it cannot continue terminating.

**Recommended Action** To determine the cause of the problem, contact the Cisco TAC.

## 716510

**Error Message** %ASA-1-716510:internal error in: *function* : Fiber scheduler is scheduling finished fiber. Cannot continue terminating

**Explanation** The fiber scheduler is scheduling finished fiber, so it cannot continue terminating.

**Recommended Action** To determine the cause of the problem, contact the Cisco TAC.

## 716512

**Error Message** %ASA-2-716512:internal error in: *function* : Fiber has joined fiber waited upon by someone else

**Explanation** The fiber has joined fiber that is waited upon by someone else.

**Recommended Action** To determine the cause of the problem, contact the Cisco TAC.

## 716513

**Error Message** %ASA-2-716513: internal error in: *function* : Fiber in callback blocked on other channel

**Explanation** The fiber in the callback was blocked on the other channel.

**Recommended Action** To determine the cause of the problem, contact the Cisco TAC.

## 716515

**Error Message** %ASA-2-716515:internal error in: *function* : OCCAM failed to allocate memory for AK47 instance

**Explanation** The OCCAM failed to allocate memory for the AK47 instance.

**Recommended Action** To determine the cause of the problem, contact the Cisco TAC.

## 716516

**Error Message** %ASA-1-716516: internal error in: *function* : OCCAM has corrupted ROL array. Cannot continue terminating

**Explanation** The OCCAM has a corrupted ROL array, so it cannot continue terminating.

**Recommended Action** To determine the cause of the problem, contact the Cisco TAC.

## 716517

**Error Message** %ASA-2-716517: internal error in: *function* : OCCAM cached block has no associated arena

**Explanation** The OCCAM cached block has no associated arena.

**Recommended Action** To determine the cause of the problem, contact the Cisco TAC.

## 716518

**Error Message** %ASA-2-716518: internal error in: *function* : OCCAM pool has no associated arena

**Explanation** The OCCAM pool has no associated arena.

**Recommended Action** To determine the cause of the problem, contact the Cisco TAC.

## 716519

**Error Message** %ASA-1-716519: internal error in: *function* : OCCAM has corrupted pool list. Cannot continue terminating

**Explanation** The OCCAM has a corrupted pool list, so it cannot continue terminating.

**Recommended Action** To determine the cause of the problem, contact the Cisco TAC.

## 716520

**Error Message** %ASA-2-716520: internal error in: *function* : OCCAM pool has no block list

**Explanation** The OCCAM pool has no block list.

**Recommended Action** To determine the cause of the problem, contact the Cisco TAC.

## 716521

**Error Message** %ASA-2-716521: internal error in: *function* : OCCAM no realloc allowed in named pool

**Explanation** The OCCAM did not allow reallocation in the named pool.

**Recommended Action** To determine the cause of the problem, contact the Cisco TAC.

## 716522

**Error Message** %ASA-2-716522: internal error in: *function* : OCCAM corrupted standalone block

**Explanation** The OCCAM has a corrupted standalone block.

**Recommended Action** To determine the cause of the problem, contact the Cisco TAC.

## 716525

**Error Message** %ASA-2-716525: UNICORN\_SYSLOGID\_SAL\_CLOSE\_PRIVDATA\_CHANGED

**Explanation** An internal SAL error has occurred.

**Recommended Action** Contact the Cisco TAC.

## 716526

**Error Message** %ASA-2-716526: UNICORN\_SYSLOGID\_PERM\_STORAGE\_SERVER\_LOAD\_FAIL

**Explanation** A failure in the mounting of the permanent storage server directory occurred.

**Recommended Action** Contact the Cisco TAC.

## 716527

**Error Message** %ASA-2-716527: UNICORN\_SYSLOGID\_PERM\_STORAGE\_SERVER\_STORE\_FAIL

**Explanation** A failure in the mounting of the permanent storage file occurred.

**Recommended Action** Contact the Cisco TAC.

## 716528

**Error Message** %ASA-1-716528: Unexpected fiber scheduler error; possible out-of-memory condition

**Explanation** The Secure Firewall ASA has experienced an unexpected error and has recovered.

**Recommended Action** Check for high CPU usage or CPU hogs, and potential memory leaks. If the problem persists, contact the Cisco TAC.

## 716600

**Error Message** %ASA-3-716600: Rejected *size-recv* KB Hostscan data from IP *src-ip* . Hostscan results exceed *default* | *configured* limit of *size-conf* KB.

**Explanation** When the size of the received Hostscan data exceeds the limit configured on the Secure Firewall ASA, the data is discarded.

- *size-recv* —Size of received Hostscan data in kilobytes
- *src-ip* —Source IP address
- *default* | *configured* —Keyword specifying whether the value of the Hostscan data limit is the default or configured by the administrator
- *size-conf* —Configured upper limit on the size of the Hostscan data that the Secure Firewall ASA accepts from clients

**Recommended Action** Contact Cisco TAC to increase the upper limit on the size of Hostscan data that the Secure Firewall ASA accepts from clients.

## 716601

**Error Message** %ASA-3-716601: Rejected *size-recv* KB Hostscan data from IP *src-ip* . System-wide limit on the amount of Hostscan data stored on FTD exceeds the limit of *data-max* KB.

**Explanation** When the amount of Hostscan data stored on the Secure Firewall ASA exceeds the limit, new Hostscan results are rejected.

- *size-recv* —Size of received Hostscan data in kilobytes
- *src-ip* —Source IP address
- *data-max* —Limit on the amount of Hostscan results to be stored by the Secure Firewall ASA in kilobytes

**Recommended Action** Contact Cisco TAC to change the limit on stored Hostscan data.

## 716602

**Error Message** %ASA-3-716602: Memory allocation error. Rejected *size-recv* KB Hostscan data from IP *src-ip* .

**Explanation** An error occurred while memory was being allocated for Hostscan data.

- *size-recv* —Size of received Hostscan data in kilobytes
- *src-ip* —Source IP address

**Recommended Action** Set the Hostscan limit to the default value if it is configured. If the problem persists, contact Cisco TAC.

## 716603

**Error Message** %ASA-7-716603: Received *size-recv* KB Hostscan data from IP *src-ip* .

**Explanation** The Hostscan data of a specified size was successfully received.

- *size-recv* —Size of received Hostscan data in kilobytes
- *src-ip* —Source IP address

**Recommended Action** None required.

## Messages 717001 to 717064

This section includes messages from 717001 to 717064.

### 717001

**Error Message** %ASA-3-717001: Querying keypair failed.

**Explanation** A required keypair was not found during an enrollment request.

**Recommended Action** Verify that a valid keypair exists in the trustpoint configuration, then resubmit the enrollment request.

### 717002

**Error Message** %ASA-3-717002: Certificate enrollment failed for trustpoint *trustpoint\_name*. Reason: *reason\_string* .

**Explanation** An enrollment request for this trustpoint has failed.

- *trustpoint name* —Trustpoint name that the enrollment request was for
- *reason\_string* —The reason the enrollment request failed

**Recommended Action** Check the CA server for the failure reason.

### 717003

**Error Message** %ASA-6-717003: Certificate received from Certificate Authority for trustpoint *trustpoint\_name* .

**Explanation** A certificate was successfully received from the CA for this trustpoint.

- *trustpoint\_name* —Trustpoint name

**Recommended Action** None required

### 717004

**Error Message** %ASA-6-717004: PKCS #12 export failed for trustpoint *trustpoint\_name* .

**Explanation** The trustpoint failed to export, because of one of the following: only a CA certificate exists, and an identity certificate does not exist for the trustpoint, or a required keypair is missing.

- *trustpoint\_name* —Trustpoint name

**Recommended Action** Make sure that required certificates and keypairs are present for the given trustpoint.

## 717005

**Error Message** %ASA-6-717005: PKCS #12 export succeeded for trustpoint *trustpoint\_name* .

**Explanation** The trustpoint was successfully exported.

- *trustpoint\_name* —Trustpoint name

**Recommended Action** None required

## 717006

**Error Message** %ASA-6-717006: PKCS #12 import failed for trustpoint *trustpoint\_name* .

**Explanation** Import of the requested trustpoint failed to be processed.

- *trustpoint\_name* —Trustpoint name

**Recommended Action** Verify the integrity of the imported data. Then make sure that the entire pkcs12 record is correctly pasted, and reimport the data.

## 717007

**Error Message** %ASA-6-717007: PKCS #12 import succeeded for trustpoint *trustpoint\_name* .

**Explanation** Import of the requested trustpoint was successfully completed.

- *trustpoint\_name* —Trustpoint name

**Recommended Action** None required.

## 717008

**Error Message** %ASA-2-717008: Insufficient memory to *process\_requiring\_memory*.

**Explanation** An internal error occurred while attempting to allocate memory for the process that requires memory. Other processes may experience problems allocating memory and prevent further processing.

- **process\_requiring\_memory**—The specified process that requires memoryr

**Recommended Action** Collect memory statistics and logs for further debugging and reload the Secure Firewall ASA.

## 717009

**Error Message** %ASA-3-717009: Certificate validation failed. Reason: *reason\_string* .

**Explanation** A certificate validation failed, which might be caused by a validation attempt of a revoked certificate, invalid certificate attributes, or configuration issues.

- *reason\_string* —The reason that the certificate validation failed

**Recommended Action** Make sure the configuration has a valid trustpoint configured for validation if the reason indicates that no suitable trustpoints were found. Check the Secure Firewall ASA time to ensure that it is accurate relative to the certificate authority time. Check the reason for the failure and correct any issues

that are indicated. If certificate validation fails due to the CA key size being too small or a weak crypto being used, you can use the **crypto ca permit-weak-crypto** command to override these restrictions.

## 717010

**Error Message** %ASA-3-717010: CRL polling failed for trustpoint *trustpoint\_name* .

**Explanation** .CRL polling has failed and may cause connections to be denied if CRL checking is required.

- **trustpoint\_name**—The name of the trustpoint that requested the CRL

**Recommended Action** Verify that connectivity exists with the configured CRL distribution point and make sure that manual CRL retrieval also functions correctly.

## 717011

**Error Message** %ASA-2-717011: Unexpected event *event event\_ID*

**Explanation** An event that is not expected under normal conditions has occurred.

**Recommended Action** If the problem persists, contact the Cisco TAC.

## 717012

**Error Message** %ASA-3-717012: Failed to refresh CRL cache entry from the server for trustpoint *trustpoint\_name* at *time\_of\_failure*

**Explanation** An attempt to refresh a cached CRL entry has failed for the specified trustpoint at the indicated time of failure. This may result in obsolete CRLs on the Secure Firewall ASA, which may cause connections that require a valid CRL to be denied.

- **trustpoint\_name**—The name of the trustpoint
- **time\_of\_failure** —The time of failure

**Recommended Action** Check connectivity issues to the server, such as a downed network or server. Try to retrieve the CRL manually using the **crypto ca crl retrieve** command.

## 717013

**Error Message** %ASA-5-717013: Removing a cached CRL to accommodate an incoming CRL. Issuer: *issuer*

**Explanation** When the device is configured to authenticate IPsec tunnels using digital certificates, CRLs may be cached in memory to avoid requiring a CRL download during each connection. If the cache fills to the point where an incoming CRL cannot be accommodated, older CRLs will be removed until the required space is made available. This message is generated for each purged CRL.

- **issuer**—The name of the device that removes cached CRLs

**Recommended Action** None required.



## 717014

**Error Message** %ASA-5-717014: Unable to cache a CRL received from CDP due to size limitations (CRL size = *size* , available cache space = *space* )

**Explanation** When the device is configured to authenticate IPsec tunnels using digital certificates, CRLs may be cached in memory to avoid requiring a CRL download during each connection. This message is generated if a received CRL is too large to fit in the cache. Large CRLs are still supported even though they are not cached. This means that the CRL will be downloaded with each IPsec connection, which may affect performance during IPsec connection bursts.

**Recommended Action** None required.

## 717015

**Error Message** %ASA-3-717015: CRL received from *issuer* is too large to process (CRL size = *crl\_size* , maximum CRL size = *max\_crl\_size* )

**Explanation** An IPsec connection caused a CRL that is larger than the maximum permitted CRL size to be downloaded. This error condition causes the connection to fail. This message is rate limited to one message every 10 seconds.

**Recommended Action** Scalability is perhaps the most significant drawback to the CRL method of revocation checking. To solve this problem, the only options are to investigate a CA-based solution to reduce the CRL size or configure the Secure Firewall ASA not to require CRL validation.

## 717016

**Error Message** %ASA-6-717016: Removing expired CRL from the CRL cache. Issuer: *issuer*

**Explanation** When the Secure Firewall ASA is configured to authenticate IPsec tunnels using digital certificates, CRLs may be cached in memory to avoid requiring a CRL download during each connection. This message is generated when either the CA specified expiration time or the configured cache time has lapsed and the CRL is removed from the cache.

**Recommended Action** None required.

## 717017

**Error Message** %ASA-3-717017: Failed to query CA certificate for trustpoint *trustpoint\_name* from *enrollment\_url*

**Explanation** An error occurred when an attempt was made to authenticate a trustpoint by requesting a CA certificate from a certificate authority.

**Recommended Action** Make sure that an enrollment URL is configured with this trustpoint, ensure connectivity with the CA server, then retry the request.

## 717018

**Error Message** %ASA-3-717018: CRL received from *issuer* has too many entries to process (number of entries = *number\_of\_entries* , maximum number allowed = *max\_allowed* )

**Explanation** An IPsec connection caused a CRL that includes more revocation entries than can be supported to be downloaded. This is an error condition that will cause the connection to fail. This message is rate limited to one message every 10 seconds.

- **issuer**—The X.500 name of the CRLs issuer
- **number\_of\_entries**—The number of revocation entries in the received CRL
- **max\_allowed**—The maximum number of CRL entries that the Secure Firewall ASA supports

**Recommended Action** Scalability is perhaps the most significant drawback to the CRL method of revocation checking. The only options to solve this problem are to investigate a CA-based solution to reduce the CRL size or configure the Secure Firewall ASA not to require CRL validation.

## 717019

**Error Message** %ASA-3-717019: Failed to insert CRL for trustpoint *trustpoint\_name* . Reason: *failure\_reason* .

**Explanation** A CRL is retrieved, but found to be invalid and cannot be inserted into the cache because of the **failure\_reason**.

- **trustpoint\_name**—The name of the trustpoint that requested the CRL
- **failure\_reason**—The reason that the CRL failed to be inserted into cache

**Recommended Action** Make sure that the current Secure Firewall ASA time is correct relative to the CA time. If the NextUpdate field is missing, configure the trustpoint to ignore the NextUpdate field.

## 717020

**Error Message** %ASA-3-717020: Failed to install device certificate for trustpoint *label* . Reason: *reason\_string* .

**Explanation** A failure occurred while trying to enroll or import an enrolled certificate into a trustpoint.

- **label** —Label of the trustpoint that failed to install the enrolled Secure Firewall ASA certificate
- **reason\_string** —The reason that the certificate cannot be verified

**Recommended Action** Use the failure reason to remedy the cause of failure and retry the enrollment. Common failures are due to invalid certificates being imported into the Secure Firewall ASA or a mismatch of the public key included in the enrolled certificate with the keypair referenced in the trustpoint.

## 717021

**Error Message** %ASA-3-717021: Certificate data could not be verified. Locate Reason: *reason\_string* serial number: *serial number* , subject name: *subject name* , key length *key length* bits.

**Explanation** An attempt to verify the certificate that is identified by the serial number and subject name was unsuccessful for the specified reason. When verifying certificate data using the signature, several errors can occur that should be logged, including invalid key types and unsupported key size.

- **reason\_string** —The reason that the certificate cannot be verified
- **serial number** —Serial number of the certificate that is being verified
- **subject name** —Subject name included in the certificate that is being verified
- **key length** —The number of bits in the key used to sign this certificate

**Recommended Action** Check the specified certificate to ensure that it is valid, that it includes a valid key type, and that it does not exceed the maximum supported key size.

## 717022

**Error Message** %ASA-6-717022: Certificate was successfully validated. *certificate\_identifiers*

**Explanation** The identified certificate was successfully validated.

- *certificate\_identifiers* —Information to identify the certificate that was validated successfully, which might include a reason, serial number, subject name, and additional information

**Recommended Action** None required.

## 717023

**Error Message** %ASA-3-717023: SSL failed to set device certificate for trustpoint *trustpoint name* . Reason: *reason\_string* .

**Explanation** A failure occurred while trying to set an Secure Firewall ASA certificate for the given trustpoint for authenticating the SSL connection.

- *trustpoint name* —Name of the trustpoint for which SSL failed to set an Secure Firewall ASA certificate
- *reason\_string* —Reason indicating why the Secure Firewall ASA certificate cannot be set

**Recommended Action** Resolve the issue indicated by the reason reported for the failure by doing the following:

- Make sure that the specified trustpoint is enrolled and has an Secure Firewall ASA certificate.
- Make sure the Secure Firewall ASA certificate is valid.
- Reenroll the trustpoint, if required.

## 717024

**Error Message** %ASA-7-717024: Checking CRL from trustpoint: *trustpoint name* for purpose

**Explanation** A CRL is being retrieved.

- *trustpoint name* —Name of the trustpoint for which the CRL is being retrieved
- *purpose* —Reason that the CRL is being retrieved

**Recommended Action** None required.

## 717025

**Error Message** %ASA-7-717025: Validating certificate chain containing *number of certs* certificate(s).

**Explanation** A certificate chain is being validated.

- *>number of certs*— Number of certificates in the chain

**Recommended Action** None required.

## 717026

**Error Message** %ASA-4-717026: Name lookup failed for hostname *hostname* during PKI operation.

**Explanation** The given hostname cannot be resolved while attempting a PKI operation.

- *>hostname* —The hostname that failed to resolve

**Recommended Action** Check the configuration and the DNS server entries for the given hostname to make sure that it can be resolved. Then retry the operation.

## 717027

**Error Message** %ASA-3-717027: Certificate chain failed validation. *reason\_string* .

**Explanation** A certificate chain cannot be validated.

- *reason\_string*—Reason for the failure to validate the certificate chain. The reasons could be non reachability of a CA server, trustpoint not being available, the validity period for the certificate identity has elapsed, or when the certificate is revoked.

**Recommended Action** Resolve the issue noted by the reason and retry the validation attempt by performing any of the following actions:

- Make sure that connectivity to a CA is available if CRL checking is required.
- Make sure that a trustpoint is authenticated and available for validation.
- Make sure that the identity certificate within the chain is valid based on the validity dates.
- Make sure that the certificate is not revoked.

## 717028

**Error Message** %ASA-6-717028: Certificate chain was successfully validated *additional info* .

**Explanation** A certificate chain was successfully validated.

- *>additional info* —More information for how the certificate chain was validated (for example, “with warning” indicates that a CRL check was not performed)

**Recommended Action** None required.

## 717029

**Error Message** %ASA-7-717029: Identified client certificate within certificate chain. serial number: *serial\_number* , subject name: *subject\_name* .

**Explanation** The certificate specified as the client certificate is identified.

- **serial\_number**—Serial number of the certificate that is identified as the client certificate
- **subject\_name**—Subject name included in the certificate that is identified as the client certificate

**Recommended Action** None required.

## 717030

**Error Message** %ASA-7-717030: Found a suitable trustpoint *trustpoint name* to validate certificate.

**Explanation** A suitable or usable trustpoint is found that can be used to validate the certificate.

- *trustpoint name* —Trustpoint that will be used to validate the certificate

**Recommended Action** None required.

## 717031

**Error Message** %ASA-4-717031: Failed to find a suitable trustpoint for the issuer: *issuer*  
Reason: *reason\_string*

**Explanation** A usable trustpoint cannot be found. During certificate validation, a suitable trustpoint must be available in order to validate a certificate.

- *>issuer* —Issuer of the certificate that was being validated
- *reason\_string* —The reason that a suitable trustpoint cannot be found

**Recommended Action** Resolve the issue indicated in the reason by checking the configuration to make sure that a trustpoint is configured, authenticated, and enrolled. Also make sure that the configuration allows for specific types of certificates, such as identity certificates.

## 717032

**Error Message** %ASA-3-717032: OCSP status check failed. Reason: *reason\_string*

**Explanation** When the OCSP status check fails, this message is generated with the reason for the failure. The following list mentions the failure reasons:

- HTTP transaction failed for OCSP request.
- Invalid OCSP Response Status - unauthorized.
- Failed OCSP response processing.
- Failed to query an OCSP response from the server
- Failed to parse HTTP OCSP response from the server
- Invalid revocation status, server returned status: unknown
- Invalid OCSP response type
- Nonce missing in OCSP response
- NONCE mismatch
- Failed to verify OCSP response
- Validity period of OCSP response invalid
- Certificate is revoked

- CRL check for OCSP responder cert failed

**Recommended Action** None.

## 717033

**Error Message** %ASA-6-717033: OCSP response status - Successful.

**Explanation** An OCSP status check response was received successfully.

**Recommended Action** None required.

## 717034

**Error Message** %ASA-7-717034: No-check extension found in certificate. OCSP check bypassed.

**Explanation** An OCSP responder certificate was received that includes an “id-pkix-ocsp-nocheck” extension, which allows this certificate to be validated without an OCSP status check.

**Recommended Action** None required.

## 717035

**Error Message** %ASA-4-717035: OCSP status is being checked for certificate.  
*certificate\_identifier*.

**Explanation** The certificate for which an OCSP status check occurs is identified.

- *certificate\_identifier* —Information that identifies the certificate being processed by the certificate map rules

**Recommended Action** None required.

## 717036

**Error Message** %ASA-7-717036: Looking for a tunnel group match based on certificate maps for peer certificate with *certificate\_identifier* .

**Explanation** The peer certificate identified by the certificate identifier is being processed through the configured certificate maps to attempt a possible tunnel group match.

- *certificate\_identifier* —Information that identifies the certificate being processed by the certificate map rules

**Recommended Action** None required.

## 717037

**Error Message** %ASA-4-717037: Tunnel group search using certificate maps failed for peer certificate: *certificate\_identifier* .

**Explanation** The peer certificate identified by the certificate identifier was processed through the configured certificate maps to attempt a possible tunnel group match, but no match can be found.

- *certificate\_identifier*—Information that identifies the certificate being processed by the certificate map rules

**Recommended Action** Make sure that the warning is expected based on the received peer certificate and the configured crypto CA certificate map rules.

## 717038

**Error Message** %ASA-7-717038: Tunnel group match found. Tunnel Group: *tunnel\_group\_name* , Peer certificate: *certificate\_identifier* .

**Explanation** The peer certificate identified by the certificate identifier was processed by the configured certificate maps, and a match was found to the tunnel group.

- *certificate\_identifier*—Information that identifies the certificate being processed by the certificate map rules
- *tunnel\_group\_name*—The name of the tunnel group matched by the certificate map rules

**Recommended Action** None required.

## 717039

**Error Message** %ASA-3-717039: Local CA Server internal error detected: *error*.

**Explanation** An internal processing error has occurred with the local CA server.

- *error*—Error string

**Recommended Action** Based on the error, take the necessary steps to resolve the issue. Currently, the possible errors include:

- CA key does not exist—Make sure that the CA key is present, or restore the key from a backup, if necessary.
- Failed to rollover expired CA certificate—Make sure that the clock is correct and that the CA certificate is expired, then restart the CA server to try to reissue the certificate.
- Failed to generate self-signed certificate for Local CA Server certificate rollover upon expiration—Make sure that the clock is correct and that the CA certificate is about to expire, then restart the CA server to try to reissue the certificate.
- Failed to configure Local CA Server—Turn on debugging and try to configure the CA server again to determine the cause of the failure.
- Invalid issuer name configured—Change the issuer name DN to a valid DN string.

## 717040

**Error Message** %ASA-2-717040: Local CA Server has failed and is being disabled. Reason: *reason*.

**Explanation** The local CA server is being disabled because of an error.

- *reason*—Reason string

Currently, the possible errors include:

- Storage down—Make sure that storage is accessible, and reenablen the CA server by using the **no shut** command.

**Recommended Action** Based on the reason, take the necessary steps to resolve the issue.

## 717041

**Error Message** %ASA-7-717041: Local CA Server event: *event info* .

**Explanation** Event details that have occurred on the CA server are reported to allow you to track or debug the CA server health, including when the CA server is created, enabled, or disabled, or when the CA server certificate is rolled over.

- *event info* —Details of the event that occurred

**Recommended Action** None required.

## 717042

**Error Message** %ASA-3-717042: Failed to enable Local CA Server.Reason: *reason* .

**Explanation** Errors occurred when an attempt was made to enable the local CA server.

- *reason* —Reason that the local CA server failed to enable

**Recommended Action** Resolve the issue encountered that is reported in the reason string. Currently, the possible reasons include:

- Failed to create server trustpoint
- Failed to create server keypair
- Time has not been set
- Failed to init storage
- Storage not accessible
- Failed to validate self-signed CA certificate
- Failed to generate self-signed CA certificate
- CA certificate has expired
- Failed to generate CRL
- Failed to archive CA key and certificate
- Failed to generate empty user or certificate database file
- Failed to load user or certificate database file

## 717043

**Error Message** %ASA-6-717043: Local CA Server certificate enrollment related info for user: *user* . Info: *info* .

**Explanation** Enrollment-related activities for a user are being monitored. The username and specific enrollment information are reported so that enrollments, e-mail invitation generation, and renewal reminder generation can be monitored.

- *user* —Username about whom the enrollment information log is being generated
- *info* —Enrollment information string

**Recommended Action** None required.



## 717044

**Error Message** %ASA-3-717044: Local CA server certificate enrollment related error for user: *user* . Error: *error* .

**Explanation** Errors that occur in the processing of certificate enrollment are reported, which may include errors in notifying users via e-mail for renewal reminders, errors during issuance of a certificate to complete enrollment, invalid username or OTP, and expired enrollment attempts.

- *user* —Username for whom the enrollment error log is being generated
- *error* —Enrollment error

**Recommended Action** If the error does not provide enough information to diagnose and resolve the issue, turn on debugging and try enrollment again.

## 717045

**Error Message** %ASA-7-717045:Local CA Server CRL info: *info*

**Explanation** The CRL file is monitored when it is generated and regenerated.

- *info* —Informational string of the CRL event

**Recommended Action** None required.

## 717046

**Error Message** %ASA-3-717046: Local CA Server CRL error: *error* .

**Explanation** Errors that are encountered while trying to generate and reissue the local CA server CRL file are reported.

- *error* —Error string

**Recommended Action** Take appropriate action to resolve the reported issue, which may include verifying that storage is accessible, and that the CRL file is valid in storage and signed by the existing local CA server.

## 717047

**Error Message** %ASA-6-717047: Revoked certificate issued to user: *username*, with serial number *serial number* .

**Explanation** Any certificates issued by the local CA server that have been revoked are being monitored.

- *username* —Username of the owner of the certificate that is being revoked
- *serial number* —Serial number of the certificate that has been revoked

**Recommended Action** None required.

## 717048

**Error Message** %ASA-6-717048: Unrevoked certificate issued to user: *username*, with serial number *serial number* .

**Explanation** Any certificates that were issued by the local CA server that were previously revoked, and that are now being unrevoked and removed from the CRL are being monitored.

- *username* —Username of the owner of the certificate that is being unrevoked
- *serial number* —Serial number of the certificate that has been unrevoked

**Recommended Action** None required.

## 717049

**Error Message** %ASA-1-717049: Local CA Server certificate is due to expire in *number* days and a replacement certificate is available for export.

**Explanation** The administrator is alerted to an upcoming CA certificate expiration so that the administrator can take action to export the replacement certificate to all ASAs that will require the new certificate.

- *number* —The number of days before the local CA server certificate expires

**Recommended Action** To avoid certificate validation failures on any ASAs that require the local CA server certificate, action should be taken before the actual expiration of the current local CA server certificate, which is indicated by the *number* value. Note that the local CA server does not require any action because the CA certificate will be replaced automatically. Use the **show crypto ca server certificate** command to view the replacement or rollover local CA server certificate and copy it for import into any ASA that will require the new certificate.

## 717050

**Error Message** %ASA-5-717050: SCEP Proxy: Processed request type *type* from IP *client ip address* , User *username* , TunnelGroup *tunnel\_group name* , GroupPolicy *group-policy name* to CA IP *ca ip address*

**Explanation** The SCEP proxy received a message and relayed it to the CA. The response from the CA is relayed back to the client.

- *type* —The request type string that is received by the SCEP proxy, which can be one of the following SCEP message types: PKIOperation, GetCACaps, GetCACert, GetNextCACert, and GetCACertChain.
- *client ip address* —The source IP address of the request received
- *username* —The username that is associated with the VPN session in which the SCEP request is received
- *tunnel-group name* —The tunnel group that is associated with the VPN session in which the SCEP request is received
- *group-policy name* —The group policy that is associated with the VPN session in which the SCEP request is received
- *ca ip address* —The IP address of the CA that is configured in the group policy

**Recommended Action** None required.

## 717051

**Error Message** %ASA-3-717051: SCEP Proxy: Denied processing the request type *type* received from IP *client ip address* , User *username* , TunnelGroup *tunnel group name* , GroupPolicy *group policy name* to CA *ca ip address* . Reason: *msg*

**Explanation** The SCEP proxy denied processing of the request, which may be caused by a misconfiguration, an error condition in the proxy, or an invalid request.

- *type* —The request type string that is received by the SCEP proxy, which can be one of the following SCEP message types: PKIOperation, GetCACaps, GetCACert, GetNextCACert, and GetCACertChain.
- *client ip address* —The source IP address of the request received
- *username* —The username that is associated with the VPN session in which the SCEP request is received
- *tunnel-group name* —The tunnel group that is associated with the VPN session in which the SCEP request is received
- *group-policy name* —The group policy that is associated with the VPN session in which the SCEP request is received
- *ca ip address* —The IP address of the CA that is configured in the group policy
- *msg*—The reason string that explains the reason or error for why the request processing is denied

**Recommended Action** Identify the cause from the reason printed. If the reason indicates that the request is invalid, check the CA URL configuration. Otherwise, confirm that the tunnel group is enabled for SCEP enrollment and debug further by using the **debug crypto ca scep-proxy** command.

## 717052

**Error Message** %ASA-4-717052: Group *group name* User *user name* IP *IP Address* Session disconnected due to periodic certificate authentication failure. Subject Name *id subject name* Issuer Name *id issuer name* Serial Number *id serial number*

**Explanation** Periodic certificate authentication failed, and the session was disconnected.

- *group name* —The name of the group policy to which the session belongs
- *user name* —The username of the session
- *IP* —The public IP address of the session
- *id subject name* —The subject name in the ID certificate of the session
- *id issuer name* —The issuer name in the ID certificate of the session
- *id serial number* —The serial number in the ID certificate of the session

**Recommended Action** None required.

## 717053

SSP-whole topic

**Error Message** %ASA-5-717053: Group *group name* User *user name* IP *IP Address* Periodic certificate authentication succeeded. Subject Name *id subject name* Issuer Name *id issuer name* Serial Number *id serial number*

**Explanation** Periodic certificate authentication succeeded.

- *group name* —The name of the group policy to which the session belongs
- *user name* —The username of the session
- *id subject name* —The subject name in the ID certificate of the session
- *id issuer name* —The issuer name in the ID certificate of the session
- *id serial number* —The serial number in the ID certificate of the session

**Recommended Action** None required.

## 717054

SSP-whole topic

**Error Message** %ASA-1-717054: The *type* certificate in the trustpoint *tp name* is due to expire in *number* days. Expiration *date and time* Subject Name *subject name* Issuer Name *issuer name* Serial Number *serial number*

**Explanation** The specified certificate in the trustpoint is about to expire.

- *type* —The type of certificate: CA or ID
- *tp name* —The name of the trustpoint to which the certificate belongs
- *number* —The number of days until expiration
- *date and time* : The expiration date and time
- *subject name* —The subject name in the certificate
- *issuer name* —The issuer name in the certificate
- *serial number* —The serial number in the certificate

**Recommended Action** Renew the certificate.

## 717055

**Error Message** %ASA-1-717055: The *type* certificate in the trustpoint *tp name* has expired. Expiration *date and time* Subject Name *subject name* Issuer Name *issuer name* Serial Number *serial number*

**Explanation** The specified certificate in the trustpoint has expired.

- *type* —The type of certificate: CA or ID
- *tp name* —The name of the trustpoint to which the certificate belongs
- *date and time* : The expiration date and time
- *subject name* —The subject name in the certificate
- *issuer name* —The issuer name in the certificate
- *serial number* —The serial number in the certificate

**Recommended Action** Renew the certificate.

## 717056

Only heading title SSP

**Error Message** %ASA-6-717056: Attempting *type* revocation check from *Src Interface* :*Src IP* /*Src Port* to *Dst IP* /*Dst Port* using *protocol*

**Explanation** The CA was attempting to download a CRL or send an OCSP revocation check request.

- *type* —Type of revocation check, which can be OCSP or CRL
- *Src Interface* —Name of the interface from which the revocation checking is being done
- *Src IP* —IP address from which the revocation checking is being done
- *Src Port* —Port number from which the revocation checking is being done
- *Dst IP* —IP address of the server to which the revocation checking request is being sent
- *Dst Port* —Port number of the server to which the revocation checking request is being sent
- *Protocol* —Protocol being used for revocation checking, which can be HTTP, LDAP, or SCEP

**Recommended Action** None required.

## 717057

**Error Message** %ASA-3-717057: Automatic import of trustpool certificate bundle has failed. <Maximum retry attempts reached. Failed to reach CA server> | <Cisco root bundle signature validation failed> | <Failed to update trustpool bundle in flash> | <Failed to install trustpool bundle in memory>

**Explanation** This syslog is generated with one of these error messages. This syslog is meant to update the user with results of the auto import operation and steer them towards the right debug messages especially in cases of failure. Details of each error are present in the debug output.

**Recommended Action** Verify CA accessibility and make space on flash CA root certificate.

## 717058

**Error Message** %ASA-6-717058: Automatic import of trustpool certificate bundle is successful: <No change in trustpool bundle> | <Trustpool updated in flash>.

**Explanation** This syslog is generated with one of these success messages. This syslog is meant to update the user with results of the auto import operation and steer them towards the right debug messages, especially in cases of failure. Details of each error are present in the debug output.

**Recommended Action** None.

## 717059

**Error Message** %ASA-6-717059: Peer certificate with serial number: <serial>, subject: <subject\_name>, issuer: <issuer\_name> matched the configured certificate map <map\_name>

**Explanation** This log is generated when an ASDM connection is authenticated via certificates and allowed based on the configured certificate map rules.

**Recommended Action** None required.

## 717060

**Error Message** %ASA-3-717060: Peer certificate with serial number: <serial>, subject: <subject\_name>, issuer: <issuer\_name> failed to match the configured certificate map <map\_name>

**Explanation** This log is generated when an ASDM connection is authenticated via certificates and not allowed based on the configured certificate map rules.

**Recommended Action** If the peer certificate referenced in the log is supposed to be allowed, check certificate map configuration for the referenced map\_name and correct the map to allow the connection as needed.

## 717061

SSP-only heading title

**Error Message** %ASA-5-717061: Starting *protocol certificate enrollment for the trustpoint tpname* with the CA *ca\_name*. Request Type *type* Mode *mode*

**Explanation** A CMP enrollment request has been triggered.

- *tpname* —Name of the trustpoint being enrolled
- *ca* —CA hostname or IP address as provided in the CMP configuration
- *type* —CMP request type: Initialization Request, Certification Request, and Key Update Request
- *mode* —Enrollment trigger: Manual or Automatic
- *protocol* —Enrollment protocol: CMP

**Recommended Action** None required.

## 717062

**Error Message** %ASA-5-717062: *protocol Certificate enrollment succeeded for the trustpoint tpname* with the CA *ca*. Received a new certificate with Subject Name *subject* Issuer Name *issuer* Serial Number *serial*

**Explanation** CMP enrollment request succeeded. New certificate received.

- *tpname* —Name of the trustpoint being enrolled
- *ca* —CA hostname or IP address as provided in the CMP configuration
- *subject* —Subject Name from the received certificate
- *issuer* —Issuer Name from the received certificate
- *serial*—Serial Number from the received certificate
- *protocol* —Enrollment protocol: CMP

**Recommended Action** None required.

## 717063

SSP Only heading title

**Error Message** %ASA-3-717063: *protocol Certificate enrollment failed for the trustpoint tpname* with the CA *ca*

**Explanation** CMP enrollment request failed.

- *tpname* —Name of the trustpoint being enrolled
- *ca* —CA hostname or IP address as provided in the CMP configuration
- *protocol* —Enrollment protocol: CMP

**Recommended Action** Use the CMP debug traces to fix the enrollment failure.

## 717064

SSP - only heading

**Error Message** %ASA-5-717064: *Keypair keyname in the trustpoint tpname* is regenerated for *mode protocol certificate renewal*

**Explanation** The keypair in the trustpoint is regenerated for certificate enrollment using CMP.

- *tpname* —Name of the trustpoint being enrolled
- *keyname* —Name of the keypair in the trustpoint
- *mode*—Enrollment trigger: Manual or Automatic
- *protocol* —Enrollment protocol: CMP

**Recommended Action** None required.

## Messages 718001 to 719026

This section includes messages from 718001 to 719026.

### 718001

**Error Message** %ASA-7-718001: Internal interprocess communication queue send failure: code *error\_code*

**Explanation** An internal software error has occurred while attempting to enqueue a message on the VPN load balancing queue.

**Recommended Action** This is generally a benign condition. If the problem persists, contact the Cisco TAC.

### 718002

**Error Message** %ASA-5-718002: Create peer *IP\_address* failure, already at maximum of *number\_of\_peers*

**Explanation** The maximum number of load-balancing peers has been exceeded. The new peer is ignored.

**Recommended Action** Check your load balancing and network configuration to ensure that the number of load-balancing peers does not exceed the maximum allowed.

### 718003

**Error Message** %ASA-6-718003: Got unknown peer message *message\_number* from *IP\_address* , local version *version\_number* , remote version *version\_number*

**Explanation** An unrecognized load-balancing message was received from one of the load-balancing peers. This may indicate a version mismatch between peers, but is most likely caused by an internal software error.

**Recommended Action** Verify that all load-balancing peers are compatible. If they are and this condition persists or is linked to undesirable behavior, contact the Cisco TAC.

### 718004

**Error Message** %ASA-6-718004: Got unknown internal message *message\_number*

**Explanation** An internal software error occurred.

**Recommended Action** This is generally a benign condition. If the problem persists, contact the Cisco TAC.

## 718005

**Error Message** %ASA-5-718005: Fail to send to *IP\_address* , port *port*

**Explanation** An internal software error occurred during packet transmission on the load-balancing socket. This might indicate a network problem.

**Recommended Action** Check the network-based configuration on the Secure Firewall ASA and verify that interfaces are active and protocol data is flowing through the Secure Firewall ASA. If the problem persists, contact the Cisco TAC.

## 718006

**Error Message** %ASA-5-718006: Invalid load balancing state transition [*cur=state\_number* ] [*event=event\_number* ]

**Explanation** A state machine error has occurred. This might indicate an internal software error.

**Recommended Action** This is generally a benign condition. If the problem persists, contact the Cisco TAC.

## 718007

**Error Message** %ASA-5-718007: Socket open failure [*failure\_code*]:*failure\_text*

**Explanation** An error occurred when the load-balancing socket tried to open. This might indicate a network problem or an internal software error.

**Recommended Action** Check the network-based configuration on the Secure Firewall ASA and verify that interfaces are active and protocol data is flowing through the Secure Firewall ASA. If the problem persists, contact the Cisco TAC.

## 718008

**Error Message** %ASA-5-718008: Socket bind failure [*failure\_code*]:*failure\_text*

**Explanation** An error occurred when the Secure Firewall ASA tried to bind to the load-balancing socket. This might indicate a network problem or an internal software error.

**Recommended Action** Check the network-based configuration on the Secure Firewall ASA and verify that interfaces are active and protocol data is flowing through the Secure Firewall ASA. If the problem persists, contact the Cisco TAC.

## 718009

**Error Message** %ASA-5-718009: Send HELLO response failure to *IP\_address*

**Explanation** An error occurred when the Secure Firewall ASA tried to send a hello response message to one of the load-balancing peers. This might indicate a network problem or an internal software error.

**Recommended Action** Check the network-based configuration on the Secure Firewall ASA and verify that interfaces are active and protocol data is flowing through the Secure Firewall ASA. If the problem persists, contact the Cisco TAC.



## 718010

**Error Message** %ASA-5-718010: Sent HELLO response to *IP\_address*

**Explanation** The Secure Firewall ASA transmitted a hello response message to a load-balancing peer.

**Recommended Action** None required.

## 718011

**Error Message** %ASA-5-718011: Send HELLO request failure to *IP\_address*

**Explanation** An error occurred when the Secure Firewall ASA tried to send a hello request message to one of the load-balancing peers. This may indicate a network problem or an internal software error.

**Recommended Action** Check the network-based configuration on the Secure Firewall ASA and verify that interfaces are active and protocol data is flowing through the Secure Firewall ASA. If the problem persists, contact the Cisco TAC.

## 718012

**Error Message** %ASA-5-718012: Sent HELLO request to *IP\_address*

**Explanation** The Secure Firewall ASA transmitted a hello request message to a load-balancing peer.

**Recommended Action** None required.

## 718013

**Error Message** %ASA-6-718013: Peer *IP\_address* is not answering HELLO

**Explanation** The load-balancing peer is not answering a hello request message.

**Recommended Action** Check the status of the load-balancing SSF peer and the network connections.

## 718014

**Error Message** %ASA-5-718014: Master peer *IP\_address* is not answering HELLO

**Explanation** The load balancing director peer is not answering the hello request message.

**Recommended Action** Check the status of the load balancing SSF director peer and the network connections.

## 718015

**Error Message** %ASA-5-718015: Received HELLO request from *IP\_address*

**Explanation** The Secure Firewall ASA received a hello request message from the load balancing peer.

**Recommended Action** None required.

## 718016

**Error Message** %ASA-5-718016: Received HELLO response from *IP\_address*

**Explanation** The Secure Firewall ASA received a Hello Response packet from a load balancing peer.

**Recommended Action** None required.

## 718017

**Error Message** %ASA-7-718017: Got timeout for unknown peer *IP\_address* msg type *message\_type*

**Explanation** The Secure Firewall ASA processed a timeout for an unknown peer. The message was ignored because the peer may have already been removed from the active list.

**Recommended Action** If the message persists or is linked to undesirable behavior, check the load balancing peers and verify that all are configured correctly.

## 718018

**Error Message** %ASA-7-718018: Send KEEPALIVE request failure to *IP\_address*

**Explanation** An error has occurred while attempting to send a Keepalive Request message to one of the load balancing peers. This t indicate a network problem or an internal software error.

**Recommended Action** Check the network-based configuration on the Secure Firewall ASA and verify that interfaces are active and protocol data is flowing through the Secure Firewall ASA. If the problem persists, contact the Cisco TAC.

## 718019

**Error Message** %ASA-7-718019: Sent KEEPALIVE request to *IP\_address*

**Explanation** The Secure Firewall ASA transmitted a Keepalive Request message to a load balancing peer.

**Recommended Action** None required.

## 718020

**Error Message** %ASA-7-718020: Send KEEPALIVE response failure to *IP\_address*

**Explanation** An error has occurred while attempting to send a Keepalive Response message to one of the load balancing peers. This may indicate a network problem or an internal software error.

**Recommended Action** Check the network-based configuration on the Secure Firewall ASA and verify that interfaces are active and protocol data is flowing through the Secure Firewall ASA. If the problem persists, contact the Cisco TAC.

## 718021

**Error Message** %ASA-7-718021: Sent KEEPALIVE response to *IP\_address*

**Explanation** The Secure Firewall ASA transmitted a Keepalive Response message to a load balancing peer.

**Recommended Action** None required.

## 718022

**Error Message** %ASA-7-718022: Received KEEPALIVE request from *IP\_address*

**Explanation** The Secure Firewall ASA received a Keepalive Request message from a load balancing peer.

**Recommended Action** None required.

## 718023

**Error Message** %ASA-7-718023: Received KEEPALIVE response from *IP\_address*

**Explanation** The Secure Firewall ASA received a Keepalive Response message from a load balancing peer.

**Recommended Action** None required.

## 718024

**Error Message** %ASA-5-718024: Send CFG UPDATE failure to *IP\_address*

**Explanation** An error has occurred while attempting to send a Configuration Update message to one of the load balancing peers. This might indicate a network problem or an internal software error.

**Recommended Action** Check the network-based configuration on the Secure Firewall ASA and verify that interfaces are active and protocol data is flowing through the Secure Firewall ASA. If the problem persists, contact the Cisco TAC.

## 718025

**Error Message** %ASA-7-718025: Sent CFG UPDATE to *IP\_address*

**Explanation** The Secure Firewall ASA transmitted a Configuration Update message to a load balancing peer.

**Recommended Action** None required.

## 718026

**Error Message** %ASA-7-718026: Received CFG UPDATE from *IP\_address*

**Explanation** The Secure Firewall ASA received a Configuration Update message from a load balancing peer.

**Recommended Action** None required.

## 718027

**Error Message** %ASA-6-718027: Received unexpected KEEPALIVE request from *IP\_address*

**Explanation** The Secure Firewall ASA received an unexpected Keepalive request message from a load balancing peer.

**Recommended Action** If the problem persists or is linked with undesirable behavior, verify that all load balancing peers are configured and discovered correctly.

## 718028

**Error Message** %ASA-5-718028: Send OOS indicator failure to *IP\_address*

**Explanation** An error has occurred while attempting to send an OOS indicator message to one of the load balancing peers. This might indicate a network problem or an internal software error.

**Recommended Action** Check the network-based configuration on the Secure Firewall ASA and verify that interfaces are active and protocol data is flowing through the Secure Firewall ASA. If the problem persists, contact the Cisco TAC.

## 718029

**Error Message** %ASA-7-718029: Sent OOS indicator to *IP\_address*

**Explanation** The Secure Firewall ASA transmitted an OOS indicator message to a load balancing peer.

**Recommended Action** None required.

## 718030

**Error Message** %ASA-6-718030: Received planned OOS from *IP\_address*

**Explanation** The Secure Firewall ASA received a planned OOS message from a load balancing peer.

**Recommended Action** None required.

## 718031

**Error Message** %ASA-5-718031: Received OOS obituary for *IP\_address*

**Explanation** The Secure Firewall ASA received an OOS obituary message from a load balancing peer.

**Recommended Action** None required.

## 718032

**Error Message** %ASA-5-718032: Received OOS indicator from *IP\_address*

**Explanation** The Secure Firewall ASA received an OOS indicator message from a load balancing peer.

**Recommended Action** None required.

## 718033

**Error Message** %ASA-5-718033: Send TOPOLOGY indicator failure to *IP\_address*

**Explanation** An error has occurred while attempting to send a Topology indicator message to one of the load balancing peers. This might indicate a network problem or an internal software error.

**Recommended Action** Check the network-based configuration on the Secure Firewall ASA. Verify that interfaces are active, and protocol data is flowing through the Secure Firewall ASA. If the problem persists, contact the Cisco TAC.

## 718034

**Error Message** %ASA-7-718034: Sent TOPOLOGY indicator to *IP\_address*

**Explanation** The Secure Firewall ASA sent a Topology indicator message to a load balancing peer.

**Recommended Action** None required.

## 718035

**Error Message** %ASA-7-718035: Received TOPOLOGY indicator from *IP\_address*

**Explanation** The Secure Firewall ASA received a Topology indicator message from a load balancing peer.

**Recommended Action** None required.

## 718036

**Error Message** %ASA-7-718036: Process timeout for req-type *type\_value* , exid *exchange\_ID* , peer *IP\_address*

**Explanation** The Secure Firewall ASA processed a peer timeout.

**Recommended Action** Verify that the peer should have been timed out. If not, check the load balancing peer configuration and the network connection between the peer and the Secure Firewall ASA.

## 718037

**Error Message** %ASA-6-718037: Master processed *number\_of\_timeouts* timeouts

**Explanation** The Secure Firewall ASA in the director role processed the specified number of peer timeouts.

**Recommended Action** Verify that the timeouts are legitimate. If not, check the peer load balancing configuration and the network connection between the peer and the Secure Firewall ASA.

## 718038

**Error Message** %ASA-6-718038: Slave processed *number\_of\_timeouts* timeouts

**Explanation** The Secure Firewall ASA in the member role processed the specified number of peer timeouts.

**Recommended Action** Verify that the timeouts are legitimate. If not, check the peer load balancing configuration and the network connection between the peer and the Secure Firewall ASA.

## 718039

**Error Message** %ASA-6-718039: Process dead peer *IP\_address*

**Explanation** The Secure Firewall ASA has detected a dead peer.

**Recommended Action** Verify that the dead peer detection is legitimate. If not, check the peer load balancing configuration and the network connection between the peer and the Secure Firewall ASA.

## 718040

**Error Message** %ASA-6-718040: Timed-out exchange ID *exchange\_ID* not found

**Explanation** The Secure Firewall ASA has detected a dead peer, but the exchange ID is not recognized.

**Recommended Action** None required.

## 718041

**Error Message** %ASA-7-718041: Timeout [msgType=*type* ] processed with no callback

**Explanation** The Secure Firewall ASA has detected a dead peer, but a call back was not used in the processing.

**Recommended Action** None required.

## 718042

**Error Message** %ASA-5-718042: Unable to ARP for *IP\_address*

**Explanation** The Secure Firewall ASA experienced an ARP failure when attempting to contact a peer.

**Recommended Action** Verify that the network is operational and that all peers can communicate with each other.

## 718043

**Error Message** %ASA-5-718043: Updating/removing duplicate peer entry *IP\_address*

**Explanation** The Secure Firewall ASA found and is removing a duplicate peer entry.

**Recommended Action** None required.

## 718044

**Error Message** %ASA-5-718044: Deleted peer *IP\_address*

**Explanation** The Secure Firewall ASA is deleting a load balancing peer.

**Recommended Action** None required.

## 718045

**Error Message** %ASA-5-718045: Created peer *IP\_address*

**Explanation** The Secure Firewall ASA has detected a load balancing peer.

**Recommended Action** None required.

## 718046

**Error Message** %ASA-7-718046: Create group policy *policy\_name*

**Explanation** The Secure Firewall ASA has created a group policy to securely communicate with the load balancing peers.

**Recommended Action** None required.

## 718047

**Error Message** %ASA-7-718047: Fail to create group policy *policy\_name*

**Explanation** The Secure Firewall ASA experienced a failure when attempting to create a group policy for securing the communication between load balancing peers.

**Recommended Action** Verify that the load balancing configuration is correct.

## 718048

**Error Message** %ASA-5-718048: Create of secure tunnel failure for peer *IP\_address*

**Explanation** The Secure Firewall ASA experienced a failure when attempting to establish an IPsec tunnel to a load balancing peer.

**Recommended Action** Verify that the load balancing configuration is correct and that the network is operational.

## 718049

**Error Message** %ASA-7-718049: Created secure tunnel to peer *IP\_address*

**Explanation** The Secure Firewall ASA successfully established an IPsec tunnel to a load balancing peer.

**Recommended Action** None required.

## 718050

**Error Message** %ASA-5-718050: Delete of secure tunnel failure for peer *IP\_address*

**Explanation** The Secure Firewall ASA experienced a failure when attempting to terminate an IPsec tunnel to a load balancing peer.

**Recommended Action** Verify that the load balancing configuration is correct and that the network is operational.

## 718051

**Error Message** %ASA-6-718051: Deleted secure tunnel to peer *IP\_address*

**Explanation** The Secure Firewall ASA successfully terminated an IPsec tunnel to a load balancing peer.

**Recommended Action** None required.

## 718052

**Error Message** %ASA-5-718052: Received GRAT-ARP from duplicate master *MAC\_address*

**Explanation** The Secure Firewall ASA received a gratuitous ARP from a duplicate director.

**Recommended Action** Check the load balancing configuration and verify that the network is operational.

## 718053

**Error Message** %ASA-5-718053: Detected duplicate master, mastership stolen *MAC\_address*

**Explanation** The Secure Firewall ASA detected a duplicate director and a stolen director.

**Recommended Action** Check the load balancing configuration and verify that the network is operational.

## 718054

**Error Message** %ASA-5-718054: Detected duplicate master *MAC\_address* and going to SLAVE

**Explanation** The Secure Firewall ASA detected a duplicate director and is switching to member mode.

**Recommended Action** Check the load balancing configuration and verify that the network is operational.

## 718055

**Error Message** %ASA-5-718055: Detected duplicate master *MAC\_address* and staying MASTER

**Explanation** The Secure Firewall ASA detected a duplicate director and is staying in member mode.

**Recommended Action** Check the load balancing configuration and verify that the network is operational.

## 718056

**Error Message** %ASA-7-718056: Deleted Master peer, IP *IP\_address*

**Explanation** The Secure Firewall ASA deleted the load balancing director from its internal tables.

**Recommended Action** None required.

## 718057

**Error Message** %ASA-5-718057: Queue send failure from ISR, msg type *failure\_code*

**Explanation** An internal software error has occurred while attempting to enqueue a message on the VPN load balancing queue from an Interrupt Service Routing.

**Recommended Action** This is generally a benign condition. If the problem persists, contact the Cisco TAC.

## 718058

**Error Message** %ASA-7-718058: State machine return code: *action\_routine* , *return\_code*

**Explanation** The return codes of action routines belonging to the load balancing finite state machine are being traced.

**Recommended Action** None required.



## 718059

**Error Message** %ASA-7-718059: State machine function trace: state=*state\_name* , event=*event\_name* , func=*action\_routine*

**Explanation** The events and states of the load balancing finite state machine are being traced.

**Recommended Action** None required.

## 718060

**Error Message** %ASA-5-718060: Inbound socket select fail: context=*context\_ID* .

**Explanation** The socket select call returned an error and the socket cannot be read. This might indicate an internal software error.

**Recommended Action** If the problem persists, contact the Cisco TAC.

## 718061

**Error Message** %ASA-5-718061: Inbound socket read fail: context=*context\_ID* .

**Explanation** The socket read failed after data was detected through the select call. This might indicate an internal software error.

**Recommended Action** If the problem persists, contact the Cisco TAC.

## 718062

**Error Message** %ASA-5-718062: Inbound thread is awake (context=*context\_ID* ).

**Explanation** The load balancing process is awakened and begins processing.

**Recommended Action** None required.

## 718063

**Error Message** %ASA-5-718063: Interface *interface\_name* is down.

**Explanation** The load balancing process found the interface down.

**Recommended Action** Check the interface configuration to make sure that the interface is operational.

## 718064

**Error Message** %ASA-5-718064: Admin. interface *interface\_name* is down.

**Explanation** The load balancing process found the administrative interface down.

**Recommended Action** Check the administrative interface configuration to make sure that the interface is operational.

## 718065

**Error Message** %ASA-5-718065: Cannot continue to run (public=*up /down* , private=*up /down* , enable=*LB\_state* , master=*IP\_address* , session=*Enable /Disable* ).

**Explanation** The load balancing process can not run because all prerequisite conditions have not been met. The prerequisite conditions are two active interfaces and load balancing enabled.

**Recommended Action** Check the interface configuration to make sure at least two interfaces are operational and load balancing is enabled.

## 718066

**Error Message** %ASA-5-718066: Cannot add secondary address to interface *interface\_name* , ip *IP\_address* .

**Explanation** Load balancing requires a secondary address to be added to the outside interface. A failure occurred in adding that secondary address.

**Recommended Action** Check the address being used as the secondary address and make sure that it is valid and unique. Check the configuration of the outside interface.

## 718067

**Error Message** %ASA-5-718067: Cannot delete secondary address to interface *interface\_name* , ip *IP\_address* .

**Explanation** The deletion of the secondary address failed, which might indicate an addressing problem or an internal software error.

**Recommended Action** Check the addressing information of the outside interface and make sure that the secondary address is valid and unique. If the problem persists, contact the Cisco TAC.

## 718068

**Error Message** %ASA-5-718068: Start VPN Load Balancing in context *context\_ID* .

**Explanation** The load balancing process has been started and initialized.

**Recommended Action** None required.

## 718069

**Error Message** %ASA-5-718069: Stop VPN Load Balancing in context *context\_ID* .

**Explanation** The load balancing process has been stopped.

**Recommended Action** None required.

## 718070

**Error Message** %ASA-5-718070: Reset VPN Load Balancing in context *context\_ID* .

**Explanation** The LB process has been reset.

**Recommended Action** None required.

## 718071

**Error Message** %ASA-5-718071: Terminate VPN Load Balancing in context *context\_ID* .

**Explanation** The LB process has been terminated.

**Recommended Action** None required.

## 718072

**Error Message** %ASA-5-718072: Becoming master of Load Balancing in context *context\_ID* .

**Explanation** The Secure Firewall ASA has become the LB director.

**Recommended Action** None required.

## 718073

**Error Message** %ASA-5-718073: Becoming slave of Load Balancing in context *context\_ID* .

**Explanation** The Secure Firewall ASA has become the LB member.

**Recommended Action** None required.

## 718074

**Error Message** %ASA-5-718074: Fail to create access list for peer *context\_ID* .

**Explanation** ACLs are used to create secure tunnels over which the LB peers can communicate. The Secure Firewall ASA was unable to create one of these ACLs. This might indicate an addressing problem or an internal software problem.

**Recommended Action** Check the addressing information of the inside interface on all peers and ensure that all peers are discovered correctly. If the problem persists, contact the Cisco TAC.

## 718075

**Error Message** %ASA-5-718075: Peer *IP\_address* access list not set.

**Explanation** While removing a secure tunnel, the Secure Firewall ASA detected a peer entry that did not have an associated ACL.

**Recommended Action** None required.

## 718076

**Error Message** %ASA-5-718076: Fail to create tunnel group for peer *IP\_address* .

**Explanation** The Secure Firewall ASA experienced a failure when trying to create a tunnel group for securing the communication between load balancing peers.

**Recommended Action** Verify that the load balancing configuration is correct.

## 718077

**Error Message** %ASA-5-718077: Fail to delete tunnel group for peer *IP\_address* .

**Explanation** The Secure Firewall ASA experienced a failure when attempting to delete a tunnel group for securing the communication between load balancing peers.

**Recommended Action** None required.

## 718078

**Error Message** %ASA-5-718078: Fail to create crypto map for peer *IP\_address* .

**Explanation** The Secure Firewall ASA experienced a failure when attempting to create a crypto map for securing the communication between load balancing peers.

**Recommended Action** Verify that the load balancing configuration is correct.

## 718079

**Error Message** %ASA-5-718079: Fail to delete crypto map for peer *IP\_address* .

**Explanation** The Secure Firewall ASA experienced a failure when attempting to delete a crypto map for securing the communication between load balancing peers.

**Recommended Action** None required.

## 718080

**Error Message** %ASA-5-718080: Fail to create crypto policy for peer *IP\_address* .

**Explanation** The Secure Firewall ASA experienced a failure when attempting to create a transform set to be used in securing the communication between load balancing peers. This might indicate an internal software problem.

**Recommended Action** If the problem persists, contact the Cisco TAC.

## 718081

**Error Message** %ASA-5-718081: Fail to delete crypto policy for peer *IP\_address* .

**Explanation** The Secure Firewall ASA experienced a failure when attempting to delete a transform set used in securing the communication between load balancing peers.

**Recommended Action** None required.

## 718082

**Error Message** %ASA-5-718082: Fail to create crypto ipsec for peer *IP\_address* .

**Explanation** When cluster encryption for VPN load balancing is enabled, the VPN load balancing device creates a set of site-to-site tunnels for every other device in the load balancing cluster. For each tunnel, a set of crypto parameters (access list, crypto maps, and transform set) is created dynamically. One or more crypto parameters failed to be created or configured.

- **IP\_address**—The IP address of the remote peer

**Recommended Action** Examine the message for other entries specific to the type of crypto parameters that failed to be created.

## 718083

**Error Message** %ASA-5-718083: Fail to delete crypto ipsec for peer *IP\_address* .

**Explanation** When the local VPN load balancing device is removed from the cluster, crypto parameters are removed. One or more crypto parameters failed to be deleted.

- **IP\_address**—The IP address of the remote peer

**Recommended Action** Examine the message for other entries specific to the type of crypto parameters that failed to be deleted.

## 718084

**Error Message** %ASA-5-718084: Public/cluster IP not on the same subnet: public *IP\_address* , mask *netmask* , cluster *IP\_address*

**Explanation** The cluster IP address is not on the same network as the outside interface of the Secure Firewall ASA.

**Recommended Action** Make sure that both the cluster (or virtual) IP address and the outside interface address are on the same network.

## 718085

**Error Message** %ASA-5-718085: Interface *interface\_name* has no IP address defined.

**Explanation** The interface does not have an IP address configured.

**Recommended Action** Configure an IP address for the interface.

## 718086

**Error Message** %ASA-5-718086: Fail to install LB NP rules: type *rule\_type* , dst *interface\_name* , port *port* .

**Explanation** The Secure Firewall ASA experienced a failure when attempting to create a SoftNP ACL rule to be used in securing the communication between load balancing peers. This may indicate an internal software problem.

**Recommended Action** If the problem persists, contact the Cisco TAC.

## 718087

**Error Message** %ASA-5-718087: Fail to delete LB NP rules: type *rule\_type* , rule *rule\_ID* .

**Explanation** The Secure Firewall ASA experienced a failure when attempting to delete the SoftNP ACL rule used in securing the communication between load balancing peers.

**Recommended Action** None required.

## 718088

**Error Message** %ASA-7-718088: Possible VPN LB misconfiguration. Offending device MAC *MAC\_address* .

**Explanation** The presence of a duplicate director indicates that one of the load balancing peers may be misconfigured.

**Recommended Action** Check the load balancing configuration on all peers, but pay special attention to the peer identified.

## 719001

**Error Message** %ASA-6-719001: Email Proxy session could not be established: session limit of *maximum\_sessions* has been reached.

**Explanation** The incoming e-mail proxy session cannot be established because the maximum session limit has been reached.

- **maximum\_sessions**—The maximum session number

**Recommended Action** None required.

## 719002

**Error Message** %ASA-3-719002: Email Proxy session pointer from *source\_address* has been terminated due to *reason* error.

**Explanation** The session has been terminated because of an error. The possible errors are failure to add a session to the session database, failure to allocate memory, and failure to write data to a channel.

- **pointer**—The session pointer
- **source\_address**—The e-mail proxy client IP address
- **reason**—The error type

**Recommended Action** None required.

## 719003

**Error Message** %ASA-6-719003: Email Proxy session *pointer* resources have been freed for *source\_address* .

**Explanation** The dynamic allocated session structure has been freed and set to NULL after the session terminated.

- **pointer**—The session pointer
- **source\_address**—The e-mail proxy client IP address

**Recommended Action** None required.

## 719004

**Error Message** %ASA-6-719004: Email Proxy session pointer has been successfully established for *source\_address* .

**Explanation** A new incoming e-mail client session has been established.

**Recommended Action** None required.

## 719005

**Error Message** %ASA-7-719005: FSM NAME has been created using *protocol* for session pointer from *source\_address* .

**Explanation** The FSM has been created for an incoming new session.

- **NAME**—The FSM instance name for the session
- **protocol**—The e-mail protocol type (for example, POP3, IMAP, and SMTP)
- **pointer**—The session pointer
- **source\_address**—The e-mail proxy client IP address

**Recommended Action** None required.

## 719006

**Error Message** %ASA-7-719006: Email Proxy session pointer has timed out for *source\_address* because of network congestion.

**Explanation** Network congestion is occurring, and data cannot be sent to either an e-mail client or an e-mail server. This condition starts the block timer. After the block timer is timed out, the session expires.

- **pointer**—The session pointer
- **source\_address**—The e-mail proxy client IP address

**Recommended Action** Retry the operation after a few minutes.

## 719007

**Error Message** %ASA-7-719007: Email Proxy session pointer cannot be found for *source\_address* .

**Explanation** A matching session cannot be found in the session database. The session pointer is bad.

- **pointer**—The session pointer
- **source\_address**—The e-mail proxy client IP address

**Recommended Action** None required.

## 719008

**Error Message** %ASA-3-719008: Email Proxy service is shutting down.

**Explanation** The e-mail proxy is disabled. All resources are cleaned up, and all threads are terminated.

**Recommended Action** None required.

## 719009

**Error Message** %ASA-7-719009: Email Proxy service is starting.

**Explanation** The e-mail proxy is enabled.

**Recommended Action** None required.

## 719010

**Error Message** %ASA-6-719010: *protocol* Email Proxy feature is disabled on interface *interface\_name* .

**Explanation** The e-mail proxy feature is disabled on a specific entry point, invoked from the CLI. This is the main off switch for the user. When all protocols are turned off for all interfaces, the main shut-down routine is invoked to clean up global resources and threads.

- **protocol**—The e-mail proxy protocol type (for example, POP3, IMAP, and SMTP)
- **interface\_name** —The Secure Firewall ASA interface name

**Recommended Action** None required.

## 719011

**Error Message** %ASA-6-719011: Protocol Email Proxy feature is enabled on interface *interface\_name* .

**Explanation** The e-mail proxy feature is enabled on a specific entry point, invoked from the CLI. This is the main on switch for the user. When it is first used, the main startup routine is invoked to allocate global resources and threads. Subsequent calls only need to start listening threads for the particular protocol.

- **protocol**—The e-mail proxy protocol type (for example, POP3, IMAP, and SMTP)
- **interface\_name** —The Secure Firewall ASA interface name

**Recommended Action** None required.

## 719012

**Error Message** %ASA-6-719012: Email Proxy server listening on port *port* for mail protocol *protocol* .

**Explanation** A listening channel is opened for a specific protocol on a configured port and has added it to a TCP select group.

- **port**—The configured port number
- **protocol**—The e-mail proxy protocol type (for example, POP3, IMAP, and SMTP)



**Recommended Action** None required.

## 719013

**Error Message** %ASA-6-719013: Email Proxy server closing port *port* for mail protocol *protocol* .

**Explanation** A listening channel is closed for a specific protocol on a configured port and has removed it from the TCP select group.

- **port**—The configured port number
- **protocol**—The e-mail proxy protocol type (for example, POP3, IMAP, and SMTP)

**Recommended Action** None required.

## 719014

**Error Message** %ASA-5-719014: Email Proxy is changing listen port from *old\_port* to *new\_port* for mail protocol *protocol* .

**Explanation** A change is signaled in the listening port for the specified protocol. All enabled interfaces for that port have their listening channels closed and have restarted listening on the new port. This action is invoked from the CLI.

- **old\_port**—The previously configured port number
- **new\_port**—The newly configured port number
- **protocol**—The e-mail proxy protocol type (for example, POP3, IMAP, and SMTP)

**Recommended Action** None required.

## 719015

**Error Message** %ASA-7-719015: Parsed emailproxy session pointer from *source\_address* username: mailuser = *mail\_user* , vpnuser = *VPN\_user* , mailserver = *server*

**Explanation** The username string is received from the client in the format *vpnuser* (name delimiter) *mailuser* (server delimiter) *mailserver* (for example: *xxx:yyy@cisco.com*). The name delimiter is optional. When the delimiter is not there, the VPN username and mail username are the same. The server delimiter is optional. When it is not present, the default configured mail server will be used.

- **pointer**—The session pointer
- **source\_address**—The e-mail proxy client IP address
- **mail\_user**—The e-mail account username
- **VPN\_user**—The WebVPN username
- **server**—The e-mail server

**Recommended Action** None required.

## 719016

**Error Message** %ASA-7-719016: Parsed emailproxy session *pointer* from *source\_address* password: mailpass = \*\*\*\*\*, vpnpass= \*\*\*\*\*

**Explanation** The password string is received from the client in the format, `vpnpass (name delimiter) mailpass` (for example: `xxx:yyy`). The name delimiter is optional. When it is not present, the VPN password and mail password are the same.

- **pointer**—The session pointer
- **source\_address**—The e-mail proxy client IP address

**Recommended Action** None required.

## 719017

**Error Message** %ASA-6-719017: WebVPN user: `vpnuser` invalid dynamic ACL.

**Explanation** The WebVPN session is aborted because the ACL has failed to parse for this user. The ACL determines what the user restrictions are on e-mail account access. The ACL is downloaded from the AAA server. Because of this error, it is unsafe to proceed with login.

- **vpnuser**—The WebVPN username

**Recommended Action** Check the AAA server and fix the dynamic ACL for this user.

## 719018

**Error Message** %ASA-6-719018: WebVPN user: `vpnuser` ACL ID `acl_ID` not found

**Explanation** The ACL cannot be found at the local maintained ACL list. The ACL determines what the user restrictions are on e-mail account access. The ACL is configured locally. Because of this error, you cannot be authorized to proceed.

- **vpnuser**—The WebVPN username
- **acl\_ID**—The local configured ACL identification string

**Recommended Action** Check the local ACL configuration.

## 719019

**Error Message** %ASA-6-719019: WebVPN user: `vpnuser` authorization failed.

**Explanation** The ACL determines what the user restrictions are on e-mail account access. The user cannot access the e-mail account because the authorization check fails.

- **vpnuser**—The WebVPN username

**Recommended Action** None required.

## 719020

**Error Message** %ASA-6-719020: WebVPN user `vpnuser` authorization completed successfully.

**Explanation** The ACL determines what the user restrictions are on e-mail account access. The user is authorized to access the e-mail account.

- **vpnuser**—The WebVPN username

**Recommended Action** None required.

## 719021

**Error Message** %ASA-6-719021: WebVPN user: *vpnuser* is not checked against ACL.

**Explanation** The ACL determines what the user restrictions are on e-mail account access. The authorization checking using the ACL is not enabled.

- **vpnuser**—The WebVPN username

**Recommended Action** Enable the ACL checking feature, if necessary.

## 719022

**Error Message** %ASA-6-719022: WebVPN user *vpnuser* has been authenticated.

**Explanation** The username is authenticated by the AAA server.

- **vpnuser**—The WebVPN username

**Recommended Action** None required.

## 719023

**Error Message** %ASA-6-719023: WebVPN user *vpnuser* has not been successfully authenticated. Access denied.

**Explanation** The username is denied by the AAA server. The session will be aborted. The user is not allowed to access the e-mail account.

- **vpnuser**—The WebVPN username

**Recommended Action** None required.

## 719024

**Error Message** %ASA-6-719024: Email Proxy piggyback auth fail: session = *pointer* user=*vpnuser* addr=*source\_address*

**Explanation** The Piggyback authentication is using an established WebVPN session to verify the username and IP address matching in the WebVPN session database. This is based on the assumption that the WebVPN session and e-mail proxy session are initiated by the same user, and a WebVPN session is already established. Because the authentication has failed, the session will be aborted. The user is not allowed to access the e-mail account.

- **pointer**—The session pointer
- **vpnuser**—The WebVPN username
- **source\_address**—The client IP address

**Recommended Action** None required.

## 719025

**Error Message** %ASA-6-719025: Email Proxy DNS name resolution failed for *hostname* .

**Explanation** The hostname cannot be resolved with the IP address because it is not valid, or no DNS server is available.

- **hostname**—The hostname that needs to be resolved

**Recommended Action** Check DNS server availability and whether or not the configured mail server name is valid.

## 719026

**Error Message** %ASA-6-719026: Email Proxy DNS name *hostname* resolved to *IP\_address* .

**Explanation** The hostname has successfully been resolved with the IP address.

- **hostname**—The hostname that needs to be resolved
- **IP\_address**—The IP address resolved from the configured mail server name

**Recommended Action** None required.

## Messages 720001 to 721019

This section includes messages from 720001 to 721019.

### 720001

**Error Message** %ASA-4-720001: (VPN-*unit* ) Failed to initialize with Chunk Manager.

**Explanation** The VPN failover subsystem fails to initialize with the memory buffer management subsystem. A system-wide problem has occurred, and the VPN failover subsystem cannot be started.

- **unit**—Either Primary or Secondary

**Recommended Action** Examine the messages for any sign of system-level initialization problems.

### 720002

**Error Message** %ASA-6-720002: (VPN-*unit* ) Starting VPN Stateful Failover Subsystem...

**Explanation** The VPN failover subsystem is starting and booting up.

- **unit**—Either Primary or Secondary

**Recommended Action** None required.

### 720003

**Error Message** %ASA-6-720003: (VPN-*unit* ) Initialization of VPN Stateful Failover Component completed successfully

**Explanation** The VPN failover subsystem initialization is completed at boot time.

- **unit**—Either Primary or Secondary

**Recommended Action** None required.

## 720004

**Error Message** %ASA-6-720004: (VPN-unit ) VPN failover main thread started.

**Explanation** The VPN failover main processing thread is started at boot time.

- **unit**—Either Primary or Secondary

**Recommended Action** None required.

## 720005

**Error Message** %ASA-6-720005: (VPN-unit ) VPN failover timer thread started.

**Explanation** The VPN failover timer processing thread is started at boot time.

- **unit**—Either Primary or Secondary

**Recommended Action** None required.

## 720006

**Error Message** %ASA-6-720006: (VPN-unit ) VPN failover sync thread started.

**Explanation** The VPN failover bulk synchronization processing thread is started at boot time.

- **unit**—Either Primary or Secondary

**Recommended Action** None required.

## 720007

**Error Message** %ASA-4-720007: (VPN-unit ) Failed to allocate chunk from Chunk Manager.

**Explanation** The set of preallocated memory buffers is running out. The Secure Firewall ASA has a resource issue. The Secure Firewall ASA may be under heavy load when too many messages are being processed.

- **unit**—Either Primary or Secondary

**Recommended Action** This condition may be improved later when the VPN failover subsystem processes outstanding messages and frees up previously allocated memory.

## 720008

**Error Message** %ASA-4-720008: (VPN-unit ) Failed to register to High Availability Framework.

**Explanation** The VPN failover subsystem failed to register to the core failover subsystem. The VPN failover subsystem cannot be started, which may be caused by initialization problems of other subsystems.

- **unit**—Either Primary or Secondary

**Recommended Action** Search the message for any sign of system-wide initialization problems.

## 720009

**Error Message** %ASA-4-720009: (VPN-unit ) Failed to create version control block.

**Explanation** The VPN failover subsystem failed to create a version control block. This step is required for the VPN failover subsystem to find out the backward compatible firmware versions for the current release. The VPN failover subsystem cannot be started, which may be caused by initialization problems of other subsystems.

- **unit**—Either Primary or Secondary

**Recommended Action** Search the message for any sign of system-wide initialization problems.

## 720010

**Error Message** %ASA-6-720010: (VPN-unit ) VPN failover client is being disabled

**Explanation** An operator enabled failover without defining a failover key. In order to use a VPN failover, a failover key must be defined.

- **unit**—Either Primary or Secondary

**Recommended Action** Use the **failover key** command to define a shared secret key between the active and standby units.

## 720011

**Error Message** %ASA-4-720011: (VPN-unit ) Failed to allocate memory

**Explanation** The VPN failover subsystem cannot allocate a memory buffer, which indicates a system-wide resource problem. The Secure Firewall ASA may be under heavy load.

- **unit**—Either Primary or Secondary

**Recommended Action** This condition may be improved later when you reduce the load on the Secure Firewall ASA by reducing incoming traffic. By reducing incoming traffic, memory allocated for processing the existing work load will be available, and the Secure Firewall ASA may return to normal operation.

## 720012

**Error Message** %ASA-6-720012: (VPN-unit ) Failed to update IPsec failover runtime data on the standby unit.

**Explanation** The VPN failover subsystem cannot update IPsec-related runtime data because the corresponding IPsec tunnel has been deleted on the standby unit.

- **unit**—Either Primary or Secondary

**Recommended Action** None required.

## 720013

**Error Message** %ASA-4-720013: (VPN-unit ) Failed to insert certificate in trustpoint  
trustpoint\_name

**Explanation** The VPN failover subsystem tried to insert a certificate in the trustpoint.

- **unit**—Either Primary or Secondary
- **trustpoint\_name**—The name of the trustpoint

**Recommended Action** Check the certificate content to determine if it is invalid.

## 720014

**Error Message** %ASA-6-720014: (VPN-unit ) Phase 2 connection entry (msg\_id=message\_number , my cookie=mine , his cookie=his ) contains no SA list.

**Explanation** No security association is linked to the Phase 2 connection entry.

- **unit**—Either Primary or Secondary
- **message\_number**—The message ID of the Phase 2 connection entry
- **mine**—The My Phase 1 cookie
- **his**—The peer Phase 1 cookie

**Recommended Action** None required.

## 720015

**Error Message** %ASA-6-720015: (VPN-unit ) Cannot found Phase 1 SA for Phase 2 connection entry (msg\_id=message\_number ,my cookie=mine , his cookie=his ).

**Explanation** The corresponding Phase 1 security association for the given Phase 2 connection entry cannot be found.

- **unit**—Either Primary or Secondary
- **message\_number**—The message ID of the Phase 2 connection entry
- **mine**—The My Phase 1 cookie
- **his**—The peer Phase 1 cookie

**Recommended Action** None required.

## 720016

**Error Message** %ASA-5-720016: (VPN-unit) Failed to initialize default timer #index .

**Explanation** The VPN failover subsystem failed to initialize the given timer event. The VPN failover subsystem cannot be started at boot time.

- **unit**—Either Primary or Secondary
- **index**—The internal index of the timer event

**Recommended Action** Search the message for any sign of system-wide initialization problems.

## 720017

**Error Message** %ASA-5-720017: (VPN-unit ) Failed to update LB runtime data

**Explanation** The VPN failover subsystem failed to update the VPN load balancing runtime data.

- **unit**—Either Primary or Secondary

**Recommended Action** None required.

## 720018

**Error Message** %ASA-5-720018: (VPN-unit ) Failed to get a buffer from the underlying core high availability subsystem. Error code code.

**Explanation** The Secure Firewall ASA may be under heavy load. The VPN failover subsystem failed to obtain a failover buffer.

- **unit**—Either Primary or Secondary
- **code**—The error code returned by the high-availability subsystem

**Recommended Action** Decrease the amount of incoming traffic to improve the current load condition. With decreased incoming traffic, the Secure Firewall ASA will free up memory allocated for processing the incoming load.

## 720019

**Error Message** %ASA-5-720019: (VPN-unit ) Failed to update cTCP statistics.

**Explanation** The VPN failover subsystem failed to update the IPsec/cTCP-related statistics.

- **unit**—Either Primary or Secondary

**Recommended Action** None required. Updates are sent periodically, so the standby unit IPsec/cTCP statistics should be updated with the next update message.

## 720020

**Error Message** %ASA-5-720020: (VPN-unit ) Failed to send type timer message.

**Explanation** The VPN failover subsystem failed to send a periodic timer message to the standby unit.

- **unit**—Either Primary or Secondary
- **type**—The type of timer message

**Recommended Action** None required. The periodic timer message will be resent during the next timeout.

## 720021

**Error Message** %ASA-5-720021: (VPN-unit ) HA non-block send failed for peer msg message\_number . HA error code .

**Explanation** The VPN failover subsystem failed to send a nonblock message. This is a temporary condition caused by the Secure Firewall ASA being under load or out of resources.

- **unit**—Either Primary or Secondary
- **message\_number**—The ID number of the peer message
- **code**—The error return code

**Recommended Action** The condition will improve as more resources become available to the Secure Firewall ASA.



## 720022

**Error Message** %ASA-4-720022: (VPN-unit ) Cannot find trustpoint *trustpoint*

**Explanation** An error occurred when the VPN failover subsystem tried to look up a trustpoint by name.

- **unit**—Either Primary or Secondary
- **trustpoint**—The name of the trustpoint.

**Recommended Action** The trustpoint may be deleted by an operator.

## 720023

**Error Message** %ASA-6-720023: (VPN-unit ) HA status callback: Peer is *not* present.

**Explanation** The VPN failover subsystem is notified by the core failover subsystem when the local Secure Firewall ASA detected that a peer is available or becomes unavailable.

- **unit**—Either Primary or Secondary
- **not**—Either “not” or left blank

**Recommended Action** None required.

## 720024

**Error Message** %ASA-6-720024: (VPN-unit ) HA status callback: Control channel is *status* .

**Explanation** The failover control channel is either up or down. The failover control channel is defined by the **failover link** and **show failover** commands, which indicate whether the failover link channel is up or down.

- **unit**—Either Primary or Secondary
- **status**—Up or Down

**Recommended Action** None required.

## 720025

**Error Message** %ASA-6-720025: (VPN-unit ) HA status callback: Data channel is *status* .

**Explanation** The failover data channel is up or down.

- **unit**—Either Primary or Secondary
- **status**—Up or Down

**Recommended Action** None required.

## 720026

**Error Message** %ASA-6-720026: (VPN-unit ) HA status callback: Current progression is being aborted.

**Explanation** An operator or other external condition has occurred and has caused the current failover progression to abort before the failover peer agrees on the role (either active or standby). For example, when the **failover active** command is entered on the standby unit during the negotiation, or when the active unit is being rebooted.

- **unit**—Either Primary or Secondary

**Recommended Action** None required.

## 720027

**Error Message** %ASA-6-720027: (VPN-unit ) HA status callback: My state state .

**Explanation** The state of the local failover device is changed.

- **unit**—Either Primary or Secondary
- **state**—Current state of the local failover device

**Recommended Action** None required.

## 720028

**Error Message** %ASA-6-720028: (VPN-unit ) HA status callback: Peer state state .

**Explanation** The current state of the failover peer is reported.

- **unit**—Either Primary or Secondary
- **state**—Current state of the failover peer

**Recommended Action** None required.

## 720029

**Error Message** %ASA-6-720029: (VPN-unit ) HA status callback: Start VPN bulk sync state.

**Explanation** The active unit is ready to send all the state information to the standby unit.

- **unit**—Either Primary or Secondary

**Recommended Action** None required.

## 720030

**Error Message** %ASA-6-720030: (VPN-unit ) HA status callback: Stop bulk sync state.

**Explanation** The active unit finished sending all the state information to the standby unit.

- **unit**—Either Primary or Secondary

**Recommended Action** None required.

## 720031

**Error Message** %ASA-7-720031: (VPN-unit ) HA status callback: Invalid event received.  
event=event\_ID .

**Explanation** The VPN failover subsystem received an invalid callback event from the underlying failover subsystem.

- **unit**—Either Primary or Secondary

- **event\_ID**—The invalid event ID received

**Recommended Action** None required.

## 720032

**Error Message** %ASA-6-720032: (VPN-**unit**) HA status callback: id=*ID* , seq=*sequence\_#* , grp=*group* , event=*event* , op=*operand* , my=*my\_state* , peer=*peer\_state* .

**Explanation** The VPN failover subsystem indicated that a status update was notified by the underlying failover subsystem.

- **unit**—Either Primary or Secondary
- **ID**—Client ID number
- **sequence\_#**—Sequence number
- **group**—Group ID
- **event**—Current event
- **operand**—Current operand
- **my\_state**—The system current state
- **peer\_state**—The current state of the peer

**Recommended Action** None required.

## 720033

**Error Message** %ASA-4-720033: (VPN-*unit* ) Failed to queue add to message queue.

**Explanation** System resources may be running low. An error occurred when the VPN failover subsystem tried to queue an internal message. This may be a temporary condition indicating that the Secure Firewall ASA is under heavy load, and the VPN failover subsystem cannot allocate resource to handle incoming traffic.

- **unit**—Either Primary or Secondary

**Recommended Action** This error condition may disappear if the current load of the Secure Firewall ASA is reduced, and additional system resources become available for processing new messages again.

## 720034

**Error Message** %ASA-7-720034: (VPN-*unit* ) Invalid type (*type* ) for message handler.

**Explanation** An error occurred when the VPN failover subsystem tried to process an invalid message type.

- **unit**—Either Primary or Secondary
- **type**—Message type

**Recommended Action** None required.

## 720035

**Error Message** %ASA-5-720035: (VPN-*unit* ) Fail to look up CTCP flow handle

**Explanation** The cTCP flow may be deleted on the standby unit before the VPN failover subsystem tries to do a lookup.

- **unit**—Either Primary or Secondary

**Recommended Action** Look for any sign of cTCP flow deletion in the message to determine the reason (for example, idle timeout) why the flow was deleted.

## 720036

**Error Message** %ASA-5-720036: (VPN-unit ) Failed to process state update message from the active peer.

**Explanation** An error occurred when the VPN failover subsystem tried to process a state update message received by the standby unit.

- **unit** - Either Primary or Secondary

**Recommended Action** None required. This may be a temporary condition because of the current load or low system resources.

## 720037

**Error Message** %ASA-6-720037: (VPN-unit ) HA progression callback: id=id ,seq=sequence\_number ,grp=group ,event=event ,op=operand , my=my\_state ,peer=peer\_state .

**Explanation** The status of the current failover progression is reported.

- **unit**—Either Primary or Secondary
- **id**—Client ID
- **sequence\_number**—Sequence number
- **group**—Group ID
- **event**—Current event
- **operand**—Current operand
- **my\_state**—Current state of the Secure Firewall ASA
- **peer\_state**—Current state of the peer

**Recommended Action** None required.

## 720038

**Error Message** %ASA-4-720038: (VPN-unit ) Corrupted message from active unit.

**Explanation** The standby unit received a corrupted message from the active unit. Messages from the active unit are corrupted, which may be caused by incompatible firmware running between the active and standby units. The local unit has become the active unit of the failover pair.

- **unit**—Either Primary or Secondary

**Recommended Action** None required.

## 720039

**Error Message** %ASA-6-720039: (VPN-unit ) VPN failover client is transitioning to active state

**Explanation** The local unit has become the active unit of the failover pair.

- **unit**—Either Primary or Secondary

**Recommended Action** None required.

## 720040

**Error Message** %ASA-6-720040: (VPN-unit ) VPN failover client is transitioning to standby state.

**Explanation** The local unit has become the standby unit of the failover pair.

- **unit**—Either Primary or Secondary

**Recommended Action** None required.

## 720041

**Error Message** %ASA-7-720041: (VPN-unit ) Sending type message id to standby unit

**Explanation** A message has been sent from the active unit to the standby unit.

- **unit**—Either Primary or Secondary
- **type**—Message type
- **id**—Identifier for the message

**Recommended Action** None required.

## 720042

**Error Message** %ASA-7-720042: (VPN-unit ) Receiving type message id from active unit

**Explanation** A message has been received from the active unit by the standby unit.

- **unit**—Either Primary or Secondary
- **type**—Message type
- **id**—Identifier for the message

**Recommended Action** None required.

## 720043

**Error Message** %ASA-4-720043: (VPN-unit ) Failed to send type message id to standby unit

**Explanation** An error occurred when the VPN failover subsystem tried to send a message from the active unit to the standby unit. The error may be caused by message 720018, in which the core failover subsystem runs out of failover buffer or the failover LAN link is down.

- **unit**—Either Primary or Secondary
- **type**—Message type
- **id**—Identifier for the message

**Recommended Action** Use the **show failover** command to see if the failover pair is running correctly and the failover LAN link is up.

## 720044

**Error Message** %ASA-4-720044: (VPN-unit ) Failed to receive message from active unit

**Explanation** An error occurred when the VPN failover subsystem tried to receive a message on the standby unit. The error may be caused by a corrupted message or an inadequate amount of memory allocated for storing the incoming message.

- **unit**—Either Primary or Secondary

**Recommended Action** Use the **show failover** command and look for receive errors to determine if this is a VPN failover-specific problem or a general failover issue. Corrupted messages may be caused by incompatible firmware versions running on the active and standby units. Use the **show memory** command to determine if a low memory condition exists.

## 720045

**Error Message** %ASA-6-720045: (VPN-unit ) Start bulk syncing of state information on standby unit.

**Explanation** The standby unit has been notified to start receiving bulk synchronization information from the active unit.

- **unit**—Either Primary or Secondary

**Recommended Action** None required.

## 720046

**Error Message** %ASA-6-720046: (VPN-unit ) End bulk syncing of state information on standby unit

**Explanation** The standby unit has been notified that bulk synchronization from the active unit is completed.

- **unit**—Either Primary or Secondary

**Recommended Action** None required.

## 720047

**Error Message** %ASA-4-720047: (VPN-unit ) Failed to sync SDI node secret file for server *IP\_address* on the standby unit.

**Explanation** An error occurred when the VPN failover subsystem tried to synchronize a node secret file for the SDI server on the standby unit. The SDI node secret file is stored in flash. The error may indicate that the flash file system is full or corrupted.

- **unit**—Either Primary or Secondary
- **IP\_address**—IP address of the server

**Recommended Action** Use the **dir** command to display the flash contents. The node secret file has the filename, *ip.sdi*.

## 720048

**Error Message** %ASA-7-720048: (VPN-unit ) FSM action trace begin: state=*state* , last event=*event* , func=*function* .

**Explanation** A VPN failover subsystem finite state machine function has started.

- **unit**—Either Primary or Secondary
- **state**—Current state
- **event**—Last event
- **function**—Current executing function

**Recommended Action** None required.

## 720049

**Error Message** %ASA-7-720049: (VPN-unit ) FSM action trace end: state=*state* , last event=*event* , return=*return* , func=*function* .

**Explanation** A VPN failover subsystem finite state machine function has finished.

- **unit**—Either Primary or Secondary
- **state**—Current state
- **event**—Last event
- **return**—Return code
- **function**—Current executing function

**Recommended Action** None required.

## 720050

**Error Message** %ASA-7-720050: (VPN-unit ) Failed to remove timer. ID = *id* .

**Explanation** A timer cannot be removed from the timer processing thread.

- **unit**—Either Primary or Secondary
- **id**—Timer ID

**Recommended Action** None required.

## 720051

**Error Message** %ASA-4-720051: (VPN-unit ) Failed to add new SDI node secret file for server *id* on the standby unit.

**Explanation** An error occurred when the VPN failover subsystem tried to add a node secret file for the SDI server on the standby unit. The SDI node secret file is stored in flash. The error may indicate that the flash file system is full or corrupted.

- **unit**—Either Primary or Secondary
- **id**—IP address of the SDI server

**Recommended Action** Use the **dir** command to display the flash contents. The node secret file has the filename, **ip.sdi**.

## 720052

**Error Message** %ASA-4-720052: (VPN-unit ) Failed to delete SDI node secret file for server *id* on the standby unit.

**Explanation** An error occurred when the VPN failover subsystem tried to delete a node secret file on the active unit. The node secret file being deleted may not exist in the flash file system, or there was problem reading the flash file system.

- **unit**—Either Primary or Secondary
- **IP\_address**—IP address of the SDI server

**Recommended Action** Use the **dir** command to display the flash contents. The node secret file has the filename, **ip.sdi**.

## 720053

**Error Message** %ASA-4-720053: (VPN-unit ) Failed to add cTCP IKE rule during bulk sync, peer=*IP\_address* , port=*port*

**Explanation** An error occurred when the VPN failover subsystem tried to load a cTCP IKE rule on the standby unit during bulk synchronization. The standby unit may be under heavy load, and the new IKE rule request may time out before completion.

- **unit**—Either Primary or Secondary
- **IP\_address**—Peer IP address
- **port**—Peer port number

**Recommended Action** None required.

## 720054

**Error Message** %ASA-4-720054: (VPN-unit ) Failed to add new cTCP record, peer=*IP\_address* , port=*port* .

**Explanation** A cTCP record is replicated to the standby unit and cannot be updated. The corresponding IPsec over cTCP tunnel may not be functioning after failover. The cTCP database may be full, or a record with the same peer IP address and port number exists already.

- **unit**—Either Primary or Secondary
- **IP\_address**—Peer IP address
- **port**—Peer port number

**Recommended Action** This may be a temporary condition and may improve when the existing cTCP tunnel is restored.

## 720055

**Error Message** %ASA-4-720055: (VPN-unit ) VPN Stateful failover can only be run in single/non-transparent mode.

**Explanation** The VPN subsystem does not start unless it is running in single (nontransparent) mode.

- **unit**—Either Primary or Secondary



**Recommended Action** Configure the Secure Firewall ASA for the appropriate mode to support VPN failover and restart the Secure Firewall ASA.

## 720056

**Error Message** %ASA-6-720056: (VPN-unit ) VPN Stateful failover Message Thread is being disabled.

**Explanation** The VPN failover subsystem main message processing thread is disabled when you have tried to enable failover, but a failover key is not defined. A failover key is required for VPN failover.

- **unit**—Either Primary or Secondary

**Recommended Action** None required.

## 720057

**Error Message** %ASA-6-720057: (VPN-unit ) VPN Stateful failover Message Thread is enabled.

**Explanation** The VPN failover subsystem main message processing thread is enabled when failover is enabled and a failover key is defined.

- **unit**—Either Primary or Secondary

**Recommended Action** None required.

## 720058

**Error Message** %ASA-6-720058: (VPN-unit ) VPN Stateful failover Timer Thread is disabled.

**Explanation** The VPN failover subsystem main timer processing thread is disabled when the failover key is not defined and failover is enabled.

- **unit**—Either Primary or Secondary

**Recommended Action** None required.

## 720059

**Error Message** %ASA-6-720059: (VPN-unit ) VPN Stateful failover Timer Thread is enabled.

**Explanation** The VPN failover subsystem main timer processing thread is enabled when the failover key is defined and failover is enabled.

- **unit**—Either Primary or Secondary

**Recommended Action** None required.

## 720060

**Error Message** %ASA-6-720060: (VPN-unit ) VPN Stateful failover Sync Thread is disabled.

**Explanation** The VPN failover subsystem main bulk synchronization processing thread is disabled when failover is enabled, but the failover key is not defined.

- **unit**—Either Primary or Secondary.

**Recommended Action** None required.

## 720061

**Error Message** %ASA-6-720061: (VPN-unit ) VPN Stateful failover Sync Thread is enabled.

**Explanation** The VPN failover subsystem main bulk synchronization processing thread is enabled when failover is enabled and the failover key is defined.

- **unit**—Either Primary or Secondary

**Recommended Action** None required.

## 720062

**Error Message** %ASA-6-720062: (VPN-unit ) Active unit started bulk sync of state information to standby unit.

**Explanation** The VPN failover subsystem active unit has started bulk synchronization of state information to the standby unit.

- **unit**—Either Primary or Secondary

**Recommended Action** None required.

## 720063

**Error Message** %ASA-6-720063: (VPN-unit ) Active unit completed bulk sync of state information to standby.

**Explanation** The VPN failover subsystem active unit has completed bulk synchronization of state information to the standby unit.

- **unit**—Either Primary or Secondary

**Recommended Action** None required.

## 720064

**Error Message** %ASA-4-720064: (VPN-unit ) Failed to update cTCP database record for peer=*IP\_address* , port=*port* during bulk sync.

**Explanation** An error occurred while the VPN failover subsystem attempted to update an existing cTCP record during bulk synchronization. The cTCP record may have been deleted from the cTCP database on the standby unit and cannot be found.

- **unit**—Either Primary or Secondary
- **IP\_address**—Peer IP address
- **port**—Peer port number

**Recommended Action** Search in the message.

## 720065

**Error Message** %ASA-4-720065: (VPN-unit ) Failed to add new cTCP IKE rule, peer=peer , port=port .

**Explanation** An error occurred when the VPN failover subsystem tried to add a new IKE rule for the cTCP database entry on the standby unit. The Secure Firewall ASA may be under heavy load, and the request for adding a cTCP IKE rule timed out and was never completed.

- **unit**—Either Primary or Secondary
- **IP\_address**—Peer IP address
- **port**—Peer port number

**Recommended Action** This may be a temporary condition.

## 720066

**Error Message** %ASA-4-720066: (VPN-unit ) Failed to activate IKE database.

**Explanation** An error occurred when the VPN failover subsystem tried to activate the IKE security association database while the standby unit was transitioning to the active state. There may be resource-related issues on the standby unit that prevent the IKE security association database from activating.

- **unit**—Either Primary or Secondary

**Recommended Action** Use the **show failover** command to see if the failover pair is still working correctly and/or look for other IKE-related errors in the message.

## 720067

**Error Message** %ASA-4-720067: (VPN-unit ) Failed to deactivate IKE database.

**Explanation** An error occurred when the VPN failover subsystem tried to deactivate the IKE security association database while the active unit was transitioning to the standby state. There may be resource-related issues on the active unit that prevent the IKE security association database from deactivating.

- **unit**—Either Primary or Secondary

**Recommended Action** Use the **show failover** command to see if the failover pair is still working correctly and/or look for IKE-related errors in the message.

## 720068

**Error Message** %ASA-4-720068: (VPN-unit ) Failed to parse peer message.

**Explanation** An error occurred when the VPN failover subsystem tried to parse a peer message received on the standby unit. The peer message received on the standby unit cannot be parsed.

- **unit**—Either Primary or Secondary

**Recommended Action** Make sure that both active and standby units are running the same version of firmware. Also, use the **show failover** command to ensure that the failover pair is still working correctly.

## 720069

**Error Message** %ASA-4-720069: (VPN-unit ) Failed to activate cTCP database.

**Explanation** An error occurred when the VPN failover subsystem tried to activate the cTCP database while the standby unit was transitioning to the active state. There may be resource-related issues on the standby unit that prevent the cTCP database from activating.

- **unit**—Either Primary or Secondary

**Recommended Action** Use the **show failover** command to see if the failover pair is still working correctly and/or look for other cTCP related errors in the message.

## 720070

**Error Message** %ASA-4-720070: (VPN-unit ) Failed to deactivate cTCP database.

**Explanation** An error occurred when the VPN failover subsystem tried to deactivate the cTCP database while the active unit was transitioning to the standby state. There may be resource-related issues on the active unit that prevent the cTCP database from deactivating.

- **unit**—Either Primary or Secondary.

**Recommended Action** Use the **show failover** command to see if the failover pair is still working correctly and/or look for cTCP related errors in the message.

## 720071

**Error Message** %ASA-5-720071: (VPN-unit ) Failed to update cTCP dynamic data.

**Explanation** An error occurred while the VPN failover subsystem tried to update cTCP dynamic data.

- **unit**—Either Primary or Secondary.

**Recommended Action** This may be a temporary condition. Because this is a periodic update, wait to see if the same error recurs. Also, look for other failover-related messages in the message.

## 720072

**Error Message** %ASA-5-720072: Timeout waiting for Integrity Firewall Server [*interface* , *ip* ] to become available.

**Explanation** The Zonelab Integrity Server cannot reestablish a connection before timeout. In an active/standby failover setup, the SSL connection between a Zonelab Integrity Server and the Secure Firewall ASA needs to be reestablished after a failover.

- *interface* —The interface to which the Zonelab Integrity Server is connected
- *ip* —The IP address of the Zonelab Integrity Server

**Recommended Action** Check that the configuration on the Secure Firewall ASA and the Zonelab Integrity Server match, and verify communication between the Secure Firewall ASA and the Zonelab Integrity Server.

## 720073

**Error Message** %ASA-4-720073: VPN Session failed to replicate - ACL *acl\_name* not found

**Explanation** When replicating VPN sessions to the standby unit, the standby unit failed to find the associated filter ACL.

- **acl\_name**—The name of the ACL that was not found

**Recommended Action** Verify that the configuration on the standby unit has not been modified while in standby state. Resynchronize the standby unit by issuing the **write standby** command on the active unit.

## 721001

**Error Message** %ASA-6-721001: (device ) WebVPN Failover SubSystem started successfully.(device ) either WebVPN-primary or WebVPN-secondary.

**Explanation** The WebVPN failover subsystem in the current failover unit, either primary or secondary, has been started successfully.

- **(device)**—Either the WebVPN primary or the WebVPN secondary device

**Recommended Action** None required.

## 721002

**Error Message** %ASA-6-721002: (device ) HA status change: event *event* , my state *my\_state* , peer state *peer* .

**Explanation** The WebVPN failover subsystem receives status notification from the core HA component periodically. The incoming event, the new state of the local Secure Firewall ASA, and the new state of the failover peer are reported.

- **(device)**—Either the WebVPN primary or the WebVPN secondary Secure Firewall ASA
- **event**—New HA event
- **my\_state**—The new state of the local Secure Firewall ASA
- **peer**—The new state of the peer

**Recommended Action** None required.

## 721003

**Error Message** %ASA-6-721003: (device ) HA progression change: event *event* , my state *my\_state* , peer state *peer* .

**Explanation** The WebVPN failover subsystem transitions from one state to another state based on the event notified by the core HA component. The incoming event, the new state of the local Secure Firewall ASA, and the new state of the failover peer are being reported.

- **(device)**—Either the WebVPN primary or the WebVPN secondary Secure Firewall ASA
- **event**—New HA event
- **my\_state**—The new state of the local Secure Firewall ASA
- **peer**—The new state of the peer

**Recommended Action** None required.

## 721004

**Error Message** %ASA-6-721004: (device ) Create access list *list\_name* on standby unit.

**Explanation** A WebVPN-specific access list is replicated from the active unit to the standby unit. A successful installation of the WebVPN access list on the standby unit has occurred.

- **(device)**—Either the WebVPN primary or the WebVPN secondary Secure Firewall ASA
- **list\_name**—The access list name

**Recommended Action** None required.

## 721005

**Error Message** %ASA-6-721005: (device ) Fail to create access list *list\_name* on standby unit.

**Explanation** When a WebVPN-specific access list is installed on the active unit, a copy is installed on the standby unit. The access list failed to be installed on the standby unit. The access list may have existed on the standby unit already.

- **(device)**—Either the WebVPN primary or the WebVPN secondary Secure Firewall ASA
- **list\_name**—Name of the access list that failed to install on the standby unit

**Recommended Action** Use the **show access-list** command on both the active and standby units. Compare the content of the output and determine whether there is any discrepancy. Resynchronize the standby unit, if needed, by using the **write standby** command on the active unit.

## 721006

**Error Message** %ASA-6-721006: (device ) Update access list *list\_name* on standby unit.

**Explanation** The content of the access list has been updated on the standby unit.

- **(device)**—Either the WebVPN primary or the WebVPN secondary Secure Firewall ASA
- **list\_name**—Name of the access list that was updated

**Recommended Action** None required.

## 721007

**Error Message** %ASA-4-721007: (device ) Fail to update access list *list\_name* on standby unit.

**Explanation** An error occurred while the standby unit tried to update a WebVPN-specific access list. The access list cannot be located on the standby unit.

- **(device)**—Either the WebVPN primary or the WebVPN= secondary Secure Firewall ASA
- **list\_name**—Name of the access list that was not updated

**Recommended Action** Use a **show access-list** command on both the active and standby units. Compare the content of the output and determine whether or not there is any discrepancy. Resynchronize the standby unit, if needed, by using the **write standby** command on the active unit.

## 721008

**Error Message** %ASA-6-721008: (device ) Delete access list *list\_name* on standby unit.

**Explanation** When a WebVPN-specific access list is removed from the active unit, a message is sent to the standby unit requesting that the same access list be removed. As a result, a WebVPN-specific access list has been removed from the standby unit.

- **(device)**—Either the WebVPN primary or the WebVPN secondary Secure Firewall ASA
- **list\_name**—Name of the access list that was removed

**Recommended Action** None required.

## 721009

**Error Message** %ASA-6-721009: (device ) Fail to delete access list *list\_name* on standby unit.

**Explanation** When a WebVPN-specific access list is removed on the active unit, a message is sent to the standby unit requesting the same access list be removed. An error condition occurred when an attempt was made to remove the corresponding access list on the standby unit. The access list did not exist on the standby unit.

- **(device)**—Either the WebVPN primary or the WebVPN secondary Secure Firewall ASA
- **list\_name**—Name of the access list that was deleted

**Recommended Action** Use a **show access-list** command on both the active and standby units. Compare the content of the output and determine whether there is any discrepancy. Resynchronize the standby unit, if needed, by using the **write standby** command on the active unit.

## 721010

**Error Message** %ASA-6-721010: (device ) Add access list rule *list\_name* , line *line\_no* on standby unit.

**Explanation** When an access list rule is added to the active unit, the same rule is added on the standby unit. A new access list rule was added successfully on the standby unit.

- **(device)**—Either the WebVPN primary or the WebVPN secondary Secure Firewall ASA
- **list\_name**—Name of the access list that was deleted
- **line\_no**—Line number of the rule added to the access list

**Recommended Action** None required.

## 721011

**Error Message** %ASA-4-721011: (device ) Fail to add access list rule *list\_name* , line *line\_no* on standby unit.

**Explanation** When an access list rule is added to the active unit, an attempt is made to add the same access list rule to the standby unit. An error occurred when an attempt is made to add a new access list rule to the standby unit. The same access list rule may exist on the standby unit.

- **(device)**—Either the WebVPN primary or the WebVPN secondary Secure Firewall ASA
- **list\_name**—Name of the access list that was deleted

- **line\_no**—Line number of the rule added to the access list

**Recommended Action** Use a **show access-list** command on both the active and standby units. Compare the content of the output and determine if there is any discrepancy. Resynchronize the standby unit, if needed, by using the **write standby** command on the active unit.

## 721012

**Error Message** %ASA-6-721012: (device ) Enable APCF XML file *file\_name* on the standby unit.

**Explanation** When an APCF XML file is installed on the active unit, an attempt is made to install the same file on the standby unit. An APCF XML file was installed successfully on the standby unit. Use the **dir** command on the standby unit to show that the XML file exists in the flash file system.

- **(device)**—Either the WebVPN primary or the WebVPN secondary Secure Firewall ASA
- **file\_name**—Name of the XML file on the flash file system

**Recommended Action** None required.

## 721013

**Error Message** %ASA-4-721013: (device ) Fail to enable APCF XML file *file\_name* on the standby unit.

**Explanation** When an APCF XML file is installed on the active unit, an attempt is made to install the same file on the standby unit. An APCF XML file failed to install on the standby unit.

- **(device)**—Either the WebVPN primary or the WebVPN secondary Secure Firewall ASA
- **file\_name**—Name of the XML file on the flash file system

**Recommended Action** Use a **dir** command on both the active and standby unit. Compare the directory listing and determine if there is any discrepancy. Resynchronize the standby unit, if needed, by using the **write standby** command on the active unit.

## 721014

**Error Message** %ASA-6-721014: (device ) Disable APCF XML file *file\_name* on the standby unit.

**Explanation** When an APCF XML file is removed on the active unit, an attempt is made to remove the same file on the standby unit. An APCF XML file was removed from the standby unit successfully.

- **(device)**—Either the WebVPN primary or the WebVPN secondary Secure Firewall ASA
- **file\_name**—Name of the XML file on the flash file system

**Recommended Action** None required.

## 721015

**Error Message** %ASA-4-721015: (device ) Fail to disable APCF XML file *file\_name* on the standby unit.

**Explanation** When an APCF XML file is removed on the active unit, an attempt is made to remove the same file on the standby unit. An error occurred when an attempt was made to remove an APCF XML file from the standby unit. The file may not be installed on the standby unit.



- **(device)**—Either the WebVPN primary or the WebVPN secondary Secure Firewall ASA
- **file\_name**—Name of the XML file on the flash file system

**Recommended Action** Use a **show running-config webvpn** command to make sure the APCF XML file of interest is not enabled. As long as it is not enabled, you may ignore this message. Otherwise, try to disable the file by using the **no apcf file\_name** command in the webvpn configuration submode.

## 721016

**Error Message** %ASA-6-721016: (device ) WebVPN session for client user user\_name , IP ip\_address has been created.

**Explanation** A remote WebVPN user has logged in successfully and the login information has been installed on the standby unit.

- **(device)**—Either the WebVPN primary or the WebVPN secondary Secure Firewall ASA
- **user\_name**—Name of the user
- **ip\_address**—IP address of the remote user

**Recommended Action** None required.

## 721017

**Error Message** %ASA-4-721017: (device ) Fail to create WebVPN session for user user\_name , IP ip\_address .

**Explanation** When a WebVPN user logs in to the active unit, the login information is replicated to the standby unit. An error occurred while replicating the login information to the standby unit.

- **(device)**—Either the WebVPN primary or the WebVPN secondary Secure Firewall ASA
- **user\_name**—Name of the user
- **ip\_address**—IP address of the remote user

**Recommended Action** Use the **show vpn-sessiondb detail webvpn** command for a regular WebVPN user, or the **show vpn-sessiondb detail svc** command for a WebVPN SVC user on both the active and standby units. Compare the entries and determine whether the same user session record appears on both Secure Firewall ASAs. Resynchronize the standby unit, if needed, by using the **write standby** command on the active unit.

## 721018

**Error Message** %ASA-6-721018: (device ) WebVPN session for client user user\_name , IP ip\_address has been deleted.

**Explanation** When a WebVPN user logs out on the active unit, a logout message is sent to the standby unit to remove the user session from the standby unit. A WebVPN user record was removed from the standby unit successfully.

- **(device)**—Either the WebVPN primary or the WebVPN secondary Secure Firewall ASA
- **user\_name**—Name of the user
- **ip\_address**—IP address of the remote user

**Recommended Action** None required.

## 721019

**Error Message** %ASA-4-721019: (device ) Fail to delete WebVPN session for client user *user\_name*, IP *ip\_address* .

**Explanation** When a WebVPN user logs out on the active unit, a logout message is sent to the standby unit to remove the user session from the standby unit. An error occurred when an attempt was made to remove a WebVPN user record from the standby unit.

- **(device)**—Either the WebVPN primary or the WebVPN secondary Secure Firewall ASA
- **user\_name**—Name of the user
- **ip\_address**—IP address of the remote user

**Recommended Action** Use the **show vpn-sessiondb detail webvpn** command for a regular WebVPN user, or the **show vpn-sessiondb detail svc** command for a WebVPN SVC user on both the active and standby units. Check whether there is any discrepancy. Resynchronize the standby unit, if needed, by using the **write standby** command on the active unit.



## CHAPTER 9

# Syslog Messages 722001 to 776020

---

This chapter contains the following sections:

- [Messages 722001 to 722056, on page 461](#)
- [Messages 723001 to 736001, on page 475](#)
- [Messages 737001 to 776254, on page 503](#)

## Messages 722001 to 722056

This section includes messages from 722001 to 722056.

### 722001

**Error Message** %ASA-4-722001: IP *IP\_address* Error parsing SVC connect request.

**Explanation** The request from the SVC was invalid.

**Recommended Action** Research as necessary to determine if this error was caused by a defect in the SVC, an incompatible SVC version, or an attack against the device.

### 722002

**Error Message** %ASA-4-722002: IP *IP\_address* Error consolidating SVC connect request.

**Explanation** There is not enough memory to perform the action.

**Recommended Action** Purchase more memory, upgrade the device, or reduce the load on the device.

### 722003

**Error Message** %ASA-4-722003: IP *IP\_address* Error authenticating SVC connect request.

**Explanation** The user took too long to download and connect.

**Recommended Action** Increase the timeouts for session idle and maximum connect time.

## 722004

**Error Message** %ASA-4-722004: Group *group* User *user-name* IP *IP\_address* Error responding to SVC connect request.

**Explanation** There is not enough memory to perform the action.

**Recommended Action** Purchase more memory, upgrade the device, or reduce the load on the device.

## 722005

**Error Message** %ASA-5-722005: Group *group* User *user-name* IP *IP\_address* Unable to update session information for SVC connection.

**Explanation** There is not enough memory to perform the action.

**Recommended Action** Purchase more memory, upgrade the device, or reduce the load on the device.

## 722006

**Error Message** %ASA-5-722006: Group *group* User *user-name* IP *IP\_address* Invalid address *IP\_address* assigned to SVC connection.

**Explanation** An invalid address was assigned to the user.

**Recommended Action** Verify and correct the address assignment, if possible. Otherwise, notify your network administrator or escalate this issue according to your security policy. For additional assistance, contact the Cisco TAC.

## 722007

**Error Message** %ASA-3-722007: Group *group* User *user-name* IP *IP\_address* SVC Message: *type-num* /ERROR: *message*

**Explanation** The SVC issued a message.

- **type-num**— A number from 0 to 31 indicating a message type. Message types are as follows:
  - 0—Normal
  - 16—Logout
  - 17—Closed due to error
  - 18—Closed due to rekey
  - 1-15, 19-31—Reserved and unused

- **message**—A text message from the SVC

**Recommended Action** None required.

## 722008

**Error Message** %ASA-3-722008: Group *group* User *user-name* IP *IP\_address* SVC Message: *type-num* /ERROR: *message*

**Explanation** The SVC issued a message.

- **type-num**— A number from 0 to 31 indicating a message type. Message types are as follows:

- 0—Normal
- 16—Logout
- 17—Closed due to error
- 18—Closed due to rekey
- 1-15, 19-31—Reserved and unused

- **message**—A text message from the SVC

**Recommended Action** None required.

## 722009

**Error Message** %ASA-3-722009: Group *group* User *user-name* IP *IP\_address* SVC Message: *type-num*  
/ERROR: *message*

**Explanation** The SVC issued a message.

- **type-num**— A number from 0 to 31 indicating a message type. Message types are as follows:

- 0—Normal
- 16—Logout
- 17—Closed due to error
- 18—Closed due to rekey
- 1-15, 19-31—Reserved and unused

- **message**—A text message from the SVC

**Recommended Action** None required.

## 722010

**Error Message** %ASA-5-722010: Group *group* User *user-name* IP *IP\_address* SVC Message: *type-num*  
/NOTICE: *message*

**Explanation** The SVC issued a message.

- **type-num**— A number from 0 to 31 indicating a message type. Message types are as follows:

- 0—Normal
- 16—Logout
- 17—Closed due to error
- 18—Closed due to rekey
- 1-15, 19-31—Reserved and unused

- **message**—A text message from the SVC

**Recommended Action** None required.

## 722011

**Error Message** %ASA-5-722011: Group *group* User *user-name* IP *IP\_address* SVC Message: *type-num*  
/NOTICE: *message*

**Explanation** The SVC issued a message.

- **type-num**— A number from 0 to 31 indicating a message type. Message types are as follows:
  - 0—Normal
  - 16—Logout
  - 17—Closed due to error
  - 18—Closed due to rekey
  - 1-15, 19-31—Reserved and unused
- **message**—A text message from the SVC

**Recommended Action** None required.

## 722012

**Error Message** %ASA-5-722012: Group *group* User *user-name* IP *IP\_address* SVC Message: *type-num*  
/INFO: *message*

**Explanation** The SVC issued a message.

- **type-num**— A number from 0 to 31 indicating a message type. Message types are as follows:
  - 0—Normal
  - 16—Logout
  - 17—Closed due to error
  - 18—Closed due to rekey
  - 1-15, 19-31—Reserved and unused
- **message**—A text message from the SVC

**Recommended Action** None required.

## 722013

**Error Message** %ASA-6-722013: Group *group* User *user-name* IP *IP\_address* SVC Message: *type-num*  
/INFO: *message*

**Explanation** The SVC issued a message.

- **type-num**— A number from 0 to 31 indicating a message type. Message types are as follows:
  - 0—Normal
  - 16—Logout
  - 17—Closed due to error
  - 18—Closed due to rekey

- 1-15, 19-31—Reserved and unused

- **message**—A text message from the SVC

**Recommended Action** None required.

## 722014

**Error Message** %ASA-6-722014: Group *group* User *user-name* IP *IP\_address* SVC Message: *type-num*  
/INFO: *message*

**Explanation** The SVC issued a message.

- **type-num**— A number from 0 to 31 indicating a message type. Message types are as follows:

- 0—Normal.

- 16—Logout

- 17—Closed due to error

- 18—Closed due to rekey

- 1-15, 19-31—Reserved and unused

- **message**—A text message from the SVC

**Recommended Action** None required.

## 722015

**Error Message** %ASA-4-722015: Group *group* User *user-name* IP *IP\_address* Unknown SVC frame  
type: *type-num*

**Explanation** The SVC sent an invalid frame type to the device, which might be caused by an SVC version incompatibility.

- **type-num**—The number identifier of the frame type

**Recommended Action** Verify the SVC version.

## 722016

**Error Message** %ASA-4-722016: Group *group* User *user-name* IP *IP\_address* Bad SVC frame length:  
*length* expected: *expected-length*

**Explanation** The expected amount of data was not available from the SVC, which might be caused by an SVC version incompatibility.

**Recommended Action** Verify the SVC version.

## 722017

**Error Message** %ASA-4-722017: Group *group* User *user-name* IP *IP\_address* Bad SVC framing:  
525446, reserved: 0

**Explanation** The SVC sent a badly framed datagram, which might be caused by an SVC version incompatibility.

**Recommended Action** Verify the SVC version.

## 722018

**Error Message** %ASA-4-722018: Group *group* User *user-name* IP *IP\_address* Bad SVC protocol version: *version* , expected: *expected-version*

**Explanation** The SVC sent a version unknown to the device, which might be caused by an SVC version incompatibility.

**Recommended Action** Verify the SVC version.

## 722019

**Error Message** %ASA-4-722019: Group *group* User *user-name* IP *IP\_address* Not enough data for an SVC header: *length*

**Explanation** The expected amount of data was not available from the SVC, which might be caused by an SVC version incompatibility.

**Recommended Action** Verify the SVC version.

## 722020

**Error Message** %ASA-3-722020: TunnelGroup *tunnel\_group* GroupPolicy *group\_policy* User *user-name* IP *IP\_address* No address available for SVC connection

**Explanation** Address assignment failed for the AnyConnect session. No IP addresses are available.

- **tunnel\_group**—The name of the tunnel group that the user was assigned to or used to log in
- **group\_policy**—The name of the group policy that the user was assigned to
- **user-name**—The name of the user with which this message is associated
- **IP\_address**—The public IP (Internet) address of the client machine

**Recommended Action** Check the configuration listed in the **ip local ip** command to see if enough addresses exist in the pools that have been assigned to the tunnel group and the group policy. Check the DHCP configuration and status. Check the address assignment configuration. Enable IPAA syslog messages to determine why the AnyConnect client cannot obtain an IP address.

## 722021

**Error Message** %ASA-3-722021: Group *group* User *user-name* IP *IP\_address* Unable to start compression due to lack of memory resources

**Explanation** There is not enough memory to perform the action.

**Recommended Action** Purchase more memory, upgrade the device, or reduce the load on the device.



## 722022

**Error Message** %ASA-6-722022: Group *group-name* User *user-name* IP *addr* (TCP | UDP) connection established (with | without) compression

**Explanation** The TCP or UDP connection was established with or without compression.

**Recommended Action** None required.

## 722023

**Error Message** %ASA-6-722023: Group *group* User *user-name* IP *IP\_address* SVC connection terminated {with|without} compression

**Explanation** The SVC terminated either with or without compression.

**Recommended Action** None required.

## 722024

**Error Message** %ASA-6-722024: SVC Global Compression Enabled

**Explanation** Subsequent SVC connections will be allowed to perform tunnel compression if SVC compression is enabled in the corresponding user or group configuration.

**Recommended Action** None required.

## 722025

**Error Message** %ASA-6-722025: SVC Global Compression Disabled

**Explanation** Subsequent SVC connections will not be allowed to perform tunnel compression.

**Recommended Action** None required.

## 722026

**Error Message** %ASA-6-722026: Group *group* User *user-name* IP *IP\_address* SVC compression history reset

**Explanation** A compression error occurred. The SVC and the ASA corrected it.

**Recommended Action** None required.

## 722027

**Error Message** %ASA-6-722027: Group *group* User *user-name* IP *IP\_address* SVC decompression history reset

**Explanation** A decompression error occurred. The SVC and the ASA corrected it.

**Recommended Action** None required.

## 722028

**Error Message** %ASA-5-722028: Group *group* User *user-name* IP *IP\_address* Stale SVC connection closed.

**Explanation** An unused SVC connection was closed.

**Recommended Action** None required. However, the client may be having trouble connecting if multiple connections are established. The SVC log should be examined.

## 722029

**Error Message** %ASA-7-722029: Group *group* User *user-name* IP *IP\_address* SVC Session Termination: Conns: *connections* , DPD Conns: *DPD\_conns* , Comp resets: *compression\_resets* , Dcmp resets: *decompression\_resets*

**Explanation** The number of connections, reconnections, and resets that have occurred are reported. If **connections** is greater than 1 or the number of **DPD\_conns**, **compression\_resets**, or **decompression\_resets** is greater than 0, it may indicate network reliability problems, which may be beyond the control of the Secure Firewall ASA administrator. If there are many connections or DPD connections, the user may be having problems connecting and may experience poor performance.

- **connections**—The total number of connections during this session (one is normal)
- **DPD\_conns**—The number of reconnections due to DPD
- **compression\_resets**—The number of compression history resets
- **decompression\_resets**—The number of decompression history resets

**Recommended Action** The SVC log should be examined. You may want to research and take appropriate action to resolve possible network reliability problems.

## 722030

**Error Message** %ASA-7-722030: Group *group* User *user-name* IP *IP\_address* SVC Session Termination: In: *data\_bytes* (+*ctrl\_bytes* ) bytes, *data\_pkts* (+*ctrl\_pkts* ) packets, *drop\_pkts* drops

**Explanation** End-of-session statistics are being recorded.

- **data\_bytes**—The number of inbound (from SVC) data bytes
- **ctrl\_bytes**—The number of inbound control bytes
- **data\_pkts**—The number of inbound data packets
- **ctrl\_pkts**—The number of inbound control packets
- **drop\_pkts**—The number of inbound packets that were dropped

**Recommended Action** None required.

## 722031

**Error Message** %ASA-7-722031: Group *group* User *user-name* IP *IP\_address* SVC Session Termination: Out: *data\_bytes* (+*ctrl\_bytes* ) bytes, *data\_pkts* (+*ctrl\_pkts* ) packets, *drop\_pkts* drops.

**Explanation** End-of-session statistics are being recorded. The statistics include data bytes, control packet bytes, data packets, control packets, and dropped packets.

- **data\_bytes**—The number of outbound (to SVC) data bytes
- **ctrl\_bytes**—The number of outbound control bytes
- **data\_pkts**—The number of outbound data packets
- **ctrl\_pkts**—The number of outbound control packets
- **drop\_pkts**—The number of outbound packets that were dropped

In some cases, the dropped packets count is more than the overall data and control packets because this syslog does not provide the break-down of the dropped packets. Few examples of such instances:

```
2020-09-30T09:06:09.254798+00:00 local4.err pg122d-vpn116 %ASA-3-722031: Group <GP_1> User
<xxxxxxxxxxxxx.xxxxxxxxxxx@intel.com> IP <x.x.x.x> SVC Session Termination: Out: 800808 (+32)
bytes, 1957 (+4) packets, 3358 drops.
```

```
2020-09-30T08:53:11.359833+00:00 local4.err srr10c-vpn103 %ASA-3-722031: Group <GP_2> User
<xxxxxxxxxxxxx.xxxxxxxxxxx@intel.com> IP <x.x.x.x> SVC Session Termination: Out: 413194 (+32)
bytes, 1540 (+4) packets, 2059 drops.
```

```
2020-09-30T08:37:59.287415+00:00 local4.err srr10c-vpn115 %ASA-3-722031: Group <GP_3> User
<xxxxxxxxxxxxx.xxxxxxxxxxx@intel.com> IP <x.x.x.x> SVC Session Termination: Out: 571473 (+48)
bytes, 1283 (+6) packets, 1323 drops.
```

```
2020-09-30T08:31:48.105943+00:00 local4.err srr10c-vpn114 %ASA-3-722031: Group <GP_4> User
<xxxxxxxxxxxxx.xxxxxxxxxxx@intel.com> IP <x.x.x.x> SVC Session Termination: Out: 131566 (+0)
bytes, 283 (+0) packets, 320 drops.
```

```
2020-09-30T08:28:38.053003+00:00 local4.err pg122d-vpn117 %ASA-3-722031: Group <GP_5> User
<xxxxxxxxxxxxx.xxxxxxxxxxx@intel.com> IP <x.x.x.x> SVC Session Termination: Out: 497446 (+23)
bytes, 1048 (+1) packets, 1128 drops.
```

```
2020-09-30T07:45:43.044373+00:00 local4.err srr10c-vpn114 %ASA-3-722031: Group <GP_6> User
<xxxxxxxxxxxxx.xxxxxxxxxxx@intel.com> IP <x.x.x.x> SVC Session Termination: Out: 153165 (+16)
bytes, 398 (+2) packets, 1045 drops.
```

**Recommended Action** None required.

## 722032

**Error Message** %ASA-5-722032: Group *group* User *user-name* IP *IP\_address* New SVC connection replacing old connection.

**Explanation** A new SVC connection is replacing an existing one. You may be having trouble connecting.

**Recommended Action** Examine the SVC log.

## 722033

**Error Message** %ASA-5-722033: Group *group* User *user-name* IP *IP\_address* First SVC connection established for SVC session.

**Explanation** The first SVC connection was established for the SVC session.

**Recommended Action** None required.

## 722034

**Error Message** %ASA-5-722034: Group *group* User *user-name* IP *IP\_address* New SVC connection, no existing connection.

**Explanation** A reconnection attempt has occurred. An SVC connection is replacing a previously closed connection. There is no existing connection for this session because the connection was already dropped by the SVC or the Secure Firewall ASA. You may be having trouble connecting.

**Recommended Action** Examine the Secure Firewall ASA log and SVC log.

## 722035

**Error Message** %ASA-3-722035: Group *group* User *user-name* IP *IP\_address* Received large packet *length* (threshold *num* ).

**Explanation** A large packet was received from the client.

- **length**—The length of the large packet
- **num**—The threshold

**Recommended Action** Enter the **anyconnect ssl df-bit-ignore enable** command under the group policy to allow the Secure Firewall ASA to fragment the packets arriving with the DF bit set.

## 722036

**Error Message** %ASA-6-722036: Group *group* User *user-name* IP *IP\_address* Transmitting large packet *length* (threshold *num* ).

**Explanation** A large packet was sent to the client. The source of the packet may not be aware of the MTU of the client. This could also be due to compression of non-compressible data.

- **length**—The length of the large packet
- **num**—The threshold

**Recommended Action** Turn off SVC compression, otherwise, none required.

## 722037

**Error Message** %ASA-5-722037: Group *group* User *user-name* IP *IP\_address* SVC closing connection: *reason* .

**Explanation** An SVC connection was terminated for the given reason. This behavior may be normal, or you may be having trouble connecting.

- **reason**—The reason that the SVC connection was terminated

**Recommended Action** Examine the SVC log.

## 722038

**Error Message** %ASA-5-722038: Group *group-name* User *user-name* IP *IP\_address* SVC terminating session: *reason* .

**Explanation** An SVC session was terminated for the given reason. This behavior may be normal, or you may be having trouble connecting.

- **reason**—The reason that the SVC session was terminated

**Recommended Action** Examine the SVC log if the reason for termination was unexpected.

## 722039

**Error Message** %ASA-4-722039: Group *group*, User *user*, IP *ip*, SVC *vpn-filter acl* is an IPv6 ACL; ACL not applied.

**Explanation** The type of ACL to be applied is incorrect. An IPv6 ACL has been configured as an IPv4 ACL through the **vpn-filter** command.

- *group* —The group policy name of the user
- *user* —The username
- *ip* —The public (not assigned) IP address of the user
- *acl* —The name of the invalid ACL

**Recommended Action** Validate the VPN filter and IPv6 VPN filter configurations on the ASA, and the filter parameters on the AAA (RADIUS) server. Make sure that the correct type of ACL is specified.

## 722040

**Error Message** %ASA-4-722040: Group *group*, User *user*, IP *ip*, SVC '*ipv6-vpn-filter acl*' is an IPv4 ACL; ACL not applied

**Explanation** The type of ACL to be applied is incorrect. An IPv4 ACL has been configured as an IPv6 ACL through the **ipv6-vpn-filter** command.

- *group* —The group policy name of the user
- *user* —The username
- *ip* —The public (not assigned) IP address of the user
- *acl* —The name of the invalid ACL

**Recommended Action** Validate the VPN filter and IPv6 VPN filter configurations on the ASA and the filter parameters on the AAA (RADIUS) server. Make sure that the correct type of ACL is specified.

## 722041

**Error Message** %ASA-4-722041: TunnelGroup *tunnel\_group* GroupPolicy *group\_policy* User *username* IP *peer\_address* No IPv6 address available for SVC connection.

**Explanation** An IPv6 address was not available for assignment to the remote SVC client.

- *n* —The SVC connection identifier

**Recommended Action** Augment or create an IPv6 address pool, if desired.

## 722042

**Error Message** %ASA-4-722042: Group *group* User *user* IP *ip* Invalid Cisco SSL Tunneling Protocol version.

**Explanation** An invalid SVC or AnyConnect client is trying to connect.

- *group* —The name of the group policy with which the user is trying to connect
- *user* —The name of the user who is trying to connect
- *ip* —The IP address of the user who is trying to connect

**Recommended Action** Validate that the SVC or AnyConnect client is compatible with the Secure Firewall ASA.

## 722043

**Error Message** %ASA-5-722043: Group *group* User *user* IP *ip* DTLS disabled: unable to negotiate cipher.

**Explanation** The DTLS (UDP transport) cannot be established. The SSL encryption configuration was probably changed.

- *group* —The name of the group policy with which the user is trying to connect
- *user* —The name of the user who is trying to connect
- *ip* —The IP address of the user who is trying to connect

**Recommended Action** Revert the SSL encryption configuration. Make sure there is at least one block cipher (AES, DES, or 3DES) in the SSL encryption configuration.

## 722044

**Error Message** %ASA-5-722044: Group *group* User *user* IP *ip* Unable to request *ver* address for SSL tunnel.

**Explanation** An IP address cannot be requested because of low memory on the Secure Firewall ASA.

- *group* —The name of the group policy with which the user is trying to connect
- *user* —The name of the user who is trying to connect
- *ip* —The IP address of the user who is trying to connect
- *ver* —Either IPv4 or IPv6, based on the IP address version being requested

**Recommended Action** Reduce the load on the Secure Firewall ASA or add more memory.

## 722045

**Error Message** %ASA-3-722045: Connection terminated: no SSL tunnel initialization data.

**Explanation** Data to establish a connection is missing. This is a defect in the Secure Firewall ASA software.

**Recommended Action** Contact the Cisco TAC for assistance.

## 722046

**Error Message** %ASA-3-722046: Group *group* User *user* IP *ip* Session terminated: unable to establish tunnel.

**Explanation** The Secure Firewall ASA cannot set up connection parameters. This is a defect in the Secure Firewall ASA software.

- *group* —The name of the group policy with which the user is trying to connect
- *user* —The name of the user who is trying to connect
- *ip* —The IP address of the user who is trying to connect

**Recommended Action** Contact the Cisco TAC for assistance.

## 722047

**Error Message** %ASA-4-722047: Group *group* User *user* IP *ip* Tunnel terminated: SVC not enabled or invalid SVC image on the ASA.

**Explanation** The user logged in via the web browser and tried to start the SVC or AnyConnect client. The SVC service is not enabled globally, or the SVC image is invalid or corrupted. The tunnel connection has been terminated, but the clientless connection remains.

- *group* —The name of the group policy with which the user is trying to connect
- *user* —The name of the user who is trying to connect
- *ip* —The IP address of the user who is trying to connect

**Recommended Action** Enable the SVC globally using the **svc enable** command. Validate the integrity of versions of the SVC images by reloading new images using the **svc image** command.

## 722048

**Error Message** %ASA-4-722048: Group *group* User *user* IP *ip* Tunnel terminated: SVC not enabled for the user.

**Explanation** The user logged in via the web browser, and tried to start the SVC or AnyConnect client. The SVC service is not enabled for this user. The tunnel connection has been terminated, but the clientless connection remains.

- *group* —The name of the group policy with which the user is trying to connect
- *user* —The name of the user who is trying to connect
- *ip* —The IP address of the user who is trying to connect

**Recommended Action** Enable the service for this user using the **group-policy** and **username** commands.

## 722049

**Error Message** %ASA-4-722049: Group *group* User *user* IP *ip* Session terminated: SVC not enabled or invalid image on the ASA.

**Explanation** The user logged in via the AnyConnect client. The SVC service is not enabled globally, or the SVC image is invalid or corrupted. The session connection has been terminated.

- *group* —The name of the group policy with which the user is trying to connect
- *user* —The name of the user who is trying to connect
- *ip* —The IP address of the user who is trying to connect

**Recommended Action** Enable the SVC globally using the **svc-enable** command. Validate the integrity and versions of the SVC images by reloading new images using the **svc image** command.

## 722050

**Error Message** %ASA-4-722050: Group *group* User *user* IP *ip* Session terminated: SVC not enabled for the user.

**Explanation** The user logged in through the AnyConnect client. The SVC service is not enabled for this user. The session connection has been terminated.

- *group* —The name of the group policy with which the user is trying to connect
- *user* —The name of the user who is trying to connect
- *ip* —The IP address of the user who is trying to connect

**Recommended Action** Enable the service for this user using the **group-policy** and **username** commands.

## 722051

**Error Message** %ASA-6-722051: Group *group-policy* User *username* IP *public-ip* IPv4 Address *assigned-ip* IPv6 Address *assigned-ip* assigned to session

**Explanation** The specified address has been assigned to the given user.

- *group-policy* —The group policy that allowed the user to gain access
- *username* —The name of the user
- *public-ip* —The public IP address of the connected client
- *assigned-ip* —The IPv4 or IPv6 address that is assigned to the client

**Recommended Action** None required.

## 722053

**Error Message** %ASA-6-722053: Group *g* User *u* IP *ip* Unknown client *user-agent* connection.

**Explanation** An unknown or unsupported SSL VPN client has connected to the Secure Firewall ASA. Older clients include the Cisco SVC and the Cisco AnyConnect client earlier than Version 2.3.1.

- *g* —The group policy under which the user logged in
- *u* —The name of the user
- *ip* —The IP address of the client
- *user-agent* —The user agent (usually includes the version) received from the client

**Recommended Action** Upgrade to a supported Cisco SSL VPN client.

## 722054

**Error Message** %ASA-4-722054: Group *group policy* User *user name* IP *remote IP* SVC terminating connection: Failed to install Redirect URL: *redirect URL* Redirect ACL: *non\_exist* for *assigned IP*

**Explanation** An error occurred for an AnyConnect VPN connection when a redirect URL was installed, and the ACL was received from the ISE, but the redirect ACL does not exist on the Secure Firewall ASA.

- *group policy* —The group policy that allowed the user to gain access
- *user name* —Username of the requester for the remote access



- *remote IP* — Remote IP address that the connection request is coming from
- *redirect URL* —The URL for the HTTP traffic redirection
- *assigned IP* —The IP address that is assigned to the user

**Recommended Action** Configure the redirect ACL on the Secure Firewall ASA.

## 722055

**Error Message** %ASA-6-722055: Group *group-policy* User *username* IP *public-ip* Client Type: *user-agent*

**Explanation** The indicated user is attempting to connect with the given user-agent.

- *group-policy* —The group policy that allowed the user to gain access
- *username* —The name of the user
- *public-ip* —The public IP address of the connected client
- *user-agent* —The user-agent string provided by the connecting client. Usually includes the AnyConnect version and host operating system for AnyConnect clients.

**Recommended Action** None required.

## 722056

**Error Message** %ASA-4-722055: Unsupported AnyConnect client connection rejected from ip address. Client info: user-agent string. Reason: reason

**Explanation** This syslog indicates that an AnyConnect client connection is rejected. The reason for this is provided in the syslog along with the client information.

- *ip address* —IP address from which a connection with the old client is attempted,
- *user-agent string* —User-Agent header in the client request. Usually includes the AnyConnect version and host operating system for AnyConnect clients
- *reason* —Reason for rejection

**Recommended Action** Use the client information and reason provided in the syslog to resolve the issue.

## Messages 723001 to 736001

This section includes messages from 723001 to 736001.

### 723001

**Error Message** %ASA-6-723001: Group *group-name* , User *user-name* , IP *IP\_address* : WebVPN Citrix ICA connection *connection* is up.

**Explanation** The Citrix connection is up.

- **group-name**—The name of the Citrix group
- **user-name**—The name of the Citrix user
- **IP\_address**—The IP address of the Citrix user
- **connection**—The Citrix connection identifier

**Recommended Action** None required.

## 723002

**Error Message** %ASA-6-723002: Group *group-name* , User *user-name* , IP *IP\_address* : WebVPN Citrix ICA connection *connection* is down.

**Explanation** The Citrix connection is down.

- **group-name**—The name of the Citrix group
- **user-name**—The name of the Citrix user
- **IP\_address**—The IP address of the Citrix user
- **connection**—The Citrix connection identifier

**Recommended Action** No action is required when the Citrix ICA connection is terminated intentionally by the client, the server, or the Secure Firewall ASA administrator. However, if this is not the case, verify that the WebVPN session in which the Citrix ICA connection is set up is still active. If it is inactive, then receiving this message is normal. If the WebVPN session is still active, verify that the ICA client and Citrix server both work correctly and that there is no error displayed. If not, bring either or both up or respond to any error. If this message is still received, contact the Cisco TAC and provide the following information:

- Network topology
- Delay and packet loss
- Citrix server configuration
- Citrix ICA client information
- Steps to reproduce the problem
- Complete text of all associated messages

## 723003

**Error Message** %ASA-7-723003: No memory for WebVPN Citrix ICA connection *connection* .

**Explanation** The Secure Firewall ASA is running out of memory. The Citrix connection was rejected.

- **connection**—The Citrix connection identifier

**Recommended Action** Verify that the Secure Firewall ASA is working correctly. Pay special attention to memory and buffer usage. If the Secure Firewall ASA is under heavy load, buy more memory and upgrade the Secure Firewall ASA or reduce the load on the Secure Firewall ASA. If the problem persists, contact the Cisco TAC.

## 723004

**Error Message** %ASA-7-723004: WebVPN Citrix encountered bad flow control *flow* .

**Explanation** The Secure Firewall ASA encountered an internal flow control mismatch, which can be caused by massive data flow, such as might occur during stress testing or with a high volume of ICA connections.

**Recommended Action** Reduce ICA connectivity to the Secure Firewall ASA. If the problem persists, contact the Cisco TAC.

## 723005

**Error Message** %ASA-7-723005: No channel to set up WebVPN Citrix ICA connection.

**Explanation** The Secure Firewall ASA was unable to create a new channel for Citrix.

**Recommended Action** Verify that the Citrix ICA client and the Citrix server are still alive. If not, bring them back up and retest. Check the Secure Firewall ASA load, paying special attention to memory and buffer usage. If the Secure Firewall ASA is under heavy load, upgrade the Secure Firewall ASA, add memory, or reduce the load. If the problem persists, contact the Cisco TAC.

## 723006

**Error Message** %ASA-7-723006: WebVPN Citrix SOCKS errors.

**Explanation** An internal Citrix SOCKS error has occurred on the Secure Firewall ASA.

**Recommended Action** Verify that the Citrix ICA client is working correctly. In addition, check the network connection status between the Citrix ICA client and the Secure Firewall ASA, paying attention to packet loss. Resolve any abnormal network conditions. If the problem persists, contact the Cisco TAC.

## 723007

**Error Message** %ASA-7-723007: WebVPN Citrix ICA connection *connection* list is broken.

**Explanation** The Secure Firewall ASA internal Citrix connection list is broken.

- **connection**—The Citrix connection identifier

**Recommended Action** Verify that the Secure Firewall ASA is working correctly, paying special attention to memory and buffer usage. If the Secure Firewall ASA is under heavy load, upgrade the Secure Firewall ASA, add memory, or reduce the load. If the problem persists, contact the Cisco TAC.

## 723008

**Error Message** %ASA-7-723008: WebVPN Citrix ICA SOCKS Server *server* is invalid.

**Explanation** An attempt was made to access a Citrix Socks server that does not exist.

- **server**—The Citrix server identifier

**Recommended Action** Verify that the Secure Firewall ASA is working correctly. Note whether or not there is any memory or buffer leakage. If this issue occurs frequently, capture information about memory usage, network topology, and the conditions during which this message is received. Send this information to the Cisco TAC for review. Make sure that the WebVPN session is still up while this message is being received. If not, determine the reason that the WebVPN session is down. If the Secure Firewall ASA is under heavy load, upgrade the Secure Firewall ASA, add memory, or reduce the load. If the problem persists, contact the Cisco TAC.

## 723009

**Error Message** %ASA-7-723009: Group *group-name* , User *user-name* , IP *IP\_address* : WebVPN Citrix received data on invalid connection *connection* .

**Explanation** Data was received on a Citrix connection that does not exist.

- **group-name**—The name of the Citrix group
- **user-name**—The name of the Citrix user
- **IP\_address**—The IP address of the Citrix user
- **connection**—The Citrix connection identifier

**Recommended Action** The original published Citrix application connection was probably terminated, and the remaining active published applications lost connectivity. Restart all published applications to generate a new Citrix ICA tunnel. If the Secure Firewall ASA is under heavy load, upgrade the Secure Firewall ASA, add memory, or reduce the load. If the problem persists, contact the Cisco TAC.

## 723010

**Error Message** %ASA-7-723010: Group *group-name* , User *user-name* , IP *IP\_address* : WebVPN Citrix received closing channel *channel* for invalid connection *connection* .

**Explanation** An abort was received on a nonexistent Citrix connection, which can be caused by massive data flow (such as stress testing) or a high volume of ICA connections, especially during network delay or packet loss.

- **group-name**—The name of the Citrix group
- **user-name**—The name of the Citrix user
- **IP\_address**—The IP address of the Citrix user
- **channel**—The Citrix channel identifier
- **connection**—The Citrix connection identifier

**Recommended Action** Reduce the number of ICA connections to the Secure Firewall ASA, obtain more memory for the Secure Firewall ASA, or resolve the network problems.

## 723011

**Error Message** %ASA-7-723011: Group *group-name* , User *user-name* , IP *IP\_address* : WebVPN Citrix receives bad SOCKS *socks* message length *msg-length*. Expected length is *exp-msg-length* .

**Explanation** The Citrix SOCKS message length is incorrect.

- **group-name**—The name of the Citrix group
- **user-name**—The name of the Citrix user
- **IP\_address**—The IP address of the Citrix user

**Recommended Action** Verify that the Citrix ICA client is working correctly. In addition, check the network connection status between the ICA client and the Secure Firewall ASA, paying attention to packet loss. After resolving any abnormal network conditions, if the problem still exists, contact the Cisco TAC.

## 723012

**Error Message** %ASA-7-723012: Group *group-name* , User *user-name* , IP *IP\_address* : WebVPN Citrix received bad SOCKS *socks* message format.

**Explanation** The Citrix SOCKS message format is incorrect.

- **group-name**—The name of the Citrix group
- **user-name**—The name of the Citrix user
- **IP\_address**—The IP address of the Citrix user

**Recommended Action** Verify that the Citrix ICA client is working correctly. In addition, check the network connection status between the ICA client and the Secure Firewall ASA, paying attention to packet loss. After resolving any abnormal network conditions, if the problem still exists, contact the Cisco TAC.

## 723013

**Error Message** %ASA-7-723013: WebVPN Citrix encountered invalid connection *connection* during periodic timeout.

**Explanation** The Secure Firewall ASA internal Citrix timer has expired, and the Citrix connection is invalid.

- **connection**—The Citrix connection identifier

**Recommended Action** Check the network connection between the Citrix ICA client and the Secure Firewall ASA, and between the Secure Firewall ASA and the Citrix server. Resolve any abnormal network conditions, especially delay and packet loss. Verify that the Secure Firewall ASA works correctly, paying special attention to memory or buffer problems. If the Secure Firewall ASA is under heavy load, obtain more memory, upgrade the Secure Firewall ASA, or reduce the load. If the problem persists, contact the Cisco TAC.

## 723014

**Error Message** %ASA-7-723014: Group *group-name* , User *user-name* , IP *IP\_address* : WebVPN Citrix TCP connection *connection* to server *server* on channel *channel* initiated.

**Explanation** The Secure Firewall ASA internal Citrix Secure Gateway is connected to the Citrix server.

- **group-name**—The name of the Citrix group
- **user-name**—The name of the Citrix user
- **IP\_address**—The IP address of the Citrix user
- **connection**—The connection name
- **server**—The Citrix server identifier
- **channel**—The Citrix channel identifier (hexadecimal)

**Recommended Action** None required.

## 724001

**Error Message** %ASA-4-724001: Group *group-name* User *user-name* IP *IP\_address* WebVPN session not allowed. Unable to determine if Cisco Secure Desktop was running on the client's workstation.

**Explanation** The session was not allowed because an error occurred during processing of the CSD Host Integrity Check results on the Secure Firewall ASA.

- **group-name**—The name of the group
- **user-name**—The name of the user
- **IP\_address**—The IP address

**Recommended Action** Determine whether the client firewall is truncating long URLs. Uninstall CSD from the client and reconnect to the Secure Firewall ASA.

## 724002

**Error Message** %ASA-4-724002: Group *group-name* User *user-name* IP *IP\_address* WebVPN session not terminated. Cisco Secure Desktop was not running on the client's workstation.

**Explanation** CSD is not running on the client machine.

- **group-name**—The name of the group
- **user-name**—The name of the user
- **IP\_address**—The IP address

**Recommended Action** Verify that the end user can install and run CSD on the client machine.

## 725001

**Error Message** %ASA-6-725001: Starting SSL handshake with *peer-type* interface *:src-ip /src-port* to *dst-ip /dst-port* for *protocol* session.

**Explanation** The SSL handshake has started with the remote device, which can be a client or server.

- **peer-type**—Either the server or the client, depending on the device that initiated the connection
- **interface**—The interface name that the SSL session is using
- **source-ip**—The source IPv4 or IPv6 address
- **src-port**—The source port number
- **dst-ip**—The destination IP address
- **dst-port**—The destination port number
- **protocol**—The SSL version used for the SSL handshake

**Recommended Action** None required.

## 725002

**Error Message** %ASA-6-725002: Device completed SSL handshake with *peer-type* interface *:src-ip /src-port* to *dst-ip /dst-port* for *protocol-version* session

**Explanation** The SSL handshake has completed successfully with the remote device.

- **peer-type**—Either the server or the client, depending on the device that initiated the connection
- **interface**—The interface name that the SSL session is using
- **source-ip**—The source IPv4 or IPv6 address
- **src-port**—The source port number
- *dst-ip*—The destination IP address
- *dst-port*—The destination port number
- *protocol-version*—The version of the SSL protocol being used: SSLv3, TLSv1, DTLSv1, DTLSv1.2, TLSv1.1 or TLSv1.2

**Recommended Action** None required.

## 725003

**Error Message** %ASA-6-725003: SSL *peer-type interface :src-ip /src-port to dst-ip /dst-port* request to resume previous session.

**Explanation** The remote device is trying to resume a previous SSL session.

- **peer-type**—Either the server or the client, depending on the device that initiated the connection
- **interface**—The interface name that the SSL session is using
- **source-ip**—The source IPv4 or IPv6 address
- **src-port**—The source port number
- *dst-ip* —The destination IP address
- *dst-port* —The destination port number

**Recommended Action** None required.

## 725004

**Error Message** %ASA-6-725004: Device requesting certificate from SSL *peer-type interface :src-ip /src-port to dst-ip /dst-port* for authentication.

**Explanation** The Secure Firewall ASA has requested a client certificate for authentication.

- **peer-type**—Either the server or the client, depending on the device that initiated the connection
- **interface**—The interface name that the SSL session is using
- **source-ip**—The source IPv4 or IPv6 address
- **src-port**—The source port number
- *dst-ip* —The destination IP address
- *dst-port* —The destination port number

**Recommended Action** None required.

## 725005

**Error Message** %ASA-6-725005: SSL *peer-type interface :src-ip /src-port to dst-ip /dst-port* requesting our device certificate for authentication.

**Explanation** The server has requested the certificate of the Secure Firewall ASA for authentication.

- **peer-type**—Either the server or the client, depending on the device that initiated the connection
- **interface**—The interface name that the SSL session is using
- **source-ip**—The source IPv4 or IPv6 address
- **src-port**—The source port number
- *dst-ip* —The destination IP address
- *dst-port* —The destination port number

**Recommended Action** None required.

## 725006

**Error Message** %ASA-6-725006: Device failed SSL handshake with *peer-type interface :src-ip /src-port to dst-ip /dst-port*

**Explanation** The SSL handshake with the remote device has failed.

- **peer-type**—Either the server or the client, depending on the device that initiated the connection
- **interface**—The interface name that the SSL session is using
- **source-ip**—The source IPv4 or IPv6 address
- **src-port**—The source port number
- *dst-ip* —The destination IP address
- *dst-port* —The destination port number

**Recommended Action** Look for syslog message 725014, which indicates the reason for the failure.

## 725007

**Error Message** %ASA-6-725007: SSL session with *peer-type interface :src-ip /src-port to dst-ip /dst-port* terminated.

**Explanation** The SSL session has terminated.

- **peer-type**—Either the server or the client, depending on the device that initiated the connection
- **interface**—The interface name that the SSL session is using
- **source-ip**—The source IPv4 or IPv6 address
- **src-port**—The source port number
- *dst-ip* —The destination IP address
- *dst-port* —The destination port number

**Recommended Action** None required.

## 725008

**Error Message** %ASA-7-725008: SSL *peer-type interface :src-ip /src-port to dst-ip /dst-port* proposes the following *n* cipher(s).

**Explanation** The number of ciphers proposed by the remote SSL device are listed.

- **peer-type**—Either the server or the client, depending on the device that initiated the connection
- **interface**—The interface name that the SSL session is using
- **source-ip**—The source IPv4 or IPv6 address
- **src-port**—The source port number
- *dst-ip* —The destination IP address
- *dst-port* —The destination port number
- *n* —The number of supported ciphers

**Recommended Action** None required.

## 725009

**Error Message** %ASA-7-725009 Device proposes the following *n* cipher(s) *peer-type interface :src-ip /src-port to dst-ip /dst-port* .

**Explanation** The number of ciphers proposed to the SSL server are listed.

- **peer-type**—Either the server or the client, depending on the device that initiated the connection



- **interface**—The interface name that the SSL session is using
- **source-ip**—The source IPv4 or IPv6 address
- **src-port**—The source port number
- *dst-ip*—The destination IP address
- *dst-port*—The destination port number
- *n*—The number of supported ciphers

**Recommended Action** None required.

## 725010

**Error Message** %ASA-7-725010: Device supports the following *n* cipher(s).

**Explanation** The number of ciphers supported by the Secure Firewall ASA for an SSL session are listed.

- *n*—The number of supported ciphers

**Recommended Action** None required.

## 725011

**Error Message** %ASA-7-725011 Cipher[*order* ]: *cipher\_name*

**Explanation** Always following messages 725008, 725009, and 725010, this message indicates the cipher name and its order of preference.

- **order**—The order of the cipher in the cipher list
- **cipher\_name**—The name of the OpenSSL cipher from the cipher list

**Recommended Action** None required.

## 725012

**Error Message** %ASA-7-725012: Device chooses cipher *cipher* for the SSL session with *peer-type* *interface* :*src-ip* /*src-port* to *dst-ip* /*dst-port*.

**Explanation** The cipher that was chosen by the Cisco device for the SSL session is listed.

- **cipher**—The name of the OpenSSL cipher from the cipher list
- **peer-type**—Either the server or the client, depending on the device that initiated the connection
- **interface**—The interface name that the SSL session is using
- **source-ip**—The source IPv4 or IPv6 address
- **src-port**—The source port number
- *dst-ip*—The destination IP address
- *dst-port*—The destination port number

**Recommended Action** None required.

## 725013

**Error Message** %ASA-7-725013 SSL *peer-type* *interface* :*src-ip* /*src-port* to *dst-ip* /*dst-port* chooses cipher *cipher*

**Explanation** The cipher that was chosen by the server for the SSL session is identified.

- **peer-type**—Either the server or the client, depending on the device that initiated the connection
- **interface**—The interface name that the SSL session is using
- **source-ip**—The source IPv4 or IPv6 address
- **src-port**—The source port number
- *dst-ip* —The destination IP address
- *dst-port* —The destination port number
- **cipher**—The name of the OpenSSL cipher from the cipher list

**Recommended Action** None required.

## 725014

**Error Message** %ASA-7-725014 SSL lib error. Function: *function* Reason: *reason*

**Explanation** The reason for failure of the SSL handshake is indicated.

- **function**—The function name where the failure is reported
- **reason**—The description of the failure condition

**Recommended Action** Include this message when reporting any SSL-related issue to the Cisco TAC.

## 725015

**Error Message** %ASA-3-725015 Error verifying client certificate. Public key size in client certificate exceeds the maximum supported key size.

**Explanation** The verification of an SSL client certificate failed because of an unsupported (large) key size.

**Recommended Action** Use client certificates with key sizes that are less than or equal to 4096 bits.

## 725016

**Error Message** %ASA-6-725016: Device selects trust-point *trustpoint* for *peer-type* interface *:src-ip /src-port* to *dst-ip /dst-port*

**Explanation** With server-name indication (SNI), the certificate used for a given connection may not be the certificate configured on the interface. There is also no indication of which certificate trustpoint has been selected. This syslog gives an indication of the trustpoint used by the connection (given by *interface :src-ip /src-port*).

- *trustpoint* —The name of the configured trustpoint that is being used for the specified connection
- *interface* —The name of the interface on the Secure Firewall ASA
- *src-ip* —The IP address of the peer
- *src-port* —The port number of the peer
- *dst-ip* —The IP address of the destination
- *dst-port* —The port number of the destination

**Recommended Action** None required.

## 725017

**Error Message** %ASA-7-725017: No certificates received during the handshake with %s %s :%B /%d to %B /%d for %s session

**Explanation** A remote client has not sent a valid certificate.

- *remote\_device* —Identifies whether a handshake is performed with the client or server
- *ctm->interface* —The interface name on which the handshake is sent
- *ctm->src\_ip* —The IP address of the SSL server, which will communicate with the client
- *ctm->src\_port* —The port of the SSL server, which will communicate with the client
- *ctm->dst\_ip* —The IP address of the client
- *ctm->dst\_port* —The port of the client through which it responds
- *s->method->version* —The protocol version involved in the transaction (SSLv3, TLSv1, or DTLSv1)

**Recommended Action** None required.

## 725021

**Error Message** %ASA-7-725021: Device preferring *cipher-suite* cipher(s). Connection info: *interface :src-ip /src-port to dst-ip /dst-port*

**Explanation** The cipher suites being preferred when negotiating the handshake is listed in this message.

- **cipher-suite**—Preferred cipher suite string
- **interface**—The interface name that the SSL session is using
- **src-ip**—The source IPv4 or IPv6 address
- **src-port**—The source port number
- **dst-ip**—The destination IPv4 or IPv6 address
- **dst-port**—The destination port number

Following is a list of preferred cipher suite strings that are used when negotiating the handshake:

- server
- SUITE-B
- ChaCha20
- client
- SHA-256 hash

**Recommended Action** None required.

## 725022

**Error Message** %ASA-7-725022: Device skipping cipher : *cipher - reason*. Connection info: *interface :src-ip /src-port to dst-ip /dst-port*

**Explanation** This syslog displays the reason for skipping a particular cipher in a list of cipher suites when negotiating the handshake.

- **cipher-suite**—Preferred cipher suite string
- **reason**—Reason for skipping a cipher.
- **interface**—The interface name that the SSL session is using
- **src-ip**—The source IPv4 or IPv6 address
- **src-port**—The source port number
- **dst-ip**—The destination IPv4 or IPv6 address
- **dst-port**—The destination port number

Following list provides few example reason for skipping a particular cipher:

- Ephemeral EC key is not compatible with trust-point <trust point>
- Not supported by protocol version
- PSK server callback is not set
- Not permitted by security callbacks
- ECDHE-ECDSA is broken on Safari
- Cipher suite does not use SHA256
- Unknown cipher
- Wrong cipher
- Message digest changed
- Ciphersuite from previous session not selected

**Recommended Action** None required.

## 725025

**Error Message** %ASA-6-725025: SSL Pre-auth connection rate limit hit %s watermark

**Explanation** When the device reaches the rate-limit threshold for the number of pre-authenticated SSL connections. This message appears when the number of pre-authenticated SSL connections is high (90% of the limit) or when it is low (70% of the limit). The syslog is rate-limited to one syslog for every 10 seconds. In this message, %s denotes high or low of the threshold limit.

**Recommended Action** Contact Cisco TAC.

## 726001

**Error Message** %ASA-6-726001: Inspected *im\_protocol im\_service* Session between Client *im\_client\_1* and *im\_client\_2* Packet flow from *src\_ifc* *:/sip /sport* to *dest\_ifc* *:/dip /dport*  
Action: *action* Matched Class *class\_map\_id class\_map\_name*

**Explanation** An IM inspection was performed on an IM message and the specified criteria were satisfied. The configured action is taken.

- *im\_protocol* —MSN IM or Yahoo IM
- *im\_service* —The IM services, such as chat, conference, file transfer, voice, video, games, or unknown
- *im\_client\_1* , *im\_client\_2* —The client peers that are using the IM service in the session: *client\_login\_name* or “?”
- *src\_ifc* —The source interface name
- *sip* —The source IP address
- *sport* —The source port
- *dest\_ifc* —The destination interface name
- *dip* —The destination IP address
- *dport* —The destination port
- *action* —The action taken: reset connection, dropped connection, or received
- *class\_map\_id* —The matched class-map ID
- *class\_map\_name* —The matched class-map name

**Recommended Action** None required.

## 730001

**Error Message** %ASA-7-730001 Group *groupname* , User *username* , IP *ipaddr* : VLAN MAPPING to VLAN *vlanid*

**Explanation** VLAN mapping succeeded.

- *groupname* —The group name
- *username* —The username
- *ipaddr* —The IP address of this session
- *vlanid* — The VLAN ID that is used for the VLAN mapping session

**Recommended Action** None required.

## 730002

**Error Message** %ASA-7-730002 Group *groupname* , User *username* , IP *ipaddr* : VLAN MAPPING to VLAN *vlanid* failed

**Explanation** VLAN mapping failed.

- *groupname* —The group name
- *username* —The username
- *ipaddr* —The IP address of this session
- *vlanid* — The VLAN ID that is used for the VLAN mapping session

**Recommended Action** Verify that all the VLAN mapping-related configurations are correct, and that the VLAN ID is valid.

## 730003

**Error Message** %ASA-7-730003: NACApp sets IP *ipaddr* VLAN to *vlanid*

**Explanation** ASA receives an SNMP set message from NACApp to set the new VLAN ID for the session.

- *ipaddr* —The IP address of this session
- *vlanid* — The VLAN ID that is used for the VLAN mapping session

**Recommended Action** None required

## 730004

**Error Message** %ASA-6-730004: Group *groupname* User *username* IP *ipaddr* VLAN ID *vlanid* from AAA ignored.

**Explanation** The VLAN ID received from AAA is different from the current one in use, and it is ignored for the current session.

- *groupname* —The group name
- *username* —The username
- *ipaddr* —The IP address of this session
- *vlanid* — The VLAN ID that is used for the VLAN mapping session

**Recommended Action** If the newly received VLAN ID must be used, then the current session needs to be torn down. Otherwise, no action is required.

## 730005

**Error Message** %ASA-3-730005: Group *DfltGrpPolicy* User *username* IP VLAN Mapping error. VLAN *vlan\_id* may be out of range, unassigned to any interface or assigned to multiple interfaces

**Explanation** A VLAN mapping error has occurred. A VLAN may be out of range, unassigned to any interfaces, or assigned to multiple interfaces.

**Recommended Action** Verify the VLAN ID configurations on the AAA server and ASA are both correct.

## 730006

**Error Message** %ASA-7-730006: Group *groupname* , User *username* , IP *ipaddr* : is on NACApp AUTH VLAN *vlanid* .

**Explanation** The session is under NACApp posture assessment.

- *groupname* —The group name
- *username* —The username
- *ipaddr* —The IP address of this session
- *vlanid* — The VLAN ID that is used for the VLAN mapping session

**Recommended Action** None required.

## 730007

**Error Message** %ASA-7-730007: Group *groupname* , User *username* , IP *ipaddr* : changed VLAN to <%s > ID *vlanid*

**Explanation** NACApp (Cisco NAC appliance) posture assessment is done with the session, the VLAN is changed from AUTH VLAN to a new VLAN.

- *groupname* —The group name
- *username* —The username
- *ipaddr* —The IP address of this session
- *%s* —A string
- *vlanid* — The VLAN ID that is used for the VLAN mapping session

**Recommended Action** None required.

## 730008

**Error Message** %ASA-6-730008: Group *groupname*, User *username*, IP *ipaddr*, VLAN MAPPING timeout waiting NACApp.

**Explanation** NACApp (Cisco NAC appliance) posture assessment takes longer than the timeout value configured.

- *groupname* —The group name
- *username* —The username
- *ipaddr* —The IP address of this session

**Recommended Action** Check the status of the NACApp setup.

## 730009

**Error Message** %ASA-5-730009: Group *groupname*, User *username*, IP *ipaddr*, CAS *casaddr*, capacity exceeded, terminating connection.

**Explanation** The load capacity of the NACApp (Cisco NAC appliance) CAS is exceeded, the new incoming session that uses it is terminating.

- *groupname* —The group name
- *username* —The username
- *ipaddr* —The IP address of this session
- *casaddr* —The IP Address of CAS (Clean Access Server)

**Recommended Action** Review and revise planning for how many groups, and which groups, are associated with the CAS to ensure that its load capacity is not exceeded.

## 730010

**Error Message** %ASA-7-730010: Group *groupname*, User *username*, IP *ipaddr*, VLAN Mapping is enabled on VLAN *vlanid*.

**Explanation** VLAN mapping is enabled in the session.

- *groupname* —The group name
- *username* —The username
- *ipaddr* —The IP address of this session
- *vlanid* —The VLAN ID that is used for the VLAN mapping session

**Recommended Action** None required.

## 731001

**Error Message** %ASA-6-731001: NAC policy added: name: *policyname* Type: *policytype* .

**Explanation** A new NAC-policy has been added to the ASA.

- **policyname**—The NAC policy name
- **policytype**—The type of NAC policy

**Recommended Action** None required.

## 731002

**Error Message** %ASA-6-731002: NAC policy deleted: name: *policyname* Type: *policytype* .

**Explanation** A NAC policy has been removed from the ASA.

- **policyname**—The NAC policy name
- **policytype**—The type of NAC policy

**Recommended Action** None required.

## 731003

**Error Message** %ASA-6-731003: nac-policy unused: name: *policyname* Type: *policytype* .

**Explanation** The NAC policy is unused because there is an existing NAC policy with the same name, but a different type.

- **policyname**—The NAC policy name
- **policytype**—The type of NAC policy

**Recommended Action** If the new NAC policy must be used, the existing NAC policy must be removed first. Otherwise, no action is required.

## 732001

**Error Message** %ASA-6-732001: Group *groupname*, User *username*, IP *ipaddr*, Fail to parse NAC-SETTINGS *nac-settings-id* , terminating connection.

**Explanation** The ASA cannot apply the NAC settings because no memory is available.

- *groupname* —The group name
- *username* —The username
- *ipaddr* —The IP address of this session
- *nac-settings-id* — The ID that is used for the NAC filter

**Recommended Action** Upgrade the ASA memory. Resolve any errors in the log before this problem occurs. If the problem persists, contact the Cisco TAC.



## 732002

**Error Message** %ASA-6-732002: Group *groupname*, User *username*, IP *ipaddr*, NAC-SETTINGS *settingsid* from AAA ignored, existing NAC-SETTINGS *settingsid\_inuse* used instead.

**Explanation** The NAC settings ID cannot be applied because there is a different one for the session.

- *groupname* —The group name
- *username* —The username
- *ipaddr* —The IP address of this session
- *settingsid* — The settings ID, which should be a NAC policy name
- *settingsid\_inuse* — The NAC settings ID that is currently in use

**Recommended Action** If the new NAC settings ID must be applied, then all the active sessions that use it must be torn down first. Otherwise, no action is required.

## 732003

**Error Message** %ASA-6-732003: Group *groupname*, User *username*, IP *ipaddr*, NAC-SETTINGS *nac-settings-id* from AAA is invalid, terminating connection.

**Explanation** The NAC settings received from AAA are invalid.

- *groupname* —The group name
- *username* —The username
- *ipaddr* —The IP address of this session
- *nac-settings-id* — The ID that is used for the NAC filter

**Recommended Action** Verify that the NAC settings configurations on the AAA server and ASA are both correct.

## 733100

**Error Message** %ASA-4-733100: *Object* drop rate *rate\_ID* exceeded. Current burst rate is *rate\_val* per second, max configured rate is *rate\_val* ; Current average rate is *rate\_val* per second, max configured rate is *rate\_val* ; Cumulative total count is *total\_cnt*

**Explanation** The specified object in the message has exceeded the specified burst threshold rate or average threshold rate. The object can be a drop activity of a host, TCP/UDP port, IP protocol, or various drops caused by potential attacks. The Secure Firewall ASA may be under attack.

- *Object* —The general or particular source of a drop rate count, which might include the following:
  - Firewall
  - Bad pkts
  - Rate limit
  - DoS attack
  - ACL drop
  - Conn limit
  - ICMP attack

- Scanning
- SYN attck
- Inspect
- Interface

(A citation of a particular interface object might take a number of forms. For example, you might see 80/HTTP, which would signify port 80, with the well-known protocol HTTP.)

- *rate\_ID* —The configured rate that is being exceeded. Most objects can be configured with up to three different rates for different intervals.
- *rate\_val* —A particular rate value.
- *total\_cnt* —The total count since the object was created or cleared.

The following three examples show how these variables occur:

- For an interface drop caused by a CPU or bus limitation:

```
%ASA-4-733100: [Interface] drop rate 1 exceeded. Current burst rate is 1 per second, max
configured rate is 8000; Current average rate is 2030 per second, max configured rate is
2000; Cumulative total count is 3930654."
```

- For a scanning drop caused by potential attacks:

```
%ASA-4-733100: [Scanning] drop rate-1 exceeded. Current burst rate is 10 per second_max
configured rate is 10; Current average rate is 245 per second_max configured rate is 5;
Cumulative total count is 147409 (35 instances received)
```

- For bad packets caused by potential attacks:

```
%ASA-4-733100: [Bad pkts] drop rate 1 exceeded. Current burst rate is 0 per second, max
configured rate is 400; Current average rate is 760 per second, max configured rate is 100;
Cumulative total count is 1938933
```

- Because of the scanning rate configured and the **threat-detection rate scanning-rate 3600 average-rate 15** command:

```
%ASA-4-733100: [144.60.88.2] drop rate-2 exceeded. Current burst rate is 0 per second, max
configured rate is 8; Current average rate is 5 per second, max configured rate is 4;
Cumulative total count is 38086
```

Perform the following steps according to the specified object type that appears in the message:

1. If the object in the message is one of the following:

- Firewall
- Bad pkts
- Rate limit
- DoS attck
- ACL drop
- Conn limit
- ICMP attck
- Scanning
- SYN attck
- Inspect
- Interface

**Recommended Action** Check whether the drop rate is acceptable for the running environment.

1. Adjust the threshold rate of the particular drop to an appropriate value by using the threat-detection rate `xxx` command, where `xxx` is one of the following:
  - `acl-drop`
  - `bad-packet-drop`
  - `conn-limit-drop`
  - `dos-drop`
  - `fw-drop`
  - `icmp-drop`
  - `inspect-drop`
  - `interface-drop`
  - `scanning-threat`
  - `syn-attack`
2. If the object in the message is a TCP or UDP port, an IP address, or a host drop, check whether or not the drop rate is acceptable for the running environment.
3. Adjust the threshold rate of the particular drop to an appropriate value by using the threat-detection rate `bad-packet-drop` command.




---

**Note** If you do not want the drop rate exceed warning to appear, you can disable it by using the `no threat-detection basic-threat` command.

---

## 733101

**Error Message** `%ASA-4-733101: Object objectIP (is targeted|is attacking). Current burst rate is rate_val per second, max configured rate is rate_val ; Current average rate is rate_val per second, max configured rate is rate_val ; Cumulative total count is total_cnt.`

**Explanation** The Secure Firewall ASA detected that a specific host (or several hosts in the same 1024-node subnet) is either scanning the network (attacking), or is being scanned (targeted).

- `object` —Attacker or target (a specific host or several hosts in the same 1024-node subnet)
- `objectIP` —The IP address of the scanning attacker or scanned target
- `rate_val` —A particular rate value
- `total_cnt` —The total count

The following two examples show how these variables occur:

```
%ASA-4-733101: Subnet 100.0.0.0 is targeted. Current burst rate is 200 per second, max
configured rate is 0; Current average rate is 0 per second, max configured rate is 0;
Cumulative total count is 2028.
%ASA-4-733101: Host 175.0.0.1 is attacking. Current burst rate is 200 per second, max
configured rate is 0; Current average rate is 0 per second, max configured rate is 0;
Cumulative total count is 2024
```

**Recommended Action** For the specific host or subnet, use the `show threat-detection statistics host ip-address ip-mask` command to check the overall situation and then adjust the threshold rate of the scanning threat to the appropriate value. After the appropriate value is determined, an optional action can be taken to shun those host attackers (not subnet attacker) by configuring the `threat-detection scanning-threat shun-host` command.

You may specify certain hosts or object groups in the shun-host except list. For more information, see the CLI configuration guide. If scanning detection is not desirable, you can disable this feature by using the **no threat-detection scanning** command.

## 733102

**Error Message** %ASA-4-733102:Threat-detection adds host %I to shun list

**Explanation** A host has been shunned by the threat detection engine. When the **threat-detection scanning-threat shun** command is configured, the attacking hosts will be shunned by the threat detection engine.

- %I—A particular hostname

The following message shows how this command was implemented:

```
%ASA-4-733102: Threat-detection add host 11.1.1.40 to shun list
```

**Recommended Action** To investigate whether the shunned host is an actual attacker, use the **threat-detection statistics host ip-address** command. If the shunned host is not an attacker, you can remove the shunned host from the threat detection engine by using the **clear threat-detection shun ip address** command. To remove all shunned hosts from the threat detection engine, use the **clear shun** command.

If you receive this message because an inappropriate threshold rate has been set to trigger the threat detection engine, then adjust the threshold rate by using the **threat-detection rate scanning-threat rate-interval x average-rate y burst-rate z** command.

## 733103

**Error Message** %ASA-4-733103: Threat-detection removes host %I from shun list

**Explanation** A host has been shunned by the threat detection engine. When you use the **clear-threat-detection shun** command, the specified host will be removed from the shunned list.

- %I—A particular hostname

The following message shows how this command is implemented:

```
%ASA-4-733103: Threat-detection removes host 11.1.1.40 from shun list
```

**Recommended Action** None required.

## 733104

**Error Message** %ASA-4-733104: TD\_SYSLOG\_TCP\_INTERCEPT\_AVERAGE\_RATE\_EXCEED

**Explanation** The Secure Firewall ASA is under Syn flood attack and protected by the TCP intercept mechanism, if the average rate for intercepted attacks exceeds the configured threshold. The message is showing which server is under attack and where the attacks are coming from.

**Recommended Action** Write an ACL to filter out the attacks.

## 733105

**Error Message** %ASA-4-733105: TD\_SYSLOG\_TCP\_INTERCEPT\_BURST\_RATE\_EXCEED

**Explanation** The Secure Firewall ASA is under Syn flood attack and protected by the TCP intercept mechanism, if the burst rate for intercepted attacks exceeds the configured threshold. The message is showing which server is under attack and where the attacks are coming from.

**Recommended Action** Write an ACL to filter out the attacks.

## 733201

(For IKEv2 connection requests) **Error Message** %ASA-4-733201: Threat-detection:  
Service[remote-access-client-initiations] Peer[peer-ip]: failure threshold of *threshold-value* exceeded: adding shun to interface *interface*. IKEv2: RA excessive client initiation requests.

(For SSL connection requests) **Error Message** %ASA-4-733201: Threat-detection:  
Service[remote-access-client-initiations] Peer[peer-ip]: failure threshold of *value* exceeded: adding shun to interface *interface*. SSL: RA excessive client initiation requests.

**Explanation** This message appears when the threat-detection service shunned an IP address due to excessive number of remote access client initiation requests to the headend from that host.

**Recommended Action** An IP address is shunned because it met the configured service threshold for mischievous activity. If this IP address should not be blocked, remove the shun manually using the **shun** CLI

## 734001

**Error Message** %ASA-6-734001: DAP: User *user*, Addr *ipaddr*, Connection *connection*: The following DAP records were selected for this connection: *DAP record names*

**Explanation** The DAP records that were selected for the connection are listed.

- *user* —The authenticated username
- *ipaddr* —The IP address of the remote client
- *connection* —The type of client connection, which can be one of the following:

- IPsec
- AnyConnect
- Clientless (web browser)
- Cut-Through-Proxy
- L2TP

- *DAP record names* —The comma-separated list of the DAP record names

**Recommended Action** None required.

## 734002

**Error Message** %ASA-5-734002: DAP: User *user*, Addr *ipaddr* : Connection terminated by the following DAP records: *DAP record names*

**Explanation** The DAP records that terminated the connection are listed.

- *user* —The authenticated username
- *ipaddr* —The IP address of the remote client
- *DAP record names* —The comma-separated list of the DAP record names

**Recommended Action** None required.

## 734003

**Error Message** %ASA-7-734003: DAP: User *name*, Addr *ipaddr* : Session Attribute: *attr name/value*

**Explanation** The AAA and endpoint session attributes that are associated with the connection are listed.

- *user* —The authenticated username
- *ipaddr* —The IP address of the remote client
- *attr/value* —The AAA or endpoint attribute name and value

**Recommended Action** None required.

## 734004

**Error Message** %ASA-3-734004: DAP: Processing error: *internal error code*

**Explanation** A DAP processing error occurred.

- *internal error code* —The internal error string

**Recommended Action** Enable the **debug dap errors** command and re-run DAP processing for further debugging information. If this does not resolve the issue, contact the Cisco TAC and provide the internal error code and any information about the conditions that generated the error.

## 735001

**Error Message** %ASA-1-735001 IPMI: Cooling Fan *var1* : OK

**Explanation** A cooling fan has been restored to normal operation.

- *var1* —The device number markings

**Recommended Action** None required.

## 735002

**Error Message** %ASA-1-735002 IPMI: Cooling Fan *var1* : Failure Detected

**Explanation** A cooling fan has failed.

- *var1* —The device number markings

**Recommended Action** Perform the following steps:

1. Check for obstructions that would prevent the fan from rotating.
2. Replace the cooling fan.
3. If the problem persists, record the message as it appears and contact the Cisco TAC.

## 735003

**Error Message** %ASA-1-735003 IPMI: Power Supply var1 : OK

**Explanation** A power supply has been restored to normal operation.

- *var1* —The device number markings

**Recommended Action** None required.

## 735004

**Error Message** %ASA-1-735004 IPMI: Power Supply var1 : Failure Detected

**Explanation** AC power has been lost, or the power supply has failed.

- *var1* —The device number markings

**Recommended Action** Perform the following steps:

1. Check for AC power failure.
2. Replace the power supply.
3. If the problem persists, record the message as it appears and contact the Cisco TAC.

## 735005

**Error Message** %ASA-1-735005 IPMI: Power Supply Unit Redundancy OK

**Explanation** Power supply unit redundancy has been restored.

**Recommended Action** None required.

## 735006

**Error Message** %ASA-1-735006 IPMI: Power Supply Unit Redundancy Lost

**Explanation** A power supply failure occurred. Power supply unit redundancy has been lost, but the Secure Firewall ASA is functioning normally with minimum resources. Any further failures will result in an Secure Firewall ASA shutdown.

**Recommended Action** To regain full redundancy, perform the following steps:

1. Check for AC power failure.
2. Replace the power supply.
3. If the problem persists, record the message as it appears and contact the Cisco TAC.

## 735007

**Error Message** %ASA-1-735007 IPMI: CPU var1 : Temp: var2 var3 , Critical

**Explanation** The CPU has reached a critical temperature.

- *var1* —The device number markings
- *var2* —The temperature value
- *var3* —Temperature value units (C, F)

**Recommended Action** Record the message as it appears and contact the Cisco TAC.

## 735008

**Error Message** %ASA-1-735008 IPMI: Chassis Ambient *var1* : Temp: *var2* *var3* , Critical

**Explanation** A chassis ambient temperature sensor has reached a critical level.

- *var1* —The device number markings
- *var2* —The temperature value
- *var3* —Temperature value units (C, F)

**Recommended Action** Record the message as it appears and contact the Cisco TAC.

## 735009

**Error Message** %ASA-2-735009: IPMI: Environment Monitoring has failed initialization and configuration. Environment Monitoring is not running.

**Explanation** Environment monitoring has experienced a fatal error during initialization and was unable to continue.

**Recommended Action** Collect the output of the **show environment** and **debug ipmi** commands. Record the message as it appears and contact the Cisco TAC.

## 735010

**Error Message** %ASA-3-735010: IPMI: Environment Monitoring has failed to update one or more of its records.

**Explanation** Environment monitoring has experienced an error that temporarily prevented it from updating one or more of its records.

**Recommended Action** If this message appears repeatedly, collect the output from the **show environment driver** and **debug ipmi** commands. Record the message as it appears and contact the Cisco TAC.

## 735011

**Error Message** %ASA-1-735011: Power Supply *var1* : Fan OK

**Explanation** The power supply fan has returned to a working operating state.

- *var1* — Fan number

**Recommended Action** None required.



## 735012

**Error Message** %ASA-1-735012: Power Supply *var1* : Fan Failure Detected

**Explanation** The power supply fan has failed.

- *var1* — Fan number

**Recommended Action** Contact Cisco TAC to troubleshoot the failure. Power down the unit until this failure is resolved.

## 735013

**Error Message** %ASA-1-735013: Voltage Channel *var1* : Voltage OK

**Explanation** A voltage channel has returned to a normal operating level.

- *var1* — Voltage channel number

**Recommended Action** None required.

## 735014

**Error Message** %ASA-1-735014: Voltage Channel *var1*: Voltage Critical

**Explanation** A voltage channel has changed to a critical level.

- *var1* — Voltage channel number

**Recommended Action** Contact Cisco TAC to troubleshoot the failure. Power down the unit until this failure is resolved.

## 735015

**Error Message** %ASA-4-735015: CPU *var1* : Temp: *var2* *var3* , Warm

**Explanation** The CPU temperature is warmer than the normal operating range.

- *var1* —CPU Number
- *var2* —Temperature Value
- *var3* —Units

**Recommended Action** Continue to monitor this component to ensure that it does not reach a critical temperature.

## 735016

**Error Message** %ASA-4-735016: Chassis Ambient *var1* : Temp: *var2* *var3* , Warm

**Explanation** The chassis temperature is warmer than the normal operating range.

- *var1* —Chassis Sensor Number
- *var2* —Temperature Value
- *var3* —Units

**Recommended Action** Continue to monitor this component to ensure that it does not reach a critical temperature.

## 735017

**Error Message** %ASA-1-735017: Power Supply *var1* : Temp: *var2* *var3* , OK

**Explanation** The power supply temperature has returned to a normal operating temperature.

- *var1* —Power Supply Number
- *var2* —Temperature Value
- *var3* —Units

**Recommended Action** None required.

## 735018

**Error Message** %ASA-4-735018: Power Supply *var1* : Temp: *var2* *var3* , Critical

**Explanation** The power supply has reached a critical operating temperature.

- *var1* —Power Supply Number
- *var2* —Temperature Value
- *var3* —Units

**Recommended Action** Contact Cisco TAC to troubleshoot the failure. Power down the unit until this failure is resolved.

## 735019

**Error Message** %ASA-4-735019: Power Supply *var1* : Temp: *var2* *var3* , Warm

**Explanation** The power supply temperature is warmer than the normal operating range.

- *var1* —Power Supply Number
- *var2* —Temperature Value
- *var3* —Units

**Recommended Action** Continue to monitor this component to ensure that it does not reach a critical temperature.

## 735020

**Error Message** %ASA-1-735020: CPU *var1*: Temp: *var2* *var3* OK

**Explanation** The CPU temperature has returned to the normal operating temperature.

- *var1* —CPU Number
- *var2* —Temperature Value
- *var3* —Units

**Recommended Action** None required.

## 735021

**Error Message** %ASA-1-735021: Chassis *var1*: Temp: *var2* *var3* OK

**Explanation** The chassis temperature has returned to the normal operating temperature.

- *var1* —Chassis Sensor Number
- *var2* —Temperature Value
- *var3* —Units

**Recommended Action** None required.

## 735022

**Error Message** %ASA-1-735022: CPU# is running beyond the max thermal operating temperature and the device will be shutting down immediately to prevent permanent damage to the CPU.

**Explanation** The Secure Firewall ASA has detected a CPU running beyond the maximum thermal operating temperature, and will shut down immediately after detection.

**Recommended Action** The chassis and CPU need to be inspected immediately for ventilation issues.

## 735023

**Error Message** %ASA-2-735023: ASA was previously shutdown due to the CPU complex running beyond the maximum thermal operating temperature. The chassis needs to be inspected immediately for ventilation issues.

**Explanation** At boot time, the Secure Firewall ASA detected a shutdown that occurred because a CPU was running beyond the maximum safe operating temperature. Using the **show environment** command will indicate that this event has occurred.

**Recommended Action** The chassis need to be inspected immediately for ventilation issues.

## 735024

**Error Message** %ASA-1-735024: IO Hub *var1* : Temp: *var2* *var3* , OK

**Explanation** The IO hub temperature has returned to the normal operating temperature.

- *ar1* - IO hub number
- *var2* - Temperature value
- *var3* - Units

**Recommended Action** None required.

## 735025

**Error Message** %ASA-1-735025: IO Hub *var1* : Temp: *var2* *var3* , Critical

**Explanation** The IO hub temperature has a critical temperature.

- *ar1* - IO hub number
- *var2* - Temperature value

- *var3* – Units

**Recommended Action** Record the message as it appears and contact the Cisco TAC.

## 735026

**Error Message** %ASA-4-735026: IO Hub *var1* : Temp: *var2* *var3* , Warm

**Explanation** The IO hub temperature is warmer than the normal operating range.

- *ar1* - IO hub number
- *var2* - Temperature value
- *var3* – Units

**Recommended Action** Continue to monitor this component to ensure that it does not reach a critical temperature.

## 735027

**Error Message** %ASA-1-735027: CPU *cpu\_num* Voltage Regulator is running beyond the max thermal operating temperature and the device will be shutting down immediately. The chassis and CPU need to be inspected immediately for ventilation issues.

**Explanation** The Secure Firewall ASA has detected a CPU voltage regulator running beyond the maximum thermal operating temperature, and shuts down immediately after detection.

- *cpu\_num* —The number to identify which CPU voltage regulator experienced the thermal event

**Recommended Action** The chassis and CPU need to be inspected immediately for ventilation issues.

## 735028

**Error Message** %ASA-2-735028: ASA was previously shutdown due to a CPU Voltage Regulator running beyond the max thermal operating temperature. The chassis and CPU need to be inspected immediately for ventilation issues.

**Explanation** At boot time, the Secure Firewall ASA detected a shutdown that occurred because of a CPU voltage regulator running beyond the maximum safe operating temperature. Enter the **show environment** command to indicate that this event has occurred.

**Recommended Action** The chassis and CPU need to be inspected immediately for ventilation issues.

## 735029

**Error Message** %ASA-1-735029: IO Hub is running beyond the max thermal operating temperature and the device will be shutting down immediately to prevent permanent damage to the circuit.

**Explanation** The Secure Firewall ASA has detected that the IO hub is running beyond the maximum thermal operating temperature, and will shut down immediately after detection.

**Recommended Action** The chassis and IO hub need to be inspected immediately for ventilation issues.

## 736001

**Error Message** %ASA-2-736001: Unable to allocate enough memory at boot for jumbo-frame reservation. Jumbo-frame support has been disabled.

**Explanation** Insufficient memory has been detected when jumbo frame support was being configured. As a result, jumbo-frame support was disabled.

**Recommended Action** Try reenabling jumbo frame support using the **jumbo-frame reservation** command. Save the running configuration and reboot the Secure Firewall ASA. If the problem persists, contact the Cisco TAC.

## Messages 737001 to 776254

This section includes messages from 737001 to 776254.

### 737001

**Error Message** %ASA-7-737001: IPAA: Session= *session*, Received message *message-type*

**Explanation** The IP address assignment process received a message.

- *session* —The session is the VPN session ID in hexadecimal.
- *message-type* —The message received by the IP address assignment process

**Recommended Action** None required.

### 737002

**Error Message** %ASA-3-737002: IPAA: Session= *session*,Received unknown message *num* variables

**Explanation** The IP address assignment process received a message.

- *session* —The session is the VPN session ID in hexadecimal.
- *num* —The identifier of the message received by the IP address assignment process

**Recommended Action** None required.

### 737003

**Error Message** %ASA-5-737003: IPAA: Session= *session*, DHCP configured, no viable servers found for tunnel-group *tunnel-group*

**Explanation** The DHCP server configuration for the given tunnel group is not valid.

- *session* —The session is the VPN session ID in hexadecimal.
- *tunnel-group* —The tunnel group that IP address assignment is using for configuration

**Recommended Action** Validate the DHCP configuration for the tunnel group. Make sure that the DHCP server is online.

## 737004

**Error Message** %ASA-5-737004: IPAA: Session= *session*, DHCP configured, request failed for tunnel-group '*tunnel-group*'

**Explanation** The DHCP server configuration for the given tunnel group is not valid.

- *session* —The session is the VPN session ID in hexadecimal.
- *tunnel-group* —The tunnel group that IP address assignment is using for configuration

**Recommended Action** Validate the DHCP configuration for the tunnel group. Make sure that the DHCP server is online.

## 737005

**Error Message** %ASA-6-737005: IPAA: Session= *session*, DHCP configured, request succeeded for tunnel-group *tunnel-group*

**Explanation** The DHCP server request has succeeded.

- *session* —The session is the VPN session ID in hexadecimal.
- *tunnel-group* —The tunnel group that IP address assignment is using for configuration

**Recommended Action** None required.

## 737006

**Error Message** %ASA-6-737006: IPAA: Session= *session*, Local pool request succeeded for tunnel-group *tunnel-group*

**Explanation** The local pool request has succeeded.

- *session* —The session is the VPN session ID in hexadecimal.
- *tunnel-group* —The tunnel group that IP address assignment is using for configuration

**Recommended Action** None required.

## 737007

**Error Message** %ASA-5-737007: IPAA: Session= *session*, Local pool request failed for tunnel-group *tunnel-group*

**Explanation** The local pool request has failed. The pool assigned to the tunnel group may be exhausted.

- *session* —The session is the VPN session ID in hexadecimal.
- *tunnel-group* —The tunnel group that IP address assignment is using for configuration

**Recommended Action** Validate the IP local pool configuration by using the **show ip local pool** command.

## 737008

**Error Message** %ASA-5-737008: IPAA: Session= *session*, '*tunnel-group*' not found

**Explanation** The tunnel group was not found when trying to acquire an IP address for configuration. A software defect may cause this message to be generated.

- *session* —The session is the VPN session ID in hexadecimal.
- *tunnel-group* —The tunnel group that IP address assignment is using for configuration

**Recommended Action** Check the tunnel group configuration. Contact the Cisco TAC and report the issue.

## 737009

**Error Message** %ASA-6-737009: IPAA: Session= *session*, AAA assigned address *ip-address*, request failed

**Explanation** The remote access client software requested the use of a particular address. The request to the AAA server to use this address failed. The address may be in use.

- *session* —The session is the VPN session ID in hexadecimal.
- *ip-address* —The IPv4 or IPv6 address that the client requested

**Recommended Action** Check the AAA server status and the status of IP local pools.

## 737010

**Error Message** %ASA-6-737010: IPAA: Session= *session*, AAA assigned address *ip-address*, request succeeded

**Explanation** The remote access client software requested the use of a particular address and successfully received this address.

- *session* —The session is the VPN session ID in hexadecimal.
- *ip-address* —The IPv4 or IPv6 address that the client requested

**Recommended Action** None required.

## 737011

**Error Message** %ASA-5-737011: IPAA: Session= *session*, AAA assigned *ip-address*, not permitted, retrying

**Explanation** The remote access client software requested the use of a particular address. The **vpn-addr-assign aaa** command is not configured. An alternatively configured address assignment method will be used.

- *session* —The session is the VPN session ID in hexadecimal.
- *ip-address* —The IPv4 or IPv6 address that the client requested

**Recommended Action** If you want to permit clients to specify their own address, enable the **vpn-addr-assign aaa** command.

## 737012

**Error Message** %ASA-4-737012: IPAA: Session= *session*, Address assignment failed

**Explanation** The remote access client software request of a particular address failed.

- *session* —The session is the VPN session ID in hexadecimal.
- *ip-address* —The IP address that the client requested

**Recommended Action** If using IP local pools, validate the local pool configuration. If using AAA, validate the configuration and status of the AAA server. If using DHCP, validate the configuration and status of the DHCP server. Increase the logging level (use notification or informational) to obtain additional messages to identify the reason for the failure.

## 737013

**Error Message** %ASA-4-737013: IPAA: Session= *session*, Error freeing address *ip-address* , not found

**Explanation** The Secure Firewall ASA tried to free an address, but it was not on the allocated list because of a recent configuration change.

- *session* —The session is the VPN session ID in hexadecimal.
- *ip-address* —The IPv4 or IPv6 address to be released

**Recommended Action** Validate your address assignment configuration. If this message recurs, it might be due to a software defect. Contact the Cisco TAC and report the issue.

## 737014

**Error Message** %ASA-6-737014: IPAA: Session= *session*, Freeing AAA address *ip-address*

**Explanation** The Secure Firewall ASA successfully released the IP address assigned through AAA.

- *session* —The session is the VPN session ID in hexadecimal.
- *ip-address* —The IPv4 or IPv6 address to be released

**Recommended Action** None required.

## 737015

**Error Message** %ASA-6-737015: IPAA: Session= *session*, Freeing DHCP address *ip-address*

**Explanation** The Secure Firewall ASA successfully released the IP address assigned through DHCP.

- *session* —The session is the VPN session ID in hexadecimal.
- *ip-address* —The IP address to be released

**Recommended Action** None required.

## 737016

**Error Message** %ASA-6-737016: IPAA: Session= *session*, Freeing local pool *pool-name* address *ip-address*

**Explanation** The Secure Firewall ASA successfully released the IP address assigned through local pools.



- *session* —The session is the VPN session ID in hexadecimal.
- *ip-address* —The IPv4 or IPv6 address to be released
- *pool-name* —The pool to which the address is being returned to

**Recommended Action** None required.

## 737017

**Error Message** %ASA-6-737017: IPAA: Session= *session*, DHCP request attempt *num* succeeded

**Explanation** The Secure Firewall ASA successfully sent a request to a DHCP server.

- *session* —The session is the VPN session ID in hexadecimal.
- *num* —The attempt number

**Recommended Action** None required.

## 737018

**Error Message** %ASA-5-737018: IPAA: Session= *session*, DHCP request attempt *num* failed

**Explanation** The Secure Firewall ASA failed to send a request to a DHCP server.

- *session* —The session is the VPN session ID in hexadecimal.
- *num* —The attempt number

**Recommended Action** Validate the DHCP configuration and connectivity to the DHCP server.

## 737019

**Error Message** %ASA-4-737019: IPAA: Session= *session*, Unable to get address from group-policy or tunnel-group local pools

**Explanation** The Secure Firewall ASA failed to acquire an address from the local pools configured on the group policy or tunnel group. The local pools may be exhausted.

- *session* —The session is the VPN session ID in hexadecimal.

**Recommended Action** Validate the local pool configuration and status. Validate the group policy and tunnel group configuration of local pools.

## 737023

**Error Message** %ASA-5-737023: IPAA: Session= *session*, Unable to allocate memory to store local pool address *ip-address*

**Explanation** The Secure Firewall ASA is low on memory.

- *session* —The session is the VPN session ID in hexadecimal.
- *ip-address* —The IP address that was acquired

**Recommended Action** The Secure Firewall ASA may be overloaded and need more memory, or there may be a memory leak caused by a software defect. Contact the Cisco TAC and report the issue.

## 737024

**Error Message** %ASA-5-737024: IPAA: Session= *session*, Client requested address *ip-address*, already in use, retrying

**Explanation** The client requested an IP address that is already in use. The request will be tried using a new IP address.

- *session* —The session is the VPN session ID in hexadecimal.
- *ip-address* —The IP address that the client requested

**Recommended Action** None required.

## 737025

**Error Message** %ASA-5-737025: IPAA:Session= *session*, Duplicate local pool address found, *ip-address* in quarantine

**Explanation** The IP address that was to be given to the client is already in use. The IP address has been removed from the pool and will not be reused.

- *session* —The session is the VPN session ID in hexadecimal.
- *ip-address* —The IP address that was acquired

**Recommended Action** Validate the local pool configuration; there may be an overlap caused by a software defect. Contact the Cisco TAC and report the issue.

## 737026

**Error Message** %ASA-6-737026: IPAA:Session= *session*, Client assigned *ip-address* from local pool *pool-name*

**Explanation** The client has assigned the given address from a local pool.

- *session* —The session is the VPN session ID in hexadecimal.
- *ip-address* —The IP address that was assigned to the client
- *pool-name*—The pool from which the address was allocated

**Recommended Action** None required.

## 737027

**Error Message** %ASA-3-737027: IPAA:Session= *session*, No data for address request

**Explanation** A software defect has been found.

- *session* —The session is the VPN session ID in hexadecimal.

**Recommended Action** Contact the Cisco TAC and report the issue.

## 737028

**Error Message** %ASA-4-737028: IPAA:Session= *session*, Unable to send *ip-address* to standby: communication failure

**Explanation** The active Secure Firewall ASA was unable to communicate with the standby Secure Firewall ASA. The failover pair may be out-of-sync.

- *session* —The session is the VPN session ID in hexadecimal.
- *ip-address* —The IP address that was assigned to the client

**Recommended Action** Validate the failover configuration and status.

## 737029

**Error Message** %ASA-6-737029: IPAA:Session= *session*, Added *ip-address* to standby

**Explanation** The standby Secure Firewall ASA accepted the IP address assignment.

- *session* —The session is the VPN session ID in hexadecimal.
- *ip-address* —The IP address that was assigned to the client

**Recommended Action** None required.

## 737030

**Error Message** %ASA-4-737030: IPAA:Session= *session*, Unable to send *ip-address* to standby: address in use

**Explanation** The standby Secure Firewall ASA has the given address already in use when the active Secure Firewall ASA attempted to acquire it. The failover pair may be out-of-sync.

- *session* —The session is the VPN session ID in hexadecimal.
- *ip-address* —The IP address that was assigned to the client

**Recommended Action** Validate the failover configuration and status.

## 737031

**Error Message** %ASA-6-737031: IPAA:Session= *session*, Removed *ip-address* from standby

**Explanation** The standby Secure Firewall ASA cleared the IP address assignment.

- *session* —The session is the VPN session ID in hexadecimal.
- *ip-address* —The IP address that was assigned to the client

**Recommended Action** None required.

## 737032

**Error Message** %ASA-4-737032: IPAA:Session= *session*, Unable to remove *ip-address* from standby: address not found

**Explanation** The standby Secure Firewall ASA did not have an IP address in use when the active Secure Firewall ASA attempted to release it. The failover pair may be out-of-sync.

- *session* —The session is the VPN session ID in hexadecimal.
- *ip-address* —The IP address that was assigned to the client

**Recommended Action** Validate the failover configuration and status.

## 737033

**Error Message** %ASA-4-737033: IPAA:Session= *session*, Unable to assign *addr\_allocator* provided IP address *ip\_addr* to client. This IP address has already been assigned by *previous\_addr\_allocator*

**Explanation** The address assigned by the AAA/DHCP/local pool is already in use.

- *session* —The session is the VPN session ID in hexadecimal.
- *addr\_allocator* —The DHCP/AAA/local pool
- *ip\_addr* —The IP address allocated by the DHCP/AAA/local pool
- *previous\_addr\_allocator* —The address allocator that already assigned the IP address (local pool, AAA, or DHCP)

**Recommended Action** Validate the AAA/DHCP/local pool address configurations. Overlap may occur.

## 737034

**Error Message** %ASA-5-737034: IPAA: Session= *session*, <IP version> address: <*explanation*>

**Explanation** The IP address assignment process is unable to provide an address. The <*explanation*> text will describe the reason.

- *session* —The session is the VPN session ID in hexadecimal.

**Recommended Action** Action will be based on explanation.

## 737035

**Error Message** %ASA-7-737035: IPAA: Session= *session*, '<*message type*>' message queued

**Explanation** A message is queued to the IP address assignment. This corresponds with syslog 737001. This message is not rate limited.

- *session* —The session is the VPN session ID in hexadecimal.

**Recommended Action** No action required.

## 737036

**Error Message** %ASA-6-737035:IPAA: Session= *session*, Client assigned <*address*> from DHCP

**Explanation** IP address assignment process has provided a DHCP provisioned address back to the VPN client. This message is not rate limited.

- *session* —The session is the VPN session ID in hexadecimal.

**Recommended Action** No action required.

## 737038

**Error Message** %ASA7-737038: IPAA: Session=*session*, specified address *ip-address* was in-use, trying to get another.

**Explanation** This log occurs when the AAA server (internal or external) has specified an address to assign to the user; but this address already in-use. The request is being re-queued without a specified address to fall back to DHCP or local pools.

- *session* —The VPN session ID of the requesting session.
- *ip-address* —The IPv4 or IPv6 address specified by AAA

**Recommended Action** None required

## 737200

**Error Message** %ASA-7-737200: VPNFIP: Pool=*pool*, Allocated *ip-address* from pool

**Explanation** This log occurs an address is allocated from a local pool.

- *pool* —The local pool name.
- *ip-address* —The IPv4 or IPv6 address specified by AAA

**Recommended Action** None required

## 737201

**Error Message** %ASA-7-737201: VPNFIP: Pool=*pool*, Returned *ip-address* to pool (*recycle=recycle*)

**Explanation** This log occurs when an address returned to a local pool. The recycle flag indicates whether this address should be re-used for the next request. For rare situation, the recycle flag will be FALSE. For example, when there is an address collision, the address has been assigned to a VPN session by other means such as by AAA or DHCP. In this case, we will not immediately try to reuse that address for the next request.

- *pool* —The local pool name.
- *ip-address* —The IPv4 or IPv6 address specified by AAA

**Recommended Action** None required

## 737202

**Error Message** %ASA-3-737202: VPNFIP: Pool=*pool*, ERROR: *message*

**Explanation** This log is generated when an error event is detected related to the VPN FIP database.

- *pool* —The local pool name.
- *message* —The details for the event.

**Recommended Action** If error is persistent, contact Cisco TAC.

## 737203

**Error Message** %ASA-4-737203: VPNFIP: Pool=*pool*, WARN: *message*

**Explanation** This log is generated to warn of an event related to the VPN FIP database.

- *pool* —The local pool name.
- *message* —The details for the event.

**Recommended Action** If warning is persistent, contact Cisco TAC.

## 737204

**Error Message** %ASA-5-737204: VPNFIP: Pool=*pool*, NOTIFY: *message*

**Explanation** This log is generated to notify of an event related to the VPN FIP database.

- *pool* —The local pool name.
- *message* —The details for the event.

**Recommended Action** None required

## 737205

**Error Message** %ASA-6-737205: VPNFIP: Pool=*pool*, INFO: *message*

**Explanation** This log is generated to inform of an event related to the VPN FIP database.

- *pool* —The local pool name.
- *message* —The details for the event.

**Recommended Action** None required

## 737206

**Error Message** %ASA-7-737206: VPNFIP: Pool=*pool*, DEBUG: *message*

**Explanation** This log is generated to debug an event related to the VPN FIP database.

- *pool* —The local pool name.
- *message* —The details for the event.

**Recommended Action** None required

## 737400

**Error Message** %ASA-7-737400: POOLIP: Pool=*pool*, Allocated *ip-address* from pool

**Explanation** This log occurs an address is allocated from a local pool.

- *pool* —The local pool name
- *ip-address* —The IPv4 or IPv6 address specified by AAA

**Recommended Action** None required

## 737401

**Error Message** %ASA-7-737401: POOLIP: Pool=*pool*, Returned *ip-address* to pool (*recycle=recycle*).

**Explanation** This log occurs an address returned to a local pool. The recycle flag indicates whether this address should be re-used for the next request. For rare situation, the recycle flag will be FALSE. For example, when there is an address collision—the address has been assigned to a VPN session by other means such as by AAA or DHCP. In this case, we will not immediately try to reuse that address for the next request.

- *pool* —The local pool name
- *ip-address* —The IPv4 or IPv6 address specified by AAA

**Recommended Action** None required

## 737402

**Error Message** %ASA-4-737402: POOLIP: Pool=*pool*, Failed to return *ip-address* to pool (*recycle=recycle*). Reason: *message*

**Explanation** This log occurs unable to return an address to an address pool.

- *pool* —The local pool name
- *ip-address* —The IPv4 or IPv6 address specified by AAA
- *message*—The details of the failure. (For example, address not in pool range)

**Recommended Action** None required

## 737403

**Error Message** %ASA-3-737403: POOLIP: Pool=*pool*, ERROR: *message*

**Explanation** This log is generated when an error event is detected related to an IP local pool database.

- *pool* —The local pool name
- *message* —The details for the event.

**Recommended Action** If error is persistent, contact Cisco TAC.

## 737404

**Error Message** %ASA-4-737404: POOLIP: Pool=*pool*, WARN: *message*

**Explanation** This log is generated to warn of an event related to an IP local pool database.

- *pool* —The local pool name

- *message* —The details for the event.

**Recommended Action** If warning is persistent, contact Cisco TAC.

## 737405

**Error Message** %ASA-5-737405: POOLIP: Pool=*pool*, NOTIFY: *message*

**Explanation** This log is generated to notify of an event related to an IP local pool database.

- *pool* —The local pool name
- *message* —The details for the event.

**Recommended Action** None required

## 737406

**Error Message** %ASA-6-737406: POOLIP: Pool=*pool*, INFO: *message*

**Explanation** This log is generated to inform of an event related to an IP local pool database.

- *pool* —The local pool name
- *message* —The details for the event.

**Recommended Action** None required

## 737407

**Error Message** %ASA-7-737407: POOLIP: Pool=*pool*, DEBUG: *message*

**Explanation** This log is generated to debug an event related to an IP local pool database.

- *pool* —The local pool name
- *message* —The details for the event.

**Recommended Action** None required

## 741000

**Error Message** %ASA-6-741000: Coredump filesystem image created on *variable 1* -size *variable 2* MB

**Explanation** A core dump file system was successfully created. The file system is used to manage core dumps by capping the amount of disk space that core dumps may use.

- *variable 1* —The file system on which the core dumps are placed (for example, disk0:, disk1:, and flash:)
- *variable 2* —The size of the created core dump file system in MB

**Recommended Action** Make sure that you save your configuration after creating the core dump file system.



## 741001

**Error Message** %ASA-6-741001: Coredump filesystem image on *variable 1* - resized from *variable 2* MB to *variable 3* MB

**Explanation** The core dump file system has been successfully resized.

- *variable 1* —The file system on which the core dumps are placed
- *variable 2* —The size of the previous core dump file system in MB
- *variable 3* —The size of the current, newly resized core dump file system in MB

**Recommended Action** Make sure that you save your configuration after resizing the core dump file system. Resizing the core dump file system deletes the contents of the existing core dump file system. As a result, make sure that you archive any information before you resize the core dump file system.

## 741002

**Error Message** %ASA-6-741002: Coredump log and filesystem contents cleared on *variable 1*

**Explanation** All core dumps have been deleted from the core dump file system, and the core dump log has been cleared. The core dump file system and coredump log are always synchronized with each other.

- *variable 1* —The file system on which the core dumps are placed (for example, disk0:, disk1:,and flash:)

**Recommended Action** None required. You can clear the core dump file system to reset it to a known state using the **clear coredump** command.

## 741003

**Error Message** %ASA-6-741003: Coredump filesystem and its contents removed on *variable 1*

**Explanation** The core dump file system and its contents have been removed, and the core dump feature has been disabled.

- *variable 1* —The file system on which the core dumps are placed (for example, disk0:, disk1:,and flash:)

**Recommended Action** Make sure that you save your configuration after the core dump feature has been disabled.

## 741004

**Error Message** %ASA-6-741004: Coredump configuration reset to default values

**Explanation** The core dump configuration has been reset to its default value, which is disabled.

**Recommended Action** Make sure that you save your configuration after the core dump feature has been disabled.

## 741005

**Error Message** %ASA-4-741005: Coredump operation *variable 1* failed with error *variable 2* *variable 3*

**Explanation** An error occurred during the performance of a core dump-related operation.

- *variable 1* —This variable may have the following values:
  - CREATE\_FSYS—An error occurred when creating the core dump file system.
  - CLEAR\_LOG—An error occurred when clearing the core dump log.
  - DELETE\_FSYS—An error occurred when deleting the core dump file system.
  - CLEAR\_FSYS—An error occurred when removing the contents of the core dump file system.
  - MOUNT\_FSYS—An error occurred when mounting the core dump file system.
- *variable 2* —The decimal number that provides additional information about the cause of the error specified in *variable 1*.
- *variable 3* —The descriptive ASCII string associated with *variable 2*. The ASCII string can have the following values:
  - coredump files already exist
  - unable to create coredump filesystem
  - unable to create loopback device
  - filesystem type not supported
  - unable to delete the coredump filesystem
  - unable to delete loopback device
  - unable to unmount coredump filesystem
  - unable to mount coredump filesystem
  - unable to mount loopback device
  - unable to clear coredump filesystem
  - coredump filesystem not found
  - requested coredump filesystem too big
  - coredump operation aborted by administrator
  - coredump command execution failed
  - coredump IFS error encountered
  - coredump, unidentified error encountered

**Recommended Action** Make sure that the core dump feature is disabled in the configuration, and send the message to the Cisco TAC for further analysis.

## 741006

**Error Message** %ASA-4-741006: Unable to write Coredump Helper configuration, reason *variable 1*

**Explanation** An error occurred when writing to the coredump helper configuration file. This error occurs only if disk0: is full. The configuration file is located in disk0:.coredumpinfo/coredump.cfg.

- *variable 1* —This variable includes a basic file system-related string that indicates why the writing of the core dump helper configuration file failed.

**Recommended Action** Disable the core dump feature, remove unneeded items from disk0:, and then reenable core dumps, if desired.

## 742001

**Error Message** %ASA-3-742001: failed to read master key for password encryption from persistent store

**Explanation** An attempt to read the primary password encryption key from the nonvolatile memory after bootup failed. Encrypted passwords in the configuration are not decrypted unless the primary key is set to the correct value using the **key config-key password encryption** command.

**Recommended Action** If there are encrypted passwords in the configuration that must be used, set the primary key to the previous value used to encrypt the password using the **key config-key password encryption** command. If there are no encrypted passwords or they can be discarded, set a new primary key. If password encryption is not used, no action is required.

## 742002

**Error Message** %ASA-3-742002: failed to set master key for password encryption

**Explanation** An attempt to read the **key config-key password encryption** command failed. The error may be caused by the following reasons:

- Configuration from a nonsecure terminal (for example, over a Telnet connection) was made.
- Failover is enabled, but it does not use an encrypted link.
- Another user is setting the key at the same time.
- When trying to change the key, the old key is incorrect.
- The key is too small to be secure.

Other reasons for the error may be valid. In these cases, the actual error is printed in response to the command.

**Recommended Action** Correct the problem indicated in the command response.

## 742003

**Error Message** %ASA-3-742003: failed to save master key for password encryption, reason *reason\_text*

**Explanation** An attempt to save the primary key to nonvolatile memory failed. The actual reason is specified by the *reason\_text* parameter. The reason can be an out-of-memory condition, or the nonvolatile store can be inconsistent.

**Recommended Action** If the problem persists, reformat the nonvolatile store that is used to save the key by using the **write erase** command. Before performing this step, make sure that you back up the out-of-the-box configuration. Then reenter the **write erase** command.

## 742004

**Error Message** %ASA-3-742004: failed to sync master key for password encryption, reason *reason\_text*

**Explanation** An attempt to synchronize the primary key to the peer failed. The actual reason is specified by the *reason\_text* parameter.

**Recommended Action** Try to correct the problem specified in the *reason\_text* parameter.

## 742005

**Error Message** %ASA-3-742005: cipher text enc\_pass is not compatible with the configured master key or the cipher text has been tampered with

**Explanation** An attempt to decrypt a password failed. The password may have been encrypted using a primary key that is different from the current primary key, or the encrypted password has been changed from its original form.

**Recommended Action** If the correct primary key is not being used, correct the problem. If the encrypted password has been modified, reapply the configuration in question with a new password.

## 742006

**Error Message** %ASA-3-742006: password decryption failed due to unavailable memory

**Explanation** An attempt to decrypt a password failed because no memory was available. Features using this password will not work as desired.

**Recommended Action** Correct the memory problem.

## 742007

**Error Message** %ASA-3-742007: password encryption failed due to unavailable memory

**Explanation** An attempt to encrypt a password failed because no memory was available. Passwords may be left in clear text form in the configuration.

**Recommended Action** Correct the memory problem, and reapply the configuration that failed password encryption.

## 742008

**Error Message** %ASA-3-742008: password enc\_pass decryption failed due to decoding error

**Explanation** Password decryption failed because of decoding errors, which may occur if the encrypted password has been modified after being encrypted.

**Recommended Action** Reapply the configuration in question with a clear text password.

## 742009

**Error Message** %ASA-3-742009: password encryption failed due to decoding error

**Explanation** Password encryption failed because of decoding errors, which may be an internal software error.

**Recommended Action** Reapply the configuration in question with a clear text password. If the problem persists, contact the Cisco TAC.

## 742010

**Error Message** %ASA-3-742010: encrypted password *enc\_pass* is not well formed

**Explanation** The encrypted password provided in the command is not well formed. The password may not be a valid, encrypted password, or it may have been modified since it was encrypted.

- *reason\_text* —A string that represents the actual cause of the failure
- *enc\_pass* —The encrypted password that is related to the issue

**Recommended Action** Reapply the configuration in question with a clear text password.

## 743000

**Error Message** %ASA-1-743000: The PCI device with vendor ID: *vendor\_id* device ID: *device\_id* located at bus:device.function bus\_num:dev\_num, func\_num has a link *link\_attr\_name* of *actual\_link\_attr\_val* when it should have a link *link\_attr\_name* of *expected\_link\_attr\_val* .

**Explanation** A PCI device in the system is not configured correctly, which may result in the system not performing at its optimum level.

**Recommended Action** Collect the output of the **show controller pci detail** command, and contact the Cisco TAC.

## 743001

**Error Message** %ASA-1-743001: Backplane health monitoring detected link failure

**Explanation** A hardware failure has probably occurred and has been detected on one of the links between the Secure Firewall ASA Services Module and the switch chassis.

**Recommended Action** Contact the Cisco TAC.

## 743002

**Error Message** %ASA-1-743002: Backplane health monitoring detected link OK

**Explanation** A link has been restored between the Secure Firewall ASA Services Module and the switch chassis. However, the failure and subsequent recovery probably indicates a hardware failure.

**Recommended Action** Contact the Cisco TAC.

## 743004

**Error Message** %ASA-1-743004: System is not fully operational - PCI device with vendor ID *vendor\_id* (*vendor\_name* ), device ID *device\_id* (*device\_name* ) not found

**Explanation** A PCI device in the system that is needed for it to be fully operational was not found.

- *vendor\_id* —Hexadecimal value that identifies the device vendor
- *vendor\_name* —Text string that identifies the vendor name
- *device\_id* —Hexadecimal value that identifies the vendor device
- *device\_name* —Text string that identifies the device name

**Recommended Action** Collect the output of the **show controller pci detail** command and contact the Cisco TAC.

## 743010

**Error Message** %ASA-3-743010: EOBC RPC server failed to start for client module *client name* .

**Explanation** The service failed to start for a particular client of the EOBC RPC service on the server.

**Recommended Action** Call the Cisco TAC.

## 743011

**Error Message** %ASA-3-743011: EOBC RPC call failed, return code *code* string.

**Explanation** The EOBC RPC client failed to make an RPC to the intended server.

**Recommended Action** Call the Cisco TAC.

## 746001

**Error Message** %ASA-6-746001: user-identity: *activated import user groups | activated host names | user-to-IP address databases* download started

**Explanation** A database (user groups, hostnames, or IP addresses) download has started.

**Recommended Action** None required.

## 746002

**Error Message** %ASA-6-746002: user-identity: *activated import user groups | activated host names | user-to-IP address databases* download complete

**Explanation** A database (user groups, hostnames, or IP addresses) download has completed.

**Recommended Action** None required.

## 746003

**Error Message** %ASA-3-746003: user-identity: *activated import user groups | activated host names | user-to-IP address databases* download failed - *reason*

**Explanation** A database (user groups, hostnames, or IP addresses) download has failed because of a timeout.

**Recommended Action** Check the off-box AD agent status. If the AD agent is down, resolve that issue first. If the AD agent is up and running, try to download the database again. If the problem persists, contact the Cisco TAC.

## 746004

**Error Message** %ASA-4-746004: user identity: Total number of activated user groups exceeds the *max\_groups* groups for this platform.

**Explanation** The total number of activated user groups exceeds the maximum number of 256 user groups for this platform.

**Recommended Action** Too many user groups have been configured and activated. Reduce the number of configured user groups. Run the **clear user-identity user no-policy-activated** command to release user records that have not been activated in any policy. Run the **show user-identity user all** command to check the total number of users in the database.

## 746005

**Error Message** %ASA-3-746005: user-identity: The AD Agent *AD agent IP address* cannot be reached - *reason* [*action* ]

**Explanation** The ASA cannot reach the AD agent. There has been no response from the AD agent, or the RADIUS registration failed because the buffer was too small.

**Recommended Action** Check the network connection between the AD agent and the ASA. Try to reach another AD agent, if one is configured and available. If the problem persists, contact the Cisco TAC.

## 746006

**Error Message** %ASA-4-746006: user-identity: Out of sync with AD Agent, start bulk download

**Explanation** The AD agent cannot update the IP-user mapping events on the ASA and the AD agent event log overflows, which causes inconsistency between the AD agent and the ASA IP-user database.

**Recommended Action** None required. If this message persists, check the connection between the AD agent and the ASA.

## 746007

**Error Message** %ASA-5-746007: user-identity: NetBIOS response failed from User *user\_name* at *user\_ip*

**Explanation** No NetBIOS response was received for the number of retries made.

**Recommended Action** None required.

## 746008

**Error Message** %ASA-6-746008: user-identity: NetBIOS Probe Process started

**Explanation** The NetBIOS process has started.

**Recommended Action** None required.

## 746009

**Error Message** %ASA-6-746009: user-identity: NetBIOS Probe Process stopped

**Explanation** The NetBIOS process has stopped.

**Recommended Action** None required.

## 746010

**Error Message** %ASA-3-746010: user-identity: update import-user *domain\_name* \\group\_name - Import Failed [*reason* ]

**Explanation** Entering the **user-identity update import-user username** command failed to update a user element. Reasons for failure include the following: timeout, partial update, import aborted, group does not exist, or no reason given.

**Recommended Action** If the reason for failure does not exist, verify that the group name is correct in the policy. Otherwise, check the connectivity between the ASA and the AD server.

## 746011

**Error Message** %ASA-4-746011: Total number of users created exceeds the maximum number of *max\_users* for this platform.

**Explanation** The AD group has more than the hard-coded maximum number (64000) of levels. Too many users have been configured in the activated policy.

**Recommended Action** Change your policies so that the number of configured users and users under configured groups does not exceed the limit.

## 746012

**Error Message** %ASA-5-746012: user-identity: Add IP-User mapping IP Address - *domain\_name* \user\_name result - reason

**Explanation** A new user-IP mapping has been added to the user-to-IP address mapping database. The status of the operation (success or failure) is indicated. The success reason is VPN user. The failure reasons include the following: Maximum user limit reached and Duplicated address.

**Recommended Action** None required.

## 746013

**Error Message** %ASA-5-746013: user-identity: Delete IP-User mapping IP Address - *domain\_name* \user\_name result - reason

**Explanation** A change has been made to the user-to-IP address mapping database. The status of the operation (success or failure) is indicated. The success reasons include the following: Inactive timeout, NetBIOS probing failed, PIP notification, VPN user logout, Cut-through-proxy user logout, and MAC address mismatch. The failure reason is PIP notification.

**Recommended Action** None required.

## 746014

**Error Message** %ASA-5-746014: user-identity: [FQDN] *fqdn* address IP Address obsolete.

**Explanation** A fully qualified domain name has become obsolete.

**Recommended Action** None required.



## 746015

**Error Message** %ASA-5-746015: user-identity: FQDN] fqdn resolved IP address .

**Explanation** A fully qualified domain name lookup has succeeded.

**Recommended Action** None required.

## 746016

**Error Message** %ASA-3-746016: user-identity: DNS lookup failed, reason: reason

**Explanation** A DNS lookup has failed. Failure reasons include timeout, unresolvable, and no memory.

**Recommended Action** Verify that the FQDN is valid, and that the DNS server is reachable from the ASA. If the problem persists, contact the Cisco TAC.

## 746017

**Error Message** %ASA-6-746017: user-identity: Update import-user domain\_name \\group\_name

**Explanation** The **user-identity update import-user** command has been issued.

**Recommended Action** None required.

## 746018

**Error Message** %ASA-6-746018: user-identity: Update import-user domain\_name \\group\_name done

**Explanation** The **user-identity update import-user** command has been issued, and the import has been completed successfully.

**Recommended Action** None required.

## 746019

**Error Message** %ASA-3-746019: user-identity: Update |Remove AD Agent AD agent IP Address IP-user mapping user\_IP - domain\_name \user\_name failed

**Explanation** The ASA failed to update or remove an IP-user mapping on the AD agent.

**Recommended Action** Check the status of the AD agent and the connectivity between the ASA and the AD agent. If the problem persists, contact the Cisco TAC.

## 747001

**Error Message** %ASA-3-747001: Clustering: Recovered from state machine event queue depleted. Event (event-id , ptr-in-hex , ptr-in-hex ) dropped. Current state state-name , stack ptr-in-hex , ptr-in-hex , ptr-in-hex , ptr-in-hex , ptr-in-hex , ptr-in-hex

**Explanation** The cluster FSM event queue is full, and a new event has been dropped.

**Recommended Action** None.

## 747002

**Error Message** %ASA-5-747002: Clustering: Recovered from state machine dropped event (*event-id* , *ptr-in-hex* , *ptr-in-hex* ). Intended state: *state-name* . Current state: *state-name* .

**Explanation** The cluster FSM received an event that is incompatible with the current state.

**Recommended Action** None.

## 747003

**Error Message** %ASA-5-747003: Clustering: Recovered from state machine failure to process event (*event-id* , *ptr-in-hex* , *ptr-in-hex* ) at state *state-name* .

**Explanation** The cluster FSM failed to process an event for all reasons given.

**Recommended Action** None.

## 747004

**Error Message** %ASA-6-747004: Clustering: state machine changed from state *state-name* to *state-name* .

**Explanation** The cluster FSM has progressed to a new state.

**Recommended Action** None.

## 747005

**Error Message** %ASA-7-747005: Clustering: State machine notify event *event-name* (*event-id* , *ptr-in-hex* , *ptr-in-hex* )

**Explanation** The cluster FSM has notified clients about an event.

**Recommended Action** None.

## 747006

**Error Message** %ASA-7-747006: Clustering: State machine is at state *state-name*

**Explanation** The cluster FSM moved to a stable state; that is, Disabled, Slave, or Master.

**Recommended Action** None.

## 747007

**Error Message** %ASA-5-747007: Clustering: Recovered from finding stray config sync thread, stack *ptr-in-hex* , *ptr-in-hex* , *ptr-in-hex* , *ptr-in-hex* , *ptr-in-hex* , *ptr-in-hex* .

**Explanation** A stray configuration sync thread has been detected.

**Recommended Action** None.

## 747008

**Error Message** %ASA-4-747008: Clustering: New cluster member *name* with serial number *serial-number-A* rejected due to name conflict with existing unit with serial number *serial-number-B* .

**Explanation** The same unit name has been configured on multiple units.

**Recommended Action** None.

## 747009

**Error Message** %ASA-2-747009: Clustering: Fatal error due to failure to create RPC server for module *module name* .

**Explanation** The Secure Firewall ASA failed to create an RPC server.

**Recommended Action** Disable clustering on this unit and try to re-enable it. Contact the Cisco TAC if the problem persists.

## 747010

**Error Message** %ASA-3-747010: Clustering: RPC call failed, message *message-name* , return code *code-value* .

**Explanation** An RPC call failure has occurred. The system tries to recover from the failure.

**Recommended Action** None.

## 747011

**Error Message** %ASA-2-747011: Clustering: Memory allocation error.

**Explanation** A memory allocation failure occurred in clustering.

**Recommended Action** Disable clustering on this unit and try to re-enable it. If the problem persists, check the memory usage on the Secure Firewall ASA.

## 747012

**Error Message** %ASA-3-747012: Clustering: Failed to replicate global object id *hex-id-value* in domain *domain-name* to peer *unit-name* , continuing operation.

**Explanation** A global object ID replication failure has occurred.

**Recommended Action** None.

## 747013

**Error Message** %ASA-3-747013: Clustering: Failed to remove global object id *hex-id-value* in domain *domain-name* from peer *unit-name* , continuing operation.

**Explanation** A global object ID removal failure has occurred.

**Recommended Action** None.

## 747014

**Error Message** %ASA-3-747014: Clustering: Failed to install global object id *hex-id-value* in domain *domain-name* , continuing operation.

**Explanation** A global object ID installation failure has occurred.

**Recommended Action** None.

## 747015

**Error Message** %ASA-4-747015: Clustering: Forcing stray member *unit-name* to leave the cluster.

**Explanation** A stray cluster member has been found.

**Recommended Action** None.

## 747016

**Error Message** %ASA-4-747016: Clustering: Found a split cluster with both *unit-name-A* and *unit-name-B* as master units. Master role retained by *unit-name-A* , *unit-name-B* will leave, then join as a slave.

**Explanation** A split cluster has been found.

**Recommended Action** None.

## 747017

**Error Message** %ASA-4-747017: Clustering: Failed to enroll unit *unit-name* due to maximum member limit *limit-value* reached.

**Explanation** The Secure Firewall ASA failed to enroll a new unit because the maximum member limit has been reached.

**Recommended Action** None.

## 747018

**Error Message** %ASA-3-747018: Clustering: State progression failed due to timeout in module *module-name* .

**Explanation** The cluster FSM progression has timed out.

**Recommended Action** None.

## 747019

**Error Message** %ASA-4-747019: Clustering: New cluster member *name* rejected due to Cluster Control Link IP subnet mismatch (*ip-address /ip-mask* on new unit, *ip-address /ip-mask* on local unit).

**Explanation** The control unit found that a new joining unit has an incompatible cluster interface IP address.

**Recommended Action** None.

## 747020

**Error Message** %ASA-4-747020: Clustering: New cluster member *unit-name* rejected due to encryption license mismatch.

**Explanation** The control unit found that a new joining unit has an incompatible encryption license.

**Recommended Action** None.

## 747021

**Error Message** %ASA-3-747021: Clustering: Master unit *unit-name* is quitting due to interface health check failure on *interface-name* .

**Explanation** The control unit has disabled clustering because of an interface health check failure.

**Recommended Action** None.

## 747022

**Error Message** %ASA-3-747022: Clustering: Asking slave unit *unit-name* to quit because it failed interface health check *x* times, rejoin will be attempted after *y* min. Failed interface: *interface-name* .

**Explanation** This syslog message occurs when the maximum number of rejoin attempts has not been exceeded. A data unit has disabled clustering because of an interface health check failure for the specified amount of time. This unit will re-enable itself automatically after the specified amount of time (ms).

**Recommended Action** None.

## 747023

**Error Message** %ASA-3-747023: Master unit %s[*unit name*] is quitting due to Security Service Module health check failure, and master's Security Service Module state is %s[SSM state], which can be UP/DOWN/INIT]. Rejoin will be attempted after %d[*rejoin delay time*] minutes.

**Explanation** SSM health check failure on data unit; control unit asks data unit to quit with rejoin.

**Recommended Action** None.

## 747024

**Error Message** %ASA-3-747024: Asking slave unit %s[*unit name*] to quit due to its Security Service Module health check failure, and its Security Service Module state is %s[SSM state]. The slave will decide whether to rejoin based on the configurations.

**Explanation** SSM health check failure on data unit; control unit asks data unit to quit. The data unit would decide whether to rejoin or not.

**Recommended Action** None.

## 747025

**Error Message** %ASA-4-747025: Clustering: New cluster member *unit-name* rejected due to firewall mode mismatch.

**Explanation** A control unit found a joining unit that has an incompatible firewall mode.

**Recommended Action** None.

## 747026

**Error Message** %ASA-4-747026: Clustering: New cluster member *unit-name* rejected due to cluster interface name mismatch (*ifc-name* on new unit, *ifc-name* on local unit).

**Explanation** A control unit found a joining unit that has an incompatible cluster control link interface name.

**Recommended Action** None.

## 747027

**Error Message** %ASA-4-747027: Clustering: Failed to enroll unit *unit-name* due to insufficient size of cluster pool *pool-name* in *context-name* .

**Explanation** A control unit could not enroll a joining unit because of the size limit of the minimal cluster pool configured.

**Recommended Action** None.

## 747028

**Error Message** %ASA-4-747028: Clustering: New cluster member *unit-name* rejected due to interface mode mismatch (*mode-name* on new unit, *mode-name* on local unit).

**Explanation** A control unit found a joining unit that has an incompatible interface-mode, either spanned or individual.

**Recommended Action** None.

## 747029

**Error Message** %ASA-4-747029: Clustering: Unit *unit-name* is quitting due to Cluster Control Link down.

**Explanation** A unit disabled clustering because of a cluster interface failure.

**Recommended Action** None.

## 747030

**Error Message** %ASA-3-747030: Clustering: Asking slave unit *unit-name* to quit because it failed interface health check *x* times (last failure on *interface-name* ), Clustering must be manually enabled on the unit to re-join.

**Explanation** An interface health check has failed and the maximum number of rejoin attempts has been exceeded. A data unit has disabled clustering because of an interface health check failure.

**Recommended Action** None.

## 747031

**Error Message** %ASA-3-747031: Clustering: Platform mismatch between cluster master (*platform-type*) and joining unit *unit-name* (*platform-type*). *unit-name* aborting cluster join.

**Explanation** The joining unit's platform type does not match with that of the cluster control unit.

- *unit-name* —Name of the unit in the cluster bootstrap
- *platform-type* —Type of Secure Firewall ASA platform

**Recommended Action** Make sure that the joining unit has the same platform type as that of the cluster control unit.

## 747032

**Error Message** %ASA-3-747032: Clustering: Service module mismatch between cluster master (*module-name*) and joining unit *unit-name* (*module-name*) in slot *slot-number*. *unit-name* aborting cluster join.

**Explanation** The joining unit's external modules are not consistent (module type and order in which they are installed) with those on the cluster control unit.

- *module-name*— Name of the external module
- *unit-name* —Name of the unit in the cluster bootstrap
- *slot-number* —The number of the slot in which the mismatch occurred

**Recommended Action** Make sure that the modules installed on the joining unit are of the same type and are in the same order as they are in the cluster control unit.

## 747033

**Error Message** %ASA-3-747033: Clustering: Interface mismatch between cluster master and joining unit *unit-name*. *unit-name* aborting cluster join.

**Explanation** The joining unit's interfaces are not the same as those on the cluster control unit.

- *unit-name* —Name of the unit in the cluster bootstrap

**Recommended Action** Make sure that the interfaces available on the joining unit are the same as those on the cluster control unit.

## 747034

**Error Message** %ASA-4-747034: Unit %s is quitting due to Cluster Control Link down (%d times after last rejoin). Rejoin will be attempted after %d minutes.

**Explanation** Cluster Control Link down and the unit is kicked out with rejoin.

**Recommended Action** Wait for the unit to rejoin.

## 747035

**Error Message** %ASA-4-747035: Unit %s is quitting due to Cluster Control Link down. Clustering must be manually enabled on the unit to rejoin.

**Explanation** Cluster Control Link down and the unit is kicked out without rejoin.

**Recommended Action** Rejoin the unit manually.

## 747036

**Error Message** %ASA-3-747036: Application software mismatch between cluster master %s[Master unit name] (%s[Master application software name]) and joining unit (%s[Joining unit application software name]). %s[Joining member name] aborting cluster join.

**Explanation** The applications on control unit and the joining data unit are not the same. Data unit will be kicked out.

**Recommended Action** Make sure that the data unit run the same applications/services, and manually rejoin the unit.

## 747037

**Error Message** %ASA-3-747037: Asking slave unit %s to quit due to its Security Service Module health check failure %d times, and its Security Service Module state is %s. Rejoin will be attempted after %d minutes.

**Explanation** SSM health check failure on data unit; control unit asks data unit to quit with rejoin.

**Recommended Action** None.

## 747038

**Error Message** %ASA-3-747038: Asking slave unit %s to quit due to Security Service Module health check failure %d times, and its Security Service Card Module is %s. Clustering must be manually enabled on this unit to rejoin.

**Explanation** SSM health check failure on data; control unit asks data unit to quit with rejoin.

**Recommended Action** Manually rejoin the unit.

## 747039

**Error Message** %ASA-3-747039: Unit %s is quitting due to system failure for %d time(s) (last failure is %s[cluster system failure reason]). Rejoin will be attempted after %d minutes.

**Explanation** Clustering system failure, and the unit kicks itself out with rejoin

**Recommended Action** None required.



## 747040

**Error Message** %ASA-3-747040: Unit %s is quitting due to system failure for %d time(s) (last failure is %s[cluster system failure reason]). Clustering must be manually enabled on the unit to rejoin.

**Explanation** Clustering system failure and the unit kicks itself out without rejoin

**Recommended Action** Manually rejoin the unit.

## 747041

**Error Message** %ASA-3-747041: Master unit %s is quitting due to interface health check failure on %s[interface name], %d times. Clustering must be manually enabled on the unit to rejoin.

**Explanation** Interface health check failure on control unit; control unit kicks itself out with rejoin.

**Recommended Action** Manually rejoin the unit.

## 747042

**Error Message** %ASA-3-747042: Clustering: Master received the config hash string request message from an unknown member with id *cluster-member-id*

**Explanation** Control unit received the config hash string request event.

**Recommended Action** Verify requestor member is still in OnCall state.

## 747043

**Error Message** %ASA-3-747043: Clustering: Get config hash string from master error: *ret\_code* *ret\_code*, *string\_len* *string\_len*

**Explanation** Failed to get config hash string from control unit.

- *ret\_code* □ The error return code; 0 indicates OK, and 1 indicates Failed
- *string\_len* □ The hash\_str length

**Recommended Action** Contact technical support to troubleshoot the issue on control unit. Ensure to turn on 'debug cluster ccp' to identify the root cause.

## 747044

**Error Message** %ASA-6-747044: Configuration Hash string verification result

**Explanation** The result of configuration hash string comparison..

- *result* □ This result can be PASSED or FAILED

**Recommended Action** None required.

## 748001

**Error Message** %ASA-5-748001: Module *slot\_number* in chassis *chassis\_number* is leaving the cluster due to a chassis configuration change

**Explanation** A cluster control link has changed in the MIO, a cluster group has been removed in the MIO, or a blade module has been removed in the MIO configuration.

- *slot\_number* —The blade slot ID within the chassis
- *chassis\_number* —The chassis ID, which is unique for each chassis

**Recommended Action** None required.

## 748002

**Error Message** %ASA-4-748002: Clustering configuration on the chassis is missing or incomplete; clustering is disabled

**Explanation** Configurations are missing or incomplete in the MIO (for example, a cluster group is not configured, or a cluster control link is not configured).

- *slot\_number* —The blade slot ID within the chassis
- *chassis\_number* —The chassis ID, which is unique for each chassis

**Recommended Action** Go to the MIO console and configure the cluster service type, add the module to the service type, and define the cluster control link accordingly.

## 748003

**Error Message** %ASA-4-748003: Module *slot\_number* in chassis *chassis\_number* is leaving the cluster due to a chassis health check failure

**Explanation** The blade cannot talk to the MIO, so it relies on the MIO to detect this communication problem and de-bundle the data ports. If data ports are de-bundled, the Secure Firewall ASA will be kicked out by an interface health check.

- *slot\_number* —The blade slot ID within the chassis
- *chassis\_number* —The chassis ID, which is unique for each chassis

**Recommended Action** Check if the MIO card is up or if the communication between the MIO and the blade is still up.

## 748004

**Error Message** %ASA-5-748004: Module *slot\_number* in chassis *chassis\_number* is re-joining the cluster due to a chassis health check recovery

**Explanation** The MIO blade health check has recovered, and the Secure Firewall ASA tries to rejoin the cluster.

- *slot\_number* —The blade slot ID within the chassis
- *chassis\_number* —The chassis ID, which is unique for each chassis

**Recommended Action** Check if the MIO card is up or if the communication between the MIO and the blade is still up

## 748005

**Error Message** %ASA-3-748005: Failed to bundle the ports for module *slot\_number* in chassis *chassis\_number* ; clustering is disabled

**Explanation** The MIO failed to bundle the ports for itself.

- *slot\_number* —The blade slot ID within the chassis
- *chassis\_number* —The chassis ID, which is unique for each chassis

**Recommended Action** Check if the MIO is operating correctly.

## 748006

**Error Message** %ASA-3-748006: Asking module *slot\_number* in chassis *chassis\_number* to leave the cluster due to a port bundling failure

**Explanation** The MIO failed to bundle ports for a blade, so the blade has been kicked out.

- *slot\_number* —The blade slot ID within the chassis
- *chassis\_number* —The chassis ID, which is unique for each chassis

**Recommended Action** Check if the MIO is operating correctly.

## 748007

**Error Message** %ASA-2-748007: Failed to de-bundle the ports for module *slot\_number* in chassis *chassis\_number* ; traffic may be black holed

**Explanation** The MIO failed to de-bundle the ports.

- *slot\_number* —The blade slot ID within the chassis
- *chassis\_number* —The chassis ID, which is unique for each chassis

**Recommended Action** Check if the MIO is operating correctly.

## 748008

**Error Message** %ASA-6-748008: [CPU load *percentage* | memory load *percentage* ] of module *slot\_number* in chassis *chassis\_number* (*member-name* ) exceeds overflow protection threshold [CPU *percentage* | memory *percentage* ]. System may be oversubscribed on member failure.

**Explanation** The CPU load has exceeded  $(N-1)/N$ , where N is the total number of active cluster members, or the memory load has exceeded  $(100 - x) * (N - 1) / N + x$ , where N is the number of cluster members, and x is the baseline memory usage of the last joining member.

- *percentage* —The CPU load or memory load percentile data
- *slot\_number* —The blade slot ID within the chassis
- *chassis\_number* —The chassis ID, which is unique for each chassis

**Recommended Action** Re-plan the network and clustering deployment. Either reduce the amount of traffic or add more blades/chassis.

## 748009

**Error Message** %ASA-6-748009: [CPU load *percentage* | memory load *percentage* ] of chassis *chassis\_number* exceeds overflow protection threshold [CPU *percentage* | memory *percentage* ]. System may be oversubscribed on chassis failure.

**Explanation** The chassis traffic load exceeded a certain threshold.

- *percentage* —The CPU load or memory load percentile data
- *chassis\_number* —The chassis ID, which is unique for each chassis

**Recommended Action** Re-plan the network and clustering deployment. Either reduce the amount of traffic or add more blades/chassis.

## 748100

**Error Message** %ASA-3-748100: <application\_name> application status is changed from <status> to <status>.

**Explanation** Detect the application status change from one state to another. Application status change will trigger application health check mechanism.

- application name—snort or disk\_full
- status—init, up, down

**Recommended Action** Verify the status of the application.

## 748101

**Error Message** %ASA-3-748101: Peer unit <unit\_id> reported its <application\_name> application status is <status>.

**Explanation** Peer unit reported application status change that will trigger application health check mechanism.

- unit id—the unit id
- application name—snort or disk\_full
- status—init, up, down

**Recommended Action** Verify the status of the application.

## 748102

**Error Message** %ASA-3-748102: Master unit <unit\_id> is quitting due to <application\_name> Application health check failure, and master's application state is <status>.

**Explanation** Application health check detects that the control unit is not healthy. The control unit will leave the cluster group.

- unit id—the unit id
- application name—snort or disk\_full

- status—init, up, down

**Recommended Action** Verify the status of the application. When the application (snort) is up again, the unit will rejoin automatically.

## 748103

**Error Message** %ASA-3-748103: Asking slave unit <unit\_id> to quit due to <application\_name> Application health check failure, and slave's application state is <status>.

**Explanation** Application health check detects that the data unit is not healthy. Control unit will evict the data node.

- unit id—the unit id
- application name—snort or disk\_full
- status—init, up, down

**Recommended Action** Verify the status of the application. When the application (snort) is up again, the unit will rejoin automatically.

## 748201

**Error Message** %ASA-4-748201: <Application name> application on module <module id> in chassis <chassis id> is <status>.

**Explanation** Status of the application in the service chain gets changed.

- status—up, down

**Recommended Action** Verify the status of the application in the service chain.

## 748202

**Error Message** %ASA-3-748202: Module <module\_id> in chassis <chassis id> is leaving the cluster due to <application name> application failure\n.

**Explanation** Unit will be kicked out of cluster if the application such as vDP, fails.

**Recommended Action** Verify the status of the application in the service chain.

## 748203

**Error Message** %ASA-5-748203: Module <module\_id> in chassis <chassis id> is re-joining the cluster due to a service chain application recovery\n.

**Explanation** Unit automatically rejoins the cluster if the service chain application such as vDP, recovers.

**Recommended Action** Verify the status of the application in the service chain.

## 750001

**Error Message** %ASA-5-750001: Local:local IP :local port Remote:remote IP : remote port  
 Username: username Received request to request an IPsec tunnel; local traffic selector =  
 local selectors: range, protocol, port range ; remote traffic selector = remote selectors:  
 range, protocol, port range

**Explanation** A request is being made for an operation on the IPsec tunnel such as a rekey, a request to establish a connection, and so on.

- *local IP:local port* — Local IP address for this request. The Secure Firewall ASA IP address and port number used for this connection
- *remote IP:remote port* — Remote IP address for this request. Peer IP address and port number that the connection is coming from
- *username* —Username of the requester for remote access, if known, or the tunnel group
- *local selectors* —Locally configured traffic selectors or proxies that are being used for this IPsec tunnel
- *remote selectors* —Remote peers requested traffic selectors or proxies for this IPsec tunnel

**Recommended Action** None required.

## 750002

**Error Message** %ASA-5-750002: Local:local IP :local port Remote: remote IP : remote port  
 Username: username Received a IKE\_INIT\_SA request

**Explanation** An incoming tunnel or SA initiation request (IKE\_INIT\_SA request) has been received.

- *local IP:local port* — Local IP address for this request. The Secure Firewall ASA IP address and port number used for this connection
- *remote IP:remote port* — Remote IP address for this request. Peer IP address and port number that the connection is coming from
- *username* —Username of the requester for remote access, if known, or the tunnel group

**Recommended Action** None required.

## 750003

**Error Message** %ASA-4-750003: Local: local IP:local port Remote: remote IP:remote port  
 Username: username Negotiation aborted due to ERROR: error

**Explanation** The negotiation of an SA was aborted because of the provided error reason.

- *local IP:local port* — Local IP address for this request. The Secure Firewall ASA IP address and port number used for this connection
- *remote IP:remote port* — Remote IP address for this request. Peer IP address and port number that the connection is coming from
- *username* —Username of the requester for remote access, if known yet
- *error* —Error reason for aborting the negotiation. Errors include the following:
  - Failed to send data on the network
  - Asynchronous request queued
  - Failed to enqueue packet

- A supplied parameter is incorrect
- Failed to allocate memory
- Failed the cookie negotiation
- Failed to find a matching policy
- Failed to locate an item in the database
- Failed to initialize the policy database
- Failed to insert a policy into the database
- The peer's proposal is invalid
- Failed to compute the DH value
- Failed to construct a NONCE
- An expected payload is missing from the packet
- Failed to compute the SKEYSEED
- Failed to create child SA keys
- The peer's KE payload contained the wrong DH group
- Received invalid KE notify, yet we've tried all configured DH groups
- Failed to compute a hash value
- Failed to authenticate the IKE SA
- Failed to compute or verify a signature
- Failed to validate the certificate
- The certificate has been revoked and is consequently invalid
- Failed to build or process a certificate request
- We requested a certificate, but the peer supplied none
- While sending the certificate chain, peer did not send its certificate as the first in the chain
- Detected an unsupported ID type
- Failed to construct an encrypted payload
- Failed to decrypt an encrypted payload
- Detected an invalid value in the packet
- The initiator bit is asserted in packet from original responder
- The initiator bit isn't asserted in packet from original initiator
- The message response bit is asserted in a packet from the exchange initiator
- The message response bit isn't asserted in a packet from the exchange responder
- Detected an invalid IKE SPI
- Packet is a retransmission
- Detected an invalid protocol ID

- Detected unsupported critical payload
- Detected an invalid traffic selector type
- Failed to create new SA
- Failed to delete SA
- Failed to add new SA into session DB
- Failed to add session to PSH
- Failed to delete session from osal
- Failed to delete a session from the database
- Failed to add request to SA
- Throttling request queue exceeds reasonable limit, increase the window size on peer
- Received an IKE msg id outside supported window
- Detected unsupported version number
- Received no proposal chosen notify
- Detected an error notify payload
- Detected NAT-d hash doesn't match
- Initialize sadb failed
- Initialize session db failed
- Failed to get PSH
- Negotiation context locked currently in use
- Negotiation context was not freed!
- Invalid data state found
- Failed to open PKI session
- Failed to insert public keys
- No certificate found
- Unsupported cert encoding found or Peer requested HTTP URL but never sent HTTP\_LOOKUP\_SUPPORTED Notification
- Sending BUNDLE URL is not supported at least for now. However, processing a BUNDLE URL is supported
- Local certificate has expired
- Failed to construct State Machine
- Error encountered while navigating State Machine
- SM Validation failed
- Could not find neg context
- Failed to add work request to SM Q
- Nonce payload is missing
- Traffic selector payload is missing



- Unsupported DH group
- Expected keypair is unavailable
- Packet isn't encrypted
- Packet is missing KE payload
- Packet is missing SA payload
- Invalid SA
- Invalid negotiation context
- Remote or local ID isn't defined
- Invalid connection id
- Unsupported auth method
- Ipsec policy not found
- Failed to initialize the event priority queue
- Failed to enqueue an item to a list
- Failed to remove an item from list
- Data in the event priority queue is NULL or corrupt
- No local IKE policy found
- Can't delete IKE SA due to in-progress task
- Expected Cookie Notify not received
- Failed to generate auth data: My auth info missing
- Failed to generate auth data: Failed to sign data
- Failed to generate auth data: Signature operation successful but unable to locate generated auth material
- Failed to receive the AUTH msg before the timer expired
- Maximum number of retransmissions reached
- Initial exchange failed
- Auth exchange failed
- Create child exchange failed
- Platform errors
- Failed to log a message
- Unwanted debug level turned on
- There are additional TS possible
- A single pairs of addresses is required
- Invalid session
- There was no IPSEC policy found for received TS
- Cannot remove request from window

- There was no proposal found in configured policy
- Nat-t test failure
- No pskey found
- Invalid compression algorithm
- Failed to get profile name from platform service handle
- Failed to find profile
- Initiator failed to match profile sent by IPSEC with profile found by peer id or certificate
- Failed to get peer id from platform service handle
- The transform attribute is invalid
- Extensible Authentication Protocol failed
- Authenticator sent NULL EAP message
- The config attribute is invalid
- Failed to calculate packet hash
- The AAA context is deleted
- Cannot alloc AAA ID
- Cannot alloc AAA request
- Cannot init AAA request
- The Authen list is not configured
- Fail to send AAA request
- Fail to alloc IP addr
- Invalid message context
- Key Auth memory failure
- EAP method does not generate MSK
- Failed to register new SA with platform
- Failed to async process session register, error: %d
- Failed to insert SA due to ipsec rekey collision
- Failed while handling a ipsec rekey collision
- Failed to accept rekey on SA that caused a rekey collision
- Failed to start timer to ensure IPsec collision SA SPI %s/%s will be deleted by the peer
- Error/Debug codes and strings are not matched
- Failed to initialize SA lifetime
- Failed to find rekey SA
- Failed to generate DH shared secret
- Failed to retrieve issuer public key hash list

- Failed to build certificate payload
- Unable to initialize the timer
- Failed to generate DH shared secret
- Failed to initialized authorization request
- Incorrect author record received from AAA
- Failed to fetch the keys from AAA
- Failed to add attribute to AAA request
- Failed to send tunnel password request to AAA
- Failed to allocate AAA context
- Insertion to policy AVL tree failed
- Deletion from policy AVL tree failed
- No Matching node found in policy AVL tree
- No Matching policy found
- No Matching proposal found
- Proposal is incomplete to be attached to the policy
- Proposal is in use
- Peer authentication method configured is mismatching with the method proposed by peer
- Failed to find the session in osal
- Failed to allocate event
- Failed to create accounting record
- Accounting not required
- Accounting not started for this session
- NAT-T disabled via cli
- Negotiating limit reached, deny SA request
- SA is already in negotiation, hence not negotiating again
- AAA group authorization failed
- AAA user authorization failed
- %% Dropping received fragment, as fragmentation is not negotiated for this SA!
- Maximum number of received fragments reached for the SA
- Number of fragments exceeds maximum allowed
- Assembled packet length %d is greater than maximum ikev2 packet size %d
- Received fragment numbers were NOT continuous or IKEV2\_FRAG\_FLAG\_LAST\_FRAGMENT flag was set on the wrong packet
- Received fragment is not valid, hence being dropped
- AAA group authorization failed

- AAA user authorization failed
- AAA author not configured in IKEv2 profile
- Failed to extract the skeyid
- Failed to send a failover msg to the standby unit
- Detected unsupported failover version
- Request was received but failover is not enabled
- Received an active unit request but the negotiated role is %s
- Received a standby unit request but the negotiated role is %s
- Invalid IP Version
- GDOI is not yet supported in IKEv2
- Failed to allocate PSH from platform
- Redirect the session to another gateway
- Redirect check failed
- Accept the session on this gateway after Redirect check
- Detected unsupported Redirect gateway ID type
- Redirect accepted, initiate new request
- Redirect accepted, clean-up IKEv2 SA, platform will initiate new request
- SA got redirected, it should not do any CREATE\_CHILD\_SA exchange
- DH public key computation failed
- DH secret computation failed
- IN-NEG IKEv2 Rekey SA got deleted
- Number of cert req exceeds the reasonable limit (%d)
- The negotiation context has been freed
- Assembled packet length %d is greater than maximum ikev2 packet size %d
- Received fragment numbers were NOT continuous or IKEV2\_FRAG\_FLAG\_LAST\_FRAGMENT flag was set on the wrong packet
- AAA author not configured in IKEv2 profile
- Assembled packet is not valid, hence being dropped
- Invalid VCID context

**Recommended Action** Review the syslog and follow the flow of the logs to determine if this syslog is the final in the exchange and if it is the cause of a potential failure or a transient error that was renegotiated through. For example, a peer may suggest a DH group via the KE payload that is not configured that causes an initial request to fail, but the correct DH group is communicated so that the peer can come back with the correct group in a new request.

## 750004

**Error Message** %ASA-5-750004: Local: *local IP: local port* Remote: *remote IP: remote port*  
Username: *username* Sending COOKIE challenge to throttle possible DoS

**Explanation** An incoming connection request was challenged with a cookie based on the cookie challenge thresholds that are configured to prevent a possible DoS attack.

- *local IP:local port* — Local IP address for this request. The Secure Firewall ASA IP address and port number used for this connection
- *remote IP:remote port* — Remote IP address for this request. Peer IP address and port number that the connection is coming from
- *username* —Username of the requester for remote access, if known yet

**Recommended Action** None required.

## 750005

**Error Message** %ASA-5-750005: Local: *local IP: local port* Remote: *remote IP: remote port*  
Username: *username* IPsec rekey collision detected. I am lowest nonce initiator, deleting SA with inbound SPI *SPI*

**Explanation** A rekey collision was detected (both peers trying to initiate a rekey at the same time), and it was resolved by keeping the one initiated by this Secure Firewall ASA because it had the lowest nonce. This action caused the indicated SA referenced by the SPI to be deleted.

- *local IP:local port* — Local IP address for this request. The Secure Firewall ASA IP address and port number used for this connection
- *remote IP:remote port* — Remote IP address for this request. Peer IP address and port number that the connection is coming from
- *username* —Username of the requester for remote access, if known yet
- *SPI* —SPI handle of the SA being deleted by resolving the rekey collision that was detected

**Recommended Action** None required.

## 750006

**Error Message** %ASA-5-750006: Local: *local IP: local port* Remote: *remote IP: remote port*  
Username: *username* SA UP. Reason: *reason*

**Explanation** An SA came up for the given reason, such as for a newly established connection or a rekey.

- *local IP:local port* — Local IP address for this request. The Secure Firewall ASA IP address and port number used for this connection
- *remote IP:remote port* — Remote IP address for this request. Peer IP address and port number that the connection is coming from
- *username* —Username of the requester for remote access, if known yet
- *reason* —Reason that the SA came into the UP state

**Recommended Action** None required.

## 750007

**Error Message** %ASA-5-750007: Local: *local IP: local port* Remote: *remote IP: remote port*  
 Username: *username* SA DOWN. Reason: *reason*

**Explanation** An SA was torn down or deleted for the given reason, such as a request by the peer, operator request (via an administrator action), rekey, and so on.

- *local IP:local port* — Local IP address for this request. The Secure Firewall ASA IP address and port number used for this connection
- *remote IP:remote port* — Remote IP address for this request. Peer IP address and port number that the connection is coming from
- *username* —Username of the requester for remote access, if known yet
- *reason* —Reason that the SA came into the DOWN state

**Recommended Action** None required.

## 750008

**Error Message** %ASA-5-750008: Local: *local IP: local port* Remote: *remote IP: remote port*  
 Username: *username* SA rejected due to system resource low

**Explanation** An SA request was rejected to alleviate a low system resource condition.

- *local IP:local port* — Local IP address for this request. The Secure Firewall ASA IP address and port number used for this connection
- *remote IP:remote port* — Remote IP address for this request. Peer IP address and port number that the connection is coming from
- *username* —Username of the requester for remote access, if known yet

**Recommended Action** Check CAC settings for IKEv2 to determine if this is expected behavior based on configured thresholds; otherwise, if the condition persists, investigate further to alleviate the issue.

## 750009

**Error Message** %ASA-5-750009: Local: *local IP: local port* Remote: *remote IP: remote port*  
 Username: *username* SA request rejected due to CAC limit reached: Rejection reason: *reason*

**Explanation** A Connection Admission Control (CAC) limiting threshold was reached, which caused the SA request to be rejected.

- *local IP:local port* — Local IP address for this request. The Secure Firewall ASA IP address and port number used for this connection
- *remote IP:remote port* — Remote IP address for this request. Peer IP address and port number that the connection is coming from
- *username* —Username of the requester for remote access, if known yet
- *reason* —Reason that the SA was rejected

**Recommended Action** Check CAC settings for IKEv2 to determine if this is expected behavior based on configured thresholds; otherwise, if the condition persists, investigate further to alleviate the issue.

## 750010

**Error Message** %ASA-5-750010: Local: *local-ip* Remote: *remote-ip* Username:*username* IKEv2 local throttle-request queue depth threshold of *threshold* reached; increase the window size on peer *peer* for better performance

- *local-ip* —Local peer IP address
- *remote-ip* —Remote peer IP address
- *username* —Username of the requester for remote access or tunnel group name for L2L, if known yet
- *threshold* —Queue depth threshold of the local throttle-request queue reached
- *peer* —Remote peer IP address

**Explanation** The Secure Firewall ASA overflowed its throttle request queue to the specified peer, indicating that the peer is slow. The throttle request queue holds requests destined for the peer, which cannot be sent immediately because the maximum number of requests allowed to be in-flight based on the IKEv2 window size were already in-flight. As in-flight requests are completed, requests are pulled off of the throttle request queue and sent to the peer. If the peer is not processing these requests quickly, the throttle queue backs up.

**Recommended Action** If possible, increase the IKEv2 window size on the remote peer to allow more concurrent requests to be in-flight, which may improve performance.



---

**Note** The Secure Firewall ASA does not currently support an increased IKEv2 window size setting.

---

## 750011

**Error Message** %ASA-3-750011: Tunnel Rejected: Selected IKEv2 encryption algorithm (*IKEV2 encry algo*) is not strong enough to secure proposed IPSEC encryption algorithm (*IPSEC encry algo*).

**Explanation** The tunnel was rejected because the selected IKEv2 encryption algorithm is not strong enough to secure the proposed IPSEC encryption algorithm.

**Recommended Action** Configure a stronger IKEv2 encryption algorithm to match or exceed the strength of the IPsec child SA encryption algorithm.

## 750012

**Error Message** %ASA-4-750012: Selected IKEv2 encryption algorithm (*IKEV2 encry algo*) is not strong enough to secure proposed IPSEC encryption algorithm (*IPSEC encry algo*).

**Explanation** The selected IKEv2 encryption algorithm is not strong enough to secure the proposed IPSEC encryption algorithm.

**Recommended Action** Configure a stronger IKEv2 encryption algorithm to match or exceed the strength of the IPsec child SA encryption algorithm.

## 750013

**Error Message** %ASA-5-750013 - IKEv2 SA (iSPI <ISPI> rRSP <rSPI>) Peer Moved: Previous <prev\_remote\_ip>:<prev\_remote\_port>/<prev\_local\_ip>:<prev\_local\_port>. Updated <new\_remote\_ip>:<new\_remote\_port>/<new\_local\_ip>:<new\_local\_port>

**Explanation** The new mobike feature allows peer IP to be changed without tearing down the tunnel. For example, a mobile device (smartphone) acquires new IP after connecting to a different network. The following list describes the message values:

- *ip* —Specifies the previous, the new local, and remote IP addresses
- *port* —Specifies the previous, the new local, and remote port information
- *SPI* —Indicates the Initiator and Responder SPI
- *iSPI* —Specifies the Initiator SPI
- *rSPI* —Specifies the Responder SPI

**Recommended Action** Contact the Development engineers.

## 750014

**Error Message** %ASA-4-750014: Local:<self ip>:<self port> Remote:<peer ip>:<peer port> Username:<TG or Username> IKEv2 Session aborted. Reason: Initial Contact received for Local ID: <self ID>, Remote ID: <peer ID> from remote peer:<peer ip>:<peer port> to <self ip>:<self port>

### Explanation

For ASA IKEv2, the initial contact (IC) processing is done based on peer IP/Port and ASA IP/Port pairs and the stale sessions get deleted based on these IP/Port pairs. This could be a problem with NAT as IP/Port of peer may change for connections and the stale sessions would not get cleaned up based on IP/Port pairs. As per the IKEv2 RFC, the Initial Contact processing will be switched to use Identity pairs so that the stale sessions can be identified based on peer and ASA identities and clear them. The identities can be IPs, hostnames, Certificate DNs, and so on. This syslog displays the exact reason for clearing the stale sessions. This syslog will be generated on ASA after clearing a stale session from a peer while negotiating a new IKEv2 session with the same peer. This syslog is applicable only for standalone and clustering site-to-site VPNs and not for RA.

**Recommended Action** IKEv2 session Initial Contact processing is done to reset state between peers and clear the stale sessions. If sessions are getting cleared unexpectedly due to Initial Contact processing, ensure that all peers are configured with unique identities.

## 750015

**Error Message** %ASA-4-750015: Local:<self ip>:<self port> Remote:<peer ip>:<peer port> Username:<TG or Username> IKEv2 deleting IPSec SA. Reason: invalid SPI notification received for SPI 0x<SPI>; local traffic selector = Address Range: <start address>-<end address> Protocol: <protocol number> Port Range: <start port>-<end port> ; remote traffic selector = Address Range: <start address>-<end address> Protocol: <protocol number> Port Range: <start port>-<end port>

### Explanation



When an ESP packet gets dropped due to invalid SPI, an INFORMATIONAL exchange with the peer has been added. When peer receives this notification, the child SA causing INVALID\_SPI scenario will be cleared, thereby sync the child SAs sooner and reducing the traffic loss. This IKEv2 syslog is introduced when the child SA gets cleared due to INVALID\_SPI INFORMATIONAL exchange. The following describes the message values:

- *SPI*—SPI in hex for which INVALID\_SPI notification was received.

**Recommended Action** An out-of-sync IKEv2 child condition was detected and handled. No action is required.

## 750016

**Error Message** %ASA7-750016: Local: *localIP:port* Remote:*remoteIP:port* Username: *username*  
IKEv2 Need to send a DPD message to peer

### Explanation

The device may have terminated a connection to the peer. Dead peer detection needs to be performed for the specified peer to determine if it is still alive. The following describes the message values:

- *localIP:port* —The local IP address and port number
- *remoteIP:port* —The remote IP address and port number
- *username* —The username associated with this connection attempt

**Recommended Action** No action is required.

## 751001

**Error Message** %ASA-3-751001: Local: *localIP:port* Remote:*remoteIP:port* Username: *username/group*  
Failed to complete Diffie-Hellman operation. Error: *error*

**Explanation** A failure to complete a Diffie-Hellman operation occurred, as indicated by the error.

- *localIP:port* —The local IP address and port number
- *remoteIP:port* —The remote IP address and port number
- *username/group* —The username or group associated with this connection attempt
- *error* —The error string that indicates the specific error

**Recommended Action** A low memory issue or other internal error that should be resolved has occurred. If it persists, use the memory tracking tool to isolate the issue.

## 751002

**Error Message** %ASA-3-751002: Local: *localIP:port* Remote:*remoteIP:port* Username: *username/group*  
No preshared key or trustpoint configured for self in tunnel group *group*

**Explanation** The Secure Firewall ASA was unable to find any type of authentication information in the tunnel group that it could use to authenticate itself to the peer.

- *localIP:port* —The local IP address and port number
- *remoteIP:port* —The remote IP address and port number
- *username/group* —The username or group associated with this connection attempt

- *group* —The name of the tunnel group

**Recommended Action** Check the tunnel group configuration, and configure a preshared key or certificate for self-authentication in the indicated tunnel group.

## 751003

**Error Message** %ASA-7-751003: Local: *localIP:port* Remote: *remoteIP:port* Username: *username/group*  
Need to send a DPD message to peer

**Explanation** Dead peer detection needs to be performed for the specified peer to determine if it is still alive. The Secure Firewall ASA may have terminated a connection to the peer.

- *localIP:port* —The local IP address and port number
- *remoteIP:port* —The remote IP address and port number
- *username/group* —The username or group associated with this connection attempt

**Recommended Action** None required.

## 751004

**Error Message** %ASA-3-751004: Local: *localIP:port* Remote: *remoteIP:port* Username: *username/group*  
No remote authentication method configured for peer in tunnel group *group*

**Explanation** A method to authenticate the remote peer was not found in the configuration to allow the connection.

- *localIP:port* —The local IP address and port number
- *remoteIP:port* —The remote IP address and port number
- *username/group* —The username or group associated with this connection attempt
- *group* —The name of the tunnel group

**Recommended Action** Check the configuration to make sure that a valid remote peer authentication setting is present.

## 751005

**Error Message** %ASA-3-751005: Local: *localIP:port* Remote: *remoteIP:port* Username: *username/group*  
AnyConnect client reconnect authentication failed. Session ID: *sessionID* , Error: *error*

**Explanation** A failure occurred during an AnyConnect client reconnection attempt using the session token.

- *localIP:port* —The local IP address and port number
- *remoteIP:port* —The remote IP address and port number
- *username/group* —The username or group associated with this connection attempt
- *sessionID* —The session ID used to try to reconnect
- *error* —The error string to indicate the specific error that occurred during the reconnection attempt

**Recommended Action** Take action according to the error specified, if necessary. The error may indicate that a session was removed instead of remaining in resume state because a client disconnect was detected or sessions were cleared on the Secure Firewall ASA. If necessary, also compare this message to the event logs on the Anyconnect client.

## 751006

**Error Message** %ASA-3-751006: Local: *localIP:port* Remote:*remoteIP:port* Username: *username/group*  
Certificate authentication failed. Error: *error*

**Explanation** A failure related to certificate authentication occurred.

- *localIP:port* —The local IP address and port number
- *remoteIP:port* —The remote IP address and port number
- *username/group* —The username or group associated with this connection attempt
- *error* —The error string to indicate the specific certificate authentication failure

**Recommended Action** Take action according to the error specified, if necessary. Check the certificate trustpoint configuration and make sure that the necessary CA certificate exists to be able to correctly verify client certificate chains. Use the **debug crypto ca** commands to isolate the failure.

## 751007

**Error Message** %ASA-5-751007: Local: *localIP:port* Remote:*remoteIP:port* Username: *username/group*  
Configured attribute not supported for IKEv2. Attribute: *attribute*

**Explanation** A configured attribute could not be applied to the IKE version 2 connection because it is not supported for IKE version 2 connections.

- *localIP:port* —The local IP address and port number
- *remoteIP:port* —The remote IP address and port number
- *username/group* —The username or group associated with this connection attempt
- *attribute* —The attribute that is configured to be applied

**Recommended Action** None required, To eliminate this message from being generated, you can remove the IKE version 2 configuration setting.

## 751008

**Error Message** %ASA-3-751008: Local: *localIP:port* Remote:*remoteIP:port* Username: *username/group*  
Group=*group* , Tunnel rejected: IKEv2 not enabled in group policy

**Explanation** IKE version 2 is not allowed based on the enabled protocols for the indicated group to which a connection attempt was mapped, and the connection was rejected.

- *localIP:port* —The local IP address and port number
- *remoteIP:port* —The remote IP address and port number
- *username/group* —The username or group associated with this connection attempt
- *group* —The tunnel group used for connection

**Recommended Action** Check the group policy VPN tunnel protocol setting and enable IKE version 2, if desired.

## 751009

**Error Message** %ASA-3-751009: Local: *localIP:port* Remote:*remoteIP:port* Username: *username/group*  
Unable to find tunnel group for peer.

**Explanation** A tunnel group could not be found for the peer.

- *localIP:port* —The local IP address and port number
- *remoteIP:port* —The remote IP address and port number
- *username/group* —The username or group associated with this connection attempt

**Recommended Action** Check the configuration and tunnel group mapping rules, then configure them to allow the peer to land on a configured group.

## 751010

**Error Message** %ASA-3-751010: Local: *localIP:port* Remote:*remoteIP:port* Username: *username/group*  
Unable to determine self-authentication method. No crypto map setting or tunnel group found.

**Explanation** A method for authenticating the Secure Firewall ASA to the peer could not be found in either the tunnel group or crypto map.

- *localIP:port* —The local IP address and port number
- *remoteIP:port* —The remote IP address and port number
- *username/group* —The username or group associated with this connection attempt

**Recommended Action** Check the configuration, and configure a self-authentication method in the crypto map for the initiator L2L or in the applicable tunnel group.

## 751011

**Error Message** %ASA-3-751011: Local: *localIP:port* Remote:*remoteIP:port* Username:  
*username/group* Failed user authentication. Error: *error*

**Explanation** A failure occurred during user authentication within EAP for an IKE version 2 remote access connection.

- *localIP:port* —The local IP address and port number
- *remoteIP:port* —The remote IP address and port number
- *username/group* —The username or group associated with this connection attempt
- *error* —The error string that indicates the specific error

**Recommended Action** Make sure that the correct authentication credentials were provided and debug further to determine the exact cause of failure, if necessary.

## 751012

**Error Message** %ASA-3-751012: Local: *localIP:port* Remote:*remoteIP:port* Username: *username/group*  
Failure occurred during Configuration Mode processing. Error: *error*

**Explanation** A failure occurred during configuration mode processing while settings were being applied to the connection.

- *localIP:port* —The local IP address and port number
- *remoteIP:port* —The remote IP address and port number
- *username/group* —The username or group associated with this connection attempt
- *error* —The error string that indicates the specific error

**Recommended Action** Take action based on the indicated error. Use the **debug crypto ikev2** commands to determine the cause of the failure, or debug the indicated subsystem that is specified by the error, if necessary.

## 751013

**Error Message** %ASA-3-751013: Local: *localIP:port* Remote: *remoteIP:port* Username: *username/group*  
Failed to process Configuration Payload request for attribute *attribute ID* . Error: *error*

**Explanation** The Configuration Payload request failed to process and generate a Configuration Payload response for an attribute that was requested by the peer.

- *localIP:port* —The local IP address and port number
- *remoteIP:port* —The remote IP address and port number
- *username/group* —The username or group associated with this connection attempt
- *attribute ID* — The attribute ID on which the failure occurred
- *error* —The error string that indicates the specific error

**Recommended Action** A memory error, configuration error, or another type of error has occurred. Use the **debug crypto ikev2** commands to help isolate the cause of the failure.

## 751014

**Error Message** %ASA-4-751014: Local: *localIP:port* Remote *remoteIP:port* Username: *username/group*  
Warning Configuration Payload request for attribute *attribute ID* could not be processed.  
Error: *error*

**Explanation** A warning occurred while processing a CP request to generate a CP response for a requested attribute.

- *localIP:port* —The local IP address and port number
- *remoteIP:port* —The remote IP address and port number
- *username/group* —The username or group associated with this connection attempt
- *attribute ID* — The attribute ID on which the failure occurred
- *error* —The error string that indicates the specific error

**Recommended Action** Take action based on the attribute indicated in the warning and the indicated warning message. For example, a newer client is being used with an older Secure Firewall ASA image, which does not understand a new attribute that has been added to the client. An upgrade of the Secure Firewall ASA image may be necessary to allow the attribute to be processed.

## 751015

**Error Message** %ASA-4-751015: Local: *localIP:port* Remote *remoteIP:port* Username: *username/group*  
SA request rejected by CAC. Reason: *reason*

**Explanation** The connection was rejected by the call admission control to protect the Secure Firewall ASA based on configured thresholds or conditions indicated by the reason listed.

- *localIP:port* —The local IP address and port number
- *remoteIP:port* —The remote IP address and port number
- *username/group* —The username or group associated with this connection attempt
- *reason* —The reason that the SA request was rejected

**Recommended Action** Check the reason and resolve the condition if a new connection should have been accepted or change the configured thresholds.

## 751016

**Error Message** %ASA-4-751016: Local: *localIP:port* Remote *remoteIP:port* Username: *username/group* L2L peer initiated a tunnel with the same outer and inner addresses. Peer could be Originate only - Possible misconfiguration!

**Explanation** The peer may be configured for originate-only connections based on the received outer and inner IP addresses for the tunnel.

- *localIP:port* —The local IP address and port number
- *remoteIP:port* —The remote IP address and port number
- *username/group* —The username or group associated with this connection attempt

**Recommended Action** Check the L2L peer configuration.

## 751017

**Error Message** %ASA-3-751017: Local: *localIP:port* Remote *remoteIP:port* Username: *username/group* Configuration Error *error description*

**Explanation** An error in the configuration that prevented the connection has been detected.

- *localIP:port* —The local IP address and port number
- *remoteIP:port* —The remote IP address and port number
- *username/group* —The username or group associated with this connection attempt
- *error description* —A brief description of the configuration error

**Recommended Action** Correct the configuration based on the indicated error.

## 751018

**Error Message** %ASA-3-751018: Terminating the VPN connection attempt from *attempted group* . Reason: This connection is group locked to *locked group* .

**Explanation** The tunnel group over which the connection is attempted is not the same as the tunnel group set in the group lock.

- *attempted group* —The tunnel group over which the connection came in
- *locked group* —The tunnel group that the connection is locked or restricted to

**Recommended Action** Check the group-lock value in the group policy or the user attributes.

## 751019

**Error Message** %ASA-4-751019: Local:*LocalAddr* Remote:*RemoteAddr* Username:*username* Failed to obtain an *licenseType* license. Maximum license limit *limit* exceeded.

**Explanation** A session creation failed because the maximum license limit was exceeded, which caused a failure to either initiate or respond to a tunnel request.

- *LocalAddr*— Local address for this connection attempt

- *RemoteAddr* —Remote peer address for this connection attempt
- *username* —Username for the peer attempting the connection
- *licenseType* — License type that was exceeded (other VPN or AnyConnect Premium/Essentials)
- *limit* —Number of licenses allowed and was exceeded

**Recommended Action** Make sure that enough licenses are available for all allowed users and/or obtain more licenses to allow the rejected connections. For multiple context mode, allow more licenses for the context that reported the failure, if necessary.

## 751020

**Error Message** %ASA-3-751020: Local:%A:%u Remote:%A:%u Username:%s An %s remote access connection failed. Attempting to use an NSA Suite B crypto algorithm (%s) without an AnyConnect Premium license.

**Explanation** An IKEv2 remote access tunnel could not be created because the AnyConnect Premium license was applied but explicitly disabled with the **anyconnect-essentials** command in the webvpn configuration mode.

**Recommended Action** Make sure that an AnyConnect Premium license is installed on the Secure Firewall ASA is configured in the remote access IKEv2 policies or IPsec proposals.

## 751021

**Error Message** %ASA-4-751021: Local:variable 1 :variable 2 Remote:variable 3 :variable 4 Username:variable 5 variable 6 with variable 7 encryption is not supported with this version of the AnyConnect Client. Please upgrade to the latest Anyconnect Client.

**Explanation** An out-of-date AnyConnect client tried to connect to an Secure Firewall ASA that has IKEv2 with AES-GCM encryption policy configured.

- *variable 1* —Local IP address
- *variable 2* —Local port
- *variable 3* —Remote client IP address
- *variable 4* —Remote client port
- *variable 5* —Username of the AnyConnect client (may be unknown because this occurs before the user enters a username)
- *variable 6* —Connection protocol type (IKEv1, IKEv2)
- *variable 7* —Combined mode encryption type (AES-GCM, AES-GCM 256)

**Recommended Action** Upgrade the AnyConnect client to the latest version to use IKEv2 with AES-GCM encryption.

## 751022

**Error Message** %ASA-3-751022: Local: local-ip Remote: remote-ip Username:username Tunnel rejected: Crypto Map Policy not found for remote traffic selector rem-ts-start /rem-ts-end /rem-ts.startport /rem-ts.endport /rem-ts.protocol local traffic selector local-ts-start /local-ts-end /local-ts.startport /local-ts.endport /local-ts.protocol !

**Explanation** The Secure Firewall ASA was not able to find security policy information for the private networks or hosts indicated in the message. These networks or hosts were sent by the initiator and do not match any crypto ACLs at the Secure Firewall ASA. This is most likely a misconfiguration.

- *local-ip* —Local peer IP address
- *remote-ip* —Remote peer IP address
- *username* —Username of the requester for remote access, if known yet
- *rem-ts-start* —Remote traffic selector start address
- *rem-ts-end* —Remote traffic selector end address
- *rem-ts.startport* —Remote traffic selector start port
- *rem-ts.endport* —Remote traffic selector end port
- *rem-ts.protocol* —Remote traffic selector protocol
- *local-ts-start* —Local traffic selector start address
- *local-ts-end* —Local traffic selector end address
- *local-ts.startport* —Local traffic selector start port
- *local-ts.endport* —Local traffic selector end port
- *local-ts.protocol* —Local traffic selector protocol

**Recommended Action** Check the protected network configuration in the crypto ACLs on both sides and make sure that the local network on the initiator is the remote network on the responder and vice-versa. Pay special attention to wildcard masks and host addresses as compared to network addresses. Non-Cisco implementations may have the private addresses labeled as proxy addresses or “red” networks.

## 751023

**Error Message** %ASA-6-751023: Local *a* :*p* Remote: *a* :*p* Username:*n* Unknown client connection

**Explanation** An unknown non-Cisco IKEv2 client has connected to the Secure Firewall ASA.

- *n* —The group or username (depending on context)
- *a* —An IP address
- *p* —The port number
- *ua* —The user-agent presented by the client to the Secure Firewall ASA

**Recommended Action** Upgrade to a Cisco-supported IKEv2 client.

## 751024

**Error Message** %ASA-3-751024: Local:*ip-addr* Remote:*ip-addr* Username:*username* IKEv2 IPv6 User Filter *tempipv6* configured. This setting has been deprecated, terminating connection

**Explanation** The IPv6 VPN filter has been deprecated and if it is configured instead of a unified filter for IPv6 traffic access control, the connection will be terminated.

**Recommended Action** Configure a unified filter with IPv6 entries to control IPv6 traffic for the user.

## 751025

**Error Message** %ASA-5-751025: Local: *local IP* :*local port* Remote: *remote IP* :*remote port* Username:*username* Group:*group-policy* IPv4 Address=*assigned\_IPv4\_addr* IPv6 address=*assigned\_IPv6\_addr* assigned to session.



**Explanation** This message displays the assigned IP address information for the AnyConnect IKEv2 connection of the specified user.

- *local IP :local port* —Local IP address for this request. The Secure Firewall ASA IP address and port number used for this connection
- *remote IP :remote port* —Remote IP address for this request. Peer IP address and port number that the connection is coming from
- *username* —Username of the requester for remote access, if known yet
- *group-policy* —The group policy that allowed the user to gain access
- *assigned\_IPv4\_addr* —The IPv4 address that is assigned to the client
- *assigned\_IPv6\_addr* —The IPv6 address that is assigned to the client

**Recommended Action** None required.

## 751026

**Error Message** %ASA-6-751026: Local: *localIP:port* Remote: *remoteIP:port* Username: *username/group* IKEv2 Client OS: *client-os* Client: *client-name client-version*

**Explanation** The indicated user is attempting to connect with the shown operating system and client version.

- *localIP:port* —The local IP address and port number
- *remoteIP:port* —The remote IP address and port number
- *username/group* —The username or group associated with this connection attempt
- *client-os* —The operating system reported by the client
- *client-name* —The client name reported by the client (usually AnyConnect)
- *client-version* —The client version reported by the client

**Recommended Action** None required.

## 751027

**Error Message** %ASA-4-751027: Local:*local IP :local port* Remote:*peer IP :peer port* Username:*username* IKEv2 Received INVALID\_SELECTORS Notification from peer. Peer received a packet (SPI=*spi* ). The decapsulated inner packet didn't match the negotiated policy in the SA. Packet destination *pkt\_daddr* , port *pkt\_dest\_port* , source *pkt\_saddr* , port *pkt\_src\_port* , protocol *pkt\_prot* .

**Explanation** A peer received a packet on an IPsec security association (SA) that did not match the negotiated traffic descriptors for that SA. The peer sent an INVALID\_SELECTORS notification containing the SPI and packet data for the offending packet.

- *local IP* —The Secure Firewall ASA local IP address
- *local port* —The Secure Firewall ASA local port
- *peer IP* —Peer IP address
- *peer port* —Peer port
- *username* —Username
- *spi* —SPI of the IPsec SA for the packet
- *pkt\_daddr* —Packet destination IP address
- *pkt\_dest\_port* —Packet destination port
- *pkt\_saddr* —Packet source IP address

- *pkt\_src\_port* —Packet source port
- *pkt\_prot* —Packet protocol

**Recommended Action** Copy the error message, the configuration, and any details about the events leading up to this error, then submit them to Cisco TAC.

## 751028

**Error Message** %ASA-5-751028: Local:<localIP:port> Remote:<remoteIP:port>  
Username:<username/group> IKEv2 Overriding configured keepalive values of  
threshold:<config\_threshold>/retry:<config\_retry> to  
threshold:<applied\_threshold>/retry:<applied\_retry>.

**Explanation** When configured for distributed-site to site with clustering, the keepalive threshold and retry intervals should be increased to prevent overloading the system. If the configured values are below these required values, the required values will be applied. The following list describes the message values:

- *localIP:port* — The local IP address and port number
- *remoteIP:port* — The remote IP address and port number
- *username/group* — The username or group associated with this connection attempt
- *config\_threshold* — The configured keepalive threshold for tunnel-group
- *config\_retry* — The configured keepalive retry for tunnel-group
- *applied\_threshold* — The keepalive threshold being applied
- *applied\_retry* — The keepalive retry being applied

**Recommended Action** Configure to at least the required minimum values.

## 752001

**Error Message** %ASA-2-752001: Tunnel Manager received invalid parameter to remove record

**Explanation** A failure to remove a record from the tunnel manager that might prevent future tunnels to the same peer from initiating has occurred.

**Recommended Action** Reloading the device will remove the record, but if the error persists or recurs, perform additional debugging of the specific tunnel attempt.

## 752002

**Error Message** %ASA-7-752002: Tunnel Manager Removed entry. Map Tag = *mapTag* . Map Sequence Number = *mapSeq* .

**Explanation** An entry to initiate a tunnel was successfully removed.

- *mapTag* —Name of the crypto map for which the initiation entry was removed
- *mapSeq* —Sequence number of the crypto map for which the initiation entry was removed

**Recommended Action** None required.

## 752003

**Error Message** %ASA-5-752003: Tunnel Manager dispatching a KEY\_ACQUIRE message to IKEv2. Map Tag = *mapTag* . Map Sequence Number = *mapSeq*

**Explanation** An attempt is being made to initiate an IKEv2 tunnel that was based on the crypto map indicated.

- *mapTag* —Name of the crypto map for which the initiation entry was removed
- *mapSeq* —Sequence number of the crypto map for which the initiation entry was removed

**Recommended Action** None required.

## 752004

**Error Message** %ASA-5-752004: Tunnel Manager dispatching a KEY\_ACQUIRE message to IKEv1. Map Tag = *mapTag* . Map Sequence Number = *mapSeq*

**Explanation** An attempt is being made to initiate an IKEv1 tunnel that was based on the crypto map indicated.

- *mapTag* —Name of the crypto map for which the initiation entry was removed
- *mapSeq* —Sequence number of the crypto map for which the initiation entry was removed

**Recommended Action** None required.

## 752005

**Error Message** %ASA-2-752005: Tunnel Manager failed to dispatch a KEY\_ACQUIRE message. Memory may be low. Map Tag = *mapTag* . Map Sequence Number = *mapSeq*.

**Explanation** An attempt to dispatch a tunnel initiation attempt failed because of an internal error, such as a memory allocation failure.

- *mapTag* —Name of the crypto map for which the initiation entry was removed
- *mapSeq* —Sequence number of the crypto map for which the initiation entry was removed

**Recommended Action** Use the memory tracking tools and additional debugging to isolate the issue.

## 752006

**Error Message** %ASA-3-752006: Tunnel Manager failed to dispatch a KEY\_ACQUIRE message. Probable mis-configuration of the crypto map or tunnel-group. Map Tag = *Tag* . Map Sequence Number = *num*, SRC Addr: *address* port: *port* Dst Addr: *address* port: *port* .

**Explanation** An attempt to dispatch a tunnel initiation attempt failed because of a configuration error of the indicated crypto map or associated tunnel group.

- *Tag* —Name of the crypto map for which the initiation entry was removed
- *num* —Sequence number of the crypto map for which the initiation entry was removed
- *address* —The source IP address or destination IP address
- *port* —The source port number or destination port number

**Recommended Action** Check the configuration of the tunnel group and crypto map indicated to make sure that it is complete.

## 752007

**Error Message** %ASA-3-752007: Tunnel Manager failed to dispatch a KEY\_ACQUIRE message. Entry already in Tunnel Manager. Map Tag = *mapTag* . Map Sequence Number = *mapSeq*

**Explanation** An attempt was made to re-add an existing entry into the tunnel manager.

- *mapTag* —Name of the crypto map for which the initiation entry was removed
- *mapSeq* —Sequence number of the crypto map for which the initiation entry was removed

**Recommended Action** If the issue persists, make sure that the configuration of the peer will allow the tunnel, and debug further to make sure that the tunnel manager entries are being added and removed correctly during tunnel initiation and successful or failed initiation attempts. Debug IKE version 2 or IKE version 1 connections further, because they may still be in the process of creating the tunnel.

## 752008

**Error Message** %ASA-7-752008: Duplicate entry already in Tunnel Manager

**Explanation** A duplicate request to initiate a tunnel was made, and the tunnel manager is already attempting to initiate the tunnel.

**Recommended Action** None required. If the issue persists, either IKE version 1 or IKE version 2 may have attempted a tunnel initiation and not have timed out yet. Debug further using the applicable commands to make sure that the tunnel manager entry is removed after successful or failed initiation attempts.

## 752009

%ASA-4-752009: IKEv2 Doesn't support Multiple Peers

**Explanation** An attempt to initiate a tunnel with IKE version 2 failed because the crypto map is configured with multiple peers, which is not supported for IKE version 2. Only IKE version 1 supports multiple peers.

**Recommended Action** Check the configuration to make sure that multiple peers are not expected for IKE version 2 site-to-site initiation.

## 752010

**Error Message** %ASA-4-752010: IKEv2 Doesn't have a proposal specified

**Explanation** No IPsec proposal was found to be able to initiate an IKE version 2 tunnel .

**Recommended Action** Check the configuration, then configure an IKE version 2 proposal that can be used to initiate the tunnel, if necessary.

## 752011

**Error Message** %ASA-4-752011: IKEv1 Doesn't have a transform set specified

**Explanation** No IKE version 1 transform set was found to be able to initiate an IKE version 2 tunnel.

**Recommended Action** Check the configuration, then configure an IKE version 2 transform set that can be used to initiate the tunnel, if necessary.

## 752012

**Error Message** %ASA-4-752012: IKEv *protocol* was unsuccessful at setting up a tunnel. Map Tag = *mapTag* . Map Sequence Number = *mapSeq* .

**Explanation** The indicated protocol failed to initiate a tunnel using the configured crypto map.

- *protocol*— IKE version number 1 or 2 for IKEv1 or IKEv2
- *mapTag* —Name of the crypto map for which the initiation entry was removed
- *mapSeq* —Sequence number of the crypto map for which the initiation entry was removed

**Recommended Action** Check the configuration, then debug further within the indicated protocol to determine the cause of the failed tunnel attempt.

## 752013

**Error Message** %ASA-4-752013: Tunnel Manager dispatching a KEY\_ACQUIRE message to IKEv2 after a failed attempt. Map Tag = *mapTag* . Map Sequence Number = *mapSeq* .

**Explanation** The tunnel manager is attempting to initiate the tunnel again after it failed.

- *mapTag* —Name of the crypto map for which the initiation entry was removed
- *mapSeq* —Sequence number of the crypto map for which the initiation entry was removed

**Recommended Action** Check the configuration, and make sure that the crypto maps are correctly configured. Then determine if the tunnel is successfully created on the second attempt.

## 752014

**Error Message** %ASA-4-752014: Tunnel Manager dispatching a KEY\_ACQUIRE message to IKEv1 after a failed attempt. Map Tag = *mapTag* . Map Sequence Number = *mapSeq* .

**Explanation** The tunnel manager is falling back and attempting to initiate the tunnel using IKE version 1 after the tunnel failed.

- *mapTag* —Name of the crypto map for which the initiation entry was removed
- *mapSeq* —Sequence number of the crypto map for which the initiation entry was removed

**Recommended Action** Check the configuration, and make sure that the crypto maps are correctly configured. Then determine if the tunnel is successfully created on the second attempt.

## 752015

**Error Message** %ASA-3-752015: Tunnel Manager has failed to establish an L2L SA. All configured IKE versions failed to establish the tunnel. Map Tag = *mapTag* . Map Sequence Number = *mapSeq* .

**Explanation** An attempt to bring up an L2L tunnel to a peer failed after trying with all configured protocols.

- *mapTag* —Name of the crypto map for which the initiation entry was removed
- *mapSeq* —Sequence number of the crypto map for which the initiation entry was removed

**Recommended Action** Check the configuration, and make sure that the crypto maps are correctly configured. Debug the individual protocols to isolate the cause of the failure.

## 752016

**Error Message** %ASA-5-752016: IKEv protocol was successful at setting up a tunnel. Map Tag = *mapTag* . Map Sequence Number = *mapSeq*.

**Explanation** The indicated protocol (IKE version 1 or IKE version 2) successfully created an L2L tunnel.

- *protocol*— IKE version number 1 or 2 for IKEv1 or IKEv2
- *mapTag* —Name of the crypto map for which the initiation entry was removed
- *mapSeq* —Sequence number of the crypto map for which the initiation entry was removed

**Recommended Action** None required.

## 752017

**Error Message** %ASA-4-752017: IKEv2 Backup L2L tunnel initiation denied on interface *interface* matching crypto map *name* , sequence number *number* . Unsupported configuration.

**Explanation** The Secure Firewall ASA uses IKEv1 to initiate the connection because IKEv2 does not support the backup L2L feature.

**Recommended Action** None required if IKEv1 is enabled. You must enable IKEv1 to use the backup L2L feature.

## 753001

**Error Message** %ASA-4-753001: Unexpected IKEv2 packet received from <IP>:<port>. Error: <reason>

**Explanation** This syslog is generated when an IKEv2 packet is received when the cluster is operating in Distributed VPN clustering mode and fails early consistency and/or error checks performed on it in the datapath.

- <IP>—source IP address from where the packet was received
- <port>—source port from where the packet was received
- <reason>—Reason why the packet is considered invalid. This value could be *Corrupted SPI detected* or *Expired SPI received*.

**Recommended Action** None required if IKEv1 is enabled. You must enable IKEv1 to use the backup L2L feature.

## 767001

**Error Message** %ASA-6-767001: *Inspect-name* : Dropping an unsupported IPv6/IP46/IP64 packet from *interface :IP Addr* to *interface :IP Addr* (fail-close)

**Explanation** A fail-close option was set for a service policy, and a particular inspect received an IPv6, IP64, or IP46 packet. Based on the fail-close option setting, this syslog message is generated and the packet is dropped.

**Recommended Action** None required.

## 768001

**Error Message** %ASA-3-768001: QUOTA: *resource* utilization is high: requested *req* , current *curr* , warning level *level*

**Explanation** A system resource allocation level has reached its warning threshold. In the case of a management session, the resource is simultaneous administrative sessions.

- *resource*— The name of the system resource; in this case, it is a management session.
- *req* —The number requested; for a management session, it is always 1.
- *curr* —The current number allocated; equals *level* for a management session
- *level* —The warning threshold, which is 90 percent of the configured limit

**Recommended Action** None required.

## 768002

**Error Message** %ASA-3-768002: QUOTA: *resource* quota exceeded: requested *req* , current *curr* , limit *limit*

**Explanation** A request for a system resource would have exceeded its configured limit and was denied. In the case of a management session, the maximum number of simultaneous administrative sessions on the system has been reached.

- *resource*— The name of the system resource; in this case, it is a management session.
- *req* —The number requested; for a management session, it is always 1.
- *curr* —The current number allocated; equals *level* for a management session
- *limit* —The configured resource limit

**Recommended Action** None required.

## 768003

**Error Message** %ASA-3-768003: QUOTA: management session quota exceeded for user *user name*: current 3, user limit 3

**Explanation** The current management session exceeded the configured limits for the user.

- *current* —The current number allocated for management session for the user
- *limit* —The configured management session limit. The default value being 15.

**Recommended Action** None required.

## 768004

**Error Message** %ASA-3-768004: QUOTA: management session quota exceeded for *ssh/telnet/http* protocol: current 2, protocol limit 2

**Explanation** The maximum number of management sessions for the protocol - ssh, telnet, or http exceeded the configured limit.

- *current* —The current number allocated for a management session
- *limit* —The configured resource limit per protocol. The default values being 5.

**Recommended Action** None required.

## 769001

**Error Message** %ASA-5-769001: UPDATE: ASA image *src* was added to system boot list

**Explanation** The system image has been updated. The name of a file previously downloaded onto the system has been added to the system boot list.

- *src*— The name or URL of the source image file

**Recommended Action** None required.

## 769002

**Error Message** %ASA-5-769002: UPDATE: ASA image *src* was copied to *dest*

**Explanation** The system image has been updated. An image file has been copied onto the system.

- *src*— The name or URL of the source image file
- *dest*—The name of the destination image file

**Recommended Action** None required.

## 769003

**Error Message** %ASA-5-769003: UPDATE: ASA image *src* was renamed to *dest*

**Explanation** The system image has been updated. An existing image file has been renamed to an image file name in the system boot list.

- *src*— The name or URL of the source image file
- *dest*—The name of the destination image file

**Recommended Action** None required.

## 769004

**Error Message** %ASA-2-769004: UPDATE: ASA image *src\_file* failed verification, reason: *failure\_reason*

**Explanation** The image failed verification from either the copy command or verify command.

- *src\_file* — The file name or URL of the source image file
- *failure\_reason* —The file name of the destination image file

**Recommended Action** Possible failure reasons are: insufficient system memory, no image found in file, checksum failed, signature not found in file, signature invalid, signature algorithm not supported, signature processing issue

## 769005

**Error Message** %ASA-5-769005: UPDATE: ASA image *image\_name* passed image verification.



**Explanation** This is a notification message indicating that the image passed verification.

- *image\_name* — The file name of the Secure Firewall ASA image file

**Recommended Action** None Required.

## 769006

**Error Message** %ASA-3-769006: UPDATE: ASA boot system image *image\_name* was not found on disk.

**Explanation** This is an error message indicating that the file configured in the boot system list could not be located on disk.

- *image\_name* — The file name of the Secure Firewall ASA image file

**Recommended Action** If the device fails to boot, change the boot system command to point to a valid file or install the missing file to the disk before rebooting the device.

## 769007

**Error Message** %ASA-6-769007: UPDATE: Image version is *version\_number*

**Explanation** This message appears when the device is upgraded.

- *version\_number* — The version number of the Secure Firewall ASA image file

**Recommended Action** None required.

## 769009

**Error Message** %ASA-4-769009: UPDATE: Image booted *image\_name* is different from boot images.

**Explanation** This is an error message appears after upgrading the device indicating that the file configured is different from the existing list of boot images.

- *image\_name* — The file name of the Secure Firewall ASA image file

**Recommended Action** None required.

## 770001

**Error Message** %ASA-4-770001: Resource resource allocation is more than the permitted list of *limit* for this platform. If this condition persists, the ASA will be rebooted.

**Explanation** The CPU or memory resource allocation for the Secure Firewall ASA virtual machine has exceeded the allowed limit for this platform. This condition does not occur unless the setting for the Secure Firewall ASA virtual machine has been changed from that specified in the software downloaded from Cisco.com.

**Recommended Action** To continue Secure Firewall ASA operation, change the CPU or memory resource allocation of the virtual machine to what was specified with the software downloaded from Cisco.com. or to the resource limits specified in the *Cisco ASA 1000V CLI Configuration Guide* for this platform.

## 770002

**Error Message** %ASA-1-770002: Resource resource allocation is more than the permitted *limit* for this platform. ASA will be rebooted.

**Explanation** The CPU or memory resource allocation for the Secure Firewall ASA virtual machine has exceeded the allowed limit for this platform. This condition does not occur unless the setting for the Secure Firewall ASA virtual machine has been changed from that specified in the software downloaded from Cisco.com. The Secure Firewall ASA will continue to reboot if the resource allocation is not changed.

**Recommended Action** Change the CPU or memory resource allocation to the virtual machine to what was specified with the software downloaded from Cisco.com or to the resource limits specified in the *Cisco ASA 1000V CLI Configuration Guide* for this platform.

## 770003

**Error Message** %ASA-4-770003: Resource resource allocation is less than the minimum requirement of *value* for this platform. If this condition persists, performance will be lower than normal.

**Explanation** The CPU or memory resource allocation to the Secure Firewall ASA virtual machine is less than the minimum requirement for this platform. If this condition persists, performance will be lower than normal.

**Recommended Action** To continue Secure Firewall ASA operation, change the CPU or memory resource allocation of the virtual machine to what was specified with the software downloaded from Cisco.

## 771001

**Error Message** %ASA-5-771001: CLOCK: System clock set, source: *src* , before: *time* , after: *time*

**Explanation** The system clock was set from a local source.

- *src*— The time protocol, which can be any of the following: NTP, SNTP, VINES, or the RFC-868 time protocol
- *ip* —The IP address of the time server
- *time* —The time string in the form, “Sun Apr 1 12:34:56.789 EDT 2012”

**Recommended Action** None required.

## 771002

**Error Message** %ASA-5-771002: CLOCK: System clock set, source: *src* , IP *ip* , before: *time* , after: *time*

**Explanation** The system clock was set from a remote source.

- *src*— The time source, which can be either manual or hardware calendar
- *ip* —The IP address of the time server
- *time* —The time string in the form, “Sun Apr 1 12:34:56.789 EDT 2012”

**Recommended Action** None required.

## 772002

**Error Message** %ASA-3-772002: PASSWORD: console login warning, user *username* , cause: password expired

**Explanation** A user logged into the system console with an expired password, which is permitted to avoid system lockout.

- *username*— The name of the user

**Recommended Action** The user should change the login password.

## 772003

**Error Message** %ASA-2-772003: PASSWORD: *session* login failed, user *username* , IP *ip* , cause: password expired

**Explanation** A user logged tried to log into the system with an expired password and was denied access.

- *session*— The session type, which can be SSH or Telnet
- *username*— The name of the user
- *ip* —The IP address of the user

**Recommended Action** If the user has authorized access, an administrator must change the password for the user. Unauthorized access attempts should trigger an appropriate response, for example. traffic from that IP address can be blocked.

## 772004

**Error Message** %ASA-3-772004: PASSWORD: *session* login failed, user *username* , IP *ip* , cause: password expired

**Explanation** A user logged tried to log into the system with an expired password and was denied access.

- *session*— The session type, which is ASDM
- *username*— The name of the user
- *ip* —The IP address of the user

**Recommended Action** If the user has authorized access, an administrator must change the password for the user. Unauthorized access attempts should trigger an appropriate response, for example. traffic from that IP address can be blocked.

## 772005

**Error Message** %ASA-6-772005: REAUTH: user *username* passed authentication

**Explanation** The user authenticated successfully after changing the password.

- *username*— The name of the user

**Recommended Action** None required.

## 772006

**Error Message** %ASA-2-772006: REAUTH: user *username* failed authentication

**Explanation** The user entered the wrong password while trying to change it. As a result, the password was not changed.

- *username*— The name of the user

**Recommended Action** The user should retry changing the password using the **change-password** command.

## 774001

**Error Message** %ASA-2-774001: POST: unspecified error

**Explanation** The crypto service provider failed the power on self-test.

**Recommended Action** Contact the Cisco TAC.

## 774002

**Error Message** %ASA-2-774002: POST: error *err*, func *func* , engine *eng* , algorithm *alg* , mode *mode* , dir *dir* , key len *len*

**Explanation** The crypto service provider failed the power on self-test.

- *err* —The failure cause
- *func* —The function
- *eng* —The engine, which can be NPX, Nlite, or software
- *alg* —The algorithm, which can be any of the following: RSA, DSA, DES, 3DES, AES, RC4, MD5, SHA1, SHA256, SHA386, SHA512, HMAC-MD5, HMAC-SHA1, HMAC-SHA2, or AES-XCBC
- *mode* —The mode, which can be any of the following: none, CBC, CTR, CFB, ECB, stateful-RC4, or stateless-RC4
- *dir* —Either encryption or decryption
- *len* —The key length in bits

**Recommended Action** Contact the Cisco TAC.

## 775001

**Error Message** %ASA-6-775001: Scansafe: protocol connection *conn\_id* from *interface\_name* :*real\_address* /*real\_port* [(*idfw\_user*)] to *interface\_name* :*real\_address* /*real\_port* redirected to *server\_interface\_name* :*server\_ip\_address*

**Explanation** A ScanSafe server is configured, and traffic matches a policy that has been configured to redirect the connection to the ScanSafe server for content scanning and other malware protection services.

**Recommended Action** None required.

## 775002

**Error Message** %ASA-4-775002: Reason - protocol connection conn\_id from interface\_name:real\_address/real\_port [(idfw\_user )] to interface\_name:real\_address/real\_port is action locally

**Explanation** If the source IP address and port of the new ScanSafe redirected connection matches the existing connection, then the ASA drops the new connection and this syslog message is generated.

- *Reason* —Duplicate connection with same source *address* and port *port*

**Recommended Action** Make sure of all of the following:

- The ScanSafe license key is configured.
- The public key is configured.
- The ScanSafe server is reachable by the ASA.
- The maximum number of connections has not been reached.



---

**Note** Configuring PAT and ScanSafe on a single connection are not recommended.

---

## 775003

**Error Message** %ASA-6-775003: Scansafe:protocol connection conn\_id from interface\_name :real\_address /real\_port [(idfw\_user )] to interface\_name :real\_address /real\_port is whitelisted.

**Explanation** The traffic has been matched and does not need to be redirected to the ScanSafe server for content scanning, but can be sent directly to the intended web server.

**Recommended Action** None required.

## 775004

**Error Message** %ASA-4-775004: Scansafe: Primary server ip\_address is not reachable

**Explanation** The primary ScanSafe server is not reachable on either of the configured HTTP or HTTPS ports.

**Recommended Action** None required.

## 775005

**Error Message** %ASA-6-775005: Scansafe: Primary server ip\_address is reachable now

**Explanation** The primary ScanSafe server is reachable on both of the configured HTTP and HTTPS ports.

**Recommended Action** None required.

## 775006

**Error Message** %ASA-6-775006: Primary server interface :ip\_address is not reachable and backup server interface :ip\_address is now active

**Explanation** If the primary ScanSafe server becomes unreachable, the ASA checks the connectivity to the configured backup ScanSafe server; if the backup server is reachable, it becomes the active server.

**Recommended Action** None required.

## 775007

**Error Message** %ASA-2-775007: Scansafe: Primary server\_interface\_name :server\_ip\_address and backup server\_interface\_name :server\_ip\_address servers are not reachable.

**Explanation** Neither the primary nor backup ScanSafe server is reachable. Based on the configured default action( fail\_close or fail\_open), traffic is getting dropped or sent to the web server without being redirected.

**Recommended Action** If both the ScanSafe servers are not reachable, you can change the ScanSafe configuration to fail\_open to send traffic to the web server without having it redirected to the ScanSafe server. This configuration changes the default action to permit.

## 776001

**Error Message** %ASA-3-776001: CTS SXP: Configured source IP source ip error

**Explanation** An error occurred while using this configured source IP address to set up an SXP connection.

- *source ip* —IPv4 or IPv6 source address
- *error* —Detailed message regarding what type of error occurs while using the configured address to set up the SXP connection, which can be one of the following:

- Does not belong to this device.
- Does not match outbound interface IP address.

**Recommended Action** Reconfigure the SXP connection to have a valid source IP address. Alternatively, unconfigure the source IP address and let the device select the correct source IP address based on a route lookup.

## 776002

**Error Message** %ASA-3-776002: CTS SXP: Invalid message from peer peer IP : error

**Explanation** An error occurred while parsing an SXP message.

- *peer IP* —IPv4 or IPv6 peer address
- *error* — Description of message parsing problem

**Recommended Action** Contact the Cisco TAC for assistance.

## 776003

**Error Message** %ASA-3-776003: CTS SXP: Connection with peer peer IP failed: error

**Explanation** An SXP configuration error occurred. The connection cannot be set up correctly.

- *peer IP* —IPv4 or IPv6 peer address
- *error* — Description of SXP configuration problem. The error can be one of the following values:

- Mode mismatch with received one.
- Does not exist.
- With the same peer, but different source IP address exists.
- Version mismatch with received one.
- Received binding update while in speaker mode.

**Recommended Action** Make sure that the connection configurations on both ends have the correct mode and IP addresses.

## 776004

**Error Message** %ASA-3-776004: CTS SXP: Fail to start listening socket after TCP process restart.

**Explanation** The SXP on this device cannot accept SXP connection setup requests from remote devices, because it cannot update the binding manager.

**Recommended Action** Disable and reenale the SXP feature to see if the listening socket can be restarted.

## 776005

**Error Message** %ASA-3-776005: CTS SXP: Binding *Binding IP - SGname (SGT)* from peer IP instance *connection instance num error* .

**Explanation** An SXP binding update error has occurred.

- *Binding IP* —IPv4 or IPv6 binding address
- *SGname (SGT)*—Binding SGT information. Has the following format if SGname is available: *SGname (SGT)* and the following format if SGname is unavailable: *SGT* .
- *peer IP* —IPv4 or IPv6 peer address that sent the binding
- *connection instance num* —Instance number of the SXP connection from which the binding came
- *error* —Detailed message about the binding error

**Recommended Action** Contact the Cisco TAC for assistance.

## 776006

**Error Message** %ASA-3-776006: CTS SXP: Internal error: *error*

**Explanation** The CTS SXP system encountered an internal failure.

- *error* —Detailed message about the SXP internal error, which can be one of the following:
- Source IP address of existing SXP connection cannot change.
- Password type of existing connection cannot change.
- Connection mode is the same as the existing configuration.

- IP address does not exist.

**Recommended Action** Contact the Cisco TAC for assistance.

## 776007

**Error Message** %ASA-3-776007: CTS SXP: Connection with peer *peer IP (instance connection instance num)* state changed from *original state* to Off.

**Explanation** The CTS SXP system encountered an internal failure, because the SXP connection with the specified instance number changed its state to off.

- *peer IP* —IPv4 or IPv6 peer address
- *connection instance num* —SXP connection instance number
- *original state* —Original connection state

**Recommended Action** None required.

## 776008

**Error Message** %ASA-6-776008: CTS SXP: Connection with *peer IP (instance connection instance num)* state changed from *original state* to *final state* .

**Explanation** The SXP connection with the specified instance number changed state.

- *peer IP* —IPv4 or IPv6 peer address
- *source IP* —IPv4 or IPv6 source address
- *connection instance num* —SXP connection instance number
- *original state* —Original connection state
- *final state* —Final connection state, which can be any state except the Off state.

**Recommended Action** None required.

## 776009

**Error Message** %ASA-5-776009: CTS SXP: password changed.

**Explanation** The SXP system password has been changed.

**Recommended Action** None required.

## 776010

**Error Message** %ASA-5-776010: CTS SXP: SXP default source IP is changed *original source IP final source IP* .

**Explanation** The SXP default source IP address has been changed on this device.

- *original source IP* —IPv4 or IPv6 original default source IP address
- *final source IP* —IPv4 or IPv6 final default source IP address

**Recommended Action** None required.



## 776011

**Error Message** %ASA-5-776011: CTS SXP: *operational state* .

**Explanation** The SXP feature has changed operational state and works only when the feature is enabled.

- *operational state* —Flags the state whether CTS SXP is enabled or disabled.

**Recommended Action** None required.

## 776012

**Error Message** %ASA-7-776012: CTS SXP: *timer name* timer started for connection with peer *peer IP* .

**Explanation** The specified SXP timer started.

- *peer IP* —IPv4 or IPv6 peer address. For timers that are not triggered by connection-based events, that is, the retry open timer, a default IP address of 0.0.0.0 is used.
- *timer name* —Timer name

**Recommended Action** None required.

## 776013

**Error Message** %ASA-7-776013: CTS SXP: *timer name* timer stopped for connection with peer *peer IP* .

**Explanation** The specified SXP timer stopped.

- *peer IP* —IPv4 or IPv6 peer address. For timers that are not triggered by connection-based events, that is, the retry open timer, a default IP address of 0.0.0.0 is used.
- *timer name* —Timer name

**Recommended Action** None required.

## 776014

**Error Message** %ASA-7-776014: CTS SXP: SXP received binding forwarding request (*action*) binding *binding IP - SGname (SGT)* .

**Explanation** The SXP received a binding forwarding request. The request comes from the binding manager when it wants SXP to broadcast the latest net binding changes within the binding manager.

- *action* —Add or delete operation
- *binding IP* —IPv4 or IPv6 binding address
- *SGname (SGT)*—Binding SGT information. Has the following format if SGname is available: *SGname (SGT)* and the following format if SGname is unavailable: *SGT* .

**Recommended Action** None required.

## 776015

**Error Message** %ASA-7-776015: CTS SXP: Binding *binding IP* - *SGname (SGT)* is forwarded to peer *peer IP* (instance *connection instance num*).

**Explanation** The SXP forwarded binding to the peer.

- *binding IP* —IPv4 or IPv6 binding address
- *SGname (SGT)*—Binding SGT information. Has the following format if SGname is available: *SGname (SGT)* and the following format if SGname is unavailable: *SGT*.
- *peer IP* —IPv4 or IPv6 peer address
- *connection instance num* —SXP connection instance number

**Recommended Action** None required.

## 776016

**Error Message** %ASA-7-776016: CTS SXP: Binding *binding IP* - *SGName (SGT)* from peer *peer IP* (instance *binding's connection instance num*) changed from old instance: *old instance num*, old sgt: *old SGName (SGT)*.

**Explanation** Binding changed in the SXP database.

- *binding IP* —IPv4 or IPv6 binding address
- *SGname (SGT)*—Binding SGT information. Has the following format if SGname is available: *SGname (SGT)* and the following format if SGname is unavailable: *SGT*.
- *peer IP* —Binding source IPv4 or IPv6 address
- *binding's connection instance num* —SXP connection instance number
- *old instance num* —Old connection instance number on which the binding was learned
- *old SGName (SGT)*—Binding old SGT information. Has the following format if SGname is available: *SGname (SGT)* and the following format if SGname is unavailable: *SGT*.

**Recommended Action** None required.

## 776017

**Error Message** %ASA-7-776017: CTS SXP: Binding *binding IP* - *SGname (SGT)* from peer *peer IP* (instance *connection instance num*) deleted in SXP database.

**Explanation** Binding was deleted in the SXP database.

- *binding IP* —IPv4 or IPv6 binding address
- *SGname (SGT)*—Binding SGT information. Has the following format if SGname is available: *SGname (SGT)* and the following format if SGname is unavailable: *SGT*.
- *peer IP* —Binding source IPv4 or IPv6 peer address
- *connection instance num* —SXP connection instance number

**Recommended Action** None required.

## 776018

**Error Message** %ASA-7-776018: CTS SXP: Binding *binding IP* - *SGname (SGT)* from peer *peer IP* (*instance connection instance num*) added in SXP database.

**Explanation** Binding was added in the SXP database.

- *binding IP* —IPv4 or IPv6 binding address
- *SGname (SGT)*—Binding SGT information. Has the following format if SGname is available: *SGname (SGT)* and the following format if SGname is unavailable: *SGT*.
- *peer IP* —Binding source IPv4 or IPv6 peer address
- *connection instance num* —SXP connection instance number

**Recommended Action** None required.

## 776019

**Error Message** %ASA-7-776019: CTS SXP: Binding *binding IP* - *SGname (SGT)* action taken .  
Update binding manager.

**Explanation** The SXP updated the binding manager with the binding change.

- *binding IP* —IPv4 or IPv6 binding address
- *SGname (SGT)*—Binding SGT information. Has the following format if SGname is available: *SGname (SGT)* and the following format if SGname is unavailable: *SGT*.
- *action taken* —Action taken, which can be one of the following: added, deleted, or changed.

**Recommended Action** None required.

## 776020

**Error Message** %ASA-3-776020: CTS SXP: Unable to locate egress interface to peer *peer IP* .

**Explanation** The ASA cannot locate the egress interface to the SXP peer.

- *binding IP* —IPv4 or IPv6 address

**Recommended Action** Make sure that the SXP peer is routable from the device.





## CHAPTER 10

# Syslog Messages 776201 to 8300006

This chapter contains the following sections:

- [Messages Messages 776201 to 780004, on page 575](#)
- [Messages 802005 to 880001 and 8300001 to 8300006, on page 584](#)

## Messages Messages 776201 to 780004

This section includes messages from 776201 to 780004.

### 776201

**Error Message** %ASA-4-776201: CTS PAC: CTS PAC for Server *IP\_address* , A-ID PAC issuer name will expire in *number* days

**Explanation** A CTS PAC is nearing its expiration date.

**Recommended Action** Obtain a new PAC and import it.

### 776202

**Error Message** %ASA-3-776202: CTS PAC for Server *IP\_address* , A-ID PAC issuer name has expired

**Explanation** A CTS PAC has expired.

**Recommended Action** Obtain a new PAC and import it.

### 776203

**Error Message** %ASA-3-776203: Unable to retrieve CTS Environment data due to: *reason*

**Explanation** The ASA was unable to retrieve the CTS environment data and SGT name table for one of the following reasons:

- PAC has expired
- PAC data not available
- Error response from ISE
- Unable to retrieve server secret from the PAC

- Database error
- Invalid SG info value received
- Unable to add SG tag to database
- Error closing database
- Database update aborted

**Recommended Action** If this message persists, contact the Cisco TAC for assistance.

## 776204

**Error Message** %ASA-3-776204: CTS Environment data has expired

**Explanation** The CTS environment data and SGT name table have expired, which is likely to occur after unresolved environment data retrieval failures have occurred.

**Recommended Action** If this message persists, contact the Cisco TAC for assistance.

## 776251

**Error Message** %ASA-6-776251: CTS SGT-MAP: Binding *binding IP - SGname (SGT)* from *source name* added to binding manager.

**Explanation** Binding from the specified source was added to the binding manager.

- *binding IP* —IPv4 or IPv6 binding address.
- *SGname (SGT)*—Binding SGT information. Has the following format if SGname is available: *SGname (SGT)* and the following format if SGname is unavailable: *SGT*.
- *source name* —Name of the contributing source.

**Recommended Action** None required.

## 776252

**Error Message** %ASA-5-776252: CTS SGT-MAP: CTS SGT-MAP: Binding *binding IP - SGname (SGT)* from *source name* deleted from binding manager.

**Explanation** Binding from the specified source was deleted from the binding manager.

Binding from the specified source was added to the binding manager.

- *binding IP* —IPv4 or IPv6 binding address.
- *SGname (SGT)*—Binding SGT information. Has the following format if SGname is available: *SGname (SGT)* and the following format if SGname is unavailable: *SGT*.
- *source name* —Name of the contributing source.

**Recommended Action** None required.

## 776253

**Error Message** %ASA-6-776253: CTS SGT-MAP: Binding *binding IP - new SGname (SGT)* from *new source name* changed from old sgt: *old SGname (SGT)* from old source *old source name* .

**Explanation** A particular IP to SGT binding has changed in the binding manager.

- *binding IP* —IPv4 or IPv6 binding address.
- *new SGname (SGT)*—New binding SGT information. Has the following format if SGname is available: *SGname (SGT)* and the following format if SGname is unavailable: *SGT*.
- *new source name* —Name of the new contributing source.
- *old SGname (SGT)*—Old binding SGT information. Has the following format if SGname is available: *SGname (SGT)* and the following format if SGname is unavailable: *SGT*.
- *old source name* —Name of the old contributing source.

**Recommended Action** None required.

## 776254

**Error Message** %ASA-3-776254: CTS SGT-MAP: Binding manager unable to *action* binding *binding IP* - *SGname (SGT)* from *source name*.

**Explanation** The binding manager cannot insert, delete, or update the binding

- *action*— Binding manager operation. Either insert, delete or update.
- *binding IP* —IPv4 or IPv6 binding address.
- *SGname (SGT)*—Binding SGT information. Has the following format if SGname is available: *SGname (SGT)* and the following format if SGname is unavailable: *SGT*.
- *source name* —Name of the contributing source.

**Recommended Action** Contact the Cisco TAC for assistance.

## 776301

**Error Message** %ASA-7-776301: CTS Policy: Security-group tag *sgt* is mapped to security-group name "*sgname* "

**Explanation** The security group tag referenced in the policy is known and the lookup in the security group table is successful. As a result, the tag name mapping is derived.

- *sgt* —Security group tag referenced in the policy
- *sgname* —Security group name mapping derived from the table

**Recommended Action** None required.

## 776302

**Error Message** %ASA-7-776302: CTS Policy: Unknown security-group tag *sgt* referenced in policies

**Explanation** The security group tag referenced in the policy was unknown and the lookup in the security group table failed. However, the policy referencing the tag can still be enforced.

- *sgt* —Security group tag referenced in the policy

**Recommended Action** Check to see if the security group tag exists in the ISE. If the tag exists, it will become known after the next refresh. If the tag does not exist in the ISE, consider removing all associated policies on the ASA.

## 776303

**Error Message** %ASA-6-776303: CTS Policy: Security-group name "*sgname*" is resolved to security-group tag *sgt*

**Explanation** The securitygroup name referenced in the policy was resolved and the lookup in the security group table was successful. As a result, the tag derived from the table is used for policy enforcement.

- *sgname* —Security group name referenced in the policy
- *sgt* —Security group tag mapping derived from the table

**Recommended Action** None required.

## 776304

**Error Message** %ASA-4-776304: CTS Policy: Unresolved security-group name "*sgname*" referenced, policies based on this name will be inactive

**Explanation** The securitygroup name referenced in the policy cannot be resolved to a tag and the lookup in the security group table failed. AS a result, the policy referencing the name is inactive, but remains in the configuration.

- *sgname* —Security group name referenced in the policy

**Recommended Action** Check to see if the security group name exists in the ISE. If the name exists, the table can be refreshed so the name gets resolved and policies can be enforced. If the name does not exist in the ISE, consider removing all associated policies on the ASA.

## 776305

**Error Message** %ASA-4-776305: CTS Policy: Security-group table cleared, all polices referencing security-group names will be deactivated

**Explanation** The security group table downloaded from the ISE is cleared on the ASA and policies based on security group tags continue to be enforced. However, policies based on names become inactive, but remain in the configuration.

**Recommended Action** Refresh the security group table on the ASA so all policies based on security group names can be enforced.

## 776307

**Error Message** %ASA-7-776307: CTS Policy: Security-group name for security-group tag *sgt* renamed from *old\_sgname* " to "*new\_sgname* "

**Explanation** In the newly downloaded security group table on the ASA, a change in the security group name for a security group tag was detected; however, there was no change in policy status.

- *sgt* —Security group tag referenced in the policy
- *old\_sgname* —Old security group name
- *new\_sgname* —New security group name

**Recommended Action** None required.



## 776308

**Error Message** %ASA-7-776308: CTS Policy: Previously unknown security-group tag *sgt* is now mapped to security-group name "*sgname* "

**Explanation** In the newly downloaded security group table on the ASA, a previously unknown security group tag was found in the table; however, there was no change in policy status.

- *sgt* —Security group tag referenced in the policy
- *sgname* —Security group name derived from the new security group table

**Recommended Action** None required.

## 776309

**Error Message** %ASA-5-776309: CTS Policy: Previously known security-group tag *sgt* is now unknown

**Explanation** In the newly downloaded security group table on the ASA, a previously known security group tag no longer exists. There is no change in policy status, and the policy can still be enforced.

- *sgt* —Security group tag referenced in the policy

**Recommended Action** If the security group tag does not exist in the new table, the security group has been removed in the ISE. Consider removing all policies that reference the tag.

## 776310

**Error Message** %ASA-5-776310: CTS Policy: Security-group name "*sgname* " remapped from security-group tag *old\_sgt* to *new\_sgt*

**Explanation** In the newly downloaded security group table on the ASA, a change in the security group tag for a security group name was detected. All policies referencing the name are updated to reflect the new tag, and policies are enforced based on the new tag.

- *sgname* —Security group name referenced in the policy
- *old\_sgt* —Old security group tag
- *new\_sgt* —New security group tag

**Recommended Action** Because of the change in tag value, make sure that the configured policies are still accurate.

## 776311

**Error Message** %ASA-6-776311: CTS Policy: Previously unresolved security-group name "*sgname* " is now resolved to security-group tag *sgt*

**Explanation** In the newly downloaded security group table on the ASA, a previously unresolved security group name was resolved to a tag, and the new tag can be used to enforce policies.

- *sgname* —Security group name referenced in the policy
- *sgt* —Security group tag derived from the new security group table

**Recommended Action** None required.

## 776312

**Error Message** %ASA-4-776312: CTS Policy: Previously resolved security-group name "*sgname*" is now unresolved, policies based on this name will be deactivated

**Explanation** In the newly downloaded security group table on the ASA, a previously resolved security group name no longer exists. As a result, all policies based on this security group name become inactive, but remain in the configuration.

- *sgname* —Security group name referenced in the policy

**Recommended Action** If the security group name does not exist in the new table, the security group has been removed in the ISE. Check the policy configuration on the ASA, consider removing policies referencing the name.

## 776313

**Error Message** %ASA-3-776313: CTS Policy: Failure to update policies for security-group "*sgname*"-*sgt*

**Explanation** An error was encountered in updating the policies. Policy enforcement will continue based on old tag values and is no longer accurate.

- *sgname* —Security group name that has a change in tag value
- *sgt* —New security group tag value

**Recommended Action** To reflect the correct tag value, remove all policies referencing the security group name and reapply them. If the error persists, contact the Cisco TAC for assistance.

## 778001

**Error Message** %ASA-6-778001: VXLAN: Invalid VXLAN segment-id *segment-id* for protocol from *ifc-name* : (IP-address/port) to *ifc-name* : (IP-address/port).

**Explanation** The Secure Firewall ASA tries to create an inner connection for a VXLAN packet, but the VXLAN packet has an invalid segment ID.

**Recommended Action** None required.

## 778002

**Error Message** %ASA-6-778002: VXLAN: There is no VNI interface for segment-id *segment-id* .

**Explanation** A decapsulated ingress VXLAN packet is discarded, because the segment ID in the VXLAN header does not match the segment ID of any VNI interface configured on the Secure Firewall ASA.

**Recommended Action** None required.

## 778003

**Error Message** %ASA-6-778003: VXLAN: Invalid VXLAN segment-id *segment-id* for protocol from *ifc-name* : (IP-address/port) to *ifc-name* : (IP-address/port) in FP.

**Explanation** The Secure Firewall ASA Fast Path sees a VXLAN packet with an invalid segment ID.

**Recommended Action** Check the VNI interface segment ID configurations to see if the dropped packet has the VXLAN segment ID that does not match any VNI segment ID configuration.

## 778004

**Error Message** %ASA-6-778004: VXLAN: Invalid VXLAN header for *protocol* from *ifc-name* : (IP-address/port) to *ifc-name* : (IP-address/port) in FP.

**Explanation** The Secure Firewall ASA VTEP sees a VXLAN packet with an invalid VXLAN header.

**Recommended Action** None required.

## 778005

**Error Message** %ASA-6-778005: VXLAN: Packet with VXLAN segment-id *segment-id* from *ifc-name* is denied by FP L2 check.

**Explanation** A VXLAN packet is denied by a Fast Path L2 check.

**Recommended Action** Check the VNI interface segment ID configurations to see if the dropped packet has the VXLAN segment ID that does not match any VNI segment ID configuration. Check to see if the STS table has an entry that matches the dropped packet's segment ID.

## 778006

**Error Message** %ASA-6-778006: VXLAN: Invalid VXLAN UDP checksum from *ifc-name* : (IP-address/port) to *ifc-name* : (IP-address/port) in FP.

**Explanation** The Secure Firewall ASA VTEP received a VXLAN packet with an invalid UDP checksum value.

**Recommended Action** None required.

## 778007

**Error Message** %ASA-6-778007: VXLAN: Packet from *ifc-name* : IP-address/port to IP-address/port was discarded due to invalid NVE peer.

**Explanation** The Secure Firewall ASA VTEP received a VXLAN packet from an IP address that is different from the configured NVE peer.

**Recommended Action** None required.

## 779001

**Error Message** %ASA-6-779001: STS: Out-tag lookup failed for in-tag *segment-id* of *protocol* from *ifc-name* : IP-address /port to IP-address /port .

**Explanation** The Secure Firewall ASA tries to create a connection for a VXLAN packet, but failed to use the STS lookup table to locate the out-tag for the in-tag (segment ID) in the VXLAN packet.

**Recommended Action** None required.

## 779002

**Error Message** %ASA-6-779002: STS: STS and NAT locate different egress interface for segment-id *segment-id* , protocol from *ifc-name* :*IP-address* /*port* to *IP-address* /*port*

**Explanation** The Secure Firewall ASA tries to create a connection for a VXLAN packet, but the STS lookup table and NAT policy locate a different egress interface.

**Recommended Action** None required.

## 779003

**Error Message** %ASA-3-779003: STS: Failed to read tag-switching table - *reason*

**Explanation** The Secure Firewall ASA tried to read the tag-switching table, but failed.

**Recommended Action** None required.

## 779004

**Error Message** %ASA-3-779004: STS: Failed to write tag-switching table - *reason*

**Explanation** The Secure Firewall ASA tried to write to the tag-switching table, but failed.

**Recommended Action** None required.

## 779005

**Error Message** %ASA-3-779005: STS: Failed to parse tag-switching request from http - *reason*

**Explanation** The Secure Firewall ASA tried to parse the HTTP request to see what to do on the tag-switching table, but failed.

**Recommended Action** None required.

## 779006

**Error Message** %ASA-3-779006: STS: Failed to save tag-switching table to flash - *reason*

**Explanation** The Secure Firewall ASA tried to save the tag-switching table to flash memory, but failed.

**Recommended Action** None required.

## 779007

**Error Message** %ASA-3-779007: STS: Failed to replicate tag-switching table to peer - *reason*

**Explanation** The Secure Firewall ASA attempts to replicate the tag-switching table to the failover standby unit or clustering data units, but failed to do so.

**Recommended Action** None required.

## 780001

**Error Message** %ASA-6-780001: RULE ENGINE: Started compilation for access-group transaction - *description of the transaction* .

**Explanation** The rule engine has started compilation for an access group transaction. The description of the transaction is the command line input of the access group itself.

**Recommended Action** None required.

## 780002

**Error Message** %ASA-6-780002: RULE ENGINE: Finished compilation for access-group transaction - *description of the transaction* .

**Explanation** The rule engine has finished compilation for a transaction. Taking access group as an example, the description of the transaction is the command line input of the access group itself.

**Recommended Action** None required.

## 780003

**Error Message** %ASA-6-780003: RULE ENGINE: Started compilation for nat transaction - *description of the transaction* .

**Explanation** The rule engine has started compilation for a NAT transaction. The description of the transaction is the command line input of the **nat** command itself.

**Recommended Action** None required.

## 780004

**Error Message** %ASA-6-780004: RULE ENGINE: Finished compilation for nat transaction - *description of the transaction* .

**Explanation** The rule engine has finished compilation for a NAT transaction. The description of the transaction is the command line input of the **nat** command itself.

**Recommended Action** None required.

## 785001

**Error Message** %ASA-7-785001: Clustering: Ownership for existing flow from <in\_interface>:<src\_ip\_addr>/<src\_port> to <out\_interface>:<dest\_ip\_addr>/<dest\_port> moved from unit <old-owner-unit-id> at site <old-site-id> to <new-owner-unit-id> at site <old-site-id> due to <reason>.

**Explanation** This syslog is generated when clustering moved the flow from one unit in one site to another unit in another site in inter-DC environment. Reason must be whatever triggered the move, such as LISP notification.

**Recommended Action** Verify the flow status in the new unit at new site.

## Messages 802005 to 880001 and 8300001 to 8300006

This section includes messages from 802005 to 880001 and 8300001 to 8300006.

### 802005

**Error Message** %ASA-6-802005: IP *ip\_address* Received MDM request *details*

**Explanation** A new MDM request has been received while the MDM proxy service is active.

**Recommended Action** None required.

### 802006

**Error Message** %ASA-4-802006: IP *ip\_address* MDM request *details* has been rejected: *details*

**Explanation** An MDM request has been rejected by the device.

**Recommended Action** None required.

### 803001

**Error Message** %ASA-6-803001: bypass is continuing after power up, no protection will be provided by the system for traffic over GigabitEthernet 1/1-1/2

**Explanation** Informational message to the user that the hardware bypass will be continued after bootup.

**Recommended Action** None required.

**Error Message** %ASA-6-803001: bypass is continuing after power up, no protection will be provided by the system for traffic over GigabitEthernet 1/3-1/4

**Explanation** Informational message to the user that the hardware bypass will be continued after bootup.

**Recommended Action** None required.

### 803002

**Error Message** %ASA-6-803002: no protection will be provided by the system for traffic over GigabitEthernet 1/1-1/2

**Explanation** Informational message to the user that hardware bypass is manually enabled.

**Recommended Action** None required.

**Error Message** %ASA-6-803002: no protection will be provided by the system for traffic over GigabitEthernet 1/3-1/4

**Explanation** Informational message to the user that hardware bypass is manually enabled.

**Recommended Action** None required.

## 803003

**Error Message** %ASA-6-803003: User disabled bypass manually on GigabitEthernet 1/1-1/2.

**Explanation** Informational message to the user that hardware bypass is manually disabled.

**Recommended Action** None required.

**Error Message** %ASA-6-803003: User disabled bypass manually on GigabitEthernet 1/3-1/4.

**Explanation** Informational message to the user that hardware bypass is manually disabled.

**Recommended Action** None required.

## 804001

**Error Message** %ASA-6-804001: Interface GigabitEthernet1/3 1000BaseSX SFP has been inserted

**Explanation** Informational message to the user about the online insertion of the supported SFP module.

**Recommended Action** None required.

## 804002

**Error Message** %ASA-6-804002: Interface GigabitEthernet1/3 SFP has been removed

**Explanation** Informational message to the user about removal of the supported SFP module.

**Recommended Action** None required.

## 805001

**Error Message** %ASA-6-805001: Flow offloaded: connection conn\_id  
outside\_ifc:outside\_addr/outside\_port (mapped\_addr/mapped\_port)  
inside\_ifc:inside\_addr/inside\_port (mapped\_addr/mapped\_port) Protocol

**Explanation** Indicates flow is offloaded to the super-fast path.

**Recommended Action** None required.

## 805002

**Error Message** %ASA-6-805002: Flow is no longer offloaded: connection conn\_id  
outside\_ifc:outside\_addr/outside\_port (mapped\_addr/mapped\_port)  
inside\_ifc:inside\_addr/inside\_port (mapped\_addr/mapped\_port) Protocol

**Explanation** Indicates flow offloading is disabled on a flow which was offloaded to the super-fast path.

**Recommended Action** None required.

## 805003

**Error Message** %ASA-6-805003: TCP Flow could not be offloaded for connection conn\_id from outside\_ifc:outside\_addr/outside\_port (mapped\_addr/mapped\_port) to inside\_ifc:inside\_addr/inside\_port (mapped\_addr/mapped\_port) reason

**Explanation** Indicates flow could not be offloaded. For example, due to flow entry collision on the offload flow table.

**Recommended Action** None required.

## 806001

**Error Message** %ASA-6-806001: Primary alarm CPU temperature is High temperature

**Explanation** The CPU has reached temperature over primary alarm temperature setting for high temperature and such alarm is enabled.

- temperature – Current CPU temperature (in Celsius).

**Recommended Action** Contact Administrator who configured this alarm on following actions.

## 806002

**Error Message** %ASA-6-806002: Primary alarm for CPU high temperature is cleared

**Explanation** The CPU temperature goes down to under primary alarm temperature setting for high temperature.

**Recommended Action** None required.

## 806003

**Error Message** %ASA-6-806003: Primary alarm CPU temperature is Low temperature

**Explanation** The CPU has reached temperature under primary alarm temperature setting for low temperature and such alarm is enabled.

- temperature – Current CPU temperature (in Celsius).

**Recommended Action** Contact Administrator who configured this alarm on following actions.

## 806004

**Error Message** %ASA-6-806004: Primary alarm for CPU Low temperature is cleared

**Explanation** The CPU temperature goes up to over primary alarm temperature setting for low temperature.

**Recommended Action** None required.

## 806005

**Error Message** %ASA-6-806005: Secondary alarm CPU temperature is High temperature



**Explanation** The CPU has reached temperature over secondary alarm temperature setting for high temperature and such alarm is enabled.

- temperature – Current CPU temperature (in Celsius).

**Recommended Action** Contact Administrator who configured this alarm on following actions.

## 806006

**Error Message** %ASA-6-806006: Secondary alarm for CPU high temperature is cleared

**Explanation** The CPU temperature goes down to under secondary alarm temperature setting for high temperature.

**Recommended Action** None required.

## 806007

**Error Message** %ASA-6-806007: Secondary alarm CPU temperature is Low temperature

**Explanation** The CPU has reached temperature under secondary alarm temperature setting for low temperature and such alarm is enabled.

- temperature – Current CPU temperature (in Celsius).

**Recommended Action** Contact Administrator who configured this alarm on following actions.

## 806008

**Error Message** %ASA-6-806008: Secondary alarm for CPU Low temperature is cleared

**Explanation** The CPU temperature goes up to over secondary alarm temperature setting for low temperature.

**Recommended Action** None required.

## 806009

**Error Message** %ASA-6-806009: Alarm asserted for ALARM\_IN\_1 description

**Explanation** Alarm input port 1 is triggered.

- description – Alarm description configured by user for this alarm input port.

**Recommended Action** Contact Administrator who configured this alarm on following actions.

## 806010

**Error Message** %ASA-6-806010: Alarm cleared for ALARM\_IN\_1 alarm\_1\_description

**Explanation** Alarm input port 1 is cleared.

- description – Alarm description configured by user for this alarm input port.

**Recommended Action** None required.

## 806011

**Error Message** %ASA-6-806011: Alarm asserted for ALARM\_IN\_2 description

**Explanation** Alarm input port 2 is triggered.

- description – Alarm description configured by user for this alarm input port.

**Recommended Action** Contact Administrator who configured this alarm on following actions.

## 806012

**Error Message** %ASA-6-806012: Alarm cleared for ALARM\_IN\_2 alarm\_2\_description

**Explanation** Alarm input port 2 is cleared.

- description – Alarm description configured by user for this alarm input port.

**Recommended Action** None required.

## 812005

**Error Message** %ASA-4-812005: Link-State-Propagation activated on inline-pair due to failure of interface *interface-name* bringing down pair interface *interface-name*

**Explanation** This message is generated when the link state propagation is activated on the inline pair due to failure of an interface.

**Recommended Action** None.

## 812006

**Error Message** %ASA-4-812006: Link-State-Propagation de-activated on inline-pair due to recovery of interface *interface-name* bringing up pair interface *interface-name*

**Explanation** This message is generated when the link state propagation is deactivated on the inline pair due to recovery of failed interface.

**Recommended Action** None.

## 812007

**Error Message** %ASA-6-812007: Inline-set hardware-bypass mode configuration *status*

**Explanation** This message is generated when the state (succeeded or failed) of hardware and software bypass modes for the IPS inline interfaces changes.

**Recommended Action** None.

## 815002

**Error Message** %ASA-2-815002: Denied packet, hard limit, 10000, for object-group search exceeded for UDP from source *IP address/port* to destination *IP address/port*

**Explanation** When object-group-search threshold (by default threshold is 10K) is configured in ASA, and if any OGS search crosses 10k limit, packets are dropped and this message is generated.

**Recommended Action** None.

## 815003

**Error Message** %ASA-4-815003: Object-Group-Search threshold exceeded *current value* threshold (10000) for packet UDP from *source IP address/port* to *destination IP address/port*

**Explanation** When object-group-search threshold is not configured in ASA, and if any OGS search crosses 10000 limit, packets are dropped and this message is generated.

**Recommended Action** None.

## 815004

**Error Message** %ASA-7-815004: OGS: Packet *protocol* from *source IP address/port* to *destination IP address/port* matched *number of source network objects* source network objects and *number of source network objects* destination network objects *total search entries* *total number of entries*. Resultant key-set has *number of entries* entries

**Explanation** This message is generated to provide a detailed information on the object group search entries:

- Source network object count
- Destination network object count
- Total search (product of source and destination count)
- Resultant Key-set value (to be queried in the ACL Lookup)

**Recommended Action** None.

## 840001

**Error Message** %ASA-3-840001: Failed to create the backup for an IKEv2 session <Local IP>, <Remote IP>

**Explanation** In the high-availability setup of distributed site-to-site VPN, an attempt to create a backup session is made when a IKEv2 session is established or when the cluster membership changes. However, the attempt may fail for reasons such as capacity limit. Hence this message is generated on the unit of a session owner whenever it is notified of failing to create a backup.

**Recommended Action** None.

## 850001

**Error Message** %ASA-3-850001: SNORT ID (<snort-instance-id>/<snort-process-id>) Automatic-Application-Bypass due to delay of <delay>ms (threshold <AAB-threshold>ms) with <connection-info>

**Explanation** The Automatic-Application-Bypass (AAB) event is triggered due to packet delay exceeding the AAB threshold.

**Recommended Action** Collect troubleshoot archive, snort core files and contact Cisco TAC.

## 850002

**Error Message** %ASA-3-850002: SNORT ID (<snort-instance-id>/<snort-process-id>) Automatic-Application-Bypass due to SNORT not responding to traffics for <timeout-delay>ms (threshold <AAB-threshold>ms)

**Explanation** The Automatic-Application-Bypass (AAB) event is triggered due to SNORT not responding to traffics for a period exceeding the AAB threshold.

**Recommended Action** Collect troubleshoot archive, snort core files and contact Cisco TAC.

## 870001

**Error Message** %ASA-4-870001: policy-route path-monitoring, remote peer *interface\_name:IP\_Address reachable\_status*

**Explanation** This message appears to display whether the interface on the policy based route identified through path monitoring is reachable or not:

- *reachable\_status*—reachable or unreachable

**Recommended Action** None required.

## 880001

**Error Message** %ASA-6-880001: *Ingress interface, for traffic source ipaddress to destination ipaddress, PBR picked outside interface 1 as its metric-type became better than outside interface 2*

**Explanation** This message is generated whenever the interface chosen is different from previous while forwarding the traffic. Where, metric-types are jitter, cost, mos, packet loss, rtt.

**Recommended Action** None.

## 8300001

**Error Message** %ASA-6-8300001: VPN session redistribution <variable 1>

**Explanation** These events notify the administrator that the operation related to ‘cluster redistribute vpn-sessiondb’ has started or completed. Where,

- <variable 1>—Action: started or completed

**Recommended Action** None.

## 8300002

**Error Message** %ASA-6-8300002: Moved <variable 1> sessions to <variable 2>

**Explanation** Provides details on how many active sessions were moved to another member of the cluster.

- <variable 1>— number of active sessions moved (this can be less than the number requested)
- <variable 2>—name of the cluster member the sessions where moved to

**Recommended Action** None.

## 8300003

**Error Message** %ASA-3-8300003: Failed to send session redistribution message to <variable 1>

**Explanation** There was an error sending a request to another cluster member. This could be due to an internal error or the cluster member the message was destined for is not available.

- <variable 1>— name of the cluster member the message was destined for

**Recommended Action** If this message is persistent contact customer support.

## 8300004

**Error Message** %ASA-6-8300004: <variable 1> request to move <variable 2> sessions from <variable 3> to <variable 4>

**Explanation** This event is displayed when a member receives a request from the director to move a specific number of active sessions to another member in the group.

- <variable 1>—Action: Received, Sent
- <variable 2>—number of active sessions to move
- <variable 3>—name of member receiving the move session request
- <variable 4>—name of the member to receive the active sessions

**Recommended Action** None.

## 8300005

**Error Message** %ASA-3-8300005: Failed to receive session move response from <variable 1>

**Explanation** The director has requested a member to move active sessions to another member. If the director has not received a response to this request within a defined period, it will display this event and terminate the redistribution process.

- <variable 1>—name of member which failed to send a move response within timeout period

**Recommended Action** Re-issue the "cluster redistribute vpn-sessiondb" and if the problem persists, contact support.

## 8300006

**Error Message** %ASA-5-8300006: Cluster topology change detected. VPN session redistribution aborted.

**Explanation** The VPN session redistribution move calculations are based on the active members at the time the process is started. If a member joins or leaves during this process, the director will terminate the session redistribution.

**Recommended Action** Retry the operation when all of the members have joined or left the group.



## APPENDIX **A**

# Messages Listed by Severity Level

---

This appendix contains the following sections:



---

**Note** The ASA does not send severity 0, emergency messages to the syslog server. These are analogous to a UNIX panic message, and denote an unstable system.

---

- [Alert Messages, Severity 1, on page 593](#)
- [Critical Messages, Severity 2, on page 598](#)
- [Error Messages, Severity 3, on page 601](#)
- [Warning Messages, Severity 4, on page 621](#)
- [Notification Messages, Severity 5, on page 636](#)
- [Informational Messages, Severity 6, on page 646](#)
- [Debugging Messages, Severity 7, on page 663](#)
- [Variables Used in Syslog Messages, on page 671](#)

## Alert Messages, Severity 1

The following messages appear at severity 1, alerts:



---

**Note** The security event syslog messages (430001, 430002, 430003, 430004, 430005, and 430006) appear with varied severity levels depending on the nature of the event. For information on the messages and fields, see *Security Event Syslog Message ID* in the Cisco Secure Firewall Threat Defense Syslog Messages Guide .

---

- %ASA-1-101001: (Primary) Failover cable OK.
- %ASA-1-101002: (Primary) Bad failover cable.
- %ASA-1-101003: (Primary) Failover cable not connected (this unit).
- %ASA-1-101004: (Primary) Failover cable not connected (other unit).
- %ASA-1-101005: (Primary) Error reading failover cable status.
- %ASA-1-103001: (Primary) No response from other firewall (reason code = code).

- %ASA-1-103002: (Primary) Other firewall network interface interface\_number OK.
- %ASA-1-103003: (Primary) Other firewall network interface interface\_number failed.
- %ASA-1-103004: (Primary) Other firewall reports this firewall failed. Reason: reason-string.
- %ASA-1-103005: (Primary) Other firewall reporting failure. Reason: SSM card failure.
- %ASA-1-103006: (Primary|Secondary) Mate version ver\_num is not compatible with ours ver\_num.
- %ASA-1-103007: (Primary|Secondary) Mate version ver\_num is not identical with ours ver\_num
- %ASA-1-103008: Mate hwdib index is not compatible.
- %ASA-1-104001: (Primary) Switching to ACTIVE (cause: string).
- %ASA-1-104002: (Primary) Switching to STANDBY (cause: string).
- %ASA-1-104003: (Primary) Switching to FAILED.
- %ASA-1-104004: (Primary) Switching to OK.
- %ASA-1-104501: (Primary|Secondary) Switching to ACTIVE (cause: reason)
- %ASA-1-104501: (Primary|Secondary) Switching to BACKUP (cause: reason)
- %ASA-1-104502: (Primary|Secondary) Becoming Backup unit failed
- %ASA-1-105001: (Primary) Disabling failover.
- %ASA-1-105002: (Primary) Enabling failover.
- %ASA-1-105003: (Primary) Monitoring on interface interface\_name waiting
- %ASA-1-105004: (Primary) Monitoring on interface interface\_name normal
- %ASA-1-105005: (Primary) Lost Failover communications with mate on interface interface\_name.
- %ASA-1-105006: (Primary) Link status Up on interface interface\_name.
- %ASA-1-105007: (Primary) Link status Down on interface interface\_name.
- %ASA-1-105008: (Primary) Testing interface interface\_name.
- %ASA-1-105009: (Primary) Testing on interface interface\_name {Passed|Failed}.
- %ASA-1-105011: (Primary) Failover cable communication failure
- %ASA-1-105020: (Primary) Incomplete/slow config replication
- %ASA-1-105021: (failover\_unit) Standby unit failed to sync due to a locked context\_name config. Lock held by lock\_owner\_name.
- %ASA-1-105022: (host) Config replication failed with reason = (reason)
- %ASA-1-105031: Failover LAN interface is up.
- %ASA-1-105032: LAN Failover interface is down.
- %ASA-1-105033: LAN FO cmd Iface down and up again.
- %ASA-1-105034: Receive a LAN\_FAILOVER\_UP message from peer.



- %ASA-1-105035: Receive a LAN failover interface down msg from peer.
- %ASA-1-105036: dropped a LAN Failover command message.
- %ASA-1-105037: The primary and standby units are switching back and forth as the active unit.
- %ASA-1-105038: (Primary) Interface count mismatch.
- %ASA-1-105039: (Primary) Unable to verify the Interface count with mate. Failover may be disabled in mate.
- %ASA-1-105040: (Primary) Mate failover version is not compatible.
- %ASA-1-105041: cmd failed during sync.
- %ASA-1-105042: (Primary) Failover interface OK.
- %ASA-1-105043: (Primary) Failover interface failed.
- %ASA-1-105044: (Primary) Mate operational mode mode is not compatible with my mode mode.
- %ASA-1-105045: (Primary) Mate license (number contexts) is not compatible with my license (number contexts).
- %ASA-1-105046: (Primary|Secondary) Mate has a different chassis.
- %ASA-1-105047: Mate has a io\_card\_name1 card in slot slot\_number which is different from my io\_card\_name2
- %ASA-1-105048: (unit) Mate's service module (application) is different from mine (application).
- %ASA-1-105502: (Primary|Secondary) Restarting Cloud HA on this unit, reason: string.
- %ASA-1-106021: Deny protocol reverse path check from source\_address to dest\_address on interface interface\_name.
- %ASA-1-106022: Deny protocol connection spoof from source\_address to dest\_address on interface interface\_name.
- %ASA-1-106101: Number of cached deny-flows for ACL log has reached limit (number).
- %ASA-1-107001: RIP auth failed from IP\_address: version=number, type=string, mode=string, sequence=number on interface interface\_name.
- %ASA-1-107002: RIP pkt failed from IP\_address: version=number on interface interface\_name.
- %ASA-1-111111 error\_message.
- %ASA-1-114001: Failed to initialize 4GE SSM I/O card (error error\_string).
- %ASA-1-114002: Failed to initialize SFP in 4GE SSM I/O card (error error\_string).
- %ASA-1-114003: Failed to run cached commands in 4GE SSM I/O card (error error\_string).
- %ASA-1-1199012: Stack smash during new\_stack\_call in process/fiber process/fiber, call target f, stack size s, process/fiber name of the process/fiber that caused the stack smash.
- %ASA-1-199010: Signal 11 caught in process/fiber(rtcli async executor process)/(rtcli async executor) at address 0xf132e03b, corrective action at 0xca1961a0
- %ASA-1-199013: syslog.

- %ASA-1-199021: System memory utilization has reached the configured watchdog trigger level of Y%. System will now reload.
- %ASA-1-211004: WARNING: Minimum Memory Requirement for ASA version ver not met for ASA image. min MB required, actual MB found.
- %ASA-n-216001: internal error in: function: message
- %ASA-1-216005: ERROR: Duplex-mismatch on interface\_name resulted in transmitter lockup. A soft reset of the switch was performed.
- %ASA-1-323006: Module ips experienced a data channel communication failure, data channel is DOWN.
- %ASA-1-332004: Web Cache IP\_address/service\_ID lost.
- %ASA-1-413007: An unsupported ASA and IPS configuration is installed. mpc\_description with ips\_description is not supported.
- %ASA-1-413008: There was a backplane PCI communications failure with module module\_description\_string in slot slot\_num.
- %ASA-1-505011: Module ips data channel communication is UP.
- %ASA-1-505014: Module module\_id, application down name, version version reason.
- %ASA-1-505015: Module module\_id, application up application, version version.
- %ASA-1-709003: (Primary) Beginning configuration replication: Sending to mate.
- %ASA-1-709004: (Primary) End Configuration Replication (ACT).
- %ASA-1-709005: (Primary) Beginning configuration replication: Receiving from mate.
- %ASA-1-709006: (Primary) End Configuration Replication (STB).
- %ASA-1-713900: Descriptive\_event\_string.
- %ASA-1-716507: Fiber scheduler has reached unreachable code. Cannot continue, terminating.
- %ASA-1-716508: internal error in: function: Fiber scheduler is scheduling rotten fiber. Cannot continuing terminating.
- %ASA-1-716509: internal error in: function: Fiber scheduler is scheduling alien fiber. Cannot continue terminating.
- %ASA-1-716510: internal error in: function: Fiber scheduler is scheduling finished fiber. Cannot continue terminating.
- %ASA-1-716516: internal error in: function: OCCAM has corrupted ROL array. Cannot continue terminating.
- %ASA-1-716519: internal error in: function: OCCAM has corrupted pool list. Cannot continue terminating.
- %ASA-1-716528: Unexpected fiber scheduler error; possible out-of-memory condition.
- %ASA-1-717049: Local CA Server certificate is due to expire in number days and a replacement certificate is available for export.
- %ASA-1-717054: The type certificate in the trustpoint tp name is due to expire in number days. Expiration date and time Subject Name subject name Issuer Name issuer name Serial Number serial number.

- %ASA-1-717055: The type certificate in the trustpoint tp name has expired. Expiration date and time Subject Name subject name Issuer Name issuer name Serial Number serial number.
- %ASA-1-735001 Cooling Fan var1: OK.
- %ASA-1-735002 Cooling Fan var1: Failure Detected.
- %ASA-1-735003 Power Supply var1: OK.
- %ASA-1-735004 Power Supply var1: Failure Detected.
- %ASA-1-735005 Power Supply Unit Redundancy OK.
- %ASA-1-735006 Power Supply Unit Redundancy Lost.
- %ASA-1-735007 CPU var1: Temp: var2 var3, Critical.
- %ASA-1-735008 IPMI: Chassis Ambient var1: Temp: var2 var3, Critical.
- %ASA-1-735011: Power Supply var1: Fan OK.
- %ASA-1-735012: Power Supply var1: Fan Failure Detected.
- %ASA-1-735013: Voltage Channel var1: Voltage OK.
- %ASA-1-735014: Voltage Channel var1: Voltage Critical.
- %ASA-1-735017: Power Supply var1: Temp: var2 var3, OK.
- %ASA-1-735020: CPU var1: Temp: var2 var3 OK.
- %ASA-1-735021: Chassis var1: Temp: var2 var3 OK.
- %ASA-1-735022: CPU# is running beyond the max thermal operating temperature and the device will be shutting down immediately to prevent permanent damage to the CPU.
- %ASA-1-735024: IO Hub var1: Temp: var2 var3, OK.
- %ASA-1-735025: IO Hub var1: Temp: var2 var3, Critical.
- %ASA-1-735027: CPU cpu\_num Voltage Regulator is running beyond the max thermal operating temperature and the device will be shutting down immediately. The chassis and CPU need to be inspected immediately for ventilation issues.
- %ASA-1-735029: IO Hub is running beyond the max thermal operating temperature and the device will be shutting down immediately to prevent permanent damage to the circuit.
- %ASA-1-743000: The PCI device with vendor ID: vendor\_id device ID: device\_id located at bus:device.function bus\_num:dev\_num, func\_num has a link link\_attr\_name of actual\_link\_attr\_val when it should have a link link\_attr\_name of expected\_link\_attr\_val.
- %ASA-1-743001: Backplane health monitoring detected link failure.
- %ASA-1-743002: Backplane health monitoring detected link OK.
- %ASA-1-743004: System is not fully operational - PCI device with vendor ID vendor\_id (vendor\_name), device ID device\_id (device\_name) not found.
- %ASA-1-770002: Resource resource allocation is more than the permitted limit for this platform. ASA will be rebooted.

## Critical Messages, Severity 2

The following messages appear at severity 2, critical:

- %ASA-2-105506: (Primary|Secondary) Unable to create socket on port port for (failover connection | load balancer probes), error: error\_string
- %ASA-2-105507: (Primary|Secondary) Unable to bind socket on port port for (failover connection | load balancer probes), error: error\_string
- %ASA-2-105508: (Primary|Secondary) Error creating failover connection socket on port port
- %ASA-2-105525: (Primary|Secondary) Incomplete configuration to initiate access token change request
- %ASA-2-105526: (Primary|Secondary) Unexpected status in response to access token request: status\_string
- %ASA-2-105527: (Primary|Secondary) Failure reading response to access token request
- %ASA-2-105528: (Primary|Secondary) No access token in response to access token request
- %ASA-2-105529: (Primary|Secondary) Error creating authentication header from access token
- %ASA-2-105530: (Primary|Secondary) No response to access token request url
- %ASA-2-105531: (Primary|Secondary) Failed to obtain route-table information needed for change request for route-table route\_table\_name
- %ASA-2-105532: (Primary|Secondary) Unexpected status in response to route-table change request for route-table route\_table\_name: status\_string
- %ASA-2-105533: (Primary|Secondary) Failure reading response to route-table change request for route-table route\_table\_name
- %ASA-2-105534: (Primary|Secondary) No provisioning state in response to route-table change request route-table route\_table\_name
- %ASA-2-105535: (Primary|Secondary) No response to route-table change request for route-table route\_table\_name from url
- %ASA-2-105536: (Primary|Secondary) Failed to obtain Azure authentication header for route status request for route route\_name
- %ASA-2-105537: (Primary|Secondary) Unexpected status in response to route state request for route route\_name: status\_string
- %ASA-2-105538: (Primary|Secondary) Failure reading response to route state request for route route\_name
- %ASA-2-105539: (Primary|Secondary) No response to route state request for route route\_name from url
- %ASA-2-105540: (Primary|Secondary) No route-tables configured
- %ASA-2-105541: (Primary|Secondary) Failed to update route-table route\_table\_name, provisioning state: state\_string
- %ASA-2-105544: (Primary|Secondary) Error creating load balancer probe socket on port port

- %ASA-2-106001: Inbound TCP connection denied from IP\_address/port to IP\_address/port flags tcp\_flags on interface interface\_name
- %ASA-2-106002: protocol Connection denied by outbound list acl\_ID src inside\_address dest outside\_address
- %ASA-2-106006: Deny inbound UDP from outside\_address/outside\_port to inside\_address/inside\_port on interface interface\_name.
- %ASA-2-106007: Deny inbound UDP from outside\_address/outside\_port to inside\_address/inside\_port due to DNS {Response|Query}.
- %ASA-2-106013: Dropping echo request from IP\_address to PAT address IP\_address
- %ASA-2-106016: Deny IP spoof from (IP\_address) to IP\_address on interface interface\_name.
- %ASA-2-106017: Deny IP due to Land Attack from IP\_address to IP\_address
- %ASA-2-106018: ICMP packet type ICMP\_type denied by outbound list acl\_ID src inside\_address dest outside\_address
- %ASA-2-106020: Deny IP teardrop fragment (size = number, offset = number) from IP\_address to IP\_address
- %ASA-2-106024: Access rules memory exhausted
- %ASA-2-108002: SMTP replaced string: out source\_address in inside\_address data: string
- %ASA-2-108003: Terminating ESMTP/SMTP connection; malicious pattern detected in the mail address from source\_interface:source\_address/source\_port to dest\_interface:dest\_address/dset\_port. Data:string
- %ASA-2-109011: Authen Session Start: user 'user', sid number
- %ASA-2-112001: (string:dec) Clear complete.
- %ASA-2-113022: AAA Marking RADIUS server servername in aaa-server group AAA-Using-DNS as FAILED
- %ASA-2-113023: AAA Marking protocol server ip-addr in server group tag as ACTIVE
- %ASA-2-113027: Username could not be found in certificate
- %ASA-2-115000: Critical assertion in process: process name fiber: fiber name, component: component name, subcomponent: subcomponent name, file: filename, line: line number, cond: condition
- %ASA-2-199011: Close on bad channel in process/fiber process/fiber, channel ID p, channel state s process/fiber name of the process/fiber that caused the bad channel close operation.
- %ASA-2-199014: syslog
- %ASA-2-199020: System memory utilization has reached X%. System will reload if memory usage reaches the configured trigger level of Y%.
- %ASA-2-201003: Embryonic limit exceeded nconns/elimit for outside\_address/outside\_port (global\_address) inside\_address/inside\_port on interface interface\_name
- %ASA-2-214001: Terminating manager session from IP\_address on interface interface\_name. Reason: incoming encrypted data (number bytes) longer than number bytes
- %ASA-2-215001:Bad route\_compress() call, sdb= number
- %ASA-2-217001: No memory for string in string
- %ASA-2-218001: Failed Identification Test in slot# [fail#/res].
- %ASA-2-218002: Module (slot#) is a registered proto-type for Cisco Lab use only, and not certified for live network operation.
- %ASA-2-218003: Module Version in slot# is obsolete. The module in slot = slot# is obsolete and must be returned via RMA to Cisco Manufacturing. If it is a lab unit, it must be returned to Proto Services for upgrade.
- %ASA-2-218004: Failed Identification Test in slot# [fail#/res]
- %ASA-2-218005: Inconsistency detected in the system information programmed in non-volatile memory
- %ASA-2-304007: URL Server IP\_address not responding, ENTERING ALLOW mode.

- %ASA-2-304008: LEAVING ALLOW mode, URL Server is up.
- %ASA-2-321005: System CPU utilization reached utilization %
- %ASA-2-321006: System memory usage reached utilization %
- %ASA-2-410002: Dropped num DNS responses with mis-matched id in the past sec second(s): from src\_ifc:sip/sport to dest\_ifc:dip/dport
- %ASA-2-444004: Temporary license key key has expired. Applying permanent license key permkey
- %ASA-2-444007: Timebased activation key activation-key has expired. Reverting to [permanent | timebased] license key. The following features will be affected: feature, feature
- %ASA-2-444009: %s license has expired 30 days ago. The system will now reload.
- %ASA-2-444102: Shared license service inactive. License server is not responding
- %ASA-2-444105: Released value shared licensetype license(s). License server has been unreachable for 24 hours
- %ASA-2-444111: Shared license backup service has been terminated due to the primary license server address being unavailable for more than days days. The license server needs to be brought back online to continue using shared licensing.
- %ASA-2-444302: %SMART\_LIC-2-PLATFORM\_ERROR: Platform error.
- %ASA-2-709007: Configuration replication failed for command command
- %ASA-2-713078: Temp buffer for building mode config attributes exceeded: bufsize available\_size, used value
- %ASA-2-713176: Device\_type memory resources are critical, IKE key acquire message on interface interface\_number, for Peer IP\_address ignored
- %ASA-2-713901: Descriptive\_text\_string.
- %ASA-2-716500: internal error in: function: Fiber library cannot locate AK47 instance
- %ASA-2-716501: internal error in: function: Fiber library cannot attach AK47 instance
- %ASA-2-716502: internal error in: function: Fiber library cannot allocate default arena
- %ASA-2-716503: internal error in: function: Fiber library cannot allocate fiber descriptors pool
- %ASA-2-716504: internal error in: function: Fiber library cannot allocate fiber stacks pool
- %ASA-2-716505: internal error in: function: Fiber has joined fiber in unfinished state
- %ASA-2-716506: UNICORN\_SYSLOGID\_JOINED\_UNEXPECTED\_FIBER
- %ASA-2-716512: internal error in: function: Fiber has joined fiber waited upon by someone else
- %ASA-2-716513: internal error in: function: Fiber in callback blocked on other channel
- %ASA-2-716515: internal error in: function: OCCAM failed to allocate memory for AK47 instance
- %ASA-2-716517: internal error in: function: OCCAM cached block has no associated arena
- %ASA-2-716518: internal error in: function: OCCAM pool has no associated arena
- %ASA-2-716520: internal error in: function: OCCAM pool has no block list
- %ASA-2-716521: internal error in: function: OCCAM no realloc allowed in named pool
- %ASA-2-716522: internal error in: function: OCCAM corrupted standalone block
- %ASA-2-716525: UNICORN\_SYSLOGID\_SAL\_CLOSE\_PRIVDATA\_CHANGED
- %ASA-2-716526: UNICORN\_SYSLOGID\_PERM\_STORAGE\_SERVER\_LOAD\_FAIL
- %ASA-2-716527: UNICORN\_SYSLOGID\_PERM\_STORAGE\_SERVER\_STORE\_FAI
- %ASA-2-717008: Insufficient memory to process\_requiring\_memory.
- %ASA-2-717011: Unexpected event event event\_ID
- %ASA-2-717040: Local CA Server has failed and is being disabled. Reason: reason.
- %ASA-2-735009: IPMI: Environment Monitoring has failed initialization and configuration. Environment Monitoring is not running.

- %ASA-2-735023: ASA was previously shutdown due to the CPU complex running beyond the maximum thermal operating temperature. The chassis needs to be inspected immediately for ventilation issues.
- %ASA-2-735028: ASA was previously shutdown due to a CPU Voltage Regulator running beyond the max thermal operating temperature. The chassis and CPU need to be inspected immediately for ventilation issues.
- %ASA-2-736001: Unable to allocate enough memory at boot for jumbo-frame reservation. Jumbo-frame support has been disabled.
- %ASA-2-747009: Clustering: Fatal error due to failure to create RPC server for module module name.
- %ASA-2-747011: Clustering: Memory allocation error.%ASA-2-752001: Tunnel Manager received invalid parameter to remove record.
- %ASA-2-748007: Failed to de-bundle the ports for module slot\_number in chassis chassis\_number; traffic may be black holed
- %ASA-2-752001: Tunnel Manager received invalid parameter to remove record.
- %ASA-2-752005: Tunnel Manager failed to dispatch a KEY\_ACQUIRE message. Memory may be low. Map Tag = mapTag. Map Sequence Number = mapSeq.
- %ASA-2-772003: PASSWORD: session login failed, user username, IP ip, cause: password expired
- %ASA-2-772006: REAUTH: user username failed authentication
- %ASA-2-774001: POST: unspecified error
- %ASA-2-774002: POST: error err, func func, engine eng, algorithm alg, mode mode, dir dir, key len len
- %ASA-2-775007: Scansafe: Primary server\_interface\_name:server\_ip\_address and backup server\_interface\_name:server\_ip\_address servers are not reachable.
- %ASA-2-815002: Denied packet, hard limit, 10000, for object-group search exceeded for UDP from <source IP address/port> to <destination IP address/port>

## Error Messages, Severity 3

The following messages appear at severity 3, errors:

- %ASA-3-105010: (Primary) Failover message block alloc failed
- %ASA-3-105050: ASAv ethernet interface mismatch
- %ASA-3-105052: HA cipher in use *algorithm name* strong encryption is AVAILABLE, please reboot to use strong cipher and preferably change the key in use.
- %ASA-3-105509: (Primary|Secondary) Error sending message\_name message to peer unit peer-ip, error: error\_string
- %ASA-3-105510: (Primary|Secondary) Error receiving message from peer unit peer-ip, error: error\_string
- %ASA-3-105511: (Primary|Secondary) Incomplete read of message header of message from peer unit peer-ip: bytes bytes read of expected header\_length header bytes
- %ASA-3-105512: (Primary|Secondary) Error receiving message body of message from peer unit peer-ip, error: error\_string
- %ASA-3-105513: (Primary|Secondary) Incomplete read of message body of message from peer unit peer-ip: bytes bytes read of expected message\_length message body bytes

- %ASA-3-105514: (Primary|Secondary) Error occurred when responding to message\_name message received from peer unit peer-ip, error: error\_string
- %ASA-3-105515: (Primary|Secondary) Error receiving message\_name message from peer unit peer-ip, error: error\_string
- %ASA-3-105516: (Primary|Secondary) Incomplete read of message header of message\_name message from peer unit peer-ip: bytes bytes read of expected header\_length header bytes
- %ASA-3-105517: (Primary|Secondary) Error receiving message body of message\_name message from peer unit peer-ip, error: error\_string
- %ASA-3-105518: (Primary|Secondary) Incomplete read of message body of message\_name message from peer unit peer-ip: bytes bytes read of expected message\_length message body bytes
- %ASA-3-105519: (Primary|Secondary) Invalid response to message\_name message received from peer unit peer-ip: type message\_type, version message\_version, length message\_length
- %ASA-3-105545: (Primary|Secondary) Error starting load balancer probe socket on port port, error code: error\_code
- %ASA-3-105546: (Primary|Secondary) Error starting load balancer probe handler
- %ASA-3-105547: (Primary|Secondary) Error generating encryption key for Azure secret key
- %ASA-3-105548: (Primary|Secondary) Error storing encryption key for Azure secret key
- %ASA-3-105549: (Primary|Secondary) Error retrieving encryption key for Azure secret key
- %ASA-3-105550: (Primary|Secondary) Error encrypting Azure secret key
- %ASA-3-105551: (Primary|Secondary) Error encrypting Azure secret key
- %ASA-3-106010: Deny inbound protocol src [interface\_name: source\_address/source\_port] [(idfw\_user | FQDN\_string), sg\_info] dst [interface\_name: dest\_address/dest\_port] [(idfw\_user | FQDN\_string), sg\_info]
- %ASA-3-106011: Deny inbound (No xlate) protocol src Interface:IP/port dst Interface-name:IP/port
- %ASA-3-106014: Deny inbound icmp src interface\_name: IP\_address [(idfw\_user | FQDN\_string), sg\_info] dst interface\_name: IP\_address [(idfw\_user | FQDN\_string), sg\_info] (type dec, code dec)
- %ASA-3-109010: Auth from inside\_address/inside\_port to outside\_address/outside\_port failed (too many pending auths) on interface interface\_name.
- %ASA-3-109013: User must authenticate before using this service
- %ASA-3-109016: Can't find authorization ACL acl\_ID for user 'user'
- %ASA-3-109018: Downloaded ACL acl\_ID is empty
- %ASA-3-109019: Downloaded ACL acl\_ID has parsing error; ACE string
- %ASA-3-109020: Downloaded ACL has config error; ACE
- %ASA-3-109023: User from source\_address/source\_port to dest\_address/dest\_port on interface outside\_interface must authenticate before using this service.
- %ASA-3-109026: [aaa protocol] Invalid reply digest received; shared server key may be mismatched.
- %ASA-3-109032: Unable to install ACL access\_list, downloaded for user username; Error in ACE: ace.
- %ASA-3-109035: Exceeded maximum number (<max\_num>) of DAP attribute instances for user <user>
- %ASA-3-109037: Exceeded 5000 attribute values for the attribute name attribute for user username



- %ASA-3-109038: Attribute internal-attribute-name value string-from-server from AAA server could not be parsed as a type internal-attribute-name string representation of the attribute name
- %ASA-3-109103: CoA action-type from coa-source-ip failed for user username, with session ID: audit-session-id.
- %ASA-3-109104: CoA action-type from coa-source-ip failed for user username, session ID: audit-session-id. Action not supported.
- %ASA-3-109105: Failed to determine the egress interface for locally generated traffic destined to <protocol> <IP>:<port>
- %ASA-3-109203: UAUTH Session *session*, User *username*, Assigned IP *IP Address*, Failed adding entry.
- %ASA-3-109205: UAUTH Session *session*, User *username*, Assigned IP *IP Address*, Failed applying filter.
- %ASA-3-109206: UAUTH Session *session*, User *username*, Assigned IP *IP Address*, Removing stale entry added *hours* ago.
- %ASA-3-109208: UAUTH Session *session*, User *username*, Assigned IP *IP Address*, Failed updating entry - no entry.
- %ASA-3-109209: UAUTH Session *session*, User *username*, Assigned IP *IP Address*, Failed updating filter for entry.
- %ASA-3-109212: UAUTH Session *session*, User *username*, Assigned IP *IP Address*, Failed removing entry.
- %ASA-3-109213: UAUTH Session *session*, User *username*, Assigned IP *IP Address* Failed removing entry.
- %ASA-3-113001: Unable to open AAA session. Session limit [limit] reached.
- %ASA-3-113018: User: user, Unsupported downloaded ACL Entry: ACL\_entry, Action: action
- %ASA-3-113020: Kerberos error: Clock skew with server ip\_address greater than 300 seconds
- %ASA-3-113021: Attempted console login failed. User username did NOT have appropriate Admin Rights.
- %ASA-3-114006: Failed to get port statistics in 4GE SSM I/O card (error error\_string).
- %ASA-3-114007: Failed to get current msr in 4GE SSM I/O card (error error\_string).
- %ASA-3-114008: Failed to enable port after link is up in 4GE SSM I/O card due to either I2C serial bus access error or switch access error.
- %ASA-3-114009: Failed to set multicast address in 4GE SSM I/O card (error error\_string).
- %ASA-3-114010: Failed to set multicast hardware address in 4GE SSM I/O card (error error\_string).
- %ASA-3-114011: Failed to delete multicast address in 4GE SSM I/O card (error error\_string).
- %ASA-3-114012: Failed to delete multicast hardware address in 4GE SSM I/O card (error error\_string).
- %ASA-3-114013: Failed to set mac address table in 4GE SSM I/O card (error error\_string).
- %ASA-3-114014: Failed to set mac address in 4GE SSM I/O card (error error\_string).
- %ASA-3-114015: Failed to set mode in 4GE SSM I/O card (error error\_string).
- %ASA-3-114016: Failed to set multicast mode in 4GE SSM I/O card (error error\_string).
- %ASA-3-114017: Failed to get link status in 4GE SSM I/O card (error error\_string).
- %ASA-3-114018: Failed to set port speed in 4GE SSM I/O card (error error\_string).
- %ASA-3-114019: Failed to set media type in 4GE SSM I/O card (error error\_string).
- %ASA-3-114020: Port link speed is unknown in 4GE SSM I/O card.
- %ASA-3-114021: Failed to set multicast address table in 4GE SSM I/O card due to error.

- %ASA-3-114022: Failed to pass broadcast traffic in 4GE SSM I/O card due to error\_string
- %ASA-3-114023: Failed to cache/flush mac table in 4GE SSM I/O card due to error\_string.
- %ASA-3-115001: Error in process: process name fiber: fiber name, component: component name, subcomponent: subcomponent name, file: filename, line: line number, cond: condition.
- %ASA-3-120010: Notify command command to SCH client client failed. Reason reason.
- %ASA-3-199015: syslog
- %ASA-3-201002: Too many TCP connections on {static|xlate} global\_address! econns nconns
- %ASA-3-201004: Too many UDP connections on {static|xlate} global\_address! udp connections limit
- %ASA-3-201005: FTP data connection failed for IP\_address IP\_address
- %ASA-3-201006: RCMD backconnection failed for IP\_address/port.
- %ASA-3-201008: Disallowing new connections.
- %ASA-3-201009: TCP connection limit of number for host IP\_address on interface\_name exceeded
- %ASA-3-201011: Connection limit exceeded cnt/limit for dir packet from sip/sport to dip/dport on interface if\_name.
- %ASA-3-201013: Per-client connection limit exceeded curr num/limit for [input|output] packet from ip/port to ip/port on interface interface\_name
- %ASA-3-202001: Out of address translation slots!
- %ASA-3-202005: Non-embryonic in embryonic list outside\_address/outside\_port inside\_address/inside\_port
- %ASA-3-202010: [NAT | PAT] pool exhausted in pool-name ip\_address, port range [1-511 | 512-1023 | 1024-65535]. Unable to create protocol connection from in-interface:src-ip/src-port to out-interface:dst-ip/dst-port.
- %ASA-3-202016: "%d: Unable to pre-allocate SIP %s secondary channel for message "\ "from %s:%A/%d to %s:%A/%d with PAT and missing port information."
- %ASA-3-208005: (function:line\_num) clear command return code
- %ASA-3-210001: LU sw\_module\_name error = number
- %ASA-3-210002: LU allocate block (bytes) failed.
- %ASA-3-210003: Unknown LU Object number
- %ASA-3-210005: LU allocate secondary(optional) connection failed for protocol[TCP|UDP] connection from ingress interface name:Real IP Address/Real Port to egress interface name:Real IP Address/Real Port
- %ASA-3-210006: LU look NAT for IP\_address failed
- %ASA-3-210007: LU allocate xlate failed for type[static | dynamic]-[NAT | PAT] secondary(optional) protocol translation from ingress interface name:Real IP Address/real port (Mapped IP Address/Mapped Port) to egress interface name:Real IP Address/Real Port (Mapped IP Address/Mapped Port)
- %ASA-3-210008: LU no xlate for inside\_address/inside\_port outside\_address/outside\_port
- %ASA-3-210010: LU make UDP connection for outside\_address:outside\_port inside\_address:inside\_port failed
- %ASA-3-210020: LU PAT port port reserve failed
- %ASA-3-210021: LU create static xlate global\_address ifc interface\_name failed
- %ASA-3-211001: Memory allocation Error
- %ASA-3-211003: Error in computed percentage CPU usage value
- %ASA-3-212001: Unable to open SNMP channel (UDP port port) on interface interface\_number, error code = code
- %ASA-3-212002: Unable to open SNMP trap channel (UDP port port) on interface interface\_number, error code = code

- %ASA-3-212003: Unable to receive an SNMP request on interface interface\_number, error code = code, will try again.
- %ASA-3-212004: Unable to send an SNMP response to IP Address IP\_address Port port interface interface\_number, error code = code
- %ASA-3-212005: incoming SNMP request (number bytes) on interface interface\_name exceeds data buffer size, discarding this SNMP request.
- %ASA-3-212006: Dropping SNMP request from src\_addr/src\_port to ifc:dst\_addr/dst\_port because: reason username.
- %ASA-3-212010: Configuration request for SNMP user %s failed. Host %s reason.
- %ASA-3-212011: SNMP engineBoots is set to maximum value. Reason: %s User intervention necessary.
- %ASA-3-212012: Unable to write SNMP engine data to persistent storage.
- %ASA-3-213001: PPTP control daemon socket io string, errno = number.
- %ASA-3-213002: PPTP tunnel hashtable insert failed, peer = IP\_address.
- %ASA-3-213003: PPP virtual interface interface\_number isn't opened.
- %ASA-3-213004: PPP virtual interface interface\_number client ip allocation failed.
- %ASA-3-213005%: Dynamic-Access-Policy action (DAP) action aborted
- %ASA-3-213006%: Unable to read dynamic access policy record.
- %ASA-3-216002: Unexpected event (major: major\_id, minor: minor\_id) received by task\_string in function at line: line\_num
- %ASA-3-216003: Unrecognized timer timer\_ptr, timer\_id received by task\_string in function at line: line\_num
- %ASA-3-219002: I2C\_API\_name error, slot = slot\_number, device = device\_number, address = address, byte count = count. Reason: reason\_string
- %ASA-3-302019: H.323 library\_name ASN Library failed to initialize, error code number
- %ASA-3-302302: ACL = deny; no sa created
- %ASA-3-304003: URL Server IP\_address timed out URL url
- %ASA-3-304006: URL Server IP\_address not responding
- %ASA-3-305005: No translation group found for protocol src interface\_name: source\_address/source\_port [(idfw\_user)] dst interface\_name: dest\_address/dest\_port [(idfw\_user)]
- %ASA-3-305006: {outbound static|identity|portmap|regular) translation creation failed for protocol src interface\_name:source\_address/source\_port [(idfw\_user)] dst interface\_name:dest\_address/dest\_port [(idfw\_user)]
- %ASA-3-305008: Free unallocated global IP address.
- %ASA-3-305016: Unable to create protocol connection from real\_interface:real\_host\_ip/real\_source\_port to real\_dest\_interface:real\_dest\_ip/real\_dest\_port due to reason.
- %ASA-3-305017: Pba-interim-logging: Active ICMP block of ports for translation from <source device IP> to <destination device IP>/<Active Port Block >
- %ASA-3-305019: MAP node address <ip>/<port> has inconsistent Port Set ID encoding
- %ASA-3-305020: MAP node with address <ip> is not allowed to use port <port>\n
- %ASA-3-313001: Denied ICMP type=number, code=code from IP\_address on interface interface\_name
- %ASA-3-313008: Denied ICMPv6 type=number, code=code from IP\_address on interface interface\_name
- %ASA-3-315004: Fail to establish SSH session because RSA host key retrieval failed.
- %ASA-3-315012: Weak SSH type (alg) provided from client 'IP' on interface int. Connection failed. Not FIPS 140-2 compliant
- %ASA-3-316001: Denied new tunnel to IP\_address. VPN peer limit (platform\_vpn\_peer\_limit) exceeded
- %ASA-3-316002: VPN Handle error: protocol=protocol, src in\_if\_num:src\_addr, dst out\_if\_num:dst\_addr

- %ASA-3-317001: No memory available for limit\_slow
- %ASA-3-317002: Bad path index of number for IP\_address, number max
- %ASA-3-317003: IP routing table creation failure - reason
- %ASA-3-317004: IP routing table limit warning
- %ASA-3-317005: IP routing table limit exceeded - reason, IP\_address netmask
- %ASA-3-317006: Pdb index error pdb, pdb\_index, pdb\_type
- %ASA-3-317012: Interface IP route counter negative - nameif-string-value
- %ASA-3-318001: Internal error: reason
- %ASA-3-318002: Flagged as being an ABR without a backbone area
- %ASA-3-318003: Reached unknown state in neighbor state machine
- %ASA-3-318004: area string lsid IP\_address mask netmask adv IP\_address type number
- %ASA-3-318005: lsid ip\_address adv IP\_address type number gateway gateway\_address metric number network IP\_address mask netmask protocol hex attr hex net-metric number
- %ASA-3-318006: if interface\_name if\_state number
- %ASA-3-318007: OSPF is enabled on interface\_name during idb initialization
- %ASA-3-318008: OSPF process number is changing router-id. Reconfigure virtual link neighbors with our new router-id
- %ASA-3-318009: OSPF: Attempted reference of stale data encountered in function, line: line\_num
- %ASA-3-318101: Internal error: %REASON
- %ASA-3-318102: Flagged as being an ABR without a backbone area T
- %ASA-3-318103: Reached unknown state in neighbor state machine
- %ASA-3-318104: DB already exist : area %AREA\_ID\_STR lsid %i adv %i type 0x%x
- %ASA-3-318105: lsid %i adv %i type 0x%x gateway %i metric %d network %i mask %i protocol %i attr %i net-metric %d
- %ASA-3-318106: if %IF\_NAME if\_state %d
- %ASA-3-318107: OSPF is enabled on %IF\_NAME during idb initialization
- %ASA-3-318108: OSPF process %d is changing router-id. Reconfigure virtual link neighbors with our new router-id
- %ASA-3-318109: OSPFv3 has received an unexpected message: %0x/%0x
- %ASA-3-318110: Invalid encrypted key %s.
- %ASA-3-318111: SPI %u is already in use with ospf process %d
- %ASA-3-318112: SPI %u is already in use by a process other than ospf process %d.
- %ASA-3-318113: %s %s is already configured with SPI %u.
- %ASA-3-318114: The key length used with SPI %u is not valid
- %ASA-3-318115: %s error occurred when attempting to create an IPsec policy for SPI %u
- %ASA-3-318116: SPI %u is not being used by ospf process %d.
- %ASA-3-318117: The policy for SPI %u could not be removed because it is in use.
- %ASA-3-318118: %s error occurred when attempting to remove the IPsec policy with SPI %u
- %ASA-3-318119: Unable to close secure socket with SPI %u on interface %s
- %ASA-3-318120: OSPFv3 was unable to register with IPsec
- %ASA-3-318121: IPsec reported a GENERAL ERROR: message %s, count %d
- %ASA-3-318122: IPsec sent a %s message %s to OSPFv3 for interface %s. Recovery attempt %d .
- %ASA-3-318123: IPsec sent a %s message %s to OSPFv3 for interface %IF\_NAME. Recovery aborted
- %ASA-3-318125: Init failed for interface %IF\_NAME
- %ASA-3-318126: Interface %IF\_NAME is attached to more than one area
- %ASA-3-318127: Could not allocate or find the neighbor

- %ASA-3-319001: Acknowledge for arp update for IP address dest\_address not received (number).
- %ASA-3-319002: Acknowledge for route update for IP address dest\_address not received (number).
- %ASA-3-319003: Arp update for IP address address to NPn failed.
- %ASA-3-319004: Route update for IP address dest\_address failed (number).
- %ASA-3-320001: The subject name of the peer cert is not allowed for connection
- %ASA-3-321007: System is low on free memory blocks of size block\_size (free\_blocks CNT out of max\_blocks MAX)
- %ASA-3-322001: Deny MAC address MAC\_address, possible spoof attempt on interface interface
- %ASA-3-322002: ARP inspection check failed for arp {request|response} received from host MAC\_address on interface interface. This host is advertising MAC Address MAC\_address\_1 for IP Address IP\_address, which is {statically|dynamically} bound to MAC Address MAC\_address\_2.
- %ASA-3-322003: ARP inspection check failed for arp {request|response} received from host MAC\_address on interface interface. This host is advertising MAC Address MAC\_address\_1 for IP Address IP\_address, which is not bound to any MAC Address.
- %ASA-3-323001: Module module\_id experienced a control channel communications failure.
- %ASA-3-323002: Module module\_id is not able to shut down, shut down request not answered.
- %ASA-3-323003: Module module\_id is not able to reload, reload request not answered.
- %ASA-3-323004: Module module\_id failed to write software vnewver (currently vver), reason. Hw-module reset is required before further use.
- %ASA-3-323005: Module module\_id can not be started completely
- %ASA-3-323007: Module in slot slot experienced a firmware failure and the recovery is in progress.
- %ASA-3-324000: Drop GTPv version message msg\_type from source\_interface:source\_address/source\_port to dest\_interface:dest\_address/dest\_port Reason: reason
- %ASA-3-324001: GTPv0 packet parsing error from source\_interface:source\_address/source\_port to dest\_interface:dest\_address/dest\_port, TID: tid\_value, Reason: reason
- %ASA-3-324002: No PDP[MCB] exists to process GTPv0 msg\_type from source\_interface:source\_address/source\_port to dest\_interface:dest\_address/dest\_port, TID: tid\_value
- %ASA-3-324003: No matching request to process GTPv version msg\_type from source\_interface:source\_address/source\_port to source\_interface:dest\_address/dest\_port
- %ASA-3-324004: GTP packet with version number from source\_interface:source\_address/source\_port to dest\_interface:dest\_address/dest\_port is not supported
- %ASA-3-324005: Unable to create tunnel from source\_interface:source\_address/source\_port to dest\_interface:dest\_address/dest\_port
- %ASA-3-324006: GSN IP\_address tunnel limit tunnel\_limit exceeded, PDP Context TID tid failed
- %ASA-3-324007: Unable to create GTP connection for response from: source\_address/0 to dest\_address/dest\_port
- %ASA-3-324008: No PDP exists to update the data gsn [ggsn] PDPMCB Info REID: teid\_value, Request TEID; teid\_value, Local GSN: IPaddress (VPIfNum), Remove GSN: IPaddress (VPIfNum)
- %ASA-3-324009: Drop GTP message G-PDU from inside\_interface :inside\_ip /inside\_port to outside\_interface :outside\_ip /outside\_port <Reason>
- %ASA-3-324300: Radius Accounting Request from from\_addr has an incorrect request authenticator
- %ASA-3-324301: Radius Accounting Request has a bad header length hdr\_len, packet length pkt\_len
- %ASA-3-325001: Router ipv6\_address on interface has conflicting ND (Neighbor Discovery) settings
- %ASA-3-326001: Unexpected error in the timer library: error\_message
- %ASA-3-326002: Error in error\_message: error\_message
- %ASA-3-326004: An internal error occurred while processing a packet queue
- %ASA-3-326005: Mrib notification failed for (IP\_address, IP\_address)

- %ASA-3-326006: Entry-creation failed for (IP\_address, IP\_address)
- %ASA-3-326007: Entry-update failed for (IP\_address, IP\_address)
- %ASA-3-326008: MRIB registration failed
- %ASA-3-326009: MRIB connection-open failed
- %ASA-3-326010: MRIB unbind failed
- %ASA-3-326011: MRIB table deletion failed
- %ASA-3-326012: Initialization of string functionality failed
- %ASA-3-326013: Internal error: string in string line %d (%s)
- %ASA-3-326014: Initialization failed: error\_message error\_message
- %ASA-3-326015: Communication error: error\_message error\_message
- %ASA-3-326016: Failed to set un-numbered interface for interface\_name (string)
- %ASA-3-326017: Interface Manager error - string in string: string
- %ASA-3-326019: string in string: string
- %ASA-3-326020: List error in string: string
- %ASA-3-326021: Error in string: string
- %ASA-3-326022: Error in string: string
- %ASA-3-326023: string - IP\_address: string
- %ASA-3-326024: An internal error occurred while processing a packet queue.
- %ASA-3-326025: string
- %ASA-3-326026: Server unexpected error: error\_message
- %ASA-3-326027: Corrupted update: error\_message
- %ASA-3-326028: Asynchronous error: error\_message
- %ASA-3-327001: IP SLA Monitor: Cannot create a new process
- %ASA-3-327002: IP SLA Monitor: Failed to initialize, IP SLA Monitor functionality will not work
- %ASA-3-327003: IP SLA Monitor: Generic Timer wheel timer functionality failed to initialize
- %ASA-3-328001: Attempt made to overwrite a set stub function in string.
- %ASA-3-329001: The string0 subblock named string1 was not removed
- %ASA-3-331001: Dynamic DNS Update for 'fqdn\_name' = ip\_address failed
- %ASA-3-332001: Unable to open cache discovery socket, WCCP V2 closing down.
- %ASA-3-332002: Unable to allocate message buffer, WCCP V2 closing down.
- %ASA-3-336001 Route destination\_network stuck-in-active state in EIGRP-ddb\_name as\_num. Cleaning up
- %ASA-3-336002: Handle handle\_id is not allocated in pool.
- %ASA-3-336003: No buffers available for bytes byte packet
- %ASA-3-336004: Negative refcount in pakdesc pakdesc.
- %ASA-3-336005: Flow control error, error, on interface\_name.
- %ASA-3-336006: num peers exist on IIDB interface\_name.
- %ASA-3-336007: Anchor count negative
- %ASA-3-336008: Lingering DRDB deleting IIDB, dest network, nexthop address (interface), origin origin\_str
- %ASA-3-336009 ddb\_name as\_id: Internal Error
- %ASA-3-336012: Interface interface\_names going down and neighbor\_links links exist
- %ASA-3-336013: Route iproute, iproute\_successors successors, db\_successors rdbs
- %ASA-3-336014: "EIGRP\_PDM\_Process\_name, event\_log"
- %ASA-3-336015: Unable to open socket for AS as\_number"
- %ASA-3-336016: Unknown timer type timer\_type expiration

- %ASA-3-336018: process\_name as\_number: prefix\_source threshold prefix level (prefix\_threshold) reached
- %ASA-3-336019: process\_name as\_number: prefix\_source prefix limit reached (prefix\_threshold).
- %ASA-3-338305: Failed to download dynamic filter data file from updater server url
- %ASA-3-338306: Failed to authenticate with dynamic filter updater server url
- %ASA-3-338307: Failed to decrypt downloaded dynamic filter database file
- %ASA-3-338309: The license on this ASA does not support dynamic filter updater feature.
- %ASA-3-338310: Failed to update from dynamic filter updater server url, reason: reason string
- %ASA-3-339001: DNCRYPT certificate update failed for <num\_tries> tries
- %ASA-3-339002: Umbrella device registration failed with error code <err\_code>
- %ASA-3-339003: Umbrella device registration was successful
- %ASA-3-339004: Umbrella device registration failed due to missing token
- %ASA-3-339005: Umbrella device registration failed after <num\_tries> retries
- %ASA-3-339006: Umbrella resolver <current resolver ipv46> is reachable, resuming Umbrella redirect.
- %ASA-3-339007: Umbrella resolver <current resolver ipv46> is unreachable, moving to fail-open. Starting probe to resolver
- %ASA-3-339008: Umbrella resolver <current resolver ipv46> is unreachable, moving to fail-close
- %ASA-3-340001: Loopback-proxy info: error\_string context id context\_id, context type = version/request\_type/address\_type client socket (internal)= client\_address\_internal/client\_port\_internal server socket (internal)= server\_address\_internal/server\_port\_internal server socket (external)= server\_address\_external/server\_port\_external remote socket (external)= remote\_address\_external/remote\_port\_external
- %ASA-3-341003: Policy Agent failed to start for VNMC vnmc\_ip\_addr
- %ASA-3-341004: Storage device not available: Attempt to shutdown module %s failed.
- %ASA-3-341005: Storage device not available. Shutdown issued for module %s.
- %ASA-3-341006: Storage device not available. Failed to stop recovery of module %s .
- %ASA-3-341007: Storage device not available. Further recovery of module %s was stopped. This may take several minutes to complete.
- %ASA-3-341008: Storage device not found. Auto-boot of module %s cancelled. Install drive and reload to try again.
- %ASA-3-341011: Storage device with serial number ser\_no in bay bay\_no faulty.
- %ASA-3-342002: REST API Agent failed, reason: <reason>
- %ASA-3-342003: REST API Agent failure notification received. Agent will be restarted automatically.
- %ASA-3-342004: Failed to automatically restart the REST API Agent after 5 unsuccessful attempts. Use the 'no rest-api agent' and 'rest-api agent' commands to manually restart the Agent.
- %ASA-3-342006: Filed to install REST API image, reason: <reason>
- %ASA-3-342008:Failed to uninstall REST API image, reason: <reason>
- %ASA-3-402140: CRYPTO: RSA key generation error: modulus len len
- %ASA-3-402141: CRYPTO: Key zeroization error: key set type, reason reason
- %ASA-3-402142: CRYPTO: Bulk data op error: algorithm alg, mode mode
- %ASA-3-402143: CRYPTO: alg type key op
- %ASA-3-402144: CRYPTO: Digital signature error: signature algorithm sig, hash algorithm hash
- %ASA-3-402145: CRYPTO: Hash generation error: algorithm hash
- %ASA-3-402146: CRYPTO: Keyed hash generation error: algorithm hash, key len len
- %ASA-3-402147: CRYPTO: HMAC generation error: algorithm alg

- %ASA-3-402148: CRYPTO: Random Number Generator error
- %ASA-3-402149: CRYPTO: weak encryption type (length). Operation disallowed. Not FIPS 140-2 compliant
- %ASA-3-402150: CRYPTO: Deprecated hash algorithm used for RSA operation (hash alg). Operation disallowed. Not FIPS 140-2 compliant
- %ASA-3-403501: PPPoE - Bad host-unique in PADO - packet dropped. Intf:interface\_name AC:ac\_name
- %ASA-3-403502: PPPoE - Bad host-unique in PADS - dropping packet. Intf:interface\_name AC:ac\_name
- %ASA-3-403503: PPPoE:PPP link down:reason
- %ASA-3-403504: PPPoE:No vpdn group group\_name for PPPoE is created
- %ASA-3-403507: PPPoE:PPPoE client on interface interface failed to locate PPPoE vpdn group group\_name
- %ASA-3-414001: Failed to save logging buffer using file name filename to FTP server ftp\_server\_address on interface interface\_name: [fail\_reason]
- %ASA-3-414002: Failed to save logging buffer to flash:/syslog directory using file name: filename: [fail\_reason]
- %ASA-3-414003: TCP Syslog Server intf: IP\_Address/port not responding. New connections are [permitted|denied] based on logging permit-hostdown policy.
- %ASA-3-414005: TCP Syslog Server intf: IP\_Address/port connected, New connections are permitted based on logging permit-hostdown policy
- %ASA-3-414006: TCP Syslog Server configured and logging queue is full. New connections denied based on logging permit-hostdown policy.
- %ASA-3-418018: neighbor IP\_Address Down User reset OR neighbor IP\_Address IPv4 Unicast topology base removed from session User reset OR neighbor IP\_Address Up OR neighbor IP\_Address IPv4 Unicast topology base removed from session BGP Notification sent
- %ASA-3-418019: sent to neighbor IP\_Address, Reason: reason, Bytes: count
- %ASA-3-418040: unsupported or mal-formatted message received from IP\_Address
- %ASA-3-420001: IPS card not up and fail-close mode used, dropping ICMP packet ifc\_in:SIP to ifc\_out:DIP (typeICMP\_TYPE, code ICMP\_CODE)
- %ASA-3-420006: Virtual Sensor not present and fail-close mode used, dropping protocol packet from ifc\_in:SIP/SPORT to ifc\_out:DIP/DPORT
- %ASA-3-420008: IPS module license disabled and fail-close mode used, dropping packet.
- %ASA-3-421001: TCP|UDP flow from interface\_name:ip/port to interface\_name:ip/port is dropped because application has failed.
- %ASA-3-421003: Invalid data plane encapsulation.
- %ASA-3-421007: TCP|UDP flow from interface\_name:IP\_address/port to interface\_name:IP\_address/port is skipped because application has failed.
- %ASA-3-425006 Redundant interface redundant\_interface\_name switch active member to interface\_name failed.
- %ASA-3-429001: CXSC card not up and fail-close mode used. Dropping protocol packet from interface\_name:ip\_address/port to interface\_name:ip\_address/port
- %ASA-3-429004: Unable to set up authentication-proxy rule for the cx action on interface interface\_name for policy\_type service-policy.
- %ASA-3-444303: %SMART\_LIC-3-AGENT\_REG\_FAILED: Smart Agent for licensing registration with Cisco licensing cloud failed.
- %ASA-3-444303: %SMART\_LIC-3-AGENT\_DEREG\_FAILED: Smart Agent for licensing deregistration with CSSM failed.



- %ASA-3-444303: %SMART\_LIC-3-OUT\_OF\_COMPLIANCE: One or more entitlements are out of compliance.
- %ASA-3-444303: %SMART\_LIC-3-EVAL\_EXPIRED: Evaluation period expired.
- %ASA-3-444303: %SMART\_LIC-3-BAD\_MODE: An unknown mode was specified.
- %ASA-3-444303: %SMART\_LIC-3-BAD\_NOTIF: A bad notification type was specified.
- %ASA-3-444303: %SMART\_LIC-3-ID\_CERT\_EXPIRED: Identity certificate expired. Agent will transition to the unidentified (not registered) state.
- %ASA-3-444303: %SMART\_LIC-3-ID\_CERT\_RENEW\_NOT\_STARTED: Identity certificate start date not reached yet.
- %ASA-3-444303: %SMART\_LIC-3-ID\_CERT\_RENEW\_FAILED: Identity certificate renewal failed.
- %ASA-3-444303: %SMART\_LIC-3-ENTITLEMENT\_RENEW\_FAILED: Entitlement authorization with Cisco licensing cloud failed.
- %ASA-3-444303: %SMART\_LIC-3-COMM\_FAILED: Communications failure with Cisco licensing cloud.
- %ASA-3-444303: %SMART\_LIC-3-CERTIFICATE\_VALIDATION: Certificate validation failed by smart agent.
- %ASA-3-444303: %SMART\_LIC-3-AUTH\_RENEW\_FAILED: Authorization renewal with Cisco licensing cloud failed.
- %ASA-3-444303: %SMART\_LIC-3-INVALID\_TAG: The entitlement tag is invalid.
- %ASA-3-444303: %SMART\_LIC-3-INVALID\_ROLE\_STATE: The current role is not allowed to move to the new role.
- %ASA-3-444303: %SMART\_LIC-3-EVAL\_WILL\_EXPIRE\_WARNING: Evaluation period will expire in time.
- %ASA-3-444303: %SMART\_LIC-3-EVAL\_EXPIRED\_WARNING: Evaluation period expired on time.
- %ASA-3-444303: %SMART\_LIC-3-ID\_CERT\_EXPIRED\_WARNING: This device's registration will expire in time.
- %ASA-3-444303: %SMART\_LIC-3-CONFIG\_OUT\_OF\_SYNC: Trusted Store Enable flag not in sync with System Configuration, TS flag Config flag.
- %ASA-3-444303: %SMART\_LIC-3-REG\_EXPIRED\_CLOCK\_CHANGE: Smart Licensing registration has expired because the system time was changed outside the validity period of the registration period. The agent will transition to the un-registered state in 60 minutes.
- %ASA-3-444303: %SMART\_LIC-3-ROOT\_CERT\_MISMATCH\_PROD: Certificate type mismatch.
- %ASA-3-444303: %SMART\_LIC-3-HOT\_STANDBY\_OUT\_OF\_SYNC: Smart Licensing agent on hot standby is out of sync with active Smart Licensing agent.
- %ASA-3-444714: Azure failed to retrieve Wireserver IPv4 address.
- %ASA-3-505016: Module module\_id application changed from: name version version state state to: name version state state.

- %ASA-3-500005: connection terminated from in\_ifc\_name:src\_address/src\_port to out\_ifc\_name:dest\_address/dest\_port due to invalid combination of inspections on same flow. Inspect inspect\_name is not compatible with inspect inspect\_name\_2
- %ASA-3-507003: The flow of type protocol from the originating interface: src\_ip/src\_port to dest\_if:dest\_ip/dest\_port terminated by inspection engine, reason -
- %ASA-3-520001: error\_string
- %ASA-3-520002: bad new ID table size
- %ASA-3-520003: bad id in error\_string (id: Oxid\_num)
- %ASA-3-520004: error\_string
- %ASA-3-520005: error\_string
- %ASA-3-520010: Bad queue elem – qelem\_ptr: flink flink\_ptr, blink blink\_ptr, flink->blink flink\_blink\_ptr, blink->flink blink\_flink\_ptr
- %ASA-3-520011: Null queue elem
- %ASA-3-520013: Regular expression access check with bad list acl\_ID
- %ASA-3-520020: No memory available
- %ASA-3-520021: Error deleting trie entry, error\_message
- %ASA-3-520022: Error adding mask entry, error\_message
- %ASA-3-520023: Invalid pointer to head of tree, 0x<radix\_node\_ptr>
- %ASA-3-520024: Orphaned mask #radix\_mask\_ptr, refcount= radix\_mask\_ptr 's ref count at # radix\_node\_address, next=# radix\_node\_next
- %ASA-3-520025: No memory for radix initialization: error\_msg%ASA-3-602305: IPSEC: SA creation error, source source address, destination destination address, reason error string
- %ASA-3-602306: IPSEC: SA change peer IP error, SPI: *IPsec SPI*, (src {*original src IP address | original src port*}, dest {*original dest IP address | original dest port*} => src {*new src IP address | new src port*}, dest: {*new dest IP address | new dest port*}), reason *failure reason*
- %ASA-3-610001: NTP daemon interface interface\_name: Packet denied from IP\_address
- %ASA-3-610002: NTP daemon interface interface\_name: Authentication failed for packet from IP\_address
- %ASA-3-611313: VPN Client: Backup Server List Error: reason
- %ASA-3-613004: Internal error: memory allocation failure
- %ASA-3-613005: Flagged as being an ABR without a backbone area
- %ASA-3-613006: Reached unknown state in neighbor state machine
- %ASA-3-613007: area string lsid IP\_address mask netmask type number
- %ASA-3-613008: if inside if\_state number
- %ASA-3-613011: OSPF process number is changing router-id. Reconfigure virtual link neighbors with our new router-id
- %ASA-3-613013: OSPF LSID IP\_address adv IP\_address type number gateway IP\_address metric number forwarding addr route IP\_address /mask type number has no corresponding LSA
- %ASA-3-613029: Router-ID IP\_address is in use by ospf process number%ASA-3-613016: Area string router-LSA of length number bytes plus update overhead bytes is too large to flood.
- %ASA-3-613032: Init failed for interface inside, area is being deleted. Try again.%ASA-3-613033: Interface inside is attached to more than one area
- %ASA-3-613034: Neighbor IP\_address not configured
- %ASA-3-613035: Could not allocate or find neighbor IP\_address%ASA-4-613015: Process 1 flushes LSA ID IP\_address type-number adv-rtr IP\_address in area mask%ASA-3-702305: IPSEC: An direction tunnel\_type SA (SPI=spi) between local\_IP and remote\_IP (username) is rekeying due to sequence number rollover.

- %ASA-3-710003: {TCP|UDP} access denied by ACL from source\_IP/source\_port to interface\_name:dest\_IP/service
- %ASA-3-713004: device scheduled for reboot or shutdown, IKE key acquire message on interface interface num, for Peer IP\_address ignored
- %ASA-3-713008: Key ID in ID payload too big for pre-shared IKE tunnel
- %ASA-3-713009: OU in DN in ID payload too big for Certs IKE tunnel
- %ASA-3-713012: Unknown protocol (protocol). Not adding SA w/spi=SPI value
- %ASA-3-713014: Unknown Domain of Interpretation (DOI): DOI value
- %ASA-3-713016: Unknown identification type, Phase 1 or 2, Type ID\_Type
- %ASA-3-713017: Identification type not supported, Phase 1 or 2, Type ID\_Type
- %ASA-3-713018: Unknown ID type during find of group name for certs, Type ID\_Type
- %ASA-3-713020: No Group found by matching OU(s) from ID payload: OU\_value
- %ASA-3-713022: No Group found matching peer\_ID or IP\_address for Pre-shared key peer IP\_address
- %ASA-3-713032: Received invalid local Proxy Range IP\_address - IP\_address
- %ASA-3-713033: Received invalid remote Proxy Range IP\_address - IP\_address
- %ASA-3-713042: IKE Initiator unable to find policy: Intf interface\_number, Src: source\_address, Dst: dest\_address
- %ASA-3-713043: Cookie/peer address IP\_address session already in progress
- %ASA-3-713047: Unsupported Oakley group: Group <Diffie-Hellman group>
  
- %ASA-3-713048: Error processing payload: Payload ID: id
- %ASA-3-713056: Tunnel rejected: SA (SA\_name) not found for group (group\_name)!
- %ASA-3-713060: Tunnel Rejected: User (user) not member of group (group\_name), group-lock check failed.
- %ASA-3-713061: Tunnel rejected: Crypto Map Policy not found for Src:source\_address, Dst: dest\_address!
- %ASA-3-713062: IKE Peer address same as our interface address IP\_address
- %ASA-3-713063: IKE Peer address not configured for destination IP\_address
- %ASA-3-713065: IKE Remote Peer did not negotiate the following: proposal attribute
- %ASA-3-713072: Password for user (user) too long, truncating to number characters
- %ASA-3-713081: Unsupported certificate encoding type encoding\_type
- %ASA-3-713082: Failed to retrieve identity certificate
- %ASA-3-713083: Invalid certificate handle
- %ASA-3-713084: Received invalid phase 1 port value (port) in ID payload
- %ASA-3-713085: Received invalid phase 1 protocol (protocol) in ID payload
- %ASA-3-713086: Received unexpected Certificate payload Possible invalid Auth Method (Auth method (auth numerical value))
- %ASA-3-713088: Set Cert file handle failure: no IPSec SA in group group\_name
- %ASA-3-713098: Aborting: No identity cert specified in IPSec SA (SA\_name)!
- %ASA-3-713102: Phase 1 ID Data length number too long - reject tunnel!
- %ASA-3-713105: Zero length data in ID payload received during phase 1 or 2 processing
- %ASA-3-713107: IP\_Address request attempt failed!
- %ASA-3-713109: Unable to process the received peer certificate
- %ASA-3-713112: Failed to process CONNECTED notify (SPI SPI\_value)!
- %ASA-3-713014: Unknown Domain of Interpretation (DOI): DOI value
- %ASA-3-713016: Unknown identification type, Phase 1 or 2, Type ID\_Type
- %ASA-3-713017: Identification type not supported, Phase 1 or 2, Type ID\_Type

- %ASA-3-713118: Detected invalid Diffie-Hellman group\_descriptor group\_number, in IKE area
- %ASA-3-713122: Keep-alives configured keepalive\_type but peer IP\_address support keep-alives (type = keepalive\_type)
- %ASA-3-713123: IKE lost contact with remote peer, deleting connection (keepalive type: keepalive\_type)
- %ASA-3-713124: Received DPD sequence number rcv\_sequence\_# in DPD Action, description expected seq #
- %ASA-3-713127: Xauth required but selected Proposal does not support xauth, Check priorities of ike xauth proposals in ike proposal list
- %ASA-3-713129: Received unexpected Transaction Exchange payload type: payload\_id
- %ASA-3-713132: Cannot obtain an IP\_address for remote peer
- %ASA-3-713133: Mismatch: Overriding phase 2 DH Group(DH group DH\_group\_id) with phase 1 group(DH\_group DH\_group\_number)
- %ASA-3-713134: Mismatch: P1 Authentication algorithm in the crypto map entry different from negotiated algorithm for the L2L connection
- %ASA-3-713138: Group group\_name not found and BASE GROUP default preshared key not configured
- %ASA-3-713140: Split Tunneling Policy requires network list but none configured
- %ASA-3-713141: Client-reported firewall does not match configured firewall: action tunnel. Received -- Vendor: vendor(id), Product product(id), Caps: capability\_value. Expected -- Vendor: vendor(id), Product: product(id), Caps: capability\_value
- %ASA-3-713142: Client did not report firewall in use, but there is a configured firewall: action tunnel. Expected -- Vendor: vendor(id), Product product(id), Caps: capability\_value
- %ASA-3-713146: Could not add route for Hardware Client in network extension mode, address: IP\_address, mask: netmask
- %ASA-3-713149: Hardware client security attribute attribute\_name was enabled but not requested.
- %ASA-3-713152: Unable to obtain any rules from filter ACL\_tag to send to client for CPP, terminating connection.
- %ASA-3-713159: TCP Connection to Firewall Server has been lost, restricted tunnels are now allowed full network access
- %ASA-3-713161: Remote user (session Id - id) network access has been restricted by the Firewall Server
- %ASA-3-713162: Remote user (session Id - id) has been rejected by the Firewall Server
- %ASA-3-713163: Remote user (session Id - id) has been terminated by the Firewall Server
- %ASA-3-713165: Client IKE Auth mode differs from the group's configured Auth mode
- %ASA-3-713166: Headend security gateway has failed our user authentication attempt - check configured username and password
- %ASA-3-713167: Remote peer has failed user authentication - check configured username and password
- %ASA-3-713168: Re-auth enabled, but tunnel must be authenticated interactively!
- %ASA-3-713174: Hardware Client connection rejected! Network Extension Mode is not allowed for this group!
- %ASA-3-713182: IKE could not recognize the version of the client! IPSec Fragmentation Policy will be ignored for this connection!
- %ASA-3-713185: Error: Username too long - connection aborted
- %ASA-3-713186: Invalid secondary domain name list received from the authentication server. List Received: list\_text Character index (value) is illegal
- %ASA-3-713189: Attempted to assign network or broadcast IP\_address, removing (IP\_address) from pool.
- %ASA-3-713191: Maximum concurrent IKE negotiations exceeded!
- %ASA-3-713193: Received packet with missing payload, Expected payload: payload\_id

- %ASA-3-713194: Sending IKE|IPSec Delete With Reason message: termination\_reason
- %ASA-3-713195: Tunnel rejected: Originate-Only: Cannot accept incoming tunnel yet!
- %ASA-3-713198: User Authorization failed: user User authorization failed.
- %ASA-3-713203: IKE Receiver: Error reading from socket.
- %ASA-3-713205: Could not add static route for client address: IP\_address
- %ASA-3-713206: Tunnel Rejected: Conflicting protocols specified by tunnel-group and group-policy
- %ASA-3-713208: Cannot create dynamic rule for Backup L2L entry rule rule\_id
- %ASA-3-713209: Cannot delete dynamic rule for Backup L2L entry rule id
- %ASA-3-713210: Cannot create dynamic map for Backup L2L entry rule\_id
- %ASA-3-713212: Could not add route for L2L peer coming in on a dynamic map. address: IP\_address, mask: netmask
- %ASA-3-713214: Could not delete route for L2L peer that came in on a dynamic map. address: IP\_address, mask: netmask
- %ASA-3-713217: Skipping unrecognized rule: action: action client type: client\_type client version: client\_version
- %ASA-3-713218: Tunnel Rejected: Client Type or Version not allowed.
- %ASA-3-713226: Connection failed with peer IP\_address, no trust-point defined in tunnel-group tunnel\_group
- %ASA-3-713227: Rejecting new IPSec SA negotiation for peer Peer\_address. A negotiation was already in progress for local Proxy Local\_address/Local\_netmask, remote Proxy Remote\_address/Remote\_netmask
- %ASA-3-713230: Internal Error, ike\_lock trying to lock bit that is already locked for type type
- %ASA-3-713231: Internal Error, ike\_lock trying to unlock bit that is not locked for type type
- %ASA-3-713232: SA lock refCnt = value, bitmask = hexvalue, p1\_decrypt\_cb = value, qm\_decrypt\_cb = value, qm\_hash\_cb = value, qm\_spi\_ok\_cb = value, qm\_dh\_cb = value, qm\_secret\_key\_cb = value, qm\_encrypt\_cb = value
- %ASA-3-713238: Invalid source proxy address: 0.0.0.0! Check private address on remote client
- %ASA-3-713258: IP = var1, Attempting to establish a phase2 tunnel on var2 interface but phase1 tunnel is on var3 interface. Tearing down old phase1 tunnel due to a potential routing change.
- %ASA-3-713254: Group = groupname, Username = username, IP = peerip, Invalid IPSec/UDP port = portnum, valid range is minport - maxport, except port 4500, which is reserved for IPSec/NAT-T
- %ASA-3-713260: Output interface %d to peer was not found
- %ASA-3-713261: IPV6 address on output interface %d was not found
- %ASA-3-713262: Rejecting new IPSec SA negotiation for peer Peer\_address. A negotiation was already in progress for local Proxy Local\_address/Local\_prefix\_len, remote Proxy Remote\_address/Remote\_prefix\_len
- %ASA-3-713266: Could not add route for L2L peer coming in on a dynamic map. address: IP\_address, mask: /prefix\_len
- %ASA-3-713268: Could not delete route for L2L peer that came in on a dynamic map. address: IP\_address, mask: /prefix\_len
- %ASA-3-713270: Could not add route for Hardware Client in network extension mode, address: IP\_address, mask: /prefix\_len
- %ASA-3-713272: Terminating tunnel to Hardware Client in network extension mode, unable to delete static route for address: IP\_address, mask: /prefix\_len
- %ASA-3-713274: Could not delete static route for client address: IP\_Address IP\_Address address of client whose route is being removed
- %ASA-3-713275: IKEv1 Unsupported certificate keytype %s found at trustpoint %s
- %ASA-3-713276: Dropping new negotiation - IKEv1 in-negotiation context limit of %u reached

- %ASA-3-713902: Descriptive\_event\_string.
- %ASA-3-716057: Group group User user IP ip Session terminated, no type license available.
- %ASA-3-716061: Group DfltGrpPolicy User user IP ip addr IPv6 User Filter tempipv6 configured for AnyConnect. This setting has been deprecated, terminating connection
- %ASA-3-716158: Failed to create SAML logout request, initiated by SP. Reason: *reason*
- %ASA-3-716159: Failed to process SAML logout request, initiated by SP. Reason: *reason*
- %ASA-3-716160: Failed to create SAML authentication request. Reason: *reason*
- %ASA-3-716162: Failed to consume SAML assertion. Reason: *reason*
- %ASA-3-716600: Rejected size-recv KB Hostscan data from IP src-ip. Hostscan results exceed default | configured limit of size-conf KB.
- %ASA-3-716601: Rejected size-recv KB Hostscan data from IP src-ip. System-wide limit on the amount of Hostscan data stored on ASA exceeds the limit of data-max KB.
- %ASA-3-716602: Memory allocation error. Rejected size-recv KB Hostscan data from IP src-ip.
- %ASA-3-717001: Querying keypair failed.
- %ASA-3-717002: Certificate enrollment failed for trustpoint trustpoint\_name. Reason: reason\_string.
- %ASA-3-717009: Certificate validation failed. Reason: reason\_string.
- %ASA-3-717010: CRL polling failed for trustpoint trustpoint\_name.
- %ASA-3-717012: Failed to refresh CRL cache entry from the server for trustpoint trustpoint\_name at time\_of\_failure
- %ASA-3-717015: CRL received from issuer is too large to process (CRL size = crl\_size, maximum CRL size = max\_crl\_size)
- %ASA-3-717017: Failed to query CA certificate for trustpoint trustpoint\_name from enrollment\_url
- %ASA-3-717018: CRL received from issuer has too many entries to process (number of entries = number\_of\_entries, maximum number allowed = max\_allowed)
- %ASA-3-717019: Failed to insert CRL for trustpoint trustpoint\_name. Reason: failure\_reason.
- %ASA-3-717020: Failed to install device certificate for trustpoint label. Reason: reason\_string.
- %ASA-3-717021: Certificate data could not be verified. Locate Reason: reason\_string serial number: serial number, subject name: subject name, key length key length bits.
- %ASA-3-717023: SSL failed to set device certificate for trustpoint trustpoint name. Reason: reason\_string.
- %ASA-3-717027: Certificate chain failed validation. reason\_string.
- %ASA-3-717032: OCSP status check failed. Reason: reason\_string
- %ASA-3-717039: Local CA Server internal error detected: error.
- %ASA-3-717042: Failed to enable Local CA Server. Reason: reason.
- %ASA-3-717044: Local CA server certificate enrollment related error for user: user. Error: error.
- %ASA-3-717046: Local CA Server CRL error: error.
- %ASA-3-717051: SCEP Proxy: Denied processing the request type type received from IP client ip address, User username, TunnelGroup tunnel group name, GroupPolicy group policy name to CA ca ip address. Reason: msg
- %ASA-3-717057: Automatic import of trustpool certificate bundle has failed. <Maximum retry attempts reached. Failed to reach CA server> | <Cisco root bundle signature validation failed> | <Failed to update trustpool bundle in flash> | <Failed to install trustpool bundle in memory>
- %ASA-3-717060: Peer certificate with serial number: <serial>, subject: <subject\_name>, issuer: <issuer\_name> failed to match the configured certificate map <map\_name>
- %ASA-3-717063: protocol Certificate enrollment failed for the trustpoint tpname with the CA ca

- %ASA-3-719002: Email Proxy session pointer from source\_address has been terminated due to reason error.
- %ASA-3-719008: Email Proxy service is shutting down.
- %ASA-3-722007: Group group User user-name IP IP\_address SVC Message: type-num/ERROR: message
- %ASA-3-722008: Group group User user-name IP IP\_address SVC Message: type-num/ERROR: message
- %ASA-3-722009: Group group User user-name IP IP\_address SVC Message: type-num/ERROR: message
- %ASA-3-722020: TunnelGroup tunnel\_group GroupPolicy group\_policy User user-name IP IP\_address No address available for SVC connection
- %ASA-3-722021: Group group User user-name IP IP\_address Unable to start compression due to lack of memory resources
- %ASA-3-722035: Group group User user-name IP IP\_address Received large packet length threshold num).
- %ASA-3-722045: Connection terminated: no SSL tunnel initialization data.
- %ASA-3-722046: Group group User user IP ip Session terminated: unable to establish tunnel.
- %ASA-3-725015 Error verifying client certificate. Public key size in client certificate exceeds the maximum supported key size.
- %ASA-3-734004: DAP: Processing error: internal error code
- %ASA-3-735010: IPMI: Environment Monitoring has failed to update one or more of its records.
- %ASA-3-737002: IPAA: Received unknown message 'num'
- %ASA-3-737027: IPAA: No data for address request
- %ASA-3-737202: VPNFIP: Pool=pool, ERROR: message
- %ASA-3-737403: POOLIP: Pool=pool, ERROR: message
- %ASA-3-742001: failed to read master key for password encryption from persistent store
- %ASA-3-742002: failed to set master key for password encryption
- %ASA-3-742003: failed to save master key for password encryption, reason reason\_text
- %ASA-3-742004: failed to sync master key for password encryption, reason reason\_text
- %ASA-3-742005: cipher text enc\_pass is not compatible with the configured master key or the cipher text has been tampered with
- %ASA-3-742006: password decryption failed due to unavailable memory
- %ASA-3-742007: password encryption failed due to unavailable memory
- %ASA-3-742008: password enc\_pass decryption failed due to decoding error
- %ASA-3-742009: password encryption failed due to decoding error
- %ASA-3-742010: encrypted password enc\_pass is not well formed
- %ASA-3-743010: EOBC RPC server failed to start for client module client name.
- %ASA-3-743011: EOBC RPC call failed, return code code string.
- %ASA-3-746003: user-identity: activated import user groups | activated host names | user-to-IP address databases download failed - reason
- %ASA-3-746005: user-identity: The AD Agent AD agent IP address cannot be reached - reason [action]
- %ASA-3-746010: user-identity: update import-user domain\_name\group\_name - Import Failed [reason]
- %ASA-3-746016: user-identity: DNS lookup failed, reason: reason
- %ASA-3-746019: user-identity: Update | Remove AD Agent AD agent IP Address IP-user mapping user\_IP - domain\_name\user\_name failed
- %ASA-3-747001: Clustering: Recovered from state machine event queue depleted. Event (event-id, ptr-in-hex, ptr-in-hex) dropped. Current state state-name, stack ptr-in-hex, ptr-in-hex, ptr-in-hex, ptr-in-hex, ptr-in-hex, ptr-in-hex
- %ASA-3-747010: Clustering: RPC call failed, message message-name, return code code-value.

- %ASA-3-747012: Clustering: Failed to replicate global object id hex-id-value in domain domain-name to peer unit-name, continuing operation.
- %ASA-3-747013: Clustering: Failed to remove global object id hex-id-value in domain domain-name from peer unit-name, continuing operation.
- %ASA-3-747014: Clustering: Failed to install global object id hex-id-value in domain domain-name, continuing operation.
- %ASA-3-747018: Clustering: State progression failed due to timeout in module module-name.
- %ASA-3-747021: Clustering: Master unit unit-name is quitting due to interface health check failure on failed-interface.
- %ASA-3-747022: Clustering: Asking slave unit unit-name to quit because it failed interface health check x times, rejoin will be attempted after y min. Failed interface: interface-name.
- %ASA-3-747023: Clustering: Master unit unit-name is quitting due to card name card health check failure, and master Security Service Card state is state-name.
- %ASA-3-747024: Clustering: Asking slave unit unit-name to quit due to card name card health check failure, and its Security Service Card state is state-name.
- %ASA-3-747030: Clustering: Asking slave unit unit-name to quit because it failed interface health check x times (last failure on interface-name), Clustering must be manually enabled on the unit to re-join.
- %ASA-3-747031: Clustering: Platform mismatch between cluster master (platform-type) and joining unit unit-name (platform-type). unit-name aborting cluster join.
- %ASA-3-747032: Clustering: Service module mismatch between cluster master (module-name) and joining unit unit-name (module-name) in slot slot-number. unit-name aborting cluster join.
- %ASA-3-747033: Clustering: Interface mismatch between cluster master and joining unit unit-name. unit-name aborting cluster join.
- %ASA-3-747036: Application software mismatch between cluster master %s[Master unit name] (%s[Master application software name]) and joining unit (%s[Joining unit application software name]). %s[Joining member name] aborting cluster join.
- %ASA-3-747037: Asking slave unit %s to quit due to its Security Service Module health check failure %d times, and its Security Service Module state is %s. Rejoin will be attempted after %d minutes.
- %ASA-3-747038: Asking slave unit %s to quit due to Security Service Module health check failure %d times, and its Security Service Card Module is %s. Clustering must be manually enabled on this unit to rejoin.
- %ASA-3-747039: Unit %s is quitting due to system failure for %d time(s) (last failure is %s[cluster system failure reason]). Rejoin will be attempted after %d minutes.
- %ASA-3-747040: Unit %s is quitting due to system failure for %d time(s) (last failure is %s[cluster system failure reason]). Clustering must be manually enabled on the unit to rejoin.
- %ASA-3-747041: Unit %s is quitting due to system failure for %d time(s) (last failure is %s[cluster system failure reason]). Clustering must be manually enabled on the unit to rejoin. Master unit %s is quitting due to interface health check failure on %s[interface name], %d times. Clustering must be manually enabled on the unit to rejoin.
- %ASA-3-747042: Clustering: Master received the config hash string request message from an unknown member, id <cluster-member-id>
- %ASA-3-747043: Clustering: Get config hash string from master error.
- %ASA-6-747044: Clustering: Configuration Hash string verification <result>.



- %ASA-3-748005: Failed to bundle the ports for module slot\_number in chassis chassis\_number; clustering is disabled
- %ASA-3-748006: Asking module slot\_number in chassis chassis\_number to leave the cluster due to a port bundling failure
- %ASA-3-748100: <application\_name> application status is changed from <status> to <status>.
- %ASA-3-748101: Peer unit <unit\_id> reported its <application\_name> application status is <status>.
- %ASA-3-748102: Master unit <unit\_id> is quitting due to <application\_name> Application health check failure, and master's application state is <status>.
- %ASA-3-748103: Asking slave unit <unit\_id> to quit due to <application\_name> Application health check failure, and slave's application state is <status>.
- %ASA-3-748202: Module <module\_id> in chassis <chassis id> is leaving the cluster due to <apllication name> application failure.
- %ASA-3-750011: Tunnel Rejected: Selected IKEv2 encryption algorithm (IKEV2 encry algo) is not strong enough to secure proposed IPSEC encryption algorithm (IPSEC encry algo).
- %ASA-3-751001: Local: localIP:port Remote:remoteIP:port Username: username/group Failed to complete Diffie-Hellman operation. Error: error
- %ASA-3-751002: Local: localIP:port Remote:remoteIP:port Username: username/group No preshared key or trustpoint configured for self in tunnel group group
- %ASA-3-751004: Local: localIP:port Remote:remoteIP:port Username: username/group No remote authentication method configured for peer in tunnel group group
- %ASA-3-751005: Local: localIP:port Remote:remoteIP:port Username: username/group AnyConnect client reconnect authentication failed. Session ID: sessionID, Error: error
- %ASA-3-751006: Local: localIP:port Remote:remoteIP:port Username: username/group Certificate authentication failed. Error: error
- %ASA-3-751008: Local: localIP:port Remote:remoteIP:port Username: username/group Group=group, Tunnel rejected: IKEv2 not enabled in group policy
- %ASA-3-751009: Local: localIP:port Remote:remoteIP:port Username: username/group Unable to find tunnel group for peer.
- %ASA-3-751010: Local: localIP:port Remote:remoteIP:port Username: username/group Unable to determine self-authentication method. No crypto map setting or tunnel group found.
- %ASA-3-751011: Local: localIP:port Remote:remoteIP:port Username: username/group Failed user authentication. Error: error
- %ASA-3-751012: Local: localIP:port Remote:remoteIP:port Username: username/group Failure occurred during Configuration Mode processing. Error: error
- %ASA-3-751013: Local: localIP:port Remote:remoteIP:port Username: username/group Failed to process Configuration Payload request for attribute attribute ID. Error: error
- %ASA-3-751017: Local: localIP:port Remote remoteIP:port Username: username/group Configuration Error error description
- %ASA-3-751018: Terminating the VPN connection attempt from landing group. Reason: This connection is group locked to locked group.
- %ASA-3-751020: Local:%A:%u Remote:%A:%u Username:%s An %s remote access connection failed. Attempting to use an NSA Suite B crypto algorithm (%s) without an AnyConnect Premium license.
- %ASA-3-751022: Local: local-ip Remote: remote-ip Username:username Tunnel rejected: Crypto Map Policy not found for remote traffic selector  
rem-ts-start/rem-ts-end/rem-ts.startport/rem-ts.endport/rem-ts.protocol local traffic selector  
local-ts-start/local-ts-end/local-ts.startport/local-ts.endport/local-ts.protocol!

- %ASA-3-751024: Local:ip addr Remote:ip addr Username:username IKEv2 IPv6 User Filter tempipv6 configured. This setting has been deprecated, terminating connection
- %ASA-3-752006: Tunnel Manager failed to dispatch a KEY\_ACQUIRE message. Probable mis-configuration of the crypto map or tunnel-group. Map Tag = Tag. Map Sequence Number = num, SRC Addr: address port: port Dst Addr: address port: port.
- %ASA-3-752007: Tunnel Manager failed to dispatch a KEY\_ACQUIRE message. Entry already in Tunnel Manager. Map Tag = mapTag. Map Sequence Number = mapSeq.
- %ASA-3-752015: Tunnel Manager has failed to establish an L2L SA. All configured IKE versions failed to establish the tunnel. Map Tag = mapTag. Map Sequence Number = mapSeq.
- %ASA-3-768003: QUOTA: management session quota exceeded for user <X>: current 3, user limit 3
- %ASA-3-768004: QUOTA: management session quota exceeded for <ssh/telnet/http> protocol: current 2, protocol limit 2
- %ASA-3-769006: UPDATE: ASA boot system image image\_name was not found on disk
- %ASA-3-776001: CTS SXP: Configured source IP source ip error
- %ASA-3-776002: CTS SXP: Invalid message from peer peer IP: error
- %ASA-3-776003: CTS SXP: Connection with peer peer IP failed: error
- %ASA-3-776004: CTS SXP: Fail to start listening socket after TCP process restart.
- %ASA-3-776005: CTS SXP: Binding Binding IP - SGname(SGT) from peer IP instance connection instance num error.
- %ASA-3-776006: CTS SXP: Internal error: error
- %ASA-3-776007: CTS SXP: Connection with peer peer IP (instance connection instance num) state changed from original state to Off.
- %ASA-3-776020: CTS SXP: Unable to locate egress interface to peer peer IP.
- %ASA-3-776202: CTS PAC for Server IP\_address, A-ID PAC issuer name has expired
- %ASA-3-776203: Unable to retrieve CTS Environment data due to: reason
- %ASA-3-776204: CTS Environment data has expired
- %ASA-3-776254: CTS SGT-MAP: Binding manager unable to action binding binding IP - SGname (SGT) from source name.
- %ASA-3-776313: CTS Policy: Failure to update policies for security-group "sgname"-sgt
- %ASA-3-768001: QUOTA: resource utilization is high: requested req, current curr, warning level level
- %ASA-3-768002: QUOTA: resource quota exceeded: requested req, current curr, limit limit
- %ASA-3-772002: PASSWORD: console login warning, user username, cause: password expired
- %ASA-3-772004: PASSWORD: session login failed, user username, IP ip, cause: password expired
- %ASA-3-779003: STS: Failed to read tag-switching table - reason
- %ASA-3-779004: STS: Failed to write tag-switching table - reason
- %ASA-3-779005: STS: Failed to parse tag-switching request from http - reason
- %ASA-3-779006: STS: Failed to save tag-switching table to flash - reason
- %ASA-3-779007: STS: Failed to replicate tag-switching table to peer - reason
- %ASA-3-840001: Failed to create the backup for an IKEv2 session <Local IP>, <Remote IP>
- %ASA-3-850001: SNORT ID (<snort-instance-id>/<snort-process-id>) Automatic-Application-Bypass due to delay of <delay>ms (threshold <AAB-threshold>ms) with <connection-info>
- %ASA-3-850002: SNORT ID (<snort-instance-id>/<snort-process-id>) Automatic-Application-Bypass due to SNORT not responding to traffics for <timeout-delay>ms(threshold <AAB-threshold>ms)
- %ASA-3-8300003: Failed to send session redistribution message to <variable 1>
- %ASA-3-8300005: Failed to receive session move response from <variable 1>

## Warning Messages, Severity 4

The following messages appear at severity 4, warning:

- %ASA-4-105505: (Primary|Secondary) Failed to connect to peer unit peer-ip:port
- %ASA-4-105524: (Primary|Secondary) Transitioning to Negotiating state due to the presence of another Active HA unit
- %ASA-4-105553: (Primary|Secondary) Detected another Active HA unit
- %ASA-4-106023: Deny protocol src [interface\_name:source\_address/source\_port] [(idfw\_user|FQDN\_string), sg\_info] dst interface\_name:dest\_address/dest\_port [(idfw\_user|FQDN\_string), sg\_info] [type {string}, code {code}] by access\_group acl\_ID [0x8ed66b60, 0xf8852875]
- %ASA-4-106027: Deny src [source address] dst [destination address] by access-group "access-list name".
- %ASA-4-106103: access-list acl\_ID denied protocol for user username interface\_name/source\_address source\_port interface\_name/dest\_address dest\_port hit-cnt number first hit hash codes
- %ASA-4-108004: action\_class: action ESMTP req\_resp from src\_ifc:sip|sport to dest\_ifc:dip|dport;further\_info, page 1-23
- %ASA-4-109017: User at IP\_address exceeded auth proxy connection limit (max)
- %ASA-4-109022: exceeded HTTPS proxy process limit
- %ASA-4-109027: [aaa protocol] Unable to decipher response message Server = server\_IP\_address, User = user
- %ASA-4-109028: aaa bypassed for same-security traffic from ingress\_interface:source\_address/source\_port to egress\_interface:dest\_address/dest\_port
- %ASA-4-109030: Autodetect ACL convert wildcard did not convert ACL access\_list source | dest netmask netmask.
- %ASA-4-109031: NT Domain Authentication Failed: rejecting guest login for username.
- %ASA-4-109033: Authentication failed for admin user user from src\_IP. Interactive challenge processing is not supported for protocol connections
- %ASA-4-109040: User at IP exceeded auth proxy rate limit of 10 connections/sec
- %ASA-4-109034: Authentication failed for network user user from src\_IP/port to dst\_IP/port. Interactive challenge processing is not supported for protocol connections
- %ASA-4-109102: Received CoA action-type from coa-source-ip, but cannot find named session audit-session-id
- %ASA-4-113019: Group = group, Username = user, IP = peer\_address, Session disconnected. Session Type: type, Duration: duration, Bytes xmt: count, Bytes rcv: count, Reason: reason
- %ASA-4-113026: Error error while executing Lua script for group tunnel group
- %ASA-4-113029: Group group User user IP ipaddr Session could not be established: session limit of num reached
- %ASA-4-113030: Group group User user IP ipaddr User ACL acl from AAA doesn't exist on the device, terminating connection.
- %ASA-4-113031: Group group User user IP ipaddr AnyConnect vpn-filter filter is an IPv6 ACL; ACL not applied.
- %ASA-4-113032: Group group User user IP ipaddr AnyConnect ipv6-vpn-filter filter is an IPv4 ACL; ACL not applied.

- %ASA-4-113034: Group group User user IP ipaddr User ACL acl from AAA ignored, AV-PAIR ACL used instead.
- %ASA-4-113035: Group group User user IP ipaddr Session terminated: AnyConnect not enabled or invalid AnyConnect image on the ASA.
- %ASA-4-113036: Group group User user IP ipaddr AAA parameter name value invalid.
- %ASA-4-113038: Group group User user IP ipaddr Unable to create AnyConnect p0arent session.
- %ASA-4-113040: Terminating the VPN connection attempt from attempted group. Reason: This connection is group locked to locked group.
- %ASA-4-113041: Redirect ACL configured for assigned IP does not exist on the device.
- %ASA-4-113042: CoA: Non-HTTP connection from src\_if:src\_ip/src\_port to dest\_if:dest\_ip/dest\_port for user username at client\_IP denied by redirect filter; only HTTP connections are supported for redirection.
- %ASA-4-115002: Warning in process: process name fiber: fiber name, component: component name, subcomponent: subcomponent name, file: filename, line: line number, cond: condition
- %ASA-4-120004: Event group title is dropped. Reason reason
- %ASA-4-120005: Message group to destination is dropped. Reason reason
- %ASA-4-120006: Delivering message group to destination failed. Reason reason
- %ASA-4-199016: syslog
- %ASA-4-209003: Fragment database limit of number exceeded: src = source\_address, dest = dest\_address, proto = protocol, id = number
- %ASA-4-209004: Invalid IP fragment, size = bytes exceeds maximum size = bytes: src = source\_address, dest = dest\_address, proto = protocol, id = number
- %ASA-4-209005: Discard IP fragment set with more than number elements: src = Too many elements are in a fragment set.
- %ASA-4-209006: Fragment queue threshold exceeded, dropped TCP fragment from IP address/port to IP address/port on outside interface.
- %ASA-4-213007: L2TP: Failed to install Redirect URL: redirect URL Redirect ACL: non\_exist for assigned IP.
- %ASA-4-216004: prevented: error in function at file(line) - stack trace
- %ASA-4-302034: Unable to pre-allocate H323 GUP Connection for faddr interface: foreign address/foreign-port to laddr interface:local-address/local-port
- %ASA-4-302310: SCTP packet received from src\_ifc:src\_ip/src\_port to dst\_ifc:dst\_ip/dst\_port contains unsupported Hostname Parameter.
- %ASA-4-302311: Failed to create a new protocol[] connection from ingress interface:source IP/source port to egress interface:destination IP/destination port due to application cache memory allocation failure. The app-cache memory threshold level is threshold% and threshold check is enabled/disabled.
- %ASA-4-305021: Ports exhausted in pre-allocated PAT pool IP mapped\_ip\_address for host real\_host\_ip. Allocating from new PAT pool IP mapped\_ip\_address.
- %ASA-4-305022: Cluster unit unit\_name has been allocated num\_of\_port\_blocks port blocks for PAT usage. All units should have at least min\_num\_of\_port\_blocks port blocks.
- %ASA-4-308002: static global\_address inside\_address netmask netmask overlapped with global\_address inside\_address
- %ASA-4-308003: WARNING: The enable password is not configured.
- %ASA-4-308004: The enable password has been configured by user admin

- %ASA-4-313004: Denied ICMP type=icmp\_type, from source\_address on interface interface\_name to dest\_address:no matching session
- %ASA-4-313005: No matching connection for ICMP error message: icmp\_msg\_info on interface\_name interface. Original IP payload: embedded\_frame\_info icmp\_msg\_info = icmp src src\_interface\_name:src\_address [(idfw\_user | FQDN\_string), sg\_info] dst dest\_interface\_name:dest\_address [(idfw\_user | FQDN\_string), sg\_info] (type icmp\_type, code icmp\_code) embedded\_frame\_info = prot src source\_address/source\_port [(idfw\_user | FQDN\_string), sg\_info] dst dest\_address/dest\_port (idfw\_user|FQDN\_string), sg\_info]
- %ASA-4-313009: Denied invalid ICMP code icmp-code, for src-ifc:src-address/src-port (mapped-src-address/mapped-src-port) to dest-ifc:dest-address/dest-port (mapped-dest-address/mapped-dest-port) [user], ICMP id icmp-id, ICMP type icmp-type
- %ASA-4-315009: SSH: connection timed out: username <username> , IP <ip>
- %ASA-4-324302: Server=IPaddr:port ID=id: Rejecting the RADIUS response: Reason
- %ASA-4-325002: Duplicate address ipv6\_address/MAC\_address on interface
- %ASA-4-325004: IPv6 Extension Header hdr\_type action configuration. protocol from src\_int:src\_ipv6\_addr/src\_port to dst\_interface: dst\_ipv6\_addr/dst\_port.
- %ASA-4-325005: Invalid IPv6 Extension Header Content: string. detail regarding protocol, ingress and egress interface
- %ASA-4-325006: IPv6 Extension Header not in order: Type hdr\_type occurs after Type hdr\_type. TCP prot from inside src\_int: src\_ipv6\_addr/src\_port to dst\_interface:dst\_ipv6\_addr/dst\_port
- %ASA-4-335005: NAC Downloaded ACL parse failure - host-address
- %ASA-4-337005: Phone Proxy SRTP: Media session not found for media\_term\_ip/media\_term\_port for packet from in\_ifc:src\_ip/src\_port to out\_ifc:dest\_ip/dest\_port
- %ASA-4-338001: Dynamic filter monitored blacklisted protocol traffic from in\_interface:src\_ip\_addr/src\_port (mapped-ip/mapped-port) to out\_interface:dest\_ip\_addr/dest\_port, (mapped-ip/mapped-port), source malicious address resolved from local or dynamic list: domain name, threat-level: level\_value, category: category\_name
- %ASA-4-338002: Dynamic filter monitored blacklisted protocol traffic from in\_interface:src\_ip\_addr/src\_port (mapped-ip/mapped-port) to out\_interface:dest\_ip\_addr/dest\_port (mapped-ip/mapped-port), destination malicious address resolved from local or dynamic list: domain name, threat-level: level\_value, category: category\_name
- %ASA-4-338003: Dynamic filter monitored blacklisted protocol traffic from in\_interface:src\_ip\_addr/src\_port (mapped-ip/mapped-port) to out\_interface:dest\_ip\_addr/dest\_port, (mapped-ip/mapped-port), source malicious address resolved from local or dynamic list: ip address/netmask, threat-level: level\_value, category: category\_name
- %ASA-4-338004: Dynamic filter monitored blacklisted protocol traffic from in\_interface:src\_ip\_addr/src\_port (mapped-ip/mapped-port) to out\_interface:dest\_ip\_addr/dest\_port (mapped-ip/mapped-port), destination malicious address resolved from local or dynamic list: ip address/netmask, threat-level: level\_value, category: category\_name
- %ASA-4-338005: Dynamic filter dropped blacklisted protocol traffic from in\_interface:src\_ip\_addr/src\_port (mapped-ip/mapped-port) to out\_interface:dest\_ip\_addr/dest\_port (mapped-ip/mapped-port), source malicious address resolved from local or dynamic list: domain name, threat-level: level\_value, category: category\_name
- %ASA-4-338006: Dynamic filter dropped blacklisted protocol traffic from in\_interface:src\_ip\_addr/src\_port (mapped-ip/mapped-port) to out\_interface:dest\_ip\_addr/dest\_port (mapped-ip/mapped-port), destination malicious address resolved from local or dynamic list: domain name, threat-level: level\_value, category: category\_name

- %ASA-4-338007: Dynamic filter dropped blacklisted protocol traffic from in\_interface:src\_ip\_addr/src\_port (mapped-ip/mapped-port) to out\_interface:dest\_ip\_addr/dest\_port (mapped-ip/mapped-port), source malicious address resolved from local or dynamic list: ip address/netmask, threat-level: level\_value, category: category\_name
- %ASA-4-338008: Dynamic filter dropped blacklisted protocol traffic from in\_interface:src\_ip\_addr/src\_port (mapped-ip/mapped-port) to out\_interface:dest\_ip\_addr/dest\_port (mapped-ip/mapped-port), destination malicious address resolved from local or dynamic list: ip address/netmask, threat-level: level\_value, category: category\_name
- %ASA-4-338101: Dynamic filter action whitelisted protocol traffic from in\_interface:src\_ip\_addr/src\_port (mapped-ip/mapped-port) to out\_interface:dest\_ip\_addr/dest\_port, (mapped-ip/mapped-port), source malicious address resolved from local or dynamic list: domain name
- %ASA-4-338102: Dynamic filter action whitelisted protocol traffic from in\_interface:src\_ip\_addr/src\_port (mapped-ip/mapped-port) to out\_interface:dest\_ip\_addr/dest\_port (mapped-ip/mapped-port), destination malicious address resolved from local or dynamic list: domain name
- %ASA-4-338103: Dynamic filter action whitelisted protocol traffic from in\_interface:src\_ip\_addr/src\_port (mapped-ip/mapped-port) to out\_interface:dest\_ip\_addr/dest\_port, (mapped-ip/mapped-port), source malicious address resolved
- %ASA-4-338104: Dynamic filter action whitelisted protocol traffic from in\_interface:src\_ip\_addr/src\_port (mapped-ip/mapped-port) to out\_interface:dest\_ip\_addr/dest\_port (mapped-ip/mapped-port), destination malicious address resolved from local or dynamic list: ip address/netmask from local or dynamic list: ip address/netmask
- %ASA-4-338201: Dynamic filter monitored greylisted protocol traffic from in\_interface:src\_ip\_addr/src\_port (mapped-ip/mapped-port) to out\_interface:dest\_ip\_addr/dest\_port, (mapped-ip/mapped-port), source malicious address resolved from local or dynamic list: domain name, threat-level: level\_value, category: category\_name
- %ASA-4-338202: Dynamic filter monitored greylisted protocol traffic from in\_interface:src\_ip\_addr/src\_port (mapped-ip/mapped-port) to out\_interface:dest\_ip\_addr/dest\_port (mapped-ip/mapped-port), destination malicious address resolved from local or dynamic list: domain name, threat-level: level\_value, category: category\_name
- %ASA-4-338203: Dynamic filter dropped greylisted protocol traffic from in\_interface:src\_ip\_addr/src\_port (mapped-ip/mapped-port) to out\_interface:dest\_ip\_addr/dest\_port (mapped-ip/mapped-port), source malicious address resolved from local or dynamic list: domain name, threat-level: level\_value, category: category\_name
- %ASA-4-338204: Dynamic filter dropped greylisted protocol traffic from in\_interface:src\_ip\_addr/src\_port (mapped-ip/mapped-port) to out\_interface:dest\_ip\_addr/dest\_port (mapped-ip/mapped-port), destination malicious address resolved from local or dynamic list: domain name, threat-level: level\_value, category: category\_name
- %ASA-4-338301: Intercepted DNS reply for domain name from in\_interface:src\_ip\_addr/src\_port to out\_interface:dest\_ip\_addr/dest\_port, matched list
- %ASA-4-4000nn: IPS:number string from IP\_address to IP\_address on interface interface\_name
- %ASA-4-401001: Shuns cleared
- %ASA-4-401002: Shun added: IP\_address IP\_address port port
- %ASA-4-401003: Shun deleted: IP\_address
- %ASA-4-401004: Shunned packet: IP\_address = IP\_address on interface interface\_name
- %ASA-4-401005: Shun add failed: unable to allocate resources for IP\_address IP\_address port port
- %ASA-4-402114: IPSEC: Received an protocol packet (SPI=spi, sequence number= seq\_num) from remote\_IP to local\_IP with an invalid SPI.
- %ASA-4-402115: IPSEC: Received a packet from remote\_IP to local\_IP containing act\_prot data instead of exp\_prot data.

- %ASA-4-402116: IPSEC: Received an protocol packet (SPI=spi, sequence number= seq\_num) from remote\_IP (username) to local\_IP. The decapsulated inner packet doesn't match the negotiated policy in the SA. The packet specifies its destination as pkt\_daddr, its source as pkt\_saddr, and its protocol as pkt\_prot. The SA specifies its local proxy as id\_daddr /id\_dmask /id\_dprot /id\_dport and its remote proxy as id\_saddr /id\_smask /id\_sprot /id\_sport.
- %ASA-4-402117: IPSEC: Received a non-IPSec (protocol) packet from remote\_IP to local\_IP.
- %ASA-4-402118: IPSEC: Received an protocol packet (SPI=spi, sequence number seq\_num) from remote\_IP (username) to local\_IP containing an illegal IP fragment of length frag\_len with offset frag\_offset.
- %ASA-4-402119: IPSEC: Received an protocol packet (SPI=spi, sequence number= seq\_num) from remote\_IP (username) to local\_IP that failed anti-replay checking.
- %ASA-4-402120: IPSEC: Received an protocol packet (SPI=spi, sequence number= seq\_num) from remote\_IP (username) to local\_IP that failed authentication.
- %ASA-4-402121: IPSEC: Received an protocol packet (SPI=spi, sequence number= seq\_num) from peer\_addr (username) to lcl\_addr that was dropped by IPSec (drop\_reason).
- %ASA-4-402122: Received a cleartext packet from src\_addr to dest\_addr that was to be encapsulated in IPSec that was dropped by IPSec (drop\_reason).
- %ASA-4-402123: CRYPTO: The accel\_type hardware accelerator encountered an error (code= error\_string) while executing crypto command command.
- %ASA-4-402124: CRYPTO: The ASA hardware accelerator encountered an error (Hardware error address, Core, Hardware error code, IstatReg, PciErrReg, CoreErrStat, CoreErrAddr, Doorbell Size, DoorBell Outstanding, SWReset).
- %ASA-4-402125: The ASA hardware accelerator ring timed out (parameters).
- %ASA-4-402126: CRYPTO: The ASA created Crypto Archive File Archive Filename as a Soft Reset was necessary. Please forward this archived information to Cisco.
- %ASA-4-402127: CRYPTO: The ASA is skipping the writing of latest Crypto Archive File as the maximum # of files, max\_number, allowed have been written to archive\_directory. Please archive & remove files from Archive Directory if you want more Crypto Archive Files saved.
- %ASA-4-402131: CRYPTO: status changing the accel\_instance hardware accelerator's configuration bias from old\_config\_bias to new\_config\_bias.
- %ASA-4-403101: PPTP session state not established, but received an XGRE packet, tunnel\_id=number, session\_id=number
- %ASA-4-403102: PPP virtual interface interface\_name rcvd pkt with invalid protocol: protocol, reason: reason.
- %ASA-4-403103: PPP virtual interface max connections reached.
- %ASA-4-403104: PPP virtual interface interface\_name requires mschap for MPPE.
- %ASA-4-403106: PPP virtual interface interface\_name requires RADIUS for MPPE.
- %ASA-4-403107: PPP virtual interface interface\_name missing aaa server group info
- %ASA-4-403108: PPP virtual interface interface\_name missing client ip address option
- %ASA-4-403109: Rec'd packet not an PPTP packet. (ip) dest\_address= dest\_address, src\_addr= source\_address, data: string.
- %ASA-4-403110: PPP virtual interface interface\_name, user: user missing MPPE key from aaa server.
- %ASA-4-403505: PPPoE:PPP - Unable to set default route to IP\_address at interface\_name
- %ASA-4-403506: PPPoE:failed to assign PPP IP\_address netmask netmask at interface\_name
- %ASA-4-405001: Received ARP {request | response} collision from IP\_address/MAC\_address on interface interface\_name to IP\_address/MAC\_address on interface interface\_name
- %ASA-4-405002: Received mac mismatch collision from IP\_address/MAC\_address for authenticated host

- %ASA-4-405003: IP address collision detected between host IP\_address at MAC\_address and interface interface\_name, MAC\_address.
- %ASA-4-405101: Unable to Pre-allocate H225 Call Signalling Connection for foreign\_address outside\_address[/outside\_port] to local\_address inside\_address[/inside\_port]
- %ASA-4-405102: Unable to Pre-allocate H245 Connection for foreign\_address outside\_address[/outside\_port] to local\_address inside\_address[/inside\_port]
- %ASA-4-405103: H225 message from source\_address/source\_port to dest\_address/dest\_port contains bad protocol discriminator hex
- %ASA-4-405104: H225 message received from outside\_address/outside\_port to inside\_address/inside\_port before SETUP
- %ASA-4-405105: H323 RAS message AdmissionConfirm received from source\_address/source\_port to dest\_address/dest\_port without an AdmissionRequest
- %ASA-4-405106: H323 num channel is not created from %I/%d to %I/%d %s
- %ASA-4-405107: H245 Tunnel is detected and connection dropped from %I/%d to %I/%d %s
- %ASA-4-405201: ILS ILS\_message\_type from inside\_interface:source\_IP\_address to outside\_interface:/destination\_IP\_address has wrong embedded address embedded\_IP\_address
- %ASA-4-405300: Radius Accounting Request received from from\_addr is not allowed
- %ASA-4-405301: Attribute attribute\_number does not match for user user\_ip
- %ASA-4-406001: FTP port command low port: IP\_address/port to IP\_address on interface interface\_name
- %ASA-4-406002: FTP port command different address: IP\_address(IP\_address) to IP\_address on interface interface\_name
- %ASA-4-407001: Deny traffic for local-host interface\_name:inside\_address, license limit of number exceeded
- %ASA-4-407002: Embryonic limit nconns/elimit for through connections exceeded.outside\_address/outside\_port to global\_address (inside\_address)/inside\_port on interface interface\_name
- %ASA-4-407003: Established limit for RPC services exceeded number
- %ASA-4-408001: IP route counter negative - reason, IP\_address Attempt: number
- %ASA-4-408002: ospf process id route type update address1 netmask1 [distance1/metric1] via source IP:interface1 address2 netmask2 [distance2/metric2] interface2
- %ASA-4-408003: can't track this type of object hex
- %ASA-4-408101: KEYMAN : Type <encription\_type> encryption unknown. Interpreting keystring as literal.
- %ASA-4-408102: KEYMAN : Bad encrypted keystring for key id <key id>
- %ASA-4-409001: Database scanner: external LSA IP\_address netmask is lost, reinstalls
- %ASA-4-409002: db\_free: external LSA IP\_address netmask
- %ASA-4-409003: Received invalid packet: reason from IP\_address, interface\_name
- %ASA-4-409004: Received reason from unknown neighbor IP\_address
- %ASA-4-409005: Invalid length number in OSPF packet from IP\_address (ID IP\_address), interface\_name
- %ASA-4-409006: Invalid lsa: reason Type number, LSID IP\_address from IP\_address, IP\_address, interface\_name
- %ASA-4-409007: Found LSA with the same host bit set but using different mask LSA ID IP\_address netmask New: Destination IP\_address netmask
- %ASA-4-409008: Found generating default LSA with non-zero mask LSA type : number Mask: netmask metric: number area: string
- %ASA-4-409009: OSPF process number cannot start. There must be at least one up IP interface, for OSPF to use as router ID



- %ASA-4-409010: Virtual link information found in non-backbone area: string
- %ASA-4-409011: OSPF detected duplicate router-id IP\_address from IP\_address on interface interface\_name
- %ASA-4-409012: Detected router with duplicate router ID IP\_address in area string
- %ASA-4-409013: Detected router with duplicate router ID IP\_address in Type-4 LSA advertised by IP\_address
- %ASA-4-409014: No valid authentication [send] key is available on interface <nameif>
- %ASA-4-409015: Key ID <key-id> <received> on interface <nameif>
- %ASA-4-409016: Key chain name <key-chain-name> on <nameif> is invalid
- %ASA-4-409017: Key ID <key-id> in key chain <key-chain-name> is invalid.
- %ASA-4-409023: Attempting AAA Fallback method method\_name for request\_type request for user user:Auth-server group server\_tag unreachable
- %ASA-4-409101: Received invalid packet: %s from %P, %s
- %ASA-4-409102: Received packet with incorrect area from %P, %s, area %AREA\_ID\_STR, packet area %AREA\_ID\_STR
- %ASA-4-409103: Received %s from unknown neighbor %i
- %ASA-4-409104: Invalid length %d in OSPF packet type %d from %P (ID %i), %s
- %ASA-4-409105: Invalid lsa: %s: Type 0x%x, Length 0x%x, LSID %u from %i
- %ASA-4-409106: Found generating default LSA with non-zero mask LSA type: 0x%x Mask: %i metric: %lu area: %AREA\_ID\_STR
- %ASA-4-409107: OSPFv3 process %d could not pick a router-id, please configure manually
- %ASA-4-409108: Virtual link information found in non-backbone area: %AREA\_ID\_STR
- %ASA-4-409109: OSPF detected duplicate router-id %i from %P on interface %IF\_NAME
- %ASA-4-409110: Detected router with duplicate router ID %i in area %AREA\_ID\_STR
- %ASA-4-409111: Multiple interfaces (%IF\_NAME /%IF\_NAME) on a single link detected.
- %ASA-4-409112: Packet not written to the output queue
- %ASA-4-409113: Doubly linked list linkage is NULL
- %ASA-4-409114: Doubly linked list prev linkage is NULL %x
- %ASA-4-409115: Unrecognized timer %d in OSPF %s
- %ASA-4-409116: Error for timer %d in OSPF process %s
- %ASA-4-409117: Can't find LSA database type %x, area %AREA\_ID\_STR, interface %x
- %ASA-4-409118: Could not allocate DBD packet
- %ASA-4-409119: Invalid build flag %x for LSA %i, type 0x%x
- %ASA-4-409120: Router-ID %i is in use by ospf process %d
- %ASA-4-409121: Router is currently an ASBR while having only one area which is a stub area
- %ASA-4-409122: Could not select a global IPv6 address. Virtual links require at least one global IPv6 address.
- %ASA-4-409123: Neighbor command allowed only on NBMA networks
- %ASA-4-409125: Can not use configured neighbor: poll and priority options are allowed only for a NBMA network
- %ASA-4-409128: OSPFv3-%d Area %AREA\_ID\_STR: Router %i originating invalid type 0x%x LSA, ID %u, Metric %d on Link ID %d Link Type %d
- %ASA-4-410001: UDP DNS request from source\_interface:source\_address/source\_port to dest\_interface:dest\_address/dest\_port; (label length | domain-name length) 52 bytes exceeds remaining packet length of 44 bytes.

- %ASA-4-410003: action\_class: action DNS query\_response from src\_ifc:sip/sport to dest\_ifc:dip/dport; further\_info
- %ASA-4-411001: Line protocol on interface interface\_name changed state to up
- %ASA-4-411002: Line protocol on interface interface\_name changed state to down
- %ASA-4-411003: Configuration status on interface interface\_name changed state to downup
- %ASA-4-411004: Configuration status on interface interface\_name changed state to up
- %ASA-4-411005: Interface variable 1 experienced a hardware transmit hang. The interface has been reset.
- %ASA-4-412001: MAC MAC\_address moved from interface\_1 to interface\_2
- %ASA-4-412002: Detected bridge table full while inserting MAC MAC\_address on interface interface. Number of entries = num
- %ASA-4-413001: Module module\_id is not able to shut down. Module Error: errnum message
- %ASA-4-413002: Module module\_id is not able to reload. Module Error: errnum message
- %ASA-4-413003: Module module\_id is not a recognized type
- %ASA-4-413004: Module module\_id failed to write software vnewver (currently vver), reason. Trying again.
- %ASA-4-413005: Module module\_id, application is not supported app\_name version app\_vers type app\_type
- %ASA-4-413006: prod-id Module software version mismatch; slot slot is prod-id version running-vers. Slot slot prod-id requires required-vers.
- %ASA-4-415016: policy-map map\_name:Maximum number of unanswered HTTP requests exceeded connection\_action from int\_type:IP\_address/port\_num to int\_type:IP\_address/port\_num
- %ASA-4-416001: Dropped UDP SNMP packet from source\_interface:source\_IP/source\_port to dest\_interface:dest\_address/dest\_port; version (prot\_version) is not allowed through the firewall
- %ASA-4-417001: Unexpected event received: number
- %ASA-4-417004: Filter violation error: conn number (string:string) in string
- %ASA-4-417006: No memory for string) in string. Handling: string
- %ASA-4-418001: Through-the-device packet to/from management-only network is denied: protocol\_string from interface\_name IP\_address (port) [(idfw\_user|FQDN\_string], sg\_info)] to interface\_name IP\_address (port) [(idfw\_user|FQDN\_string), sg\_info]
- %ASA-4-419001: Dropping TCP packet from src\_ifc:src\_IP/src\_port to dest\_ifc:dest\_IP/dest\_port, reason: MSS exceeded, MSS size, data size
- %ASA-4-419002: Received duplicate TCP SYN from in\_interface:src\_address/src\_port to out\_interface:dest\_address/dest\_port with different initial sequence number.
- %ASA-4-419003: Cleared TCP urgent flag from out\_ifc:src\_ip/src\_port to in\_ifc:dest\_ip/dest\_port.
- %ASA-4-420002: IPS requested to drop ICMP packets ifc\_in:SIP to ifc\_out:DIP (typeICMP\_TYPE, code ICMP\_CODE)
- %ASA-4-420003: IPS requested to reset TCP connection from ifc\_in:SIP/SPORT to ifc\_out:DIP/DPORT
- %ASA-4-420007: application-string cannot be enabled for the module in slot slot\_id. The module's current software version does not support this feature. Please upgrade the software on the module in slot slot\_id to support this feature. Received backplane header version version\_number, required backplane header version version\_number or higher.
- %ASA-4-422004: IP SLA Monitor number0: Duplicate event received. Event number number1
- %ASA-4-422005: IP SLA Monitor Probe(s) could not be scheduled because clock is not set.
- %ASA-4-422006: IP SLA Monitor Probe number: string
- %ASA-4-423001: {Allowed | Dropped} invalid NBNS pkt\_type\_name with error\_reason\_str from ifc\_name:ip\_address/port to ifc\_name:ip\_address/port.

- %ASA-4-423002: {Allowed | Dropped} mismatched NBNS pkt\_type\_name with error\_reason\_str from ifc\_name:ip\_address/port to ifc\_name:ip\_address/port.
- %ASA-4-423003: {Allowed | Dropped} invalid NBDGM pkt\_type\_name with error\_reason\_str from ifc\_name:ip\_address/port to ifc\_name:ip\_address/port.
- %ASA-4-423004: {Allowed | Dropped} mismatched NBDGM pkt\_type\_name with error\_reason\_str from ifc\_name:ip\_address/port to ifc\_name:ip\_address/port.
- %ASA-4-423005: {Allowed | Dropped} NBDGM pkt\_type\_name fragment with error\_reason\_str from ifc\_name:ip\_address/port to ifc\_name:ip\_address/port.
- %ASA-4-424001: Packet denied protocol\_string intf\_in:src\_ip/src\_port [(idfw\_user | FQDN\_string], sg\_info) intf\_out:dst\_ip/dst\_port[(idfw\_user | FQDN\_string], sg\_info). [Ingress|Egress] interface is in a backup state.
- %ASA-4-424002: Connection to the backup interface is denied: protocol\_string intf:src\_ip/src\_port intf:dst\_ip/dst\_port
- %ASA-4-426004: PORT-CHANNEL: Interface ifc\_name1 is not compatible with ifc\_name and will be suspended (speed of ifc\_name1 is X Mbps, Y is 1000 Mbps).
- %ASA-4-429002: CXSC service card requested to drop protocol packet from interface\_name:ip\_address/port to interface\_name:ip\_address/port
- %ASA-4-429003: CXSC service card requested to reset TCP connection from interface\_name:ip\_addr/port to interface\_name:ip\_addr/port
- %ASA-4-429007: CXSC redirect will override Scansafe redirect for flow from interface\_name:ip\_address/port to interface\_name:ip\_address/port with username
- %ASA-4-429008: Unable to respond to VPN query from CX for session 0x%x. Reason %s
- %ASA-4-431001: RTP conformance: Dropping RTP packet from in\_ifc:src\_ip/src\_port to out\_ifc:dest\_ip/dest\_port, Drop reason: drop\_reason value
- %ASA-4-431002: RTCP conformance: Dropping RTCP packet from in\_ifc:src\_ip/src\_port to out\_ifc:dest\_ip/dest\_port, Drop reason: drop\_reason value
- %ASA-4-434001: SFR card not up and fail-close mode used, dropping protocol packet from ingress interface:source IP address/source port to egress interface:destination IP address/destination port
- %ASA-4-434002: SFR requested to drop protocol packet from ingress interface:source IP address/source port to egress interface:destination IP address/destination port
- %ASA-4-434003: SFR requested to reset TCP connection from ingress interface:source IP address/source port to egress interface:destination IP address/destination port
- %ASA-4-434007: SFR redirect will override Scansafe redirect for flow from ingress interface:source IP address/source port to egress interface:destination IP address/destination port (user)
- %ASA-4-444005: Timebased activation key activation-key will expire in num days.
- %ASA-4-444008: %s license has expired, and the system is scheduled to reload in x days. Apply a new activation key to enable %s license and prevent the automatic reload.
- %ASA-4-444106: Shared license backup server address is not available
- %ASA-4-444109: Shared license backup server role changed to *state*
- %ASA-4-444110: Shared license server backup has days remaining as active license server
- %ASA-4-444304: %SMART\_LIC-4-IN\_OVERAGE: One or more entitlements are in overage.
- %ASA-4-446001: Maximum TLS Proxy session limit of max\_sess reached.
- %ASA-4-446003: Denied TLS Proxy session from src\_int:src\_ip/src\_port to dst\_int:dst\_ip/dst\_port, UC-IME license is disabled.
- %ASA-4-447001: ASP DP to CP queue\_name was full. Queue length length, limit limit
- %ASA-4-448001: Denied SRTP crypto session setup on flow from src\_int:src\_ip/src\_port to dst\_int:dst\_ip/dst\_port, licensed K8 SRTP crypto session of limit exceeded

- %ASA-4-450001: Deny traffic for protocol protocol\_id src interface\_name:IP\_address/port dst interface\_name:IP\_address/port, licensed host limit of num exceeded.
- %ASA-4-500004: Invalid transport field for protocol=protocol, from source\_address/source\_port to dest\_address/dest\_port
- %ASA-4-507002: Data copy in proxy-mode exceeded the buffer limit
- %ASA-4-603110: Failed to establish L2TP session, tunnel\_id = tunnel\_id, remote\_peer\_ip = peer\_ip, user = username. Multiple sessions per tunnel are not supported
- %ASA-4-604105: DHCPD: Unable to send DHCP reply to client hardware\_address on interface interface\_name. Reply exceeds options field size (options\_field\_size) by number\_of\_octets octets.
- %ASA-4-607002: action\_class: action SIP req\_resp req\_resp\_info from src\_ifc:sip/sport to dest\_ifc:dip/dport; further\_info
- %ASA-4-607004: Phone Proxy: Dropping SIP message from src\_if:src\_ip/src\_port to dest\_if:dest\_ip/dest\_port with source MAC mac\_address due to secure phone database mismatch.
- %ASA-4-608002: Dropping Skinny message for in\_ifc:src\_ip/src\_port to out\_ifc:dest\_ip/dest\_port, SCCPPrefix length value too small
- %ASA-4-608003: Dropping Skinny message for in\_ifc:src\_ip/src\_port to out\_ifc:dest\_ip/dest\_port, SCCPPrefix length value too large
- %ASA-4-608004: Dropping Skinny message for in\_ifc:src\_ip/src\_port to out\_ifc:dest\_ip/dest\_port, message id value not allowed
- %ASA-4-608005: Dropping Skinny message for in\_ifc:src\_ip/src\_port to out\_ifc:dest\_ip/dest\_port, message id value registration not complete
- %ASA-4-612002: Auto Update failed:filename, version:number, reason:reason
- %ASA-4-612003: Auto Update failed to contact:url, reason:reason
- %ASA-4-613017: Bad LSA mask: Type number, LSID IP\_address Mask mask from IP\_address
- %ASA-4-613018: Maximum number of non self-generated LSA has been exceeded "OSPF number" - number LSAs
- %ASA-4-613019: Threshold for maximum number of non self-generated LSA has been reached "OSPF number" - number LSAs
- %ASA-4-613021: Packet not written to the output queue
- %ASA-4-613022: Doubly linked list linkage is NULL
- %ASA-4-613023: Doubly linked list prev linkage is NULL number
- %ASA-4-613024: Unrecognized timer number in OSPF string
- %ASA-4-613025: Invalid build flag number for LSA IP\_address, type number
- %ASA-4-613026: Can not allocate memory for area structure
- %ASA-4-613030: Router is currently an ASBR while having only one area which is a stub area
- %ASA-4-613031: No IP address for interface inside
- %ASA-4-613036: Can not use configured neighbor: cost and database-filter options are allowed only for a point-to-multipoint network
- %ASA-4-613037: Can not use configured neighbor: poll and priority options are allowed only for a NBMA network
- %ASA-4-613038: Can not use configured neighbor: cost or database-filter option is required for point-to-multipoint broadcast network
- %ASA-4-613039: Can not use configured neighbor: neighbor command is allowed only on NBMA and point-to-multipoint networks
- %ASA-4-613040: OSPF-1 Area string: Router IP\_address originating invalid type number LSA, ID IP\_address, Metric number on Link ID IP\_address Link Type number
- %ASA-4-613042: OSPF process number lacks forwarding address for type 7 LSA IP\_address in NSSA string - P-bit cleared

- %ASA-4-620002: Unsupported CTIQBE version: hex: from interface\_name:IP\_address/port to interface\_name:IP\_address/port
- %ASA-4-709008: (Primary | Secondary) Configuration sync in progress. Command: 'command' executed from (terminal/http) will not be replicated to or executed by the standby unit.
- %ASA-4-709013: Failover configuration replication hash comparison timeout expired.
- %ASA-4-711002: Task ran for elapsed\_time msec, process = process\_name, PC = PC Traceback = traceback
- %ASA-4-711004: Task ran for msec msec, Process = process\_name, PC = pc, Call stack = call stack
- %ASA-4-713154: DNS lookup for peer\_description Server [server\_name] failed!
- %ASA-4-713157: Timed out on initial contact to server [server\_name or IP\_address] Tunnel could not be established.
- %ASA-4-713207: Terminating connection: IKE Initiator and tunnel group specifies L2TP Over IPsec
- %ASA-4-713239: IP\_Address: Tunnel Rejected: The maximum tunnel count allowed has been reached
- %ASA-4-713240: Received DH key with bad length: received length=rlength expected length=length
- %ASA-4-713241: IE Browser Proxy Method setting\_number is Invalid
- %ASA-4-713242: Remote user is authenticated using Hybrid Authentication. Not starting IKE rekey.
- %ASA-4-713243: META-DATA Unable to find the requested certificate
- %ASA-4-713244: META-DATA Received Legacy Authentication Method(LAM) type type is different from the last type received type.
- %ASA-4-713245: META-DATA Unknown Legacy Authentication Method(LAM) type type received.
- %ASA-4-713246: META-DATA Unknown Legacy Authentication Method(LAM) attribute type type received.
- %ASA-4-713247: META-DATA Unexpected error: in Next Card Code mode while not doing SDI.
- %ASA-5-713248: META-DATA Rekey initiation is being disabled during CRACK authentication.
- %ASA-4-713249: META-DATA Received unsupported authentication results: result
- %ASA-4-713251: META-DATA Received authentication failure message
- %ASA-4-713255: IP = peer-IP, Received ISAKMP Aggressive Mode message 1 with unknown tunnel group name group-name
- %ASA-4-713903: Group = group policy, Username = user name, IP = remote IP, ERROR: Failed to install Redirect URL: redirect URL Redirect ACL: non\_exist for assigned IP.
- %ASA-4-716007: Group group User user WebVPN Unable to create session.
- %ASA-4-716022: Unable to connect to proxy server reason.
- %ASA-4-716023: Group name User user Session could not be established: session limit of maximum\_sessions reached.
- %ASA-4-716044: Group group-name User user-name IP IP\_address AAA parameter param-name value param-value out of range.
- %ASA-4-716045: Group group-name User user-name IP IP\_address AAA parameter param-name value invalid.
- %ASA-4-716046: Group group-name-name User user-name IP IP\_address User ACL access-list-name from AAA doesn't exist on the device, terminating connection.
- %ASA-4-716047: Group group-name User user-name IP IP\_address User ACL access-list from AAA ignored, AV-PAIR ACL used instead.
- %ASA-4-716048: Group group-name User user-name IP IP\_address No memory to parse ACL.
- %ASA-4-716052: Group group-name User user-name IP IP\_address Pending session terminated.
- %ASA-4-716165: SAML assertion cannot be replay protected because it does not contain time constraints.
- %ASA-4-717026: Name lookup failed for hostname hostname during PKI operation.

- %ASA-4-717031: Failed to find a suitable trustpoint for the issuer: issuer Reason: reason\_string
- %ASA-4-717035: OCSP status is being checked for certificate. certificate\_identifier.
- %ASA-4-717037: Tunnel group search using certificate maps failed for peer certificate: certificate\_identifier.
- %ASA-4-717052: Group group name User user name IP IP Address Session disconnected due to periodic certificate authentication failure. Subject Name id subject name Issuer Name id issuer name Serial Number id serial number
- %ASA-4-720001: (VPN-unit) Failed to initialize with Chunk Manager.
- %ASA-4-720007: (VPN-unit) Failed to allocate chunk from Chunk Manager.
- %ASA-4-720008: (VPN-unit) Failed to register to High Availability Framework.
- %ASA-4-720009: (VPN-unit) Failed to create version control block.
- %ASA-4-720011: (VPN-unit) Failed to allocate memory
- %ASA-4-720013: (VPN-unit) Failed to insert certificate in trust point trustpoint\_name
- %ASA-4-720022: (VPN-unit) Cannot find trust point trustpoint
- %ASA-4-720033: (VPN-unit) Failed to queue add to message queue.
- %ASA-4-720038: (VPN-unit) Corrupted message from active unit.
- %ASA-4-720043: (VPN-unit) Failed to send type message id to standby unit
- %ASA-4-720044: (VPN-unit) Failed to receive message from active unit
- %ASA-4-720047: (VPN-unit) Failed to sync SDI node secret file for server IP\_address on the standby unit.
- %ASA-4-720051: (VPN-unit) Failed to add new SDI node secret file for server id on the standby unit.
- %ASA-4-720052: (VPN-unit) Failed to delete SDI node secret file for server id on the standby unit.
- %ASA-4-720053: (VPN-unit) Failed to add cTCP IKE rule during bulk sync, peer=IP\_address, port=port
- %ASA-4-720054: (VPN-unit) Failed to add new cTCP record, peer=IP\_address, port=port.
- %ASA-4-720055: (VPN-unit) VPN Stateful failover can only be run in single/non-transparent mode.
- %ASA-4-720064: (VPN-unit) Failed to update cTCP database record for peer=IP\_address, port=port during bulk sync.
- %ASA-4-720065: (VPN-unit) Failed to add new cTCP IKE rule, peer=peer, port=port.
- %ASA-4-720066: (VPN-unit) Failed to activate IKE database.
- %ASA-4-720067: (VPN-unit) Failed to deactivate IKE database.
- %ASA-4-720068: (VPN-unit) Failed to parse peer message.
- %ASA-4-720069: (VPN-unit) Failed to activate cTCP database.
- %ASA-4-720070: (VPN-unit) Failed to deactivate cTCP database.
- %ASA-4-720073: VPN Session failed to replicate - ACL acl\_name not found
- %ASA-4-721007: (device) Fail to update access list list\_name on standby unit.
- %ASA-4-721011: (device) Fail to add access list rule list\_name, line line\_no on standby unit.
- %ASA-4-721013: (device) Fail to enable APCF XML file file\_name on the standby unit.
- %ASA-4-721015: (device) Fail to disable APCF XML file file\_name on the standby unit.
- %ASA-4-721017: (device) Fail to create WebVPN session for user user\_name, IP ip\_address.
- %ASA-4-721019: (device) Fail to delete WebVPN session for client user user\_name, IP ip\_address.
- %ASA-4-722001: IP IP\_address Error parsing SVC connect request.
- %ASA-4-722002: IP IP\_address Error consolidating SVC connect request.
- %ASA-4-722003: IP IP\_address Error authenticating SVC connect request.
- %ASA-4-722004: Group group User user-name IP IP\_address Error responding to SVC connect request.
- %ASA-4-722015: Group group User user-name IP IP\_address Unknown SVC frame type: type-num

- %ASA-4-722016: Group group User user-name IP IP\_address Bad SVC frame length: length expected: expected-length
- %ASA-4-722017: Group group User user-name IP IP\_address Bad SVC framing: 525446, reserved: 0
- %ASA-4-722018: Group group User user-name IP IP\_address Bad SVC protocol version: version, expected: expected-version
- %ASA-4-722019: Group group User user-name IP IP\_address Not enough data for an SVC header: length
- %ASA-4-722039: Group group, User user, IP ip, SVC 'vpn-filter acl' is an IPv6 ACL; ACL not applied.
- %ASA-4-722040: Group group, User user, IP ip, SVC 'ipv6-vpn-filter acl' is an IPv4 ACL; ACL not applied
- %ASA-4-722041: TunnelGroup tunnel\_group GroupPolicy group\_policy User username IP peer\_address No IPv6 address available for SVC connection
- %ASA-4-722042: Group group User user IP ip Invalid Cisco SSL Tunneling Protocol version.
- %ASA-4-722047: Group group User user IP ip Tunnel terminated: SVC not enabled or invalid SVC image on the ASA.
- %ASA-4-722048: Group group User user IP ip Tunnel terminated: SVC not enabled for the user.
- %ASA-4-722049: Group group User user IP ip Session terminated: SVC not enabled or invalid image on the ASA.
- %ASA-4-722050: Group group User user IP ip Session terminated: SVC not enabled for the user.
- %ASA-4-722054: Group group policy User user name IP remote IP SVC terminating connection: Failed to install Redirect URL: redirect URL Redirect ACL: non\_exist for assigned IP
- %ASA-4-724001: Group group-name User user-name IP IP\_address WebVPN session not allowed. Unable to determine if Cisco Secure Desktop was running on the client's workstation.
- %ASA-4-724002: Group group-name User user-name IP IP\_address WebVPN session not terminated. Cisco Secure Desktop was not running on the client's workstation.
- %ASA-4-733100: Object drop rate rate\_ID exceeded. Current burst rate is rate\_val per second, max configured rate is rate\_val; Current average rate is rate\_val per second, max configured rate is rate\_val; Cumulative total count is total\_cnt
- %ASA-4-733101: Object objectIP (is targeted|is attacking). Current burst rate is rate\_val per second, max configured rate is rate\_val; Current average rate is rate\_val per second, max configured rate is rate\_val; Cumulative total count is total\_cnt.
- %ASA-4-733102: Threat-detection adds host %I to shun list
- %ASA-4-733103: Threat-detection removes host %I from shun list
- %ASA-4-733104: TD\_SYSLOG\_TCP\_INTERCEPT\_AVERAGE\_RATE\_EXCEED
- %ASA-4-733105: TD\_SYSLOG\_TCP\_INTERCEPT\_BURST\_RATE\_EXCEED
- (For IKEv2 connection requests) %ASA-4-733201: Threat-detection: Service[remote-access-client-initiations] Peer[peer-ip]: failure threshold of *threshold-value* exceeded: adding shun to interface *interface*. IKEv2: RA excessive client initiation requests.
- (For SSL connection requests) %ASA-4-733201: Threat-detection: Service[remote-access-client-initiations] Peer[peer-ip]: failure threshold of *value* exceeded: adding shun to interface *interface*. SSL: RA excessive client initiation requests.
- %ASA-4-735015: CPU var1: Temp: var2 var3, Warm
- %ASA-4-735016: Chassis Ambient var1: Temp: var2 var3, Warm
- %ASA-4-735018: Power Supply var1: Temp: var2 var3, Critical
- %ASA-4-735019: Power Supply var1: Temp: var2 var3, Warm

- %ASA-4-735026: CPU cpu\_num Voltage Regulator is running beyond the max thermal operating temperature and the device will be shutting down immediately. The chassis and CPU need to be inspected immediately for ventilation issues.
- %ASA-4-737012: IPAA: Address assignment failed
- %ASA-4-737013: IPAA: Error freeing address ip-address, not found
- %ASA-4-737019: IPAA: Unable to get address from group-policy or tunnel-group local pools
- %ASA-4-737028: IPAA: Adding ip-address to standby: failed
- %ASA-4-737030: IPAA: Adding %m to standby: address already in use
- %ASA-4-737032: IPAA: Removing ip-address from standby: not found
- %ASA-4-737033: IPAA: Unable to assign addr\_allocator provided IP address ip\_addr to client. This IP address has already been assigned by previous\_addr\_allocator
- %ASA-4-737038: IPAA: Session=session, specified address ip-address was in-use, trying to get another.
- %ASA-4-737203: VPNFIP: Pool=pool, WARN: message
- %ASA-4-737402: POOLIP: Pool=pool, Failed to return ip-address to pool (recycle=recycle). Reason: message
- %ASA-4-737404: POOLIP: Pool=pool, WARN: message
- %ASA-4-741005: Coredump operation variable 1 failed with error variable 2 variable 3
- %ASA-4-741006: Unable to write Coredump Helper configuration, reason variable 1
- %ASA-4-746004: user identity: Total number of activated user groups exceeds the maximum number of max\_groups groups for this platform.
- %ASA-4-746006: user-identity: Out of sync with AD Agent, start bulk download
- %ASA-4-746011: Total number of users created exceeds the maximum number of max\_users for this platform.
- %ASA-4-747008: Clustering: New cluster member name with serial number serial-number-A rejected due to name conflict with existing unit with serial number serial-number-B.
- %ASA-4-747015: Clustering: Forcing stray member unit-name to leave the cluster.
- %ASA-4-747016: Clustering: Found a split cluster with both unit-name-A and unit-name-B as master units. Master role retained by unit-name-A, unit-name-B will leave, then join as a slave.
- %ASA-4-747017: Clustering: Failed to enroll unit unit-name due to maximum member limit limit-value reached.
- %ASA-4-747019: Clustering: New cluster member name rejected due to Cluster Control Link IP subnet mismatch (ip-address/ip-mask on new unit, ip-address/ip-mask on local unit).
- %ASA-4-747020: Clustering: New cluster member unit-name rejected due to encryption license mismatch.
- %ASA-4-747025: Clustering: New cluster member unit-name rejected due to firewall mode mismatch.
- %ASA-4-747026: Clustering: New cluster member unit-name rejected due to cluster interface name mismatch (ifc-name on new unit, ifc-name on local unit).
- %ASA-4-747027: Clustering: Failed to enroll unit unit-name due to insufficient size of cluster pool pool-name in context-name.
- %ASA-4-747028: Clustering: New cluster member unit-name rejected due to interface mode mismatch (mode-name on new unit, mode-name on local unit).
- %ASA-4-747029: Clustering: Unit unit-name is quitting due to Cluster Control Link down.
- %ASA-4-747034: Unit %s is quitting due to Cluster Control Link down (%d times after last rejoin). Rejoin will be attempted after %d minutes.
- %ASA-4-747035: Unit %s is quitting due to Cluster Control Link down. Clustering must be manually enabled on the unit to rejoin.
- %ASA-4-748002: Clustering configuration on the chassis is missing or incomplete; clustering is disabled.



- %ASA-4-748003: Module slot\_number in chassis chassis\_number is leaving the cluster due to a chassis health check failure
- %ASA-4-748201: <Application name> application on module <module id> in chassis <chassis id> is <status>.
- %ASA-4-750003: Local: local IP:local port Remote: remote IP:remote port Username: username Negotiation aborted due to ERROR: error
- %ASA-4-750012: Selected IKEv2 encryption algorithm (IKEV2 encry algo) is not strong enough to secure proposed IPSEC encryption algorithm (IPSEC encry algo).
- %ASA-4-750014: Local:<self ip>:<self port> Remote:<peer ip>:<peer port> Username:<TG or Username> IKEv2 Session aborted. Reason: Initial Contact received for Local ID: <self ID>, Remote ID: <peer ID> from remote peer:<peer ip>:<peer port> to <self ip>:<self port>
- %ASA-4-750015: Local:<self ip>:<self port> Remote:<peer ip>:<peer port> Username:<TG or Username> IKEv2 deleting IPsec SA. Reason: invalid SPI notification received for SPI 0x<SPI>; local traffic selector = Address Range: <start address>-<end address> Protocol: <protocol number> Port Range: <start port>-<end port> ; remote traffic selector = Address Range: <start address>-<end address> Protocol: <protocol number> Port Range: <start port>-<end port>
- %ASA-4-751014: Local: localIP:port Remote remoteIP:port Username: username/group Warning Configuration Payload request for attribute attribute ID could not be processed. Error: error
- %ASA-4-751015: Local: localIP:port Remote remoteIP:port Username: username/group SA request rejected by CAC. Reason: reason
- %ASA-4-751016: Local: localIP:port Remote remoteIP:port Username: username/group L2L peer initiated a tunnel with the same outer and inner addresses. Peer could be Originate only - Possible misconfiguration!
- %ASA-4-751019: Local:LocalAddr Remote:RemoteAddr Username:username Failed to obtain an licenseType license. Maximum license limit limit exceeded.
- %ASA-4-751021: Local:variable 1:variable 2 Remote:variable 3:variable 4 Username:variable 5 variable 6 with variable 7 encryption is not supported with this version of the AnyConnect Client. Please upgrade to the latest Anyconnect Client.
- %ASA-4-751027: Local:local IP:local port Remote:peer IP:peer port Username:username IKEv2 Received INVALID\_SELECTORS Notification from peer. Peer received a packet (SPI=spi). The decapsulated inner packet didn't match the negotiated policy in the SA. Packet destination pkt\_daddr, port pkt\_dest\_port, source pkt\_saddr, port pkt\_src\_port, protocol pkt\_prot.
- %ASA-4-752009: IKEv2 Doesn't support Multiple Peers
- %ASA-4-752010: IKEv2 Doesn't have a proposal specified
- %ASA-4-752011: IKEv1 Doesn't have a transform set specified
- %ASA-4-752012: IKEv protocol was unsuccessful at setting up a tunnel. Map Tag = mapTag. Map Sequence Number = mapSeq.
- %ASA-4-752013: Tunnel Manager dispatching a KEY\_ACQUIRE message to IKEv2 after a failed attempt. Map Tag = mapTag. Map Sequence Number = mapSeq.
- %ASA-4-752014: Tunnel Manager dispatching a KEY\_ACQUIRE message to IKEv1 after a failed attempt. Map Tag = mapTag. Map Sequence Number = mapSeq.
- %ASA-4-752017: IKEv2 Backup L2L tunnel initiation denied on interface interface matching crypto map name, sequence number number. Unsupported configuration.
- %ASA-4-753001: Unexpected IKEv2 packet received from <IP>:<port>. Error: <reason>
- %ASA-4-768003: SSH: connection timed out: username username, IP ip
- %ASA-4-769009: UPDATE: Image booted image\_name is different from boot images.

- %ASA-4-770001: Resource resource allocation is more than the permitted list of limit for this platform. If this condition persists, the ASA will be rebooted.
- %ASA-4-770003: Resource resource allocation is less than the minimum requirement of value for this platform. If this condition persists, performance will be lower than normal.
- %ASA-4-775002: Reason - protocol connection conn\_id from interface\_name:real\_address/real\_port [(idfw\_user)] to interface\_name:real\_address/real\_port is action locally
- %ASA-4-775004: Scansafe: Primary server ip\_address is not reachable
- %ASA-4-776201: CTS PAC: CTS PAC for Server IP\_address, A-ID PAC issuer name will expire in number days
- %ASA-4-776304: CTS Policy: Unresolved security-group name "sgname" referenced, policies based on this name will be inactive
- %ASA-4-776305: CTS Policy: Security-group table cleared, all polices referencing security-group names will be deactivated
- %ASA-4-776312: CTS Policy: Previously resolved security-group name "sgname" is now unresolved, policies based on this name will be deactivated
- %ASA-4-802006: IP ip\_address MDM request details has been rejected: details.
- %ASA-4-812005: Link-State-Propagation activated on inline-pair due to failure of interface <interface-name> bringing down pair interface <interface-name>
- %ASA-4-812006: Link-State-Propagation de-activated on inline-pair due to recovery of interface <interface-name> bringing up pair interface <interface-name>
- %ASA-4-815003: Object-Group-Search threshold exceeded <current value> threshold (10000) for packet UDP from <source IP address/port> to <destination IP address/port>
- %ASA-4-870001: policy-route path-monitoring, remote peer <interface\_name>:<IP\_Address> <reachable\_status>

## Notification Messages, Severity 5

The following messages appear at severity 5, notifications:

- %ASA-5-105500: (Primary|Secondary) Started HA
- %ASA-5-105501: (Primary|Secondary) Stopping HA
- %ASA-5-105503: (Primary|Secondary) Internal state change from previous\_state to new\_state
- %ASA-5-105504: (Primary|Secondary) Connected to peer peer-ip:port
- %ASA-5-105520: (Primary|Secondary) Responding to Azure Load Balancer probes
- %ASA-5-105521: (Primary|Secondary) No longer responding to Azure Load Balancer probes
- %ASA-5-105522: (Primary|Secondary) Updating route route\_table\_name
- %ASA-5-105523: (Primary|Secondary) Updated route route\_table\_name
- %ASA-5-105542: (Primary|Secondary) Enabling load balancer probe responses
- %ASA-5-105543: (Primary|Secondary) Disabling load balancer probe responses
- %ASA-5-105552: (Primary|Secondary) Stopped HA

- %ASA-5-109012: Authen Session End: user 'user', sid number, elapsed number seconds
- %ASA-5-109029: Parsing downloaded ACL: string
- %ASA-5-109039: AAA Authentication: Dropping an unsupported IPv6/IP46/IP64 packet from lifc:laddr to fifc:faddr
- %ASA-5-109201: UAUTH Session *session*, User *username*, Assigned IP *IP Address*, Succeeded adding entry.
- %ASA-5-109204: UAUTH Session *session*, User *username*, Assigned IP *IP Address*, Succeeded applying filter.
- %ASA-5-109207: UAUTH Session *session*, User *username*, Assigned IP *IP Address*, Succeeded updating entry.
- %ASA-5-109210: UAUTH Session *session*, User *username*, Assigned IP *IP Address*, Successfully removed the rules for user during tunnel torn down.
- %ASA-5-111001: Begin configuration: IP\_address writing to device
- %ASA-5-111002: Begin configuration: IP\_address reading from device
- %ASA-5-111003: IP\_address Erase configuration
- %ASA-5-111004: IP\_address end configuration: {FAILED|OK}
- %ASA-5-111005: IP\_address end configuration: OK
- %ASA-5-111007: Begin configuration: IP\_address reading from device.
- %ASA-5-111008: User user executed the command string
- %ASA-5-111010: User username, running application-name from IP ip addr, executed cmd
- %ASA-5-113024: Group tg: Authenticating type connection from ip with username, user\_name, from client certificate
- %ASA-5-113025: Group tg: FAILED to extract username from certificate while authenticating type connection from ip
- %ASA-5-120001: Smart Call-Home Module is started.
- %ASA-5-120002: Smart Call-Home Module is terminated.
- %ASA-5-120008: SCH client client is activated.
- %ASA-5-120009: SCH client client is deactivated.
- %ASA-5-120012: User username chose to choice call-home anonymous reporting at the prompt.
- %ASA-5-121001: msgId id. Telemetry support on the chassis: status.
- %ASA-5-121002: Telemetry support on the blade: status.
- %ASA-5-199001: Reload command executed from Telnet (remote IP\_address).
- %ASA-5-199017: syslog
- %ASA-5-199027: Restore operation was aborted at <HH:MM:SS> UTC <DD:MM:YY>
- %ASA-5-212009: Configuration request for SNMP group groupname failed. User username, reason.
- %ASA-5-303004: FTP cmd\_string command unsupported - failed strict inspection, terminating connection from source\_interface:source\_address/source\_port to dest\_interface:dest\_address/dest\_interface
- %ASA-5-303005: Strict FTP inspection matched match\_string in policy-map policy-name, action\_string from src\_ifc:sip/sport to dest\_ifc:dip/dport
- %ASA-5-304001: user source\_address [(idfw\_user)] Accessed URL dest\_address: url.
- %ASA-5-304002: Access denied URL chars SRC IP\_address [(idfw\_user)] DEST IP\_address: chars
- %ASA-5-305013: Asymmetric NAT rules matched for forward and reverse flows; Connection protocol src interface\_name:source\_address/source\_port [(idfw\_user)] dst interface\_name:dest\_address/dst\_port [(idfw\_user)] denied due to NAT reverse path failure.

- %ASA-5-321001: Resource var1 limit of var2 reached.
- %ASA-5-321002: Resource var1 rate limit of var2 reached.
- %ASA-5-324010: Subscriber <IMSI> PDP Context activated on network MCC/MNC <mcc><mnc> (<IE type>[/<IE type>]) [CellID <cellID>]
- %ASA-5-324011: Subscriber <IMSI> location changed during handoff from MCC/MNC <mcc><mnc> (<IE type>[/<IE type>]) [CellID <cellID>] to MCC/MNC <mcc><mnc> (<IE type>[/<IE type>]) [CellID <cellID>]
- %ASA-5-324012: GTP\_PARSE: GTP IE TYPE [GTP IE TYPE NUMBER]: Invalid Length Received Length: Length Received, Minimum Expected Length: Expected Length
- ASA-5-331002: Dynamic DNS type RR for ('fqdn\_name' - ip\_address | ip\_address - 'fqdn\_name') successfully updated in DNS server dns\_server\_ip
- %ASA-5-332003: Web Cache IP\_address/service\_ID acquired
- %ASA-5-333002: Timeout waiting for EAP response - context:EAP-context
- %ASA-5-333010: EAP-SQ response Validation Flags TLV indicates PV request - context:EAP-context
- %ASA-5-334002: EAPoUDP association successfully established - host-address
- %ASA-5-334003: EAPoUDP association failed to establish - host-address
- %ASA-5-334005: Host put into NAC Hold state - host-address
- %ASA-5-334006: EAPoUDP failed to get a response from host - host-address
- %ASA-5-335002: Host is on the NAC Exception List - host-address, OS:oper-sys
- %ASA-5-335003: NAC Default ACL applied, ACL:ACL-name - host-address
- %ASA-5-335008: NAC IPsec terminate from dynamic ACL:ACL-name - host-address
- %ASA-5-336010 EIGRP-ddb\_name tableid as\_id: Neighbor address (%interface) is event\_msg: msg
- %ASA-5-338302: Address ipaddr discovered for domain name from list, Adding rule
- %ASA-5-338303: Address ipaddr (name) timed out, Removing rule
- %ASA-5-338308: Dynamic filter updater server dynamically changed from old\_server\_host: old\_server\_port to new\_server\_host: new\_server\_port
- %ASA-5-402128: CRYPTO: An attempt to allocate a large memory block failed, size: size, limit: limit
- %ASA-5-415004: HTTP - matched matched\_string in policy-map map\_name, content-type verification failed connection\_action from int\_type:IP\_address/port\_num to int\_type:IP\_address/port\_num
- %ASA-5-415005: HTTP - matched matched\_string in policy-map map\_name, URI length exceeded connection\_action from int\_type:IP\_address/port\_num to int\_type:IP\_address/port\_num
- %ASA-5-415006: HTTP - matched matched\_string in policy-map map\_name, URI matched connection\_action from int\_type:IP\_address/port\_num to int\_type:IP\_address/port\_num
- %ASA-5-415007: HTTP - matched matched\_string in policy-map map\_name, Body matched connection\_action from int\_type:IP\_address/port\_num to int\_type:IP\_address/port\_num
- %ASA-5-415008: HTTP - matched matched\_string in policy-map map\_name, header matched connection\_action from int\_type:IP\_address/port\_num to int\_type:IP\_address/port\_num
- %ASA-5-415009: HTTP - matched matched\_string in policy-map map\_name, method matched connection\_action from int\_type:IP\_address/port\_num to int\_type:IP\_address/port\_num
- %ASA-5-415010: matched matched\_string in policy-map map\_name, transfer encoding matched connection\_action from int\_type:IP\_address/port\_num to int\_type:IP\_address/port\_num
- %ASA-5-415011: HTTP - policy-map map\_name:Protocol violation connection\_action from int\_type:IP\_address/port\_num to int\_type:IP\_address/port\_num
- %ASA-5-415012: HTTP - matched matched\_string in policy-map map\_name, Unknown mime-type connection\_action from int\_type:IP\_address/port\_num to int\_type:IP\_address/port\_num

- %ASA-5-415013: HTTP - policy-map map-name:Malformed chunked encoding connection\_action from int\_type:IP\_address/port\_num to int\_type:IP\_address/port\_num
- %ASA-5-415014: HTTP - matched matched\_string in policy-map map\_name, Mime-type in response wasn't found in the accept-types of the request connection\_action from int\_type:IP\_address/port\_num to int\_type:IP\_address/port\_num
- %ASA-5-415015: HTTP - matched matched\_string in policy-map map\_name, transfer-encoding unknown connection\_action from int\_type:IP\_address/port\_num to int\_type:IP\_address/port\_num
- %ASA-5-415018: HTTP - matched matched\_string in policy-map map\_name, Header length exceeded connection\_action from int\_type:IP\_address/port\_num to int\_type:IP\_address/port\_num
- %ASA-5-415019: HTTP - matched matched\_string in policy-map map\_name, status line matched connection\_action from int\_type:IP\_address/port\_num to int\_type:IP\_address/port\_num
- %ASA-5-415020: HTTP - matched matched\_string in policy-map map\_name, a non-ASCII character was matched connection\_action from int\_type:IP\_address/port\_num to int\_type:IP\_address/port\_num
- %ASA-5-425005 Interface interface\_name become active in redundant interface redundant\_interface\_name
- %ASA-5-434004: SFR requested ASA to bypass further packet redirection and process flow from %s:%A/%d to %s:%A/%d locally
- %ASA-5-444100: Shared request request failed. Reason: reason
- %ASA-5-444101: Shared license service is active. License server address: address
- %ASA-5-444305: %SMART\_LIC-5-SYSTEM\_CLOCK\_CHANGED: Smart Agent for Licensing System clock has been changed.
- %ASA-5-444305: %SMART\_LIC-5-IN\_COMPLIANCE: All entitlements are authorized.
- %ASA-5-444305: %SMART\_LIC-5-EVAL\_START: Entering evaluation period.
- %ASA-5-444305: %SMART\_LIC-5-AUTHORIZATION\_EXPIRED: Authorization expired.
- %ASA-5-444305: %SMART\_LIC-5-COMM\_RESTORED: Communications with Cisco licensing cloud restored.
- %ASA-5-444305: %SMART\_LIC-5-COMM\_INIT\_FAILED: Failed to initialize communications with the Cisco Licensing Cloud.
- %ASA-5-500001: ActiveX content in java script is modified: src src ip dest dest ip on interface interface name
- %ASA-5-500002: Java content in java script is modified: src src ip dest dest ip on interface interface name
- %ASA-5-500003: Bad TCP hdr length (hdrlen=bytes, pktlen=bytes) from source\_address/source\_port to dest\_address/dest\_port, flags: tcp\_flags, on interface interface\_name
- %ASA-5-501101: User transitioning priv level
- %ASA-5-502101: New user added to local dbase: Uname: user Priv: privilege\_level Encpass: string
- %ASA-5-502102: User deleted from local dbase: Uname: user Priv: privilege\_level Encpass: string
- %ASA-5-502103: User priv level changed: Uname: user From: privilege\_level To: privilege\_level
- %ASA-5-502111: New group policy added: name: policy\_name Type: policy\_type
- %ASA-5-502112: Group policy deleted: name: policy\_name Type: policy\_type
- %ASA-5-503001: Process number, Nbr IP\_address on interface\_name from string to string, reason
- %ASA-5-503002: The last key has expired for interface <nameif>, packets sent using last valid key
- %ASA-5-503003: Packet <sent | received> on interface <nameif> with expired Key ID <key-id>
- %ASA-5-503004: Key ID <key-id> in key chain <key-chain-name> does not have a key

- %ASA-5-503005: Key ID <key-id> in key chain <key-chain-name> does not have a cryptographic algorithm
- %ASA-5-504001: Security context context\_name was added to the system
- %ASA-5-504002: Security context context\_name was removed from the system
- %ASA-5-505001: Module module\_id is shutting down. Please wait...
- %ASA-5-505002: Module ips is reloading. Please wait...
- %ASA-5-505003: Module module\_id is resetting. Please wait...
- %ASA-5-505004: Module module\_id shutdown is complete.
- %ASA-5-505005: Module module\_name is initializing control communication. Please wait...
- %ASA-5-505006: Module module\_id is Up.
- %ASA-5-505007: Module module\_id is recovering. Please wait...
- %ASA-5-505008: Module module\_id software is being updated to vnewver (currently vver)
- %ASA-5-505009: Module module\_id software was updated to vnewver (previously vver)
- %ASA-5-505010: Module in slot slot removed.
- %ASA-5-505012: Module module\_id, application stopped application, version version
- %ASA-5-505013: Module module\_id application changed from: application version version to: newapplication version newversion.
- %ASA-5-506001: event\_source\_string event\_string
- %ASA-5-507001: Terminating TCP-Proxy connection from interface\_inside:source\_address/source\_port to interface\_outside:dest\_address/dest\_port - reassembly limit of limit bytes exceeded
- %ASA-5-508001: DCERPC message\_type non-standard version\_type version version\_number from src\_if:src\_ip/src\_port to dest\_if:dest\_ip/dest\_port, terminating connection.
- %ASA-5-508002: DCERPC response has low endpoint port port\_number from src\_if:src\_ip/src\_port to dest\_if:dest\_ip/dest\_port, terminating connection.
- %ASA-5-509001: Connection attempt from src\_intf:src\_ip/src\_port [[([idfw\_user | FQDN\_string], sg\_info)] to dst\_intf:dst\_ip/dst\_port [[([idfw\_user | FQDN\_string], sg\_info)] was prevented by "no forward" command.
- %ASA-5-503101: Process %d, Nbr %i on %s from %s to %s, %s
- %ASA-5-611103: User logged out: Uname: user
- %ASA-5-611104: Serial console idle timeout exceeded
- %ASA-5-612001: Auto Update succeeded:filename, version:number
- %ASA-5-711005: Traceback: call\_stack
- %ASA-5-713006: Failed to obtain state for message Id message\_number, Peer Address: IP\_address
- %ASA-5-713010: IKE area: failed to find centry for message Id message\_number
- %ASA-5-713041: IKE Initiator: new or rekey Phase 1 or 2, Intf interface\_number, IKE Peer IP\_address local Proxy Address IP\_address, remote Proxy Address IP\_address, Crypto map (crypto map tag)
- %ASA-5-713049: Security negotiation complete for tunnel\_type type (group\_name) Initiator/Responder, Inbound SPI = SPI, Outbound SPI = SPI
- %ASA-5-713050: Connection terminated for peer IP\_address. Reason: termination reason Remote Proxy IP\_address, Local Proxy IP\_address
- %ASA-5-713068: Received non-routine Notify message: notify\_type (notify\_value)
- %ASA-5-713073: Responder forcing change of Phase 1/Phase 2 rekeying duration from larger\_value to smaller\_value seconds
- %ASA-5-713074: Responder forcing change of IPSec rekeying duration from larger\_value to smaller\_value Kbs
- %ASA-5-713075: Overriding Initiator's IPSec rekeying duration from larger\_value to smaller\_value seconds

- %ASA-5-713076: Overriding Initiator's IPSec rekeying duration from larger\_value to smaller\_value Kbs
- %ASA-5-713092: Failure during phase 1 rekeying attempt due to collision
- %ASA-5-713115: Client rejected NAT enabled IPSec request, falling back to standard IPSec
- %ASA-5-713119: Group group IP ip PHASE 1 COMPLETED
- %ASA-5-713120: PHASE 2 COMPLETED (msgid=msg\_id)
- %ASA-5-713130: Received unsupported transaction mode attribute: attribute id
- %ASA-5-713131: Received unknown transaction mode attribute: attribute\_id
- %ASA-5-713135: message received, redirecting tunnel to IP\_address.
- %ASA-5-713136: IKE session establishment timed out [IKE\_state\_name], aborting!
- %ASA-5-713137: Reaper overriding refCnt [ref\_count] and tunnelCnt [tunnel\_count] -- deleting SA!
- %ASA-5-713139: group\_name not found, using BASE GROUP default preshared key
- %ASA-5-713144: Ignoring received malformed firewall record; reason - error\_reason TLV type attribute\_value correction
- %ASA-5-713148: Terminating tunnel to Hardware Client in network extension mode, unable to delete static route for address: IP\_address, mask: netmask
- %ASA-5-713155: DNS lookup for Primary VPN Server [server\_name] successfully resolved after a previous failure. Resetting any Backup Server init.
- %ASA-5-713156: Initializing Backup Server [server\_name or IP\_address]
- %ASA-5-713158: Client rejected NAT enabled IPSec Over UDP request, falling back to IPSec Over TCP
- %ASA-5-713178: IKE Initiator received a packet from its peer without a Responder cookie
- %ASA-5-713179: IKE AM Initiator received a packet from its peer without a payload\_type payload
- %ASA-5-713196: Remote L2L Peer IP\_address initiated a tunnel with same outer and inner addresses. Peer could be Originate Only - Possible misconfiguration!
- %ASA-5-713197: The configured Confidence Interval of number seconds is invalid for this tunnel\_type connection. Enforcing the second default.
- %ASA-5-713199: Reaper corrected an SA that has not decremented the concurrent IKE negotiations counter (counter\_value)!
- %ASA-5-713201: Duplicate Phase Phase packet detected. Action
- %ASA-5-713216: Rule: action [Client type]: version Client: type version allowed/ not allowed
- %ASA-5-713229: Auto Update - Notification to client client\_ip of update string: message\_string.
- %ASA-5-713237: ACL update (access\_list) received during re-key re-authentication will not be applied to the tunnel.
- %ASA-5-713248: META-DATA Rekey initiation is being disabled during CRACK authentication.
- %ASA-5-713250: META-DATA Received unknown Internal Address attribute: attribute
- %ASA-5-713252: Group = group, Username = user, IP = ip, Integrity Firewall Server is not available. VPN Tunnel creation rejected for client.
- %ASA-5-713253: Group = group, Username = user, IP = ip, Integrity Firewall Server is not available. Entering ALLOW mode. VPN Tunnel created for client.
- %ASA-5-713257: Phase var1 failure: Mismatched attribute types for class var2 : Rcv'd: var3 Cfg'd: var4
- %ASA-5-713259: Group = groupname, Username = username, IP = peerIP, Session is being torn down. Reason: reason
- %ASA-5-713904: Descriptive\_event\_string.
- %ASA-5-716053: SAML Server added: name: name Type: SP
- %ASA-5-716054: SAML Server deleted: name: name Type: SP
- %ASA-5-717013: Removing a cached CRL to accommodate an incoming CRL. Issuer: issuer

- %ASA-5-717014: Unable to cache a CRL received from CDP due to size limitations (CRL size = size, available cache space = space)
- %ASA-5-717050: SCEP Proxy: Processed request type type from IP client ip address, User username, TunnelGroup tunnel\_group name, GroupPolicy group-policy name to CA IP ca ip address
- %ASA-5-717053: Group group name User user name IP IP Address Periodic certificate authentication succeeded. Subject Name id subject name Issuer Name id issuer name Serial Number id serial number
- %ASA-5-717061: Starting protocol certificate enrollment for the trustpoint tpname with the CA ca\_name. Request Type type Mode mode
- %ASA-5-717062: protocol Certificate enrollment succeeded for the trustpoint tpname with the CA ca. Received a new certificate with Subject Name subject Issuer Name issuer Serial Number serial
- %ASA-5-717064: Keypair keyname in the trustpoint tpname is regenerated for mode protocol certificate renewal
- %ASA-5-718002: Create peer IP\_address failure, already at maximum of number\_of\_peers
- %ASA-5-718005: Fail to send to IP\_address, port port
- %ASA-5-718006: Invalid load balancing state transition [cur=state\_number][event=event\_number]
- %ASA-5-718007: Socket open failure failure\_code: failure\_text
- %ASA-5-718008: Socket bind failure failure\_code: failure\_text
- %ASA-5-718009: Send HELLO response failure to IP\_address
- %ASA-5-718010: Sent HELLO response to IP\_address
- %ASA-5-718011: Send HELLO request failure to IP\_address
- %ASA-5-718012: Sent HELLO request to IP\_address
- %ASA-5-718014: Master peer IP\_address is not answering HELLO
- %ASA-5-718015: Received HELLO request from IP\_address
- %ASA-5-718016: Received HELLO response from IP\_address
- %ASA-5-718024: Send CFG UPDATE failure to IP\_address
- %ASA-5-718028: Send OOS indicator failure to IP\_address
- %ASA-5-718031: Received OOS obituary for IP\_address
- %ASA-5-718032: Received OOS indicator from IP\_address
- %ASA-5-718033: Send TOPOLOGY indicator failure to IP\_address
- %ASA-5-718042: Unable to ARP for IP\_address
- %ASA-5-718043: Updating/removing duplicate peer entry IP\_address
- %ASA-5-718044: Deleted peer IP\_address
- %ASA-5-718045: Created peer IP\_address
- %ASA-5-718048: Create of secure tunnel failure for peer IP\_address
- %ASA-5-718050: Delete of secure tunnel failure for peer IP\_address
- %ASA-5-718052: Received GRAT-ARP from duplicate master MAC\_address
- %ASA-5-718053: Detected duplicate master, mastership stolen MAC\_address
- %ASA-5-718054: Detected duplicate master MAC\_address and going to SLAVE
- %ASA-5-718055: Detected duplicate master MAC\_address and staying MASTER
- %ASA-5-718057: Queue send failure from ISR, msg type failure\_code
- %ASA-5-718060: Inbound socket select fail: context=context\_ID.
- %ASA-5-718061: Inbound socket read fail: context=context\_ID.
- %ASA-5-718062: Inbound thread is awake (context=context\_ID).
- %ASA-5-718063: Interface interface\_name is down.
- %ASA-5-718064: Admin. interface interface\_name is down.



- %ASA-5-718065: Cannot continue to run (public=up/down, private=up/down, enable=LB\_state, master=IP\_address, session=Enable/Disable).
- %ASA-5-718066: Cannot add secondary address to interface interface\_name, ip IP\_address.
- %ASA-5-718067: Cannot delete secondary address to interface interface\_name, ip IP\_address.
- %ASA-5-718068: Start VPN Load Balancing in context context\_ID.
- %ASA-5-718069: Stop VPN Load Balancing in context context\_ID.
- %ASA-5-718070: Reset VPN Load Balancing in context context\_ID.
- %ASA-5-718071: Terminate VPN Load Balancing in context context\_ID.
- %ASA-5-718072: Becoming master of Load Balancing in context context\_ID.
- %ASA-5-718073: Becoming slave of Load Balancing in context context\_ID.
- %ASA-5-718074: Fail to create access list for peer context\_ID.
- %ASA-5-718075: Peer IP\_address access list not set.
- %ASA-5-718076: Fail to create tunnel group for peer IP\_address.
- %ASA-5-718077: Fail to delete tunnel group for peer IP\_address.
- %ASA-5-718078: Fail to create crypto map for peer IP\_address.
- %ASA-5-718079: Fail to delete crypto map for peer IP\_address.
- %ASA-5-718080: Fail to create crypto policy for peer IP\_address.
- %ASA-5-718081: Fail to delete crypto policy for peer IP\_address.
- %ASA-5-718082: Fail to create crypto ipsec for peer IP\_address.
- %ASA-5-718083: Fail to delete crypto ipsec for peer IP\_address.
- %ASA-5-718084: Public/cluster IP not on the same subnet: public IP\_address, mask netmask, cluster IP\_address
- %ASA-5-718085: Interface interface\_name has no IP address defined.
- %ASA-5-718086: Fail to install LB NP rules: type rule\_type, dst interface\_name, port port.
- %ASA-5-718087: Fail to delete LB NP rules: type rule\_type, rule rule\_ID.
- %ASA-5-719014: Email Proxy is changing listen port from old\_port to new\_port for mail protocol protocol.
- %ASA-5-720016: (VPN-unit) Failed to initialize default timer #index.
- %ASA-5-720017: (VPN-unit) Failed to update LB runtime data
- %ASA-5-720018: (VPN-unit) Failed to get a buffer from the underlying core high availability subsystem. Error code code.
- %ASA-5-720019: (VPN-unit) Failed to update cTCP statistics.
- %ASA-5-720020: (VPN-unit) Failed to send type timer message.
- %ASA-5-720021: (VPN-unit) HA non-block send failed for peer msg message\_number. HA error code.
- %ASA-5-720035: (VPN-unit) Fail to look up CTCP flow handle
- %ASA-5-720036: (VPN-unit) Failed to process state update message from the active peer.
- %ASA-5-720071: (VPN-unit) Failed to update cTCP dynamic data.
- %ASA-5-720072: Timeout waiting for Integrity Firewall Server [interface,ip] to become available.
- %ASA-5-722037: Group group User user-name IP IP\_address SVC closing connection: reason.
- %ASA-5-722038: Group group-name User user-name IP IP\_address SVC terminating session: reason.
- %ASA-5-722005: Group group User user-name IP IP\_address Unable to update session information for SVC connection.
- %ASA-5-722006: Group group User user-name IP IP\_address Invalid address IP\_address assigned to SVC connection.
- %ASA-5-722010: Group group User user-name IP IP\_address SVC Message: type-num/NOTICE: message

- %ASA-5-722011: Group group User user-name IP IP\_address SVC Message: type-num/NOTICE: message
- %ASA-5-722012: Group group User user-name IP IP\_address SVC Message: type-num/INFO: message
- %ASA-5-722028: Group group User user-name IP IP\_address Stale SVC connection closed.
- %ASA-5-722032: Group group User user-name IP IP\_address New SVC connection replacing old connection.
- %ASA-5-722033: Group group User user-name IP IP\_address First SVC connection established for SVC session.
- %ASA-5-722034: Group group User user-name IP IP\_address New SVC connection, no existing connection.
- %ASA-5-722037: Group group User user-name IP IP\_address SVC closing connection: reason.
- %ASA-5-722038: Group group-name User user-name IP IP\_address SVC terminating session: reason.
- %ASA-5-722043: Group group User user IP ip DTLS disabled: unable to negotiate cipher.
- %ASA-5-722044: Group group User user IP ip Unable to request ver address for SSL tunnel.
- %ASA-5-730009: Group groupname, User username, IP ipaddr, CAS casaddr, capacity exceeded, terminating connection.
- %ASA-5-734002: DAP: User user, Addr ipaddr: Connection terminated by the following DAP records: DAP record names
- %ASA-5-737003: IPAA: DHCP configured, no viable servers found for tunnel-group 'tunnel-group'
- %ASA-5-737004: IPAA: DHCP configured, request failed for tunnel-group 'tunnel-group'
- %ASA-5-737007: IPAA: Local pool request failed for tunnel-group 'tunnel-group'
- %ASA-5-737008: IPAA: 'tunnel-group' not found
- %ASA-5-737011: IPAA: AAA assigned address ip-address, not permitted, retrying
- %ASA-5-737018: IPAA: DHCP request attempt num failed
- %ASA-5-737021: IPAA: Address from local pool (ip-address) duplicates address from DHCP
- %ASA-5-737022: IPAA: Address from local pool (ip-address) duplicates address from AAA
- %ASA-5-737023: IPAA: Unable to allocate memory to store local pool address ip-address
- %ASA-5-737024: IPAA: Local pool assignment failed for suggested IP ip-address, retrying
- %ASA-5-737025: IPAA: Not releasing local pool ip-address, due to local pool duplicate issue
- %ASA-5-737034: IPAA: Session=<session>, <IP version> address: <explanation>
- %ASA-5-737204: VPNFIP: Pool=pool, NOTIFY: message
- %ASA-5-737405: POOLIP: Pool=pool, NOTIFY: message
- %ASA-5-746007: user-identity: NetBIOS response failed from User user\_name at user\_ip
- %ASA-5-746012: user-identity: Add IP-User mapping IP Address - domain\_name\user\_name result - reason
- %ASA-5-746013: user-identity: Delete IP-User mapping IP Address - domain\_name\user\_name result - reason
- %ASA-5-746014: user-identity: [FQDN] fqdn address IP Address obsolete
- %ASA-5-746015: user-identity: [FQDN] fqdn resolved IP address
- %ASA-5-747002: Clustering: Recovered from state machine dropped event (event-id, ptr-in-hex, ptr-in-hex). Intended state: state-name. Current state: state-name.
- %ASA-5-747003: Clustering: Recovered from state machine failure to process event (event-id, ptr-in-hex, ptr-in-hex) at state state-name.
- %ASA-5-747007: Clustering: Recovered from finding stray config sync thread, stack ptr-in-hex, ptr-in-hex, ptr-in-hex, ptr-in-hex, ptr-in-hex, ptr-in-hex.
- %ASA-5-748001: Module slot\_number in chassis chassis\_number is leaving the cluster due to a chassis configuration change

- %ASA-5-748004: Module *slot\_number* in chassis *chassis\_number* is re-joining the cluster due to a chassis health check recovery
- %ASA-5-748203: Module *<module\_id>* in chassis *<chassis id>* is re-joining the cluster due to a service chain application recovery.
- %ASA-5-750001: Local:local IP:local port Remote:remote IP: remote port Username: username Received request to request an IPsec tunnel; local traffic selector = local selectors: range, protocol, port range; remote traffic selector = remote selectors: range, protocol, port range
- %ASA-5-750002: Local:local IP:local port Remote: remote IP: remote port Username: username Received a IKE\_INIT\_SA request
- %ASA-5-750004: Local: local IP: local port Remote: remote IP: remote port Username: username Sending COOKIE challenge to throttle possible DoS
- %ASA-5-750005: Local: local IP: local port Remote: remote IP: remote port Username: username IPsec rekey collision detected. I am lowest nonce initiator, deleting SA with inbound SPI SPI
- %ASA-5-750006: Local: local IP: local port Remote: remote IP: remote port Username: username SA UP. Reason: reason
- %ASA-5-750007: Local: local IP: local port Remote: remote IP: remote port Username: username SA DOWN. Reason: reason
- %ASA-5-750008: Local: local IP: local port Remote: remote IP: remote port Username: username SA rejected due to system resource low
- %ASA-5-750009: Local: local IP: local port Remote: remote IP: remote port Username: username SA request rejected due to CAC limit reached: Rejection reason: reason
- %ASA-5-750010: Local: local-ip Remote: remote-ip Username:username IKEv2 local throttle-request queue depth threshold of threshold reached; increase the window size on peer peer for better performance
- %ASA-5-750013 - IKEv2 SA (iSPI <ISPI> rRSP <rSPI>) Peer Moved: Previous *<prev\_remote\_ip>:<prev\_remote\_port>/<prev\_local\_ip>:<prev\_local\_port>*. Updated *<new\_remote\_ip>:<new\_remote\_port>/<new\_local\_ip>:<new\_local\_port>*
- %ASA-5-751007: Local: localIP:port Remote:remoteIP:port Username: username/group Configured attribute not supported for IKEv2. Attribute: attribute
- %ASA-5-751025: Local: local IP:local port Remote: remote IP:remote port Username:username Group:group-policy IPv4 Address=assigned\_IPv4\_addr IPv6 address=assigned\_IPv6\_addr assigned to session.
- %ASA-5-751028: Local:<localIP:port> Remote:<remoteIP:port> Username:<username/group> IKEv2 Overriding configured keepalive values of threshold:<config\_threshold>/retry:<config\_retry> to threshold:<applied\_threshold>/retry:<applied\_retry>.
- %ASA-5-752003: Tunnel Manager dispatching a KEY\_ACQUIRE message to IKEv2. Map Tag = mapTag. Map Sequence Number = mapSeq.
- %ASA-5-752004: Tunnel Manager dispatching a KEY\_ACQUIRE message to IKEv1. Map Tag = mapTag. Map Sequence Number = mapSeq.
- %ASA-5-752016: IKEv protocol was successful at setting up a tunnel. Map Tag = mapTag. Map Sequence Number = mapSeq.
- %ASA-5-776009: CTS SXP: password changed.
- %ASA-5-776010: CTS SXP: SXP default source IP is changed original source IP final source IP.
- %ASA-5-776011: CTS SXP: operational state.
- %ASA-5-776252: CTS SGT-MAP: CTS SGT-MAP: Binding binding IP - SGTname(SGT) from source name deleted from binding manager.
- %ASA-5-776309: CTS Policy: Previously known security-group tag sgt is now unknown

- %ASA-5-776310: CTS Policy: Security-group name "sgname" remapped from security-group tag old\_sgt to new\_sgt
- %ASA-5-769001: UPDATE: ASA image src was added to system boot list
- %ASA-5-769002: UPDATE: ASA image src was copied to dest
- %ASA-5-769003: UPDATE: ASA image src was renamed to dest
- %ASA-5-769004: UPDATE: ASA image src\_file failed verification, reason: failure\_reason
- %ASA-5-769005: UPDATE: ASA image image\_name passed image verification
- %ASA-5-771001: CLOCK: System clock set, source: src, before: time, after: time
- %ASA-5-771002: CLOCK: System clock set, source: src, IP ip, before: time, after: time
- %ASA-5-771002: CLOCK: System clock set, source: src, IP ip, before: time, after: time
- %ASA-5-8300006: Cluster topology change detected. VPN session redistribution aborted.

## Informational Messages, Severity 6

The following messages appear at severity 6, informational:

- %ASA-6-106012: Deny IP from IP\_address to IP\_address, IP options hex.
- %ASA-6-106015: Deny TCP (no connection) from IP\_address/port to IP\_address/port flags tcp\_flags on interface interface\_name.
- %ASA-6-106025: Failed to determine the security context for the packet:sourceVlan:source\_address dest\_address source\_port dest\_port protocol
- %ASA-6-106026: Failed to determine the security context for the packet:sourceVlan:source\_address dest\_address source\_port dest\_port protocol
- %ASA-6-106100: access-list acl\_ID {permitted | denied | est-allowed} protocol interface\_name/source\_address(source\_port)(idfw\_user, sg\_info) interface\_name/dest\_address(dest\_port) (idfw\_user, sg\_info) hit-cnt number ({first hit | number-second interval})
- %ASA-6-106102: access-list acl\_ID {permitted | denied} protocol for user username interface\_name/source\_address source\_port interface\_name/dest\_address dest\_port hit-cnt number {first hit | number-second interval} hash codes
- %ASA-6-108005: action\_class: Received ESMTP req\_resp from src\_ifc:sip|sport to dest\_ifc:dip|dport;further\_info
- %ASA-6-108007: TLS started on ESMTP session between client client-side interface-name: clientIP address/client port and server server-side interface-name: server IP address/server port
- %ASA-6-109001: Auth start for user user from inside\_address/inside\_port to outside\_address/outside\_port
- %ASA-6-109002: Auth from inside\_address/inside\_port to outside\_address/outside\_port failed (server IP\_address failed) on interface interface\_name.
- %ASA-6-109003: Auth from inside\_address to outside\_address/outside\_port failed (all servers failed) on interface interface\_name, so marking all servers ACTIVE again.
- %ASA-6-109005: Authentication succeeded for user user from inside\_address/inside\_port to outside\_address/outside\_port on interface interface\_name.
- %ASA-6-109006: Authentication failed for user user from inside\_address/inside\_port to outside\_address/outside\_port on interface interface\_name.
- %ASA-6-109007: Authorization permitted for user user from inside\_address/inside\_port to outside\_address/outside\_port on interface interface\_name.
- %ASA-6-109008: Authorization denied for user user from outside\_address/outside\_port to inside\_address/inside\_port on interface interface\_name.

- %ASA-6-109024: Authorization denied from source *\_address*/source *\_port* to dest *\_address*/dest *\_port* (not authenticated) on interface *interface\_name* using protocol
- %ASA-6-109025: Authorization denied (acl=*acl\_ID*) for user 'user' from source *\_address*/source *\_port* to dest *\_address*/dest *\_port* on interface *interface\_name* using protocol
- %ASA-6-109036: Exceeded 1000 attribute values for the attribute name *attribute* for user *username*.
- %ASA-6-109100: Received CoA update from *coa-source-ip* for user *username* , with session ID: *audit-session-id* , changing authorization attributes
- %ASA-6-109101: Received CoA disconnect request from *coa-source-ip* for user *username* , with audit-session-id: *audit-session-id*
- %ASA-6-109202: UAUTH Session *session*, User *username*, Assigned IP *IP Address*, Succeeded incrementing entry use.
- %ASA-6-109211: UAUTH Session *session*, User *username*, Assigned IP *IP Address*, Successfully removed the rules for user during tunnel torn down.
- %ASA-6-110002: Failed to locate egress interface for protocol from src interface:src IP/src port to dest IP/dest port
- %ASA-6-110003: Routing failed to locate next-hop for protocol from src interface:src IP/src port to dest interface:dest IP/dest port
- %ASA-6-110004: Egress interface changed from old *\_active\_ifc* to new *\_active\_ifc* on ip\_protocol connection *conn\_id* for outside *\_zone*/parent *\_outside\_ifc*:outside *\_addr*/outside *\_port* (mapped *\_addr*/mapped *\_port*) to inside *\_zone*/parent *\_inside\_ifc*:inside *\_addr*/inside *\_port* (mapped *\_addr*/mapped *\_port*)
- %ASA-6-113003: AAA group policy for user *user* is being set to policy *\_name*.
- %ASA-6-113004: AAA user *aaa\_type* Successful: server = server *\_IP\_address*, User = *user*
- %ASA-6-113005: AAA user authentication Rejected: reason = string: server = server *\_IP\_address*, User = *user*: user IP = *user\_ip*
- %ASA-6-113006: User *user* locked out on exceeding number successive failed authentication attempts
- %ASA-6-113007: User *user* unlocked by administrator
- %ASA-6-113008: AAA transaction status ACCEPT: user = *user*
- %ASA-6-113009: AAA retrieved default group policy *policy* for user *user*
- %ASA-6-113010: AAA challenge received for user *user* from server *server\_IP\_address*
- %ASA-6-113011: AAA retrieved user specific group policy *policy* for user *user*
- %ASA-6-113012: AAA user authentication Successful: local database: user = *user*
- %ASA-6-113013: AAA unable to complete the request Error: reason = reason: user = *user*
- %ASA-6-113014: AAA authentication server not accessible: server = server *\_IP\_address*: user = *user*
- %ASA-6-113015: AAA user authentication Rejected: reason = reason: local database: user = *user*: user IP =xxx.xxx.xxx.xxx
- %ASA-6-113016: AAA credentials rejected: reason = reason: server = server *\_IP\_address*: user = *user*: user IP = xxx.xxx.xxx.xxx
- %ASA-6-113017: AAA credentials rejected: reason = reason: local database: user = *user*: user IP = user *\_ip*=xxx.xxx.xxx.xxx
- %ASA-6-113033: Group *group* User *user* IP *ipaddr* AnyConnect session not allowed. ACL parse error.
- %ASA-6-113037: Reboot pending, new sessions disabled. Denied user login.
- %ASA-6-113039: Group *group* User *user* IP *ipaddr* AnyConnect parent session started.
- %ASA-6-113045: AAA SDI server *IP\_address* in *aaa-server* group *group\_name*: status changed from previous-state to current-state
- %ASA-6-114004: 4GE SSM I/O Initialization start.

- %ASA-6-114005: 4GE SSM I/O Initialization end.
- %ASA-6-120003: Process event group title
- %ASA-6-120007: Message group to destination delivered.
- %ASA-6-121003: msgId id. Telemetry request from the chassis received. SSE connector status: connector status. Telemetry config on the blade: blade status. Telemetry data data status.
- %ASA-6-199002: startup completed. Beginning operation.
- %ASA-6-199003: Reducing link MTU dec.
- %ASA-6-199005: Startup begin
- %ASA-6-199018: syslog
- %ASA-6-201010: Embryonic connection limit exceeded econns/limit for dir packet from source\_address/source\_port to dest\_address/dest\_port on interface interface\_name
- %ASA-6-201012: Per-client embryonic connection limit exceeded curr num/limit for [input|output] packet from IP\_address/ port to ip/port on interface interface\_name
- %ASA-6-210022: LU missed number updates
- %ASA-6-302003: Built H245 connection for foreign\_address outside\_address/outside\_port local\_address inside\_address/inside\_port
- %ASA-6-302004: Pre-allocate H323 UDP backconnection for foreign\_address outside\_address/outside\_port to local\_address inside\_address/inside\_port
- %ASA-6-302010: connections in use, connections most used
- %ASA-6-302012: Pre-allocate H225 Call Signalling Connection for faddr IP\_address/port to laddr IP\_address
- %ASA-6-302013: Built {inbound|outbound} TCP connection\_id for interface:real-address/real-port (mapped-address/mapped-port) [(idfw\_user)] to interface:real-address/real-port (mapped-address/mapped-port) [(idfw\_user)] [(user)]
- %ASA-6-302014: Teardown TCP connection id for interface :real-address /real-port [(idfw\_user )] to interface :real-address /real-port [(idfw\_user )] duration hh:mm:ss bytes bytes [reason [from teardown-initiator]] [(user )]
- %ASA-6-302015: Built {inbound|outbound} UDP connection number for interface\_name:real\_address/real\_port (mapped\_address/mapped\_port) [(idfw\_user)] to interface\_name:real\_address/real\_port (mapped\_address/mapped\_port) [(idfw\_user)] [(user)]
- %ASA-6-302016: Teardown UDP connection number for interface:real-address/real-port [(idfw\_user)] to interface:real-address/real-port [(idfw\_user)] duration hh:mm:ss bytes bytes [(user)]
- %ASA-6-302017: Built {inbound|outbound} GRE connection id from interface:real\_address (translated\_address) [(idfw\_user)] to interface:real\_address/real\_cid (translated\_address/translated\_cid) [(idfw\_user)] [(user)]
- %ASA-6-302018: Teardown GRE connection id from interface:real\_address (translated\_address) [(idfw\_user)] to interface:real\_address/real\_cid (translated\_address/translated\_cid) [(idfw\_user)] duration hh:mm:ss bytes bytes [(user)]
- %ASA-6-302020: Built ICMP connection connection\_id from interface:real-address/real-port (mapped-address/mapped-port) [(idfw\_user)] to interface:real-address/real-port (mapped-address/mapped-port) [(idfw\_user)] [(user)]
- %ASA-6-302021: Teardown ICMP connection connection\_id from interface:real-address/real-port (mapped-address/mapped-port) [(idfw\_user)] to interface:real-address/real-port (mapped-address/mapped-port) [(idfw\_user)] [(user)]
- %ASA-6-302022: Built role stub TCP connection for interface:real-address/real-port (mapped-address/mapped-port) to interface:real-address/real-port (mapped-address/mapped-port)
- %ASA-6-302023: Teardown stub TCP connection for interface:real-address/real-port to interface:real-address/real-port duration hh:mm:ss forwarded bytes bytes reason

- %ASA-6-302024: Built role stub UDP connection for interface:real-address/real-port (mapped-address/mapped-port) to interface:real-address/real-port (mapped-address/mapped-port)
- %ASA-6-302025: Teardown stub UDP connection for interface:real-address/real-port to interface:real-address/real-port duration hh:mm:ss forwarded bytes bytes reason
- %ASA-6-302026: Built role stub ICMP connection for interface:real-address/real-port (mapped-address) to interface:real-address/real-port (mapped-address)
- %ASA-6-302027: Teardown stub ICMP connection for interface:real-address/real-port to interface:real-address/real-port duration hh:mm:ss forwarded bytes bytes reason
- %ASA-6-302033: Pre-allocated H323 GUP Connection for faddr interface:foreign address/foreign-port to laddr interface:local-address/local-port
- %ASA-6-302035: Built {inbound|outbound} SCTP connection conn\_id for outside\_interface:outside\_ip/outside\_port (mapped\_outside\_ip/mapped\_outside\_port)[([outside\_idfw\_user],[outside\_sg\_info])] to inside\_interface:inside\_ip/inside\_port (mapped\_inside\_ip/mapped\_inside\_port)[([inside\_idfw\_user],[inside\_sg\_info])] [(user)]
- %ASA-6-302036: Teardown SCTP connection conn\_id for outside\_interface:outside\_ip/outside\_port([([outside\_idfw\_user],[outside\_sg\_info]))] to inside\_interface:inside\_ip/inside\_port([([inside\_idfw\_user],[inside\_sg\_info]))] duration time bytes bytes reason [(user)]
- %ASA-6-302303: Built TCP state-bypass connection conn\_id from initiator\_interface:real\_ip/real\_port(mapped\_ip/mapped\_port) to responder\_interface:real\_ip/real\_port (mapped\_ip/mapped\_port)
- %ASA-6-302304: Teardown TCP state-bypass connection conn\_id from initiator\_interface:ip/port to responder\_interface:ip/port duration, bytes, teardown reason.
- %ASA-6-302305: Built SCTP state-bypass connection conn\_id for outside\_interface:outside\_ip/outside\_port (mapped\_outside\_ip/mapped\_outside\_port)[([outside\_idfw\_user],[outside\_sg\_info])] to inside\_interface:inside\_ip/inside\_port (mapped\_inside\_ip/mapped\_inside\_port)[([inside\_idfw\_user],[inside\_sg\_info])]
- %ASA-6-302306: Teardown SCTP state-bypass connection conn\_id for outside\_interface:outside\_ip/outside\_port([([outside\_idfw\_user],[outside\_sg\_info]))] to inside\_interface:inside\_ip/inside\_port([([inside\_idfw\_user],[inside\_sg\_info]))] duration time bytes bytes reason
- %ASA-6-303002: FTP connection from src\_ifc:src\_ip/src\_port to dst\_ifc:dst\_ip/dst\_port, user username action file filename
- %ASA-6-304004: URL Server IP\_address request failed URL url HTTP/1.0
- %ASA-6-305007: addrpool\_free(): Orphan IP IP\_address on interface interface\_number
- %ASA-6-305009: Built {dynamic|static} translation from interface\_name [(acl-name)]:real\_address [(idfw\_user)] to interface\_name:mapped\_address
- %ASA-6-305010: Teardown {dynamic|static} translation from interface\_name:real\_address [(idfw\_user)] to interface\_name:mapped\_address duration time
- %ASA-6-305011: Built {dynamic|static} {TCP|UDP|ICMP} translation from interface\_name:real\_address/real\_port [(idfw\_user)] to interface\_name:mapped\_address/mapped\_port
- %ASA-6-305012: Teardown {dynamic|static} {TCP|UDP|ICMP} translation from interface\_name [(acl-name)]:real\_address/{real\_port|real\_ICMP\_ID} [(idfw\_user)] to interface\_name:mapped\_address/{mapped\_port|mapped\_ICMP\_ID} duration time
- %ASA-6-305014: Allocated block of ports for translation from real\_interface : real\_host\_ip /real\_source\_port to real\_dest\_interface :real\_dest\_ip /real\_dest\_port.

- %ASA-6-305015: Released block of ports for translation from real\_interface : real\_host\_ip /real\_source\_port to real\_dest\_interface :real\_dest\_ip /real\_dest\_port.
- %ASA-6-305018: MAP translation from <src\_if>:<src\_ip>/<src\_port>-<dst\_if>:<dst\_ip>/<dst\_port> to <src\_if>:<translated\_src\_ip>/<src\_port>-<dst\_if>:<translated\_dst\_ip>/<dst\_port>
- %ASA-6-308001: console enable password incorrect for number tries (from IP\_address)
- %ASA-6-311001: LU loading standby start
- %ASA-6-311002: LU loading standby end
- %ASA-6-311003: LU recv thread up
- %ASA-6-311004: LU xmit thread up
- %ASA-6-312001: RIP hdr failed from IP\_address: cmd=string, version=number domain=string on interface interface\_name
- %ASA-6-314001: Pre-allocated RTSP UDP backconnection for src\_intf:src\_IP to dst\_intf:dst\_IP/dst\_port.
- %ASA-6-314002: RTSP failed to allocate UDP media connection from src\_intf:src\_IP to dst\_intf:dst\_IP/dst\_port: reason\_string.
- %ASA-6-314003: Dropped RTSP traffic from src\_intf:src\_ip due to: reason.
- %ASA-6-314004: RTSP client src\_intf:src\_IP accessed RTSP URL RTSP\_URL
- %ASA-6-314005: RTSP client src\_intf:src\_IP denied access to URL RTSP\_URL.
- %ASA-6-314006: RTSP client src\_intf:src\_IP exceeds configured rate limit of rate for request\_method messages.
- %ASA-6-315011: SSH session from IP\_address on interface interface\_name for user user disconnected by SSH server, reason: reason
- %ASA-6-315013: SSH session from SSH client address on interface interface\_name for user user\_name rekeyed successfully.
- %ASA-6-317007: Added route\_type route dest\_address netmask via gateway\_address [distance/metric] on interface\_name route\_type
- %ASA-6-317008: Deleted route\_type route dest\_address netmask via gateway\_address [distance/metric] on interface\_name route\_type
- %ASA-6-317077: Added <protocol\_name> route <destination\_address/subnet-mask> via <gateway-address> on <inf\_name>
- %ASA-6-317078: Deleted <protocol\_name> route <destination\_address/subnet-mask> via <gateway-address> on <inf\_name>
- %ASA-6-321003: Resource var1 log level of var2 reached.
- %ASA-6-321004: Resource var1 rate log level of var2 reached
- %ASA-6-322004: No management IP address configured for transparent firewall. Dropping protocol protocol packet from interface\_in:source\_address/source\_port to interface\_out:dest\_address/dest\_port
- %ASA-6-324303: Server=IPaddr:port ID=id The RADIUS server supports and included the Message-Authenticator payload in its response. To prevent Man-In-The-Middle attacks, consider enabling 'message-authenticator' on the aaa-server-group configuration for this server as a security best practice.
- %ASA-6-333001: EAP association initiated - context:EAP-context
- %ASA-6-333003: EAP association terminated - context:EAP-context
- %ASA-6-333009: EAP-SQ response MAC TLV is invalid - context:EAP-context
- %ASA-6-334001: EAPoUDP association initiated - host-address
- %ASA-6-334004: Authentication request for NAC Clientless host - host-address
- %ASA-6-334007: EAPoUDP association terminated - host-address
- %ASA-6-334008: NAC EAP association initiated - host-address, EAP context:EAP-context



- %ASA-6-334009: Audit request for NAC Clientless host - Assigned\_IP.
- %ASA-6-335001: NAC session initialized - host-address
- %ASA-6-335004: NAC is disabled for host - host-address
- %ASA-6-335006: NAC Applying ACL:ACL-name - host-address
- %ASA-6-335009: NAC 'Revalidate' request by administrative action - host-address
- %ASA-6-335010: NAC 'Revalidate All' request by administrative action - num sessions
- %ASA-6-335011: NAC 'Revalidate Group' request by administrative action for group-name group - num sessions
- %ASA-6-335012: NAC 'Initialize' request by administrative action - host-address
- %ASA-6-335013: NAC 'Initialize All' request by administrative action - num sessions
- %ASA-6-335014: NAC 'Initialize Group' request by administrative action for group-name group - num sessions
- %ASA-6-336011: event event
- %ASA-6-337000: Created BFD session with local discriminator id on real\_interface with neighbor real\_host\_ip.
- %ASA-6-337001: Terminated BFD session with local discriminator id on real\_interface with neighbor real\_host\_ip due to failure\_reason.
- 
- %ASA-6-338304: Successfully downloaded dynamic filter data file from updater server url
- %ASA-6-340002: Loopback-proxy info: error\_string context id context\_id, context type = version/request\_type/address\_type client socket (internal)= client\_address\_internal/client\_port\_internal server socket (internal)= server\_address\_internal/server\_port\_internal server socket (external)= server\_address\_external/server\_port\_external remote socket (external)= remote\_address\_external/remote\_port\_external
- %ASA-6-341001: Policy Agent started successfully for VNMC vnmc\_ip\_addr
- %ASA-6-341002: Policy Agent stopped successfully for VNMC vnmc\_ip\_addr
- %ASA-6-341010: Storage device with serial number ser\_no [inserted into | removed from] bay bay\_no
- %ASA-6-402129: CRYPTO: An attempt to release a DMA memory block failed, location: address
- %ASA-6-402130: CRYPTO: Received an ESP packet (SPI = xxxxxxxxxxxx, sequence number=xxxx) from 172.16.0.1 (user=user) to 192.168.0.2 with incorrect IPsec padding.
- %ASA-6-403500: PPPoE - Service name 'any' not received in PADO. Intf:interface\_name AC:ac\_name.
- %ASA-6-410004: action\_class: action DNS query\_response from src\_ifc:sip/sport to dest\_ifc:dip/dport; further\_info
- %ASA-6-414004: TCP Syslog Server intf: IP\_Address/port - Connection restored
- %ASA-6-414007: TCP Syslog Server connection restored. New connections are allowed.
- %ASA-6-414008: New connections are now allowed due to change of logging permit-hostdown policy.
- %ASA-6-415001: HTTP - matched matched\_string in policy-map map\_name, header field count exceeded connection\_action from int\_type:IP\_address/port\_num to int\_type:IP\_address/port\_num
- %ASA-6-415002: HTTP - matched matched\_string in policy-map map\_name, header field length exceeded connection\_action from int\_type:IP\_address/port\_num to int\_type:IP\_address/port\_num
- %ASA-6-415003: HTTP - matched matched\_string in policy-map map\_name, body length exceeded connection\_action from int\_type:IP\_address/port\_num to int\_type:IP\_address/port\_num
- %ASA-6-415017: HTTP - matched\_string in policy-map map\_name, arguments matched connection\_action from int\_type:IP\_address/port\_num to int\_type:IP\_address/port\_num
- %ASA-6-419004: TCP connection <ID> from <src\_ifc>:<src\_ip>/<src\_port> to <dst\_ifc>:<dst\_ip>/<dst\_port> is probed by DCD

- %ASA-6-419005: TCP connection <ID> from <src\_ifc>:<src\_ip>/<src\_port> to <dst\_ifc>:<dst\_ip>/<dst\_port> duration <hh:mm:ss> data <bytes>, is kept open by DCD as valid connection
- %ASA-6-419006: Teardown TCP connection <ID> from <src\_ifc>:<src\_ip>/<src\_port> to <dst\_ifc>:<dst\_ip>/<dst\_port> duration<hh:mm:ss> data <bytes>, DCD probe was not responded from <client/server> interface <ifc\_name>
- %ASA-6-420004: Virtual Sensor sensor\_name was added on the AIP SSM
- %ASA-6-420005: Virtual Sensor sensor\_name was deleted from the AIP SSM
- %ASA-6-421002: TCP|UDP flow from interface\_name:IP\_address/port to interface\_name:IP\_address/port bypassed application checking because the protocol is not supported.
- %ASA-6-421005: interface\_name:IP\_address is counted as a user of application
- %ASA-6-421006: There are number users of application accounted during the past 24 hours.
- %ASA-6-425001 Redundant interface redundant\_interface\_name created.
- %ASA-6-425002 Redundant interface redundant\_interface\_name removed.
- %ASA-6-425003 Interface interface\_name added into redundant interface redundant\_interface\_name.
- %ASA-6-425004 Interface interface\_name removed from redundant interface redundant\_interface\_name.
- %ASA-6-426001: PORT-CHANNEL:Interface ifc\_name bundled into EtherChannel interface Port-channel num
- %ASA-6-426002: PORT-CHANNEL:Interface ifc\_name unbundled from EtherChannel interface Port-channel num
- %ASA-6-426003: PORT-CHANNEL:Interface ifc\_name1 has become standby in EtherChannel interface Port-channel num
- %ASA-6-426101: PORT-CHANNEL:Interface ifc\_name is allowed to bundle into EtherChannel interface port-channel id by CLACP
- %ASA-6-426102: PORT-CHANNEL:Interface ifc\_name is moved to standby in EtherChannel interface port-channel id by CLACP
- %ASA-6-426103: PORT-CHANNEL:Interface ifc\_name is selected to move from standby to bundle in EtherChannel interface port-channel id by CLACP
- %ASA-6-426104: PORT-CHANNEL:Interface ifc\_name is unselected in EtherChannel interface port-channel id by CLACP
- %ASA-6-428001: WAAS confirmed from in\_interface:src\_ip\_addr/src\_port to out\_interface:dest\_ip\_addr/dest\_port, inspection services bypassed on this connection
- %ASA-6-429005: Set up authentication-proxy protocol\_type rule for the CXSC action on interface interface\_name for traffic destined to ip\_address/port for policy\_type service-policy.
- %ASA-6-429006: Cleaned up authentication-proxy rule for the CXSC action on interface interface\_name for traffic destined to ip\_address for policy\_type service-policy.
- %ASA-6-444103: Shared licensetype license usage is over 90% capacity
- %ASA-6-444104: Shared licensetype license availability: value.
- %ASA-6-444107: Shared license service status on interface ifname
- %ASA-6-444108: Shared license state client id
- %ASA-6-444306: %SMART\_LIC-6-AGENT\_READY: Smart Agent for Licensing is initialized.
- %ASA-6-444306: %SMART\_LIC-6-AGENT\_ENABLED: Smart Agent for Licensing is enabled.
- %ASA-6-444306: %SMART\_LIC-6-AGENT\_REG\_SUCCESS: Smart Agent for Licensing Registration with Cisco licensing cloud successful.

- %ASA-6-444306: %SMART\_LIC-6-AGENT\_DEREG\_SUCCESS: Smart Agent for Licensing De-registration with Cisco licensing cloud successful.
- %ASA-6-444306: %SMART\_LIC-6-DISABLED: Smart Agent for Licensing disabled.
- %ASA-6-444306: %SMART\_LIC-6-ID\_CERT\_RENEW\_SUCCESS: Identity certificate renewal successful.
- %ASA-6-444306: %SMART\_LIC-6-ENTITLEMENT\_RENEW\_SUCCESS: Entitlement authorization renewal with Cisco licensing cloud successful.
- %ASA-6-444306: %SMART\_LIC-6-AUTH\_RENEW\_SUCCESS: Authorization renewal with Cisco licensing cloud successful.
- %ASA-6-444306: %SMART\_LIC-6-HA\_ROLE\_CHANGED: Smart Agent HA role changed to role.
- %ASA-6-444306: %SMART\_LIC-6-HA\_CHASSIS\_ROLE\_CHANGED: Smart Agent HA chassis role changed to role.
- %ASA-6-444306: %SMART\_LIC-6-AGENT\_ALREADY\_REGISTER: Smart Agent is already registered with the Cisco licensing cloud.
- %ASA-6-444306: %SMART\_LIC-6-AGENT\_ALREADY\_DEREGISTER: Smart Agent is already Deregistered with the CSSM.
- %ASA-6-444306: %SMART\_LIC-6-EXPORT\_CONTROLLED: Usage of export controlled features is status.
- %ASA-6-602101: PMTU-D packet number bytes greater than effective mtu number  
dest\_addr=dest\_address, src\_addr=source\_address, prot=protocol
- %ASA-6-602103: IPSEC: Received an ICMP Destination Unreachable from src\_addr with suggested PMTU of rcvd\_mtu; PMTU updated for SA with peer peer\_addr, SPI spi, tunnel name username, old PMTU old\_mtu, new PMTU new\_mtu.
- %ASA-6-602104: IPSEC: Received an ICMP Destination Unreachable from src\_addr, PMTU is unchanged because suggested PMTU of rcvd\_mtu is equal to or greater than the current PMTU of curr\_mtu, for SA with peer peer\_addr, SPI spi, tunnel name username.
- %ASA-6-602303: IPSEC: An direction tunnel\_type SA (SPI=spi) between local\_IP and remote\_IP (username) has been created.
- %ASA-6-602304: IPSEC: An direction tunnel\_type SA (SPI=spi) between local\_IP and remote\_IP (username) has been deleted.
- %ASA-6-603101: PPTP received out of seq or duplicate pkt, tnl\_id=number, sess\_id=number, seq=number.
- %ASA-6-603102: PPP virtual interface interface\_name - user: user aaa authentication started.
- %ASA-6-603103: PPP virtual interface interface\_name - user: user aaa authentication status
- %ASA-6-603104: PPTP Tunnel created, tunnel\_id is number, remote\_peer\_ip is remote\_address, ppp\_virtual\_interface\_id is number, client\_dynamic\_ip is IP\_address, username is user, MPPE\_key\_strength is string
- %ASA-6-603105: PPTP Tunnel deleted, tunnel\_id = number, remote\_peer\_ip= remote\_address
- %ASA-6-603106: L2TP Tunnel created, tunnel\_id is number, remote\_peer\_ip is remote\_address, ppp\_virtual\_interface\_id is number, client\_dynamic\_ip is IP\_address, username is user
- %ASA-6-603107: L2TP Tunnel deleted, tunnel\_id = number, remote\_peer\_ip = remote\_address
- %ASA-6-603108: Built PPTP Tunnel at interface\_name, tunnel-id = number, remote-peer = IP\_address, virtual-interface = number, client-dynamic-ip = IP\_address, username = user, MPPE-key-strength = number

- %ASA-6-603109: Teardown PPPOE Tunnel at interface\_name, tunnel-id = number, remote-peer = IP\_address
- %ASA-6-604101: DHCP client interface interface\_name: Allocated ip = IP\_address, mask = netmask, gw = gateway\_address
- %ASA-6-604102: DHCP client interface interface\_name: address released
- %ASA-6-604103: DHCP daemon interface interface\_name: address granted MAC\_address (IP\_address)
- %ASA-6-604104: DHCP daemon interface interface\_name: address released build\_name (IP\_address)
- %ASA-6-604201: DHCPv6 PD client on interface <pd-client-iface> received delegated prefix <prefix> from DHCPv6 PD server <server-address> with preferred lifetime <in-seconds> seconds and valid lifetime <in-seconds> seconds
- %ASA-6-604202: DHCPv6 PD client on interface <pd-client-iface> releasing delegated prefix <prefix> received from DHCPv6 PD server <server-address>
- %ASA-6-604203: DHCPv6 PD client on interface <pd-client-iface> renewed delegated prefix <prefix> from DHCPv6 PD server <server-address> with preferred lifetime <in-seconds> seconds and valid lifetime <in-seconds> seconds
- %ASA-6-604204: DHCPv6 delegated prefix <delegated prefix> got expired on interface <pd-client-iface>, received from DHCPv6 PD server <server-address>
- %ASA-6-604205: DHCPv6 client on interface <client-iface> allocated address <ipv6-address> from DHCPv6 server <server-address> with preferred lifetime <in-seconds> seconds and valid lifetime <in-seconds> seconds
- %ASA-6-604206: DHCPv6 client on interface <client-iface> releasing address <ipv6-address> received from DHCPv6 server <server-address>
- %ASA-6-604207: DHCPv6 client on interface <client-iface> renewed address <ipv6-address> from DHCPv6 server <server-address> with preferred lifetime <in-seconds> seconds and valid lifetime <in-seconds> seconds
- %ASA-6-604208: DHCPv6 client address <ipv6-address > got expired on interface <client-iface>, received from DHCPv6 server <server-address>
- %ASA-6-605004: Login denied from source-address/source-port to interface:destination/service for user "username"
- %ASA-6-605005: Login permitted from source-address/source-port to interface:destination/service for user "username"
- %ASA-6-606001: ASDM session number number from IP\_address started
- %ASA-6-606002: ASDM session number number from IP\_address ended
- %ASA-6-606003: ASDM logging session number id from IP\_address started id session ID assigned
- %ASA-6-606004: ASDM logging session number id from IP\_address ended
- %ASA-6-607001: Pre-allocate SIP connection\_type secondary channel for interface\_name:IP\_address/port to interface\_name:IP\_address from string message
- %ASA-6-607003: action\_class: Received SIP req\_resp req\_resp\_info from src\_ifc:sip/sport to dest\_ifc:dip/dport; further\_info
- %ASA-6-608001: Pre-allocate Skinny connection\_type secondary channel for interface\_name:IP\_address to interface\_name:IP\_address from string message
- %ASA-6-610101: Authorization failed: Cmd: command Cmdtype: command\_modifier
- %ASA-6-611101: User authentication succeeded: IP, IP address: Uname: user
- %ASA-6-611102: User authentication failed: IP = IP address, Uname: user

- %ASA-6-611301: VPN Client: NAT configured for Client Mode with no split tunneling: NAT address: mapped\_address
- %ASA-6-611302: VPN Client: NAT exemption configured for Network Extension Mode with no split tunneling
- %ASA-6-611303: VPN Client: NAT configured for Client Mode with split tunneling: NAT address: mapped\_address Split Tunnel Networks: IP\_address/netmask IP\_address/netmask
- %ASA-6-611304: VPN Client: NAT exemption configured for Network Extension Mode with split tunneling: Split Tunnel Networks: IP\_address/netmask IP\_address/netmask
- %ASA-6-611305: VPN Client: DHCP Policy installed: Primary DNS: IP\_address Secondary DNS: IP\_address Primary WINS: IP\_address Secondary WINS: IP\_address
- %ASA-6-611306: VPN Client: Perfect Forward Secrecy Policy installed
- %ASA-6-611307: VPN Client: Head end: IP\_address
- %ASA-6-611308: VPN Client: Split DNS Policy installed: List of domains: string string
- %ASA-6-611309: VPN Client: Disconnecting from head end and uninstalling previously downloaded policy: Head End: IP\_address
- %ASA-6-611310: VNP Client: XAUTH Succeeded: Peer: IP\_address
- %ASA-6-611311: VNP Client: XAUTH Failed: Peer: IP\_address
- %ASA-6-611312: VPN Client: Backup Server List: reason
- %ASA-6-611314: VPN Client: Load Balancing Cluster with Virtual IP: IP\_address has redirected the to server IP\_address
- %ASA-6-611315: VPN Client: Disconnecting from Load Balancing Cluster member IP\_address
- %ASA-6-611316: VPN Client: Secure Unit Authentication Enabled
- %ASA-6-611317: VPN Client: Secure Unit Authentication Disabled
- %ASA-6-611318: VPN Client: User Authentication Enabled: Auth Server IP: IP\_address Auth Server Port: port Idle Timeout: time
- %ASA-6-611319: VPN Client: User Authentication Disabled
- %ASA-6-611320: VPN Client: Device Pass Thru Enabled
- %ASA-6-611321: VPN Client: Device Pass Thru Disabled
- %ASA-6-611322: VPN Client: Extended XAUTH conversation initiated when SUA disabled
- %ASA-6-611323: VPN Client: Duplicate split nw entry
- %ASA-6-613001: Checksum Failure in database in area string Link State Id IP\_address Old Checksum number New Checksum number
- %ASA-6-613002: interface interface\_name has zero bandwidth
- %ASA-6-613003: IP\_address netmask changed from area string to area string
- %ASA-6-613014: Base topology enabled on interface string attached to MTR compatible mode area string
- %ASA-6-613027: OSPF process number removed from interface interface\_name
- %ASA-6-613028: Unrecognized virtual interface inteface\_name. Treat it as loopback stub route
- %ASA-6-613041: OSPF-100 Areav string: LSA ID IP\_address, Type number, Adv-rtr IP\_address, LSA counter DoNotAge
- %ASA-6-613043:
- %ASA-6-613101: Checksum Failure in database in area %s Link State Id %i Old Checksum %#x New Checksum %#x
- %ASA-6-613102: interface %s has zero bandwidth
- %ASA-6-613103: %i%m changed from area %AREA\_ID\_STR to area %AREA\_ID\_STR
- %ASA-6-613104: Unrecognized virtual interface %IF\_NAME.
- %ASA-6-614001: Split DNS: request patched from server: IP\_address to server: IP\_address

- %ASA-6-614002: Split DNS: reply from server: IP\_address reverse patched back to original server: IP\_address
- %ASA-6-615001: vlan number not available for firewall interface
- %ASA-6-615002: vlan number available for firewall interface
- %ASA-6-616001: Pre-allocate MGCP data\_channel connection for inside\_interface:inside\_address to outside\_interface:outside\_address/port from message\_type message
- %ASA-6-617001: GTPv version msg\_type from source\_interface:source\_address/source\_port not accepted by source\_interface:dest\_address/dest\_port
- %ASA-6-617002: Removing v1 PDP Context with TID tid from GGSN IP\_address and SGSN IP\_address, Reason: reason or Removing v1 primary|secondary PDP Context with TID tid from GGSN IP\_address and SGSN IP\_address, Reason: reason
- %ASA-6-617003: GTP Tunnel created from source\_interface:source\_address/source\_port to source\_interface:dest\_address/dest\_port
- %ASA-6-617004: GTP connection created for response from source\_interface:source\_address/0 to source\_interface:dest\_address/dest\_port
- %ASA-6-617100: Teardown num\_conns connection(s) for user user\_ip
- %ASA-6-618001: Denied STUN packet <msg\_type> from <ingress\_ifc>:<source\_addr>/<source\_port> to <egress\_ifc>:<destination\_addr>/<destination\_port> for connection <conn\_id>, <drop\_reason>
- %ASA-6-620001: Pre-allocate CTIQBE {RTP | RTCP} secondary channel for interface\_name:outside\_address[/outside\_port] to interface\_name:inside\_address[/inside\_port] from CTIQBE\_message\_name message
- %ASA-6-621001: Interface interface\_name does not support multicast, not enabled
- %ASA-6-621002: Interface interface\_name does not support multicast, not enabled
- %ASA-6-621003: The event queue size has exceeded number
- %ASA-6-621006: Mrrib disconnected, (IP\_address, IP\_address) event cancelled
- %ASA-6-621007: Bad register from interface\_name:IP\_address to IP\_address for (IP\_address, IP\_address)
- %ASA-6-622001: string tracked route network mask address, distance number, table string, on interface interface-name
- %ASA-6-622101: Starting regex table compilation for match\_command; table entries = regex\_num entries
- %ASA-6-622102: Completed regex table compilation for match\_command; table size = num bytes
- %ASA-6-634001: DAP: User user, Addr ipaddr, Connection connection; The following DAP records were selected for this connection: DAP Record names
- %ASA-6-709009: (unit-role) Configuration on Active and Standby is matching. No config sync. Time elapsed <time-elapsed> ms
- %ASA-6-709010: Configuration between units doesn't match. Going for config sync (%d). Time elapsed <time-elapsed> ms.
- %ASA-6-709011: Total time to sync the config time ms.
- %ASA-6-709012: Skip configuration replication from mate as configuration on Active and Standby is matching.
- %ASA-6-713128: Connection attempt to VCPIP redirected to VCA peer IP\_address via load balancing
- %ASA-6-713145: Detected Hardware Client in network extension mode, adding static route for address: IP\_address, mask: netmask
- %ASA-6-713147: Terminating tunnel to Hardware Client in network extension mode, deleting static route for address: IP\_address, mask: netmask

- %ASA-6-713172: Automatic NAT Detection Status: Remote end is|is not behind a NAT device This end is|is not behind a NAT device
- %ASA-6-713177: Received remote Proxy Host FQDN in ID Payload: Host Name: host\_name Address IP\_address, Protocol protocol, Port port
- %ASA-6-713184: Client Type: Client\_type Client Application Version: Application\_version\_string
- %ASA-6-713202: Duplicate IP\_addr packet detected.
- %ASA-6-713211: Adding static route for L2L peer coming in on a dynamic map. address: IP\_address, mask: netmask
- %ASA-6-713213: Deleting static route for L2L peer that came in on a dynamic map. address: IP\_address, mask: netmask
- %ASA-6-713215: No match against Client Type and Version rules. Client: type version is/is not allowed by default
- %ASA-6-713219: Queuing KEY-ACQUIRE messages to be processed when P1 SA is complete.
- %ASA-6-713220: De-queuing KEY-ACQUIRE messages that were left pending.
- %ASA-6-713228: Assigned private IP address assigned\_private\_IP
- %ASA-6-713235: Attempt to send an IKE packet from standby unit. Dropping the packet!
- %ASA-6-713256: IP = peer-IP, Sending spoofed ISAKMP Aggressive Mode message 2 due to receipt of unknown tunnel group. Aborting connection.
- %ASA-6-713265: Adding static route for L2L peer coming in on a dynamic map. address: IP\_address, mask: /prefix\_len
- %ASA-6-713267: Deleting static route for L2L peer that came in on a dynamic map. address: IP\_address, mask: /prefix\_len
- %ASA-6-713269: Detected Hardware Client in network extension mode, adding static route for address: IP\_address, mask: /prefix\_len
- %ASA-6-713271: Terminating tunnel to Hardware Client in network extension mode, deleting static route for address: IP\_address, mask: /prefix\_len
- %ASA-6-713905: Descriptive\_event\_string.
- %ASA-6-716001: Group group User user WebVPN session started.
- %ASA-6-716002: Group group User user WebVPN session terminated: reason.
- %ASA-6-716003: Group group User user WebVPN access GRANTED: url
- %ASA-6-716004: Group group User user WebVPN access DENIED to specified location: url
- %ASA-6-716005: Group group User user WebVPN ACL Parse Error: reason
- %ASA-6-716006: Group name User user WebVPN session terminated. Idle timeout.
- %ASA-6-716009: Group group User user WebVPN session not allowed. WebVPN ACL parse error.
- %ASA-6-716038: Authentication: successful, group = name user = user, Session Type: WebVPN
- %ASA-6-716039: Authentication: rejected, group = name user = user, Session Type: %s
- %ASA-6-716040: Reboot pending, new sessions disabled. Denied user login.
- %ASA-6-716041: access-list acl\_ID action url url hit\_cnt count
- %ASA-6-716042: access-list acl\_ID action tcp source\_interface/source\_address (source\_port) - dest\_interface/dest\_address(dest\_port) hit-cnt count
- %ASA-6-716043 Group group-name, User user-name, IP IP\_address: WebVPN Port Forwarding Java applet started. Created new hosts file mappings
- %ASA-6-716049: Group group-name User user-name IP IP\_address Empty SVC ACL.
- %ASA-6-716050: Error adding to ACL: ace\_command\_line
- %ASA-6-716051: Group group-name User user-name IP IP\_address Error adding dynamic ACL for user.
- %ASA-6-716058: Group group User user IP ip AnyConnect session lost connection. Waiting to resume.

- %ASA-6-716059: Group group User user IP ip AnyConnect session resumed. Connection from ip2
- %ASA-6-716060: Group group User user IP ip Terminated AnyConnect session in inactive state to accept a new connection. License limit reached.
- %ASA-6-717003: Certificate received from Certificate Authority for trustpoint trustpoint\_name.
- %ASA-6-717004: PKCS #12 export failed for trustpoint trustpoint\_name.
- %ASA-6-717005: PKCS #12 export succeeded for trustpoint trustpoint\_name.
- %ASA-6-717006: PKCS #12 import failed for trustpoint trustpoint\_name.
- %ASA-6-717007: PKCS #12 import succeeded for trustpoint trustpoint\_name.
- %ASA-6-717016: Removing expired CRL from the CRL cache. Issuer: issuer
- %ASA-6-717022: Certificate was successfully validated. certificate\_identifiers
- %ASA-6-717028: Certificate chain was successfully validated additional info.
- %ASA-6-717033: OCSP response status - Successful.
- %ASA-6-717043: Local CA Server certificate enrollment related info for user: user. Info: info.
- %ASA-6-717047: Revoked certificate issued to user: username, with serial number serial number.
- %ASA-6-717048: Unrevoked certificate issued to user: username, with serial number serial number.
- %ASA-6-717056: Attempting type revocation check from Src Interface:Src IP/Src Port to Dst IP/Dst Port using protocol
- %ASA-6-717058: Automatic import of trustpool certificate bundle is successful: <No change in trustpool bundle> | <Trustpool updated in flash>
- %ASA-6-717059: Peer certificate with serial number: <serial>, subject: <subject\_name>, issuer: <issuer\_name> matched the configured certificate map <map\_name>
- %ASA-6-718003: Got unknown peer message message\_number from IP\_address, local version version\_number, remote version version\_number
- %ASA-6-718004: Got unknown internal message message\_number
- %ASA-6-718013: Peer IP\_address is not answering HELLO
- %ASA-6-718027: Received unexpected KEEPALIVE request from IP\_address
- %ASA-6-718030: Received planned OOS from IP\_address
- %ASA-6-718037: Master processed number\_of\_timeouts timeouts
- %ASA-6-718038: Slave processed number\_of\_timeouts timeouts
- %ASA-6-718039: Process dead peer IP\_address
- %ASA-6-718040: Timed-out exchange ID exchange\_ID not found
- %ASA-6-718051: Deleted secure tunnel to peer IP\_address
- %ASA-6-719001: Email Proxy session could not be established: session limit of maximum\_sessions has been reached.
- %ASA-6-719003: Email Proxy session pointer resources have been freed for source\_address.
- %ASA-6-719004: Email Proxy session pointer has been successfully established for source\_address.
- %ASA-6-719010: protocol Email Proxy feature is disabled on interface interface\_name.
- %ASA-6-719011: Protocol Email Proxy feature is enabled on interface interface\_name.
- %ASA-6-719012: Email Proxy server listening on port port for mail protocol protocol.
- %ASA-6-719013: Email Proxy server closing port port for mail protocol protocol.
- %ASA-6-719017: WebVPN user: vpnuser invalid dynamic ACL.
- %ASA-6-719018: WebVPN user: vpnuser ACL ID acl\_ID not found
- %ASA-6-719019: WebVPN user: vpnuser authorization failed.
- %ASA-6-719020: WebVPN user vpnuser authorization completed successfully.
- %ASA-6-719021: WebVPN user: vpnuser is not checked against ACL.



- %ASA-6-719022: WebVPN user vpnuser has been authenticated.
- %ASA-6-719023: WebVPN user vpnuser has not been successfully authenticated. Access denied.
- %ASA-6-719024: Email Proxy piggyback auth fail: session = pointer user=vpnuser addr=source\_address
- %ASA-6-719025: Email Proxy DNS name resolution failed for hostname.
- %ASA-6-719026: Email Proxy DNS name hostname resolved to IP\_address.
- %ASA-6-720002: (VPN-unit) Starting VPN Stateful Failover Subsystem...
- %ASA-6-720003: (VPN-unit) Initialization of VPN Stateful Failover Component completed successfully
- %ASA-6-720004: (VPN-unit) VPN failover main thread started.
- %ASA-6-720005: (VPN-unit) VPN failover timer thread started.
- %ASA-6-720006: (VPN-unit) VPN failover sync thread started.
- %ASA-6-720010: (VPN-unit) VPN failover client is being disabled
- %ASA-6-720012: (VPN-unit) Failed to update IPsec failover runtime data on the standby unit.
- %ASA-6-720014: (VPN-unit) Phase 2 connection entry (msg\_id=message\_number, my cookie=mine, his cookie=his) contains no SA list.
- %ASA-6-720015: (VPN-unit) Cannot found Phase 1 SA for Phase 2 connection entry (msg\_id=message\_number, my cookie=mine, his cookie=his).
- %ASA-6-720023: (VPN-unit) HA status callback: Peer is not present.
- %ASA-6-720024: (VPN-unit) HA status callback: Control channel is status.
- %ASA-6-720025: (VPN-unit) HA status callback: Data channel is status.
- %ASA-6-720026: (VPN-unit) HA status callback: Current progression is being aborted.
- %ASA-6-720027: (VPN-unit) HA status callback: My state state.
- %ASA-6-720028: (VPN-unit) HA status callback: Peer state state.
- %ASA-6-720029: (VPN-unit) HA status callback: Start VPN bulk sync state.
- %ASA-6-720030: (VPN-unit) HA status callback: Stop bulk sync state.
- %ASA-6-720032: (VPN-unit) HA status callback: id=ID, seq=sequence\_#, grp=group, event=event, op=operand, my=my\_state, peer=peer\_state.
- %ASA-6-720037: (VPN-unit) HA progression callback:  
id=id,seq=sequence\_number,grp=group,event=event,op=operand, my=my\_state,peer=peer\_state.
- %ASA-6-720039: (VPN-unit) VPN failover client is transitioning to active state
- %ASA-6-720040: (VPN-unit) VPN failover client is transitioning to standby state.
- %ASA-6-720045: (VPN-unit) Start bulk syncing of state information on standby unit.
- %ASA-6-720046: (VPN-unit) End bulk syncing of state information on standby unit
- %ASA-6-720056: (VPN-unit) VPN Stateful failover Message Thread is being disabled.
- %ASA-6-720057: (VPN-unit) VPN Stateful failover Message Thread is enabled.
- %ASA-6-720058: (VPN-unit) VPN Stateful failover Timer Thread is disabled.
- %ASA-6-720059: (VPN-unit) VPN Stateful failover Timer Thread is enabled.
- %ASA-6-720060: (VPN-unit) VPN Stateful failover Sync Thread is disabled.
- %ASA-6-720061: (VPN-unit) VPN Stateful failover Sync Thread is enabled.
- %ASA-6-720062: (VPN-unit) Active unit started bulk sync of state information to standby unit.
- %ASA-6-720063: (VPN-unit) Active unit completed bulk sync of state information to standby.
- %ASA-6-721001: (device) WebVPN Failover SubSystem started successfully.(device) either WebVPN-primary or WebVPN-secondary.
- %ASA-6-721002: (device) HA status change: event event, my state my\_state, peer state peer.
- %ASA-6-721003: (device) HA progression change: event event, my state my\_state, peer state peer.
- %ASA-6-721004: (device) Create access list list\_name on standby unit.
- %ASA-6-721005: (device) Fail to create access list list\_name on standby unit.

- %ASA-6-721006: (device) Update access list list\_name on standby unit.
- %ASA-6-721008: (device) Delete access list list\_name on standby unit.
- %ASA-6-721009: (device) Fail to delete access list list\_name on standby unit.
- %ASA-6-721010: (device) Add access list rule list\_name, line line\_no on standby unit.
- %ASA-6-721012: (device) Enable APCF XML file file\_name on the standby unit.
- %ASA-6-721014: (device) Disable APCF XML file file\_name on the standby unit.
- %ASA-6-721016: (device) WebVPN session for client user user\_name, IP ip\_address has been created.
- %ASA-6-721018: (device) WebVPN session for client user user\_name, IP ip\_address has been deleted.
- %ASA-6-722013: Group group User user-name IP IP\_address SVC Message: type-num/INFO: message
- %ASA-6-722014: Group group User user-name IP IP\_address SVC Message: type-num/INFO: message
- %ASA-6-722022: Group group-name User user-name IP addr (TCP | UDP) connection established (with | without) compression
- %ASA-6-722023: Group group User user-name IP IP\_address SVC connection terminated {with|without} compression
- %ASA-6-722024: SVC Global Compression Enabled
- %ASA-6-722025: SVC Global Compression Disabled
- %ASA-6-722026: Group group User user-name IP IP\_address SVC compression history reset
- %ASA-6-722027: Group group User user-name IP IP\_address SVC decompression history reset
- %ASA-6-722036: Group group User user-name IP IP\_address Transmitting large packet length (threshold num).
- %ASA-6-722051: Group group-policy User username IP public-ip Address assigned-ip assigned to session
- %ASA-6-722053: Group g User u IP ip Unknown client user-agent connection.
- %ASA-6-722055: Group group-policy User username IP public-ip Client Type: user-agent
- %ASA-6-723001: Group group-name, User user-name, IP IP\_address: WebVPN Citrix ICA connection connection is up.
- %ASA-6-723002: Group group-name, User user-name, IP IP\_address: WebVPN Citrix ICA connection connection is down.
- %ASA-6-725001: Starting SSL handshake with peer-type interface:src-ip/src-port to dst-ip/dst-port for protocol session.
- %ASA-6-725002: Device completed SSL handshake with peer-type interface:src-ip/src-port to dst-ip/dst-port for protocol-version session
- %ASA-6-725003: SSL peer-type interface:src-ip/src-port to dst-ip/dst-port request to resume previous session.
- %ASA-6-725004: Device requesting certificate from SSL peer-type interface:src-ip/src-port to dst-ip/dst-port for authentication.
- %ASA-6-725005: SSL peer-type interface:src-ip/src-port to dst-ip/dst-port requesting our device certificate for authentication.
- %ASA-6-725006: Device failed SSL handshake with peer-type interface:src-ip/src-port to dst-ip/dst-port
- %ASA-6-725007: SSL session with peer-type interface:src-ip/src-port to dst-ip/dst-port terminated.
- %ASA-6-725025: SSL Pre-auth connection rate limit hit %s watermark.
- %ASA-6-726001: Inspected im\_protocol im\_service Session between Client im\_client\_1 and im\_client\_2 Packet flow from src\_ifc:/sip/sport to dest\_ifc:/dip/dport Action: action Matched Class class\_map\_id class\_map\_name
- %ASA-6-730004: Group groupname User username IP ipaddr VLAN ID vlanid from AAA ignored.
- %ASA-6-730005: Group groupname User username IP ipaddr VLAN ID vlanid from AAA is invalid.

- %ASA-6-730008: Group groupname, User username, IP ipaddr, VLAN MAPPING timeout waiting NACApp.
- %ASA-6-725016: Device selects trust-point <trustpoint> for peer-type interface:src-ip/src-port to dst-ip/dst-port
- %ASA-6-731001: NAC policy added: name: policyname Type: policytype.
- %ASA-6-731002: NAC policy deleted: name: policyname Type: policytype.
- %ASA-6-731003: nac-policy unused: name: policyname Type: policytype.
- %ASA-6-732001: Group groupname, User username, IP ipaddr, Fail to parse NAC-SETTINGS nac-settings-id, terminating connection.
- %ASA-6-732002: Group groupname, User username, IP ipaddr, NAC-SETTINGS settingsid from AAA ignored, existing NAC-SETTINGS settingsid\_inuse used instead.
- %ASA-6-732003: Group groupname, User username, IP ipaddr, NAC-SETTINGS nac-settings-id from AAA is invalid, terminating connection.
- %ASA-6-734001: DAP: User user, Addr ipaddr, Connection connection: The following DAP records were selected for this connection: DAP record names
- %ASA-6-737005: IPAA: DHCP configured, request succeeded for tunnel-group 'tunnel-group'
- %ASA-6-737006: IPAA: Local pool request succeeded for tunnel-group 'tunnel-group'
- %ASA-6-737009: IPAA: AAA assigned address ip-address, request failed
- %ASA-6-737010: IPAA: AAA assigned address ip-address, request succeeded
- %ASA-6-737014: IPAA: Freeing AAA address ip-address
- %ASA-6-737015: IPAA: Freeing DHCP address ip-address
- %ASA-6-737016: IPAA: Freeing local pool address ip-address
- %ASA-6-737017: IPAA: DHCP request attempt num succeeded
- %ASA-6-737026: IPAA: Client assigned ip-address from local pool
- %ASA-6-737029: IPAA: Adding ip-address to standby: succeeded
- %ASA-6-737031: IPAA: Removing %m from standby: succeeded
- %ASA-6-737036: IPAA: Session=<session>, Client assigned <address> from DHCP
- %ASA-6-737205: VPNFIP: Pool=pool, INFO: message
- %ASA-6-737406: POOLIP: Pool=pool, INFO: message
- %ASA-6-741000: Coredump filesystem image created on variable 1 -size variable 2 MB
- %ASA-6-741001: Coredump filesystem image on variable 1 - resized from variable 2 MB to variable 3 MB
- %ASA-6-741002: Coredump log and filesystem contents cleared on variable 1
- %ASA-6-741003: Coredump filesystem and its contents removed on variable 1
- %ASA-6-741004: Coredump configuration reset to default values
- %ASA-6-746001: user-identity: activated import user groups | activated host names | user-to-IP address databases download started
- %ASA-6-746002: user-identity: activated import user groups | activated host names | user-to-IP address databases download complete
- %ASA-6-746008: user-identity: NetBIOS Probe Process started
- %ASA-6-746009: user-identity: NetBIOS Probe Process stopped
- %ASA-6-746017: user-identity: Update import-user domain\_name\group\_name
- %ASA-6-746018: user-identity: Update import-user domain\_name\group\_name done
- %ASA-6-747004: Clustering: state machine changed from state state-name to state-name.
- %ASA-6-748008: [CPU load *percentage* | memory load *percentage* ] of module *slot\_number* in chassis *chassis\_number* (*member-name* ) exceeds overflow protection threshold [CPU *percentage* | memory *percentage* ]. System may be oversubscribed on member failure.

- %ASA-6-748009: [CPU load percentage | memory load percentage] of chassis chassis\_number exceeds overflow protection threshold [CPU percentage | memory percentage}. System may be oversubscribed on chassis failure.
- %ASA-6-803001: Flow offloaded: connection conn\_id outside\_ifc:outside\_addr/outside\_port (mapped\_addr/mapped\_port) inside\_ifc:inside\_addr/inside\_port (mapped\_addr/mapped\_port) Protocol
- %ASA-6-803002: Flow is no longer offloaded: connection conn\_id outside\_ifc:outside\_addr/outside\_port (mapped\_addr/mapped\_port) inside\_ifc:inside\_addr/inside\_port (mapped\_addr/mapped\_port) Protocol
- %ASA-6-751023: Local a:p Remote: a:p Username:n Unknown client connection
- %ASA-6-751026: Local: localIP:port Remote: remoteIP:port Username: username/group IKEv2 Client OS: client-os Client: client-name client-version
- %ASA-6-767001: Inspect-name: Dropping an unsupported IPv6/IP46/IP64 packet from interface:IP Addr to interface:IP Addr (fail-close)
- %ASA-6-769007: UPDATE: Image version is version\_number
- %ASA-6-776008: CTS SXP: Connection with peer IP (instance connection instance num) state changed from original state to final state.
- %ASA-6-776251: CTS SGT-MAP: Binding binding IP - SGname(SGT) from source name added to binding manager.
- %ASA-6-776253: CTS SGT-MAP: Binding binding IP - new SGname(SGT) from new source name changed from old sgt: old SGname(SGT) from old source old source name.
- %ASA-6-776303: CTS Policy: Security-group name "sgname" is resolved to security-group tag sgt
- %ASA-6-776311: CTS Policy: Previously unresolved security-group name "sgname" is now resolved to security-group tag sgt
- %ASA-6-775001: Scansafe: protocol connection conn\_id from interface\_name:real\_address/real\_port [(idfw\_user)] to interface\_name:real\_address/real\_port redirected to server\_interface\_name:server\_ip\_address
- %ASA-6-775003: Scansafe:protocol connection conn\_id from interface\_name:real\_address/real\_port [(idfw\_user)] to interface\_name:real\_address/real\_port is whitelisted.
- %ASA-6-775006: Primary server interface:ip\_address is not reachable and backup server interface:ip\_address is now active
- %ASA-6-772005: REAUTH: user username passed authentication
- %ASA-6-775005: Scansafe: Primary server ip\_address is reachable now
- %ASA-6-778001: VXLAN: Invalid VXLAN segment-id segment-id for protocol from ifc-name:(IP-address/port) to ifc-name:(IP-address/port).
- %ASA-6-778002: VXLAN: There is no VNI interface for segment-id segment-id.
- %ASA-6-778003: VXLAN: Invalid VXLAN segment-id segment-id for protocol from ifc-name:(IP-address/port) to ifc-name:(IP-address/port) in FP.
- %ASA-6-778004: VXLAN: Invalid VXLAN header for protocol from ifc-name:(IP-address/port) to ifc-name:(IP-address/port) in FP.
- %ASA-6-778005: VXLAN: Packet with VXLAN segment-id segment-id from ifc-name is denied by FP L2 check.
- %ASA-6-778006: VXLAN: Invalid VXLAN UDP checksum from ifc-name:(IP-address/port) to ifc-name:(IP-address/port) in FP.
- %ASA-6-778007: VXLAN: Packet from ifc-name:IP-address/port to IP-address/port was discarded due to invalid NVE peer.
- %ASA-6-779001: STS: Out-tag lookup failed for in-tag segment-id of protocol from ifc-name:IP-address/port to IP-address/port.
- %ASA-6-779002: STS: STS and NAT locate different egress interface for segment-id segment-id, protocol from ifc-name:IP-address/port to IP-address/port

- %ASA-6-780001: RULE ENGINE: Started compilation for access-group transaction - description of the transaction.
- %ASA-6-780002: RULE ENGINE: Finished compilation for access-group transaction - description of the transaction.
- %ASA-6-780003: RULE ENGINE: Started compilation for nat transaction - description of the transaction.
- %ASA-6-780004: RULE ENGINE: Finished compilation for nat transaction - description of the transaction.
- %ASA-6-802005: IP ip\_address Received MDM request details.
- %ASA-6-803001: Bypass is continuing after power up, no protection will be provided by the system for traffic over GigabitEthernet 1/1-1/2
- %ASA-6-803002: No protection will be provided by the system for traffic over GigabitEthernet 1/1-1/2
- %ASA-6-803003: User disabled bypass manually on GigabitEthernet 1/1-1/2
- %ASA-6-804001: Interface GigabitEthernet1/3 1000BaseSX SFP has been inserted
- %ASA-6-804002: Interface GigabitEthernet1/3 SFP has been removed
- %ASA-6-805001: Flow offloaded: connection conn\_id outside\_ifc:outside\_addr/outside\_port (mapped\_addr/mapped\_port) inside\_ifc:inside\_addr/inside\_port (mapped\_addr/mapped\_port) Protocol
- %ASA-6-805002: Flow is no longer offloaded: connection conn\_id outside\_ifc:outside\_addr/outside\_port (mapped\_addr/mapped\_port) inside\_ifc:inside\_addr/inside\_port (mapped\_addr/mapped\_port) Protocol
- %ASA-6-805003: Flow could not be offloaded: connection <conn\_id> <outside\_ifc>:<outside\_addr>/<outside\_port> (<mapped\_addr>/<mapped\_port>) <inside\_ifc>:<inside\_addr>/<inside\_port> (<mapped\_addr>/<mapped\_port>) <Protocol>
- %ASA-6-806001: Primary alarm CPU temperature is High temperature
- %ASA-6-806002: Primary alarm for CPU high temperature is cleared
- %ASA-6-806003: Primary alarm CPU temperature is Low temperature
- %ASA-6-806004: Primary alarm for CPU Low temperature is cleared
- %ASA-6-806005: Secondary alarm CPU temperature is High temperature
- %ASA-6-806006: Secondary alarm for CPU high temperature is cleared
- %ASA-6-806007: Secondary alarm CPU temperature is Low temperature
- %ASA-6-806008: Secondary alarm for CPU Low temperature is cleared
- %ASA-6-806009: Alarm asserted for ALARM\_IN\_1 description
- %ASA-6-806010: Alarm cleared for ALARM\_IN\_1 alarm\_1\_description
- %ASA-6-806011: Alarm asserted for ALARM\_IN\_2 description
- %ASA-6-806012: Alarm cleared for ALARM\_IN\_2 alarm\_2\_description
- %ASA-6-812007: Inline-set hardware-bypass mode configuration <status>
- %ASA-6-880001:<Ingress interface>, for traffic <source ipaddress> to <destination ipaddress>, PBR picked <outside interface 1> as its <metric-type> became better than <outside interface 2>
- %ASA-6-830001: VPN session redistribution <variable 1>
- %ASA-6-830002: Moved <variable 1> sessions to <variable 2>
- %ASA-6-830004: <variable 1> request to move <variable 2> sessions from <variable 3> to <variable 4>

## Debugging Messages, Severity 7

The following messages appear at severity 7, debugging:

- %ASA-7-108006: Detected ESMTP size violation from src\_ifc:sip|sport to dest\_ifc:dip|dport;declared size is: decl\_size, actual size is act\_size.
- %ASA-7-109014: A non-Telnet connection was denied to the configured virtual Telnet IP address.
- %ASA-7-109021: Uauth null proxy error
- %ASA-7-111009: User user executed cmd:string
- %ASA-7-113028: Extraction of username from VPN client certificate has string. [Request num]
- %ASA-7-199019: syslog
- %ASA-7-304005: URL Server IP\_address request pending URL url
- %ASA-7-304009: Ran out of buffer blocks specified by url-block command
- %ASA-7-333004: EAP-SQ response invalid - context:EAP-context
- %ASA-7-333005: EAP-SQ response contains invalid TLV(s) - context:EAP-context
- %ASA-7-333006: EAP-SQ response with missing TLV(s) - context:EAP-context
- %ASA-7-333007: EAP-SQ response TLV has invalid length - context:EAP-context
- %ASA-7-333008: EAP-SQ response has invalid nonce TLV - context:EAP-context
- %ASA-7-335007: NAC Default ACL not configured - host-address
- %ASA-7-342001: REST API Agent started successfully.
- %ASA-7-342005: REST API image has been installed successfully.
- %ASA-7-342007: REST API image has been uninstalled successfully.
- %ASA-7-419003: Cleared TCP urgent flag
  
- %ASA-7-421004: Failed to inject {TCP|UDP} packet from IP\_address/port to IP\_address/port
- %ASA-7-444307: %SMART\_LIC-7-DAILY\_JOB\_TIMER\_RESET: Daily job timer reset.
  
- %ASA-7-609001: Built local-host zone\_name/\*: ip\_address
- %ASA-7-609002: Teardown local-host zone\_name/\*: ip\_address duration time
- %ASA-7-701001: alloc\_user() out of Tcp\_user objects
- %ASA-7-701002: alloc\_user() out of Tcp\_proxy objects
- %ASA-7-702307: IPSEC: An direction tunnel\_type SA (SPI=spi) between local\_IP and remote\_IP (username) is rekeying due to data rollover.
- %ASA-7-703001: H.225 message received from interface\_name:IP\_address/port to interface\_name:IP\_address/port is using an unsupported version number
- %ASA-7-703002: Received H.225 Release Complete with newConnectionNeeded for interface\_name:IP\_address to interface\_name:IP\_address/port
- %ASA-7-703008: Allowing early-message: %s before SETUP from %s:%Q/%d to %s:%Q/%d
- %ASA-7-709001: FO replication failed: cmd=command returned=code
- %ASA-7-709002: FO unreplicable: cmd=command
- %ASA-7-710001: TCP access requested from source\_address/source\_port to interface\_name:dest\_address/service
- %ASA-7-710002: {TCP|UDP} access permitted from source\_address/source\_port to interface\_name:dest\_address/service
- %ASA-7-710004: TCP connection limit exceeded from Src\_ip/Src\_port to In\_name:Dest\_ip/Dest\_port (current connections/connection limit = Curr\_conn/Conn\_lmt)
- %ASA-7-710005: {TCP|UDP} request discarded from source\_address/source\_port to interface\_name:dest\_address/service
- %ASA-7-710006: protocol request discarded from source\_address to interface\_name:dest\_address
- %ASA-7-710007: NAT-T keepalive received from 86.1.161.1/1028 to outside:86.1.129.1/4500
- %ASA-7-711001: debug\_trace\_msg
- %ASA-7-711003: Unknown/Invalid interface identifier(vpifnum) detected.

- %ASA-7-711006: CPU profiling has started for n-samples samples. Reason: reason-string.
- %ASA-7-713024: Group group IP ip Received local Proxy Host data in ID Payload: Address IP\_address, Protocol protocol, Port port
- %ASA-7-713025: Received remote Proxy Host data in ID Payload: Address IP\_address, Protocol protocol, Port port
- %ASA-7-713028: Received local Proxy Range data in ID Payload: Addresses IP\_address - IP\_address, Protocol protocol, Port port
- %ASA-7-713029: Received remote Proxy Range data in ID Payload: Addresses IP\_address - IP\_address, Protocol protocol, Port port
- %ASA-7-713034: Received local IP Proxy Subnet data in ID Payload: Address IP\_address, Mask netmask, Protocol protocol, Port port
- %ASA-7-713035: Group group IP ip Received remote IP Proxy Subnet data in ID Payload: Address IP\_address, Mask netmask, Protocol protocol, Port port
- %ASA-7-713039: Send failure: Bytes (number), Peer: IP\_address
- %ASA-7-713040: Could not find connection entry and can not encrypt: msgid message\_number
- %ASA-7-713052: User (user) authenticated.
- %ASA-7-713066: IKE Remote Peer configured for SA: SA\_name
- %ASA-7-713094: Cert validation failure: handle invalid for Main/Aggressive Mode Initiator/Responder!
- %ASA-7-713099: Tunnel Rejected: Received NONCE length number is out of range!
- %ASA-7-713103: Invalid (NULL) secret key detected while computing hash
- %ASA-7-713104: Attempt to get Phase 1 ID data failed while hash computation
- %ASA-7-713113: Deleting IKE SA with associated IPSec connection entries. IKE peer: IP\_address, SA address: internal\_SA\_address, tunnel count: count
- %ASA-7-713114: Connection entry (conn entry internal address) points to IKE SA (SA\_internal\_address) for peer IP\_address, but cookies don't match
- %ASA-7-713117: Received Invalid SPI notify (SPI SPI\_Value)!
- %ASA-7-713121: Keep-alive type for this connection: keepalive\_type
- %ASA-7-713143: Processing firewall record. Vendor: vendor(id), Product: product(id), Caps: capability\_value, Version Number: version\_number, Version String: version\_text
- %ASA-7-713160: Remote user (session Id - id) has been granted access by the Firewall Server
- %ASA-7-713164: The Firewall Server has requested a list of active user sessions
- %ASA-7-713169: IKE Received delete for rekeyed SA IKE peer: IP\_address, SA address: internal\_SA\_address, tunnelCnt: tunnel\_count
- %ASA-7-713170: Group group IP ip IKE Received delete for rekeyed centry IKE peer: IP\_address, centry address: internal\_address, msgid: id
- %ASA-7-713171: NAT-Traversal sending NAT-Original-Address payload
- %ASA-7-713187: Tunnel Rejected: IKE peer does not match remote peer as defined in L2L policy IKE peer address: IP\_address, Remote peer address: IP\_address
- %ASA-7-713190: Got bad refCnt (ref\_count\_value) assigning IP\_address (IP\_address)
- %ASA-7-713204: Adding static route for client address: IP\_address
- %ASA-7-713221: Static Crypto Map check, checking map = crypto\_map\_tag, seq = seq\_number...
- %ASA-7-713222: Group group Username username IP ip Static Crypto Map check, map = crypto\_map\_tag, seq = seq\_number, ACL does not match proxy IDs src:source\_address dst:dest\_address
- %ASA-7-713223: Static Crypto Map check, map = crypto\_map\_tag, seq = seq\_number, no ACL configured
- %ASA-7-713224: Static Crypto Map Check by-passed: Crypto map entry incomplete!

- %ASA-7-713225: [IKEv1], Static Crypto Map check, map map\_name, seq = sequence\_number is a successful match
- %ASA-7-713233: (VPN-unit) Remote network (remote network) validated for network extension mode.
- %ASA-7-713234: (VPN-unit) Remote network (remote network) from network extension mode client mismatches AAA configuration (aaa network).
- %ASA-7-713236: IKE\_DECODE tx/rx Message (msgid=msgid) with payloads:payload1 (payload1\_len) + payload2 (payload2\_len)...total length: tlen
- %ASA-7-713263: Received local IP Proxy Subnet data in ID Payload: Address IP\_address, Mask /prefix\_len, Protocol protocol, Port port
- %ASA-7-713264: Received local IP Proxy Subnet data in ID Payload: Address IP\_address, Mask /prefix\_len, Protocol protocol, Port port {"Received remote IP Proxy Subnet data in ID Payload: Address %a, Mask/%d, Protocol %u, Port %u"}
- %ASA-7-713273: Deleting static route for client address: IP\_Address IP\_Address address of client whose route is being removed
- %ASA-7-713906: Descriptive\_event\_string.
- %ASA-7-714001: description\_of\_event\_or\_packet
- %ASA-7-714002: IKE Initiator starting QM: msg id = message\_number
- %ASA-7-714003: IKE Responder starting QM: msg id = message\_number
- %ASA-7-714004: IKE Initiator sending 1st QM pkt: msg id = message\_number
- %ASA-7-714005: IKE Responder sending 2nd QM pkt: msg id = message\_number
- %ASA-7-714006: IKE Initiator sending 3rd QM pkt: msg id = message\_number
- %ASA-7-714007: IKE Initiator sending Initial Contact
- %ASA-7-714011: Description of received ID values
- %ASA-7-715001: Descriptive statement
- %ASA-7-715004: subroutine name() Q Send failure: RetCode (return\_code)
- %ASA-7-715005: subroutine name() Bad message code: Code (message\_code)
- %ASA-7-715006: IKE got SPI from key engine: SPI = SPI\_value
- %ASA-7-715007: IKE got a KEY\_ADD msg for SA: SPI = SPI\_value
- %ASA-7-715008: Could not delete SA SA\_address, refCnt = number, caller = calling\_subroutine\_address
- %ASA-7-715009: IKE Deleting SA: Remote Proxy IP\_address, Local Proxy IP\_address
- %ASA-7-715013: Tunnel negotiation in progress for destination IP\_address, discarding data
- %ASA-7-715018: IP Range type id was loaded: Direction %s, From: %a, Through: %a
- %ASA-7-715019: Group group Username username IP ip IKEGetUserAttributes: Attribute name = name
- %ASA-7-715020: construct\_cfg\_set: Attribute name = name
- %ASA-7-715021: Delay Quick Mode processing, Cert/Trans Exch/RM DSID in progress
- %ASA-7-715022: Resume Quick Mode processing, Cert/Trans Exch/RM DSID completed
- %ASA-7-715027: IPSec SA Proposal # chosen\_proposal, Transform # chosen\_transform acceptable Matches global IPSec SA entry # crypto\_map\_index
- %ASA-7-715028: IKE SA Proposal # 1, Transform # chosen\_transform acceptable Matches global IKE entry # crypto\_map\_index
- %ASA-7-715031: Obtained IP addr (%s) prior to initiating Mode Cfg (XAuth %s)
- %ASA-7-715032: Sending subnet mask (%s) to remote client
- %ASA-7-715033: Processing CONNECTED notify (MsgId message\_number)
- %ASA-7-715034: action IOS keep alive payload: proposal=time 1/time 2 sec.
- %ASA-7-715035: Starting IOS keepalive monitor: seconds sec.



- %ASA-7-715036: Sending keep-alive of type notify\_type (seq number number)
- %ASA-7-715037: Unknown IOS Vendor ID version: major.minor.variance
- %ASA-7-715038: action Spoofing\_information Vendor ID payload (version: major.minor.variance, capabilities: value)
- %ASA-7-715039: Unexpected cleanup of tunnel table entry during SA delete.
- %ASA-7-715040: Deleting active auth handle during SA deletion: handle = internal\_authentication\_handle
- %ASA-7-715041: Received keep-alive of type keepalive\_type, not the negotiated type
- %ASA-7-715042: IKE received response of type failure\_type to a request from the IP\_address utility
- %ASA-7-715044: Ignoring Keepalive payload from vendor not support KeepAlive capability
- %ASA-7-715045: ERROR: malformed Keepalive payload
- %ASA-7-715046: Group = groupname, Username = username, IP = IP\_address, constructing payload\_description payload
- %ASA-7-715047: processing payload\_description payload
- %ASA-7-715048: Send VID\_type VID
- %ASA-7-715049: Received VID\_type VID
- %ASA-7-715050: Claims to be IOS but failed authentication
- %ASA-7-715051: Received unexpected TLV type TLV\_type while processing FWTYPE ModeCfg Reply
- %ASA-7-715052: Old P1 SA is being deleted but new SA is DEAD, cannot transition centries
- %ASA-7-715053: MODE\_CFG: Received request for attribute\_info!
- %ASA-7-715054: MODE\_CFG: Received attribute\_name reply: value
- %ASA-7-715055: Send attribute\_name
- %ASA-7-715056: Client is configured for TCP\_transparency
- %ASA-7-715057: Auto-detected a NAT device with NAT-Traversal. Ignoring IPSec-over-UDP configuration.
- %ASA-7-715058: NAT-Discovery payloads missing. Aborting NAT-Traversal.
- %ASA-7-715059: Proposing/Selecting only UDP-Encapsulated-Tunnel and UDP-Encapsulated-Transport modes defined by NAT-Traversal
- %ASA-7-715060: Dropped received IKE fragment. Reason: reason
- %ASA-7-715061: Rcv'd fragment from a new fragmentation set. Deleting any old fragments.
- %ASA-7-715062: Error assembling fragments! Fragment numbers are non-continuous.
- %ASA-7-715063: Successfully assembled an encrypted pkt from rcv'd fragments!
- %ASA-7-715064 -- IKE Peer included IKE fragmentation capability flags: Main Mode: true/false Aggressive Mode: true/false
- %ASA-7-715065: IKE state\_machine subtype FSM error history (struct data\_structure\_address) state, event: state/event pairs
- %ASA-7-715066: Can't load an IPSec SA! The corresponding IKE SA contains an invalid logical ID.
- %ASA-7-715067: QM IsRekeyed: existing sa from different peer, rejecting new sa
- %ASA-7-715068: QM IsRekeyed: duplicate sa found by address, deleting old sa
- %ASA-7-715069: Invalid ESP SPI size of SPI\_size
- %ASA-7-715070: Invalid IPComp SPI size of SPI\_size
- %ASA-7-715071: AH proposal not supported
- %ASA-7-715072: Received proposal with unknown protocol ID protocol\_ID
- %ASA-7-715074: Could not retrieve authentication attributes for peer IP\_address
- %ASA-7-715075: Group = group\_name, IP = IP\_address Received keep-alive of type message\_type (seq number number)
- %ASA-7-715076: Computing hash for ISAKMP

- %ASA-7-715077: Pitcher: msg string, spi spi
- %ASA-7-715078: Received %s LAM attribute
- %ASA-7-715079: INTERNAL\_ADDRESS: Received request for %s
- %ASA-7-715080: VPN: Starting P2 rekey timer: 28800 seconds.
- %ASA-7-716008: WebVPN ACL: action
- %ASA-7-716010: Group group User user Browse network.
- %ASA-7-716011: Group group User user Browse domain domain.
- %ASA-7-716012: Group group User user Browse directory directory.
- %ASA-7-716013: Group group User user Close file filename.
- %ASA-7-716014: Group group User user View file filename.
- %ASA-7-716015: Group group User user Remove file filename.
- %ASA-7-716016: Group group User user Rename file old\_filename to new\_filename.
- %ASA-7-716017: Group group User user Modify file filename.
- %ASA-7-716018: Group group User user Create file filename.
- %ASA-7-716019: Group group User user Create directory directory.
- %ASA-7-716020: Group group User user Remove directory directory.
- %ASA-7-716021: File access DENIED, filename.
- %ASA-7-716024: Group name User user Unable to browse the network. Error: description
- %ASA-7-716025: Group name User user Unable to browse domain domain. Error: description
- %ASA-7-716026: Group name User user Unable to browse directory directory. Error: description
- %ASA-7-716027: Group name User user Unable to view file filename. Error: description
- %ASA-7-716028: Group name User user Unable to remove file filename. Error: description
- %ASA-7-716029: Group name User user Unable to rename file filename. Error: description
- %ASA-7-716030: Group name User user Unable to modify file filename. Error: description
- %ASA-7-716031: Group name User user Unable to create file filename. Error: description
- %ASA-7-716032: Group name User user Unable to create folder folder. Error: description
- %ASA-7-716033: Group name User user Unable to remove folder folder. Error: description
- %ASA-7-716034: Group name User user Unable to write to file filename.
- %ASA-7-716035: Group name User user Unable to read file filename.
- %ASA-7-716036: Group name User user File Access: User user logged into the server server.
- %ASA-7-716037: Group name User user File Access: User user failed to login into the server server.
- %ASA-7-716603: Received size-recv KB Hostscan data from IP src-ip.
- %ASA-7-717024: Checking CRL from trustpoint: trustpoint name for purpose
- %ASA-7-717025: Validating certificate chain containing number of certs certificate(s).
- %ASA-7-717029: Identified client certificate within certificate chain. serial number: serial\_number, subject name: subject\_name.
- %ASA-7-717030: Found a suitable trustpoint trustpoint name to validate certificate.
- %ASA-7-717034: No-check extension found in certificate. OCSP check bypassed.
- %ASA-7-717036: Looking for a tunnel group match based on certificate maps for peer certificate with certificate\_identifier.
- %ASA-7-717038: Tunnel group match found. Tunnel Group: tunnel\_group\_name, Peer certificate: certificate\_identifier.
- %ASA-7-717041: Local CA Server event: event info.
- %ASA-7-717045: Local CA Server CRL info: info
- %ASA-7-718001: Internal interprocess communication queue send failure: code error\_code

- %ASA-7-718017: Got timeout for unknown peer IP\_address msg type message\_type
- %ASA-7-718018: Send KEEPALIVE request failure to IP\_address
- %ASA-7-718019: Sent KEEPALIVE request to IP\_address
- %ASA-7-718020: Send KEEPALIVE response failure to IP\_address
- %ASA-7-718021: Sent KEEPALIVE response to IP\_address
- %ASA-7-718022: Received KEEPALIVE request from IP\_address
- %ASA-7-718023: Received KEEPALIVE response from IP\_address
- %ASA-7-718025: Sent CFG UPDATE to IP\_address
- %ASA-7-718026: Received CFG UPDATE from IP\_address
- %ASA-7-718029: Sent OOS indicator to IP\_address
- %ASA-7-718034: Sent TOPOLOGY indicator to IP\_address
- %ASA-7-718035: Received TOPOLOGY indicator from IP\_address
- %ASA-7-718036: Process timeout for req-type type\_value, exid exchange\_ID, peer IP\_address
- %ASA-7-718041: Timeout [msgType=type] processed with no callback
- %ASA-7-718046: Create group policy policy\_name
- %ASA-7-718047: Fail to create group policy policy\_name
- %ASA-7-718049: Created secure tunnel to peer IP\_address
- %ASA-7-718056: Deleted Master peer, IP IP\_address
- %ASA-7-718058: State machine return code: action\_routine, return\_code
- %ASA-7-718059: State machine function trace: state=state\_name, event=event\_name, func=action\_routine
- %ASA-7-718088: Possible VPN LB misconfiguration. Offending device MAC MAC\_address.
- %ASA-7-719005: FSM NAME has been created using protocol for session pointer from source\_address.
- %ASA-7-719006: Email Proxy session pointer has timed out for source\_address because of network congestion.
- %ASA-7-719007: Email Proxy session pointer cannot be found for source\_address.
- %ASA-7-719009: Email Proxy service is starting.
- %ASA-7-719015: Parsed emailproxy session pointer from source\_address username: mailuser = mail\_user, vpnuser = VPN\_user, mailserv = server
- %ASA-7-719016: Parsed emailproxy session pointer from source\_address password: mailpass = \*\*\*\*\*, vpnpass= \*\*\*\*\*
- %ASA-7-720031: (VPN-unit) HA status callback: Invalid event received. event=event\_ID.
- %ASA-7-720034: (VPN-unit) Invalid type (type) for message handler.
- %ASA-7-720041: (VPN-unit) Sending type message id to standby unit
- %ASA-7-720042: (VPN-unit) Receiving type message id from active unit
- %ASA-7-720048: (VPN-unit) FSM action trace begin: state=state, last event=event, func=function.
- %ASA-7-720049: (VPN-unit) FSM action trace end: state=state, last event=event, return=return, func=function.
- %ASA-7-720050: (VPN-unit) Failed to remove timer. ID = id.
- %ASA-7-722029: Group group User user-name IP IP\_address SVC Session Termination: Conns: connections, DPD Conns: DPD\_conns, Comp resets: compression\_resets, Dcmp resets: decompression\_resets
- %ASA-7-722030: Group group User user-name IP IP\_address SVC Session Termination: In: data\_bytes (+ctrl\_bytes) bytes, data\_pkts (+ctrl\_pkts) packets, drop\_pkts drops
- %ASA-7-722031: Group group User user-name IP IP\_address SVC Session Termination: Out: data\_bytes (+ctrl\_bytes) bytes, data\_pkts (+ctrl\_pkts) packets, drop\_pkts drops.
- %ASA-7-723003: No memory for WebVPN Citrix ICA connection connection.
- %ASA-7-723004: WebVPN Citrix encountered bad flow control flow.

- %ASA-7-723005: No channel to set up WebVPN Citrix ICA connection.
- %ASA-7-723006: WebVPN Citrix SOCKS errors.
- %ASA-7-723007: WebVPN Citrix ICA connection connection list is broken.
- %ASA-7-723008: WebVPN Citrix ICA SOCKS Server server is invalid.
- %ASA-7-723009: Group group-name, User user-name, IP IP\_address: WebVPN Citrix received data on invalid connection connection.
- %ASA-7-723010: Group group-name, User user-name, IP IP\_address: WebVPN Citrix received closing channel channel for invalid connection connection.
- %ASA-7-723011: Group group-name, User user-name, IP IP\_address: WebVPN Citrix receives bad SOCKS socks message length msg-length. Expected length is exp-msg-length.
- %ASA-7-723012: Group group-name, User user-name, IP IP\_address: WebVPN Citrix received bad SOCKS socks message format.
- %ASA-7-723013: WebVPN Citrix encountered invalid connection connection during periodic timeout.
- %ASA-7-723014: Group group-name, User user-name, IP IP\_address: WebVPN Citrix TCP connection connection to server server on channel channel initiated.
- %ASA-7-725008: SSL peer-type interface:src-ip/src-port to dst-ip/dst-port proposes the following n cipher(s).
- %ASA-7-725009: Device proposes the following n cipher(s) peer-type interface:src-ip/src-port to dst-ip/dst-port.
- %ASA-7-725010: Device supports the following n cipher(s).
- %ASA-7-725011: Cipher[order]: cipher\_name
- %ASA-7-725012: Device chooses cipher cipher for the SSL session with peer-type interface:src-ip/src-port to dst-ip/dst-port.
- %ASA-7-725013: SSL peer-type interface:src-ip/src-port to dst-ip/dst-port chooses cipher cipher
- %ASA-7-725014: SSL lib error. Function: function Reason: reason
- %ASA-7-725017: No certificates received during the handshake with %s %s:%B/%d to %B/%d for %s session
- %ASA-7-725021: Device preferring cipher-suite cipher(s). Connection info: interface :src-ip /src-port to dst-ip /dst-port
- %ASA-7-725022: Device skipping cipher : cipher - reason. Connection info: interface :src-ip /src-port to dst-ip /dst-port
- %ASA-7-730001: Group groupname, User username, IP ipaddr: VLAN MAPPING to VLAN vlanid
- %ASA-7-730002: Group groupname, User username, IP ipaddr: VLAN MAPPING to VLAN vlanid failed
- %ASA-7-730003: NACApp sets IP ipaddr VLAN to vlanid
- %ASA-7-730006: Group groupname, User username, IP ipaddr: is on NACApp AUTH VLAN vlanid.
- %ASA-7-730007: Group groupname, User username, IP ipaddr: changed VLAN to <%s> ID vlanid
- %ASA-7-730010: Group groupname, User username, IP ipaddr, VLAN Mapping is enabled on VLAN vlanid.
- %ASA-7-734003: DAP: User name, Addr ipaddr: Session Attribute: attr name/value
- %ASA-7-737001: IPAA: Received message 'message-type'
- %ASA-7-737035: IPAA: Session=<session>, '<message type>' message queued
- %ASA-7-747005: Clustering: State machine notify event event-name (event-id, ptr-in-hex, ptr-in-hex)
- %ASA-7-747006: Clustering: State machine is at state state-name
- %ASA-7-737200: VPNFIP: Pool=pool, Allocated ip-address from pool
- %ASA-7-737201: VPNFIP: Pool=pool, Returned ip-address to pool (recycle=recycle)
- %ASA-7-737206: VPNFIP: Pool=pool, DEBUG: message

- %ASA-7-737400: POOLIP: Pool=pool, Allocated ip-address from pool
- %ASA-7-737401: POOLIP: Pool=pool, Returned ip-address to pool (recycle=recycle)
- %ASA-7-737407: POOLIP: Pool=pool, DEBUG: message
- %ASA-7-750016: Local: localIP:port Remote:remoteIP:port Username: username IKEv2 Need to send a DPD message to peer
- %ASA-7-751003: Local: localIP:port Remote:remoteIP:port Username: username/group Need to send a DPD message to peer
- %ASA-7-752002: Tunnel Manager Removed entry. Map Tag = mapTag. Map Sequence Number = mapSeq.
- %ASA-7-752008: Duplicate entry already in Tunnel Manager.
- %ASA-7-776012: CTS SXP: timer name timer started for connection with peer peer IP.
- %ASA-7-776013: CTS SXP: timer name timer stopped for connection with peer peer IP.
- %ASA-7-776014: CTS SXP: SXP received binding forwarding request (action) binding binding IP - SGname(SGT).
- %ASA-7-776015: CTS SXP: Binding binding IP - SGname(SGT) is forwarded to peer peer IP (instance connection instance num).
- %ASA-7-776016: CTS SXP: Binding binding IP - SGname(SGT) from peer peer IP (instance binding's connection instance num) changed from old instance: old instance num, old sgt: old SGname(SGT).
- %ASA-7-776017: CTS SXP: Binding binding IP - SGname(SGT) from peer peer IP (instance connection instance num) deleted in SXP database.
- %ASA-7-776018: CTS SXP: Binding binding IP - SGname(SGT) from peer peer IP (instance connection instance num) added in SXP database.
- %ASA-7-776019: CTS SXP: Binding binding IP - SGname(SGT) action taken. Update binding manager.
- %ASA-7-776301: CTS Policy: Security-group tag sgt is mapped to security-group name "sgname"
- %ASA-7-776302: CTS Policy: Unknown security-group tag sgt referenced in policies
- %ASA-7-776307: CTS Policy: Security-group name for security-group tag sgt renamed from old\_sgname" to "new\_sgname"
- %ASA-7-776308: CTS Policy: Previously unknown security-group tag sgt is now mapped to security-group name "sgname"
- %ASA-7-785001: Clustering: Ownership for existing flow from <in\_interface>:<src\_ip\_addr>/<src\_port> to <out\_interface>:<dest\_ip\_addr>/<dest\_port> moved from unit <old-owner-unit-id> at site <old-site-id> to <new-owner-unit-id> at site <old-site-id> due to <reason>.
- %ASA-7-815004: OGS: Packet <protocol> from <source IP address/port> to <destination IP address/port> matched <number of source network objects> source network objects and <number of source network objects> destination network objects total search entries <total number of entries>. Resultant key-set has <number of entries> entries

## Variables Used in Syslog Messages

Syslog messages often include variables. The following table lists most variables that are used in this guide to describe syslog messages. Some variables that appear in only one syslog message are not listed.

Variable Fields in Syslog Messages

Variable	Description
<i>acl_ID</i>	An ACL name.

Variable	Description
<i>bytes</i>	The number of bytes.
<i>code</i>	A decimal number returned by the syslog message to indicate the cause or source of the error, according to the syslog message generated.
<i>command</i>	A command name.
<i>command_modifier</i>	The <b>command_modifier</b> is one of the following strings: <ul style="list-style-type: none"> <li>• cmd (this string means the command has no modifier)</li> <li>• clear</li> <li>• no</li> <li>• show</li> </ul>
<i>connections</i>	The number of connections.
<i>connection_type</i>	The connection type: <ul style="list-style-type: none"> <li>• SIGNALLING UDP</li> <li>• SIGNALLING TCP</li> <li>• SUBSCRIBE UDP</li> <li>• SUBSCRIBE TCP</li> <li>• Via UDP</li> <li>• Route</li> <li>• RTP</li> <li>• RTCP</li> </ul>
<i>dec</i>	Decimal number.
<i>dest_address</i>	The destination address of a packet.
<i>dest_port</i>	The destination port number.
<i>device</i>	The memory storage device. For example, the floppy disk, internal flash memory, TFTP, the failover standby unit, or the console terminal.
<i>econns</i>	Number of embryonic connections.
<i>elimit</i>	Number of embryonic connections specified in the <b>static</b> or <b>nat</b> command.
<i>filename</i>	A filename of the type ASAimage, ASDM file, or configuration.
<i>ftp-server</i>	External FTP server name or IP address.
<i>gateway_address</i>	The network gateway IP address.
<i>global_address</i>	Global IP address, an address on a lower security level interface.
<i>global_port</i>	The global port number.
<i>hex</i>	Hexadecimal number.
<i>inside_address</i>	Inside (or local) IP address, an address on a higher security level interface.

<b>Variable</b>	<b>Description</b>
<i>inside_port</i>	The inside port number.
<i>interface_name</i>	The name of the interface.
<i>IP_address</i>	IP address in the form <i>n n n n</i> , where <i>n</i> is an integer from 1 to 255.
<i>MAC_address</i>	The MAC address.
<i>mapped_address</i>	The translated IP address.
<i>mapped_port</i>	The translated port number.
<i>message_class</i>	Category of syslog message associated with a functional area of the ASA.
<i>message_list</i>	Name of a file you create containing a list of syslog message ID numbers, classes, or severity levels.
<i>message_number</i>	The syslog message ID.
<i>nconns</i>	Number of connections permitted for the static or xlate table.
<i>netmask</i>	The subnet mask.
<i>number</i>	A number. The exact form depends on the syslog message.
<i>octal</i>	Octal number.
<i>outside_address</i>	Outside (or foreign) IP address, an address of a syslog server typically on a lower security level interface in a network beyond the outside router.
<i>outside_port</i>	The outside port number.
<i>port</i>	The TCP or UDP port number.
<i>privilege_level</i>	The user privilege level.
<i>protocol</i>	The protocol of the packet, for example, ICMP, TCP, or UDP.
<i>real_address</i>	The real IP address, before NAT.
<i>real_port</i>	The real port number, before NAT.
<i>reason</i>	A text string describing the reason for the syslog message.
<i>service</i>	The service specified by the packet, for example, SNMP or Telnet.
<i>severity_level</i>	The severity level of a syslog message.
<i>source_address</i>	The source address of a packet.
<i>source_port</i>	The source port number.
<i>string</i>	Text string (for example, a username).

Variable	Description
<i>tcp_flags</i>	Flags in the TCP header such as: <ul style="list-style-type: none"><li>• ACK</li><li>• FIN</li><li>• PSH</li><li>• RST</li><li>• SYN</li><li>• URG</li></ul>
<i>time</i>	Duration, in the format <i>hh mm ss</i>
<i>url</i>	A URL.
<i>user</i>	A username.





## INDEX

4GE SSM [63, 72](#)

### A

AAA [xviii, 35–38, 48–52, 201, 212, 281, 313, 436–437](#)

authentication [51, 437](#)

authorization [37](#)

messages [35–36, 38, 48–52, 201, 212, 281, 313](#)

server [xviii, 37, 51, 201, 281, 436–437](#)

ABR [135](#)

without backbone area [135](#)

access denied [119](#)

URL [119](#)

access lists [389](#)

See ACLs [389](#)

access permittedUDP [317](#)

access permittedTCP [317](#)

access permitted [317](#)

access requestedTCP [317](#)

access requested [317](#)

access-list command [29–30, 36](#)

deny-flow-max optionaccess-list deny-flow-max command [30](#)

interval option [29](#)

omitting [36](#)

access-list commandaccess-list commandaccess-list command

command [24, 29, 115](#)

to permit traffic on UDP port 53 [24](#)

to permit traffic on UDP port 53access-list command [24, 29, 115](#)

ACLs [28–30, 36–37, 52, 115, 327, 337, 350–351, 382–383, 389, 429, 431–432, 436](#)

ACL\_ID [389](#)

compilation out of memory [28](#)

configuration error [36](#)

crypto map [327](#)

deny [115](#)

deny-flows [30](#)

empty ACL downloaded [36](#)

failed check [37](#)

logging matches [29](#)

no ACL configured [351](#)

packet denied [28](#)

parsing error [36](#)

peer context ID [429](#)

ACLs (*continued*)

peer context IDaccess-list commandaccess-list commandaccess-list command [429](#)

to permit traffic on UDP port 53 [429](#)

peer IP address not set [429](#)

proxy ID mismatch [350](#)

SoftNP error [431–432](#)

split tunneling policy [337](#)

unsupported format [52](#)

WebVPN [382–383, 436](#)

ACL ID not found [436](#)

parse error [382–383, 436](#)

user authorization failure [436](#)

address translation slots [88, 204–205](#)

no more available [204](#)

no more available address translation slots, no more available [88](#)

anchor count negative [169](#)

area border router [135](#)

See ABR [135](#)

ARP packet mismatch [204](#)

ARP poisoning attackattacks [204](#)

ARP poisoning [204](#)

ARP spoofing attack [145](#)

asymmetric routing [27](#)

attacks [31, 35, 144–145](#)

ARP spoofing [145](#)

DoS [35](#)

spoofing [144–145](#)

suspicious e-mail address pattern [31](#)

Auth from IP address/port to IP address/port failed [33](#)

Auth start for user [33](#)

Authen Session End [35](#)

authentication [33–34, 281](#)

failed [34](#)

request [281](#)

request succeeds [33](#)

response [281](#)

authorization [34, 293](#)

command [293](#)

user [293](#)

user denied [34](#)

Auto Update URL unreachable [299](#)

**B**

- backup server list [296](#)
  - downloadedEasy VPN Remote [296](#)
    - backup server list [296](#)
    - downloaded [296](#)
  - errorEasy VPN Remote [296](#)
    - backup server list [296](#)
    - error [296](#)
- bridge table [220](#)
  - full [220](#)
- broadcast, invalid source address [26](#)
- built H245 connection [105](#)

**C**

- cannot specify PAT host [25](#)
- certificate data could not be verified [404](#)
- classes, logging [xviii](#)
  - message class variables [xviii](#)
  - types [xviii](#)
- clear command [207](#)
  - local-host option [207](#)
- config commandconfig commandconfig command [47](#)
- configuration [47, 219, 315](#)
  - erase [47](#)
  - replication [315](#)
    - beginning [315](#)
    - failed [315](#)
  - status changed [219](#)
- configure commandconfigure commandconfigure command [47](#)
- connection limit exceeded [86–87](#)
- connection limit exceededTCP [318, 663](#)
  - connection limit exceeded [318, 663](#)
- CTIQBE [309–310](#)
  - connection object pre-allocation [309](#)
  - unsupported version [310](#)

**D**

- deny [24–26](#)
  - inbound from outside [24](#)
  - inbound ICMP [25](#)
  - inbound UDP [24](#)
  - inbound UDP due to query/response [24](#)
  - IP from address to address [25](#)
  - IP spoof [26](#)
  - self route [25](#)
  - TCP (no connection) [25](#)
- device pass through [297](#)
  - disabledEasy VPN Remote [297](#)
    - device pass through [297](#)
    - disabled [297](#)

- device pass through (*continued*)
  - enabledEasy VPN Remote [297](#)
    - device pass through [297](#)
    - enabled [297](#)
- DNS HINFO request attackattacks [187](#)
  - DNS HINFO request [187](#)
- DNS query or response is denied [24](#)
- DNS request for all records attackattacks [187](#)
  - DNS request for all records [187](#)
- DNS server too slow [24](#)
- DNS zone transfer attackattacks [187](#)
  - DNS zone transfer [187](#)
- DNS zone transfer from high port attackattacks [187](#)
  - DNS zone transfer from high port [187](#)
- DoS attackattacks [30, 90, 207](#)
  - DoS [30, 90, 207](#)

**E**

- Easy VPN Remote [298](#)
  - SUA [298](#)
    - disabled [298](#)
- embryonic limit exceeded [85](#)

**F**

- failover [1–2, 7–12, 91–93, 316, 438–443, 445–448](#)
  - bad cable [1](#)
  - block allocation failed [8](#)
  - cable communication failed [8](#)
  - cable not connected [1](#)
  - cable status [2](#)
  - configuration replication [8](#)
  - configuration replication failed [316](#)
  - continuous failovers [10](#)
  - failover active command [443](#)
  - failover command message dropped [10](#)
  - incompatible software on mate [11](#)
  - interface link down [11](#)
  - LAN interface down [9](#)
  - license mismatch with mate [12](#)
  - lost communications with mate [7](#)
  - mate card configuration mismatch [12](#)
  - mate has different chassis [12](#)
  - mate may be disabled [10](#)
  - operational mode mismatch with mate [12](#)
  - peer LAN link down [10](#)
  - replication interrupted [10](#)
  - show failover command [447–448](#)
  - standby unit failed to sync [8](#)
  - stateful error [91](#)
  - stateful failover [91–93](#)
  - VPN failover [438–443, 445–446, 448](#)
    - buffer error [442](#)
    - client being disabled [440](#)

failover (*continued*)VPN failover (*continued*)

- CTCP flow handle error [445](#)
- failed to allocate chunk [439](#)
- failed to initialize [438](#)
- memory allocation error [440](#)
- non-block message not sent [442](#)
- registration failure [439](#)
- SDI node secret file failed to synchronize [448](#)
- standby unit received corrupted message from active unit [446](#)
- state update message failure [446](#)
- timer error [441](#)
- trustpoint certification failure [440](#)
- trustpoint name not found [443](#)
- unable to add to message queue [445](#)
- version control block failure [440](#)

failover command [4, 10, 443](#)

- active option [443](#)
- active option failover command [4](#)
- active option failover command [4](#)
- active option [4](#)

failover command failover command [6](#)failover messages [1–2, 315](#)failover message testing [7](#)

- interface [7](#)

filter allow command [120](#)filter command [120](#)

- allow option filter command [120](#)
- allow option [120](#)

Flood Defender [313](#)floodguard command floodguard command floodguard command [34](#)flow control error [168](#)fragmented ICMP traffic attack attacks [187](#)

- fragmented ICMP traffic [187](#)

FTP [86](#)

- data connection failed [86](#)

**H**H.225 [205](#)H.245 connection [105](#)

- foreign address H.245 H.245 [105](#)

H.323 [314](#)

- unsupported packet version [314](#)

H.323 H.323 [105](#)

- back-connection, preallocated [105](#)

handle not allocated [168](#)hello packet with duplicate router ID OSPF [211](#)

- hello packet with duplicate router ID [211](#)

host limit [207](#)host move [219](#)hostile event [201](#)hostile event hostile event [27](#)

- firewall circumvented hostile event hostile event [27](#)

HTTPS process limit [36](#)ICMP [25](#)

- packet denied conduit command [25](#)
- permit ICMP option [25](#)
- packet denied dropping echo request [25](#)

IDB initialization OSPF [136](#)

- IDB initialization [136](#)

inbound TCP connection denied [23](#)inspect ESMTP command [31](#)insufficient memory [88, 204](#)

- error caused by [88, 204](#)

interface [98, 299](#)

- virtual interface [98](#)

PPP virtual virtual interface PPP virtual interface [98](#)

- zero bandwidth bandwidth [299](#)

reported as zero [299](#)

Internet phone, detecting use of detecting use of Internet phone [105](#)invalid character replaced in e-mail address [31](#)invalid source addresses [26](#)IP address [283](#)

- DHCP client [283](#)

- DHCP server [283](#)

IP fragment attack attacks [187](#)

- IP fragment [187](#)

IP fragments overlap attack attacks [187](#)

- IP fragments overlap [187](#)

IP impossible packet attack attacks [187](#)

- IP impossible packet [187](#)

IP route counter decrement failure [208](#)IP routing table [30–31, 133, 136](#)

- attack attacks [30–31](#)

IP routing table [30–31](#)

- creation error [133](#)

- limit exceeded [133](#)

- limit warning [133](#)

- OSPF inconsistency OSPF [136](#)

IP routing table inconsistency [136](#)

ip verify reverse-path command [27](#)ip verify reverse-path command ip verify reverse-path command [27](#)IPSec [48–52, 115, 132, 322, 325–326, 328, 330, 332–333, 340, 343–344,](#)

[370–371, 376, 378–379, 402–403, 425, 450](#)

- connection entries [332](#)

- connections [49–52, 403](#)

failure [403](#)

- cTCP tunnel [450](#)

- encryption [370](#)

- fragmentation policy ignored [344](#)

- negotiation [326](#)

- over UDP [340, 376](#)

- over TCP [376](#)

- packet triggered IKE [325](#)

- proposal [379](#)

SA [379](#)

unsupported [379](#)

- protocol [322](#)

IPSec (*continued*)

- proxy mismatch [115](#)
- rekeying duration [328](#)
- request rejected [332](#)
- SA [326, 330, 333, 370–371, 378](#)
  - proposal [378](#)
- tunnels [48, 132, 326, 343, 402–403, 425](#)

## L

L2TP [282](#)

- tunnel [282](#)

land attackattacks [26](#)

- land [26](#)

large ICMP traffic attackattacks [187](#)

- large ICMP traffic [187](#)

Leaving ALLOW mode, URL Server [120](#)link state advertisement [135](#)

- See LSA [135](#)

link status Up or Down [7](#)load balancing cluster [296](#)

- disconnectedEasy VPN Remote [296](#)
  - load balancing cluster [296](#)
  - disconnected [296](#)
- redirectedEasy VPN Remote [296](#)
  - load balancing cluster [296](#)
  - redirected [296](#)

logging [xviii](#)

- classes [xviii](#)
- types [xviii](#)

loopback network, invalid source address [26](#)lost failover communications with mate [7](#)LSA [210](#)

- default with wrong maskOSPF [210](#)
  - LSA [210](#)
- default with wrong mask [210](#)
- invalid typeOSPF [210](#)
  - LSA [210](#)
- invalid type [210](#)

## M

MAC address mismatch [204](#)man in the middle attackattacks [143](#)

- man in the middle [143](#)

memory [8, 88, 132, 135, 299](#)

- block depleted [8](#)
- corruptionOSPF [299](#)
  - checksum error [299](#)
- insufficientinsufficient memory [88](#)
- leakLSA [135](#)
  - not foundOSPF [135](#)
    - LSA [135](#)
    - not found [135](#)

memory (*continued*)

- lowlow memorylow memory [132](#)
  - failed operation [132](#)
- message block alloc failed [8](#)
- messages [31, 91–93, 130, 671](#)
  - Mail Guard [31](#)
  - SSH [130](#)
  - stateful failover [91–93](#)
  - variables used in [671](#)
- messages, logging [xviii](#)
  - classes [xviii](#)
  - list of [xviii](#)
- Microsoft Point-to-Point Encryption [200](#)
  - See MPPE [200](#)
- MPPE [201](#)
  - encryption policy setup [201](#)
- MS-CHAPMS-CHAP [200](#)
  - authentication [200](#)

## N

nat command [120](#)no associated connection within connection tableTCP [25](#)

- no associated connection in table [25](#)

no translation group foundpacket [120](#)

- not matched outbound NAT rules [120](#)

## O

OSPF [135, 209–210, 266, 299](#)

- ABR without backbone area [135](#)
- configuration change [299](#)
- database request from unknown neighborOSPF [209](#)
  - database description from unknown neighborOSPF [209](#)
  - hello from unknown neighbor [209](#)
- invalid packet [209](#)
- neighbor state changed [266](#)
- network range area changed [299](#)
- packet of invalid length [210](#)
- out of address translation slots! [88](#)
- outbound deny commandoutbound deny command [24](#)

## P

packet [24–25, 28](#)

- denied [24–25, 28](#)

PAT [25, 88, 204–205](#)

- address [88, 204–205](#)
- global address [25](#)
- host unspecified [25](#)

pdb index error [133](#)ping of death attackattacks [187](#)

- ping of death [187](#)

PPTP [98, 200, 281–282](#)

- packet out of sequence [281](#)

PPTP (*continued*)

- tunnel [98, 282](#)
- XGRE packet [200](#)
- preallocate H323 UDP back connection [105](#)
- privilege level, changed [265](#)
- proxied RPC request attackattacks [187](#)
- proxied RPC request [187](#)

**R**

- RADIUS authentication [200](#)
- RCMD, back connection failed [86](#)
- reload commandreload commandreload command [47, 79](#)
- request discardedUDP [318](#)
  - request discardedTCP [318](#)
  - request discarded [318](#)
- router ID allocation failureOSPF [210](#)
  - router ID allocation failure [210](#)
- rsh commandrsh commandrsh command [86](#)

**S**

- security [25, 28, 267](#)
  - breach [25](#)
  - context [28, 267](#)
    - added [267](#)
    - context cannot be determined [28](#)
    - removed [267](#)
- self route [25](#)
- SETUP message [205](#)
- Severity level 4 [260](#)
  - ASA-4-447001 [260](#)
- show command [8, 24, 85–86, 93, 207, 447–448](#)
  - blocks optionshow command [8](#)
    - blocks option [8](#)
  - failover option [93, 447–448](#)
  - local-host option [207](#)
  - outbound optionshow command [24](#)
    - outbound option [24](#)
  - static optionshow command [85–86](#)
    - static option [86](#)
    - static optionshow static command [85](#)
  - version option [207](#)
- shuns [190](#)
- SIP connection [288](#)
- skinny connection [290](#)
- SMTP [31](#)
- software version mismatch [222](#)
- split network entry duplicateEasy VPN Remote [298](#)
  - split network entry duplicate [298](#)
- spoofing attackattacks [26–27, 204](#)
  - spoofing [26–27, 204](#)
- SSH [130](#)
- SSM 4GE [63, 72](#)

- statd buffer overflow attackattacks [187](#)
  - statd buffer overflow [187](#)
- stateful failover [91–93](#)
- SUA [296–297](#)
  - disabledEasy VPN Remote [297](#)
    - SUA [297](#)
    - disabled [297](#)
  - enabledEasy VPN Remote [296](#)
    - SUA [296](#)
    - enabled [296](#)
- SYN [85](#)
  - attackattacks [85](#)
    - SYN [85](#)
- SYNSYN [25](#)
  - flag [25](#)
- system log messages [xviii](#)
  - classes [xviii](#)

**T**

- TCP [121, 317](#)
  - connections [317](#)
  - translation creation failedUDP [121](#)
    - translation creation failedICMP [121](#)
    - translation creation failed [121](#)
- TCP FIN only flags attackattacks [187](#)
  - TCP FIN only flags [187](#)
- TCP NULL flags attackattacks [187](#)
  - TCP NULL flags [187](#)
- TCP state-bypass connection creation [115](#)
- TCP state-bypass connection teardown [115](#)
- TCP SYN+FIN flags attackattacks [187](#)
  - TCP SYN+FIN flags [187](#)
- timeout uauth commandtimeout uauth command [35](#)
- timeouts, recommended values [207](#)
- too many connections on staticconnection limit exceeded [85](#)
- tunnel, PPTP [98](#)

**U**

- UDP [24, 121, 187, 317](#)
  - bomb attackattacks [187](#)
    - UDP bomb [187](#)
  - chargen DoS attackattacks [187](#)
    - UDP chargen DoS [187](#)
  - connections [317](#)
  - messages [121](#)
  - packet [24](#)
  - snork attackattacks [187](#)
    - UDP snork [187](#)
- unsupported application [221](#)
- URL [119–120](#)
  - buffer block space [120](#)
  - filtering, disabledweb requests, unfiltered [120](#)
  - Server [119](#)

user authentication [36, 297](#)  
     disabledEasy VPN Remote [297](#)  
         user authentication [297](#)  
         disabled [297](#)  
     enabledEasy VPN Remote [297](#)  
         user authentication [297](#)  
         enabled [297](#)  
     error [36](#)  
 user logged out [293](#)  
 username [265](#)  
     created [265](#)  
     deleted [265](#)

## V

variables [671](#)  
     in messages [671](#)  
     in messagesmessages [671](#)  
         variables used in [671](#)  
     list of [671](#)  
 virtual linksOSPF [136](#)  
     virtual linksrouter-ID resetOSPF [136](#)  
         router-id resetOSPF [136](#)  
         process reset [136](#)  
 vpdn group command [200](#)  
 VPN [132](#)  
     peer limit [132](#)  
     tunnel [132](#)  
 VPN failover [438–443, 445–446, 448](#)  
     client being disabled [440](#)  
     CTCP flow handle error [445](#)

VPN failover (*continued*)  
     failed to allocate chunk [439](#)  
     failed to initialize [438](#)  
     memory allocation error [440](#)  
     non-block message not sent [442](#)  
     registration failure [439](#)  
     SDI node secret file failed to synchronize [448](#)  
     standby unit received corrupted message from active unit [446](#)  
     state update message failure [446](#)  
     timer error [441](#)  
     trustpoint certification failure [440](#)  
     trustpoint name not found [443](#)  
     unable to add to message queue [445](#)  
     version control block failure [440](#)

## W

Websense server [119](#)  
 write command [47, 92–93](#)  
     erase option [47](#)  
     standby command [93](#)  
     standby option [92](#)  
 write commandwrite command [47](#)  
 write erase commandwrite erase command [47](#)

## X

XAUTH enabledEasy VPN Remote [298](#)  
     XAUTH enabled [298](#)  
 XGRE, packet with invalid protocol field [200](#)