

# ASDMの設定、認証、およびその他の問題のトラブルシューティング

## 内容

---

### [はじめに](#)

### [背景](#)

### [ASDM設定の問題のトラブルシューティング](#)

[問題 1. ASDMでは、インターフェイスに適用されているアクセスコントロールリスト\(ACL\)は表示されません](#)

[問題 2. ASA CLIとASDM UI間のヒットカウントの不一致](#)

[問題 3. 「ERROR: % Invalid input detected at '^' marker.」というエラーメッセージが表示されません](#)

[問題 4. 「ERROR: ACL is associated with route-map and inactive not supported, instead remove the acl」というエラーメッセージが特定のケースで表示される](#)

[問題 5. 暗黙的に拒否された接続に関するログがASDMリアルタイムログビューアに表示されない](#)

[問題 6. ネットワークオブジェクトまたはオブジェクトグループを変更しようとするとASDMがフリーズする](#)

[問題 7. ASDMでは、異なるインターフェイスのアクセスコントロールリスト\(ACL\)ルールを表示できません](#)

[問題 8. リアルタイムログはリアルタイムログビューアでは使用できません](#)

[問題 9. リアルタイムログビューアで日付と時刻の列が空になっているトラブルシューティング : 推奨処置](#)

[問題 10. マルチコンテキストASAで別のコンテキストに切り替えた後にASDMへのロギングが失敗する可能性がある](#)

[問題 11. 異なるコンテキスト間の切り替え時にASDMセッションが突然終了する](#)

[問題 12. ASDMがランダムに終了/終了し、「ASDM received a message from the ASA device to disconnect.ASDMを終了します。」](#)

[問題 13. ASDMロードが「Authentication FirePOWER login」メッセージでハングする](#)

[問題 14. ASDMにFirepowerモジュールの管理/設定が表示されない](#)

[問題 15. ASDMでセキュアクライアントプロファイルにアクセスできない](#)

[問題 16. ASDMでセキュアクライアントプロファイルXMLプロファイルを編集できない](#)

[問題 17. 設定を変更した後にSecure Clientイメージが失われる](#)

[問題 18. 無効なhttp server session-timeoutコマンドおよびhttp server idle-timeoutコマンド](#)

[問題 19. ASDMでのdap.xmlコピーの失敗](#)

[問題 20. ASDMにIKEポリシーとIPSECプロポーザルが表示されない](#)

[問題 21. ASDMでメッセージ「The enable password is not set.今すぐ設定してください。」](#)

[問題 22. ASDM UIの更新後にASDNオブジェクトが表示されない](#)

[問題 23. 4.5より前のバージョンのAnyConnectクライアントプロファイルを編集できない](#)

[問題 24. Edit Service Policy > Rule Actions > ASA FirePOWER Inspectionタブに移動できない](#)

[問題 25. ASDM上のAnyConnectイメージバージョン5.1およびAnyConnectプロファイルエディタ](#)

[問題 26. AAA属性タイプ\(Radius/LDAP\)がASDMに表示されない](#)

[問題 27. ASDMに「Post Quantum key cannot be empty」エラーが表示される](#)

[問題 28. ASDMで「where used」オプションを使用しても結果が表示されない](#)

[問題 29. ネットワークオブジェクトを削除するときに、警告メッセージ「\[Network Object\]は次](#)

---

[の場所で使用されているため削除できません」が表示される](#)

[問題 30.ASDMのNetwork Objects/Groupタブのユーザビリティの問題](#)

## [ASDM認証問題のトラブルシューティング](#)

[問題 1.ASDMログインに失敗しました](#)

[問題 2.ASDMコマンドの許可に失敗しました](#)

[問題3.ASDMの読み取り専用アクセスの設定](#)

[問題 4.ASDM多要素認証\(MFA\)](#)

[問題 5.ASDM外部認証設定](#)

[問題 6.ASDMローカル認証が失敗する](#)

[問題 7.ASDMワンタイムパスワード](#)

[問題 8.接続プロファイルにすべてのメソッドが表示されない](#)

[問題 9.ASDMセッションがタイムアウトしない](#)

[問題 10.ASDM LDAP認証が失敗する](#)

[問題 11.ASDM Webvpn DAP設定が欠落している](#)

## [ASDMのその他の問題のトラブルシューティング](#)

[問題 1.ASDMでセキュアクライアントプロファイルにアクセスできない](#)

[問題 2.ASDMにホストスキャンのポップアップが表示される – イメージに重要なセキュリティ修正が含まれていない](#)

[問題3.ASDM経由でイメージをコピーするときに「Error writing request body to server」が発生する](#)

---

## はじめに

このドキュメントでは、Adaptive Security Appliance(ASA)Device Manager(ASDM)の設定、認証、およびその他の問題のトラブルシューティングプロセスについて説明します。

## 背景

このドキュメントは、次のドキュメントとともにASDMトラブルシューティングシリーズの一部です。

[リンク1<>](#)

[リンク2<>](#)

[リンク3<>](#)

## ASDM設定の問題のトラブルシューティング

**問題 1.ASDMでは、インターフェイスに適用されているアクセスコントロールリス**

## ト(ACL)は表示されません

ASDMでは、対象のインターフェイスに適用された有効なaccess-groupがあっても、そのインターフェイスに適用されたアクセスコントロールリスト(ACL)は表示されません。代わりに、メッセージに「0 incoming rules」と表示されます。これらの症状は、インターフェイスのアクセスグループ設定で設定されたL3およびL2 ACLで確認できます。

```
<#root>
```

```
firewall(config)#
```

```
access-list 1 extended permit ip any
```

```
firewall(config)#
```

```
any access-list 2 extended permit udp any any
```

```
firewall(config)#
```

```
access-list 3 ethertype permit dsap bpdu
```

```
firewall(config)#
```

```
access-group 3 in interface inside
```

```
firewall(config)#
```

```
access-group 1 in interface inside
```

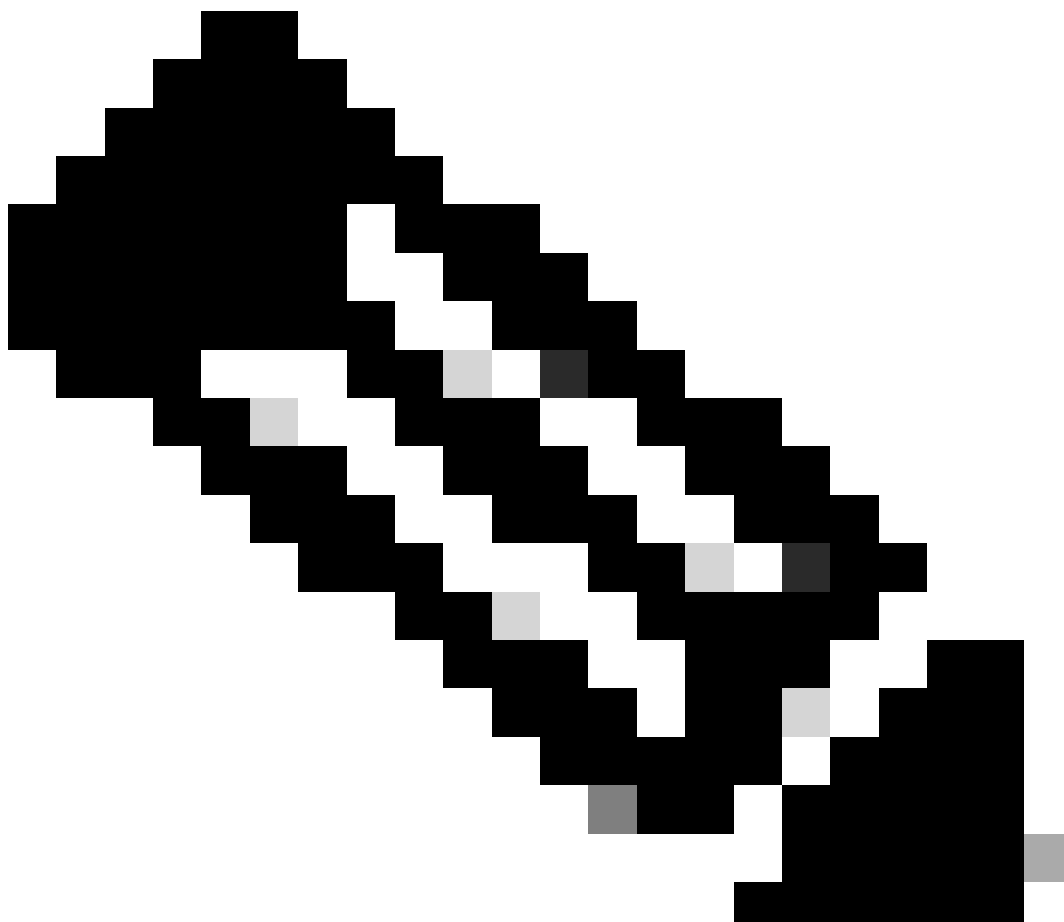
```
firewall(config)#
```

```
access-group 2 in interface outside
```

## トラブルシューティング – 推奨処置

Cisco Bug ID [CSCwj14147](#) 「L2とL3のACLが混在している場合に、ASDMがアクセスグループ設定をロードできない」を参照してください。

---



注：この不具合は、最近のASDMソフトウェアリリースで修正されています。詳細については、不具合の詳細を確認してください。

---

## 問題 2.ASA CLIとASDM UI間のヒットカウントの不一致

ASDMのヒットカウントエントリは、ファイアウォールの出力でshow access-listコマンドによって報告されるアクセスリストのヒットカウントと一致しません。

トラブルシューティング – 推奨処置

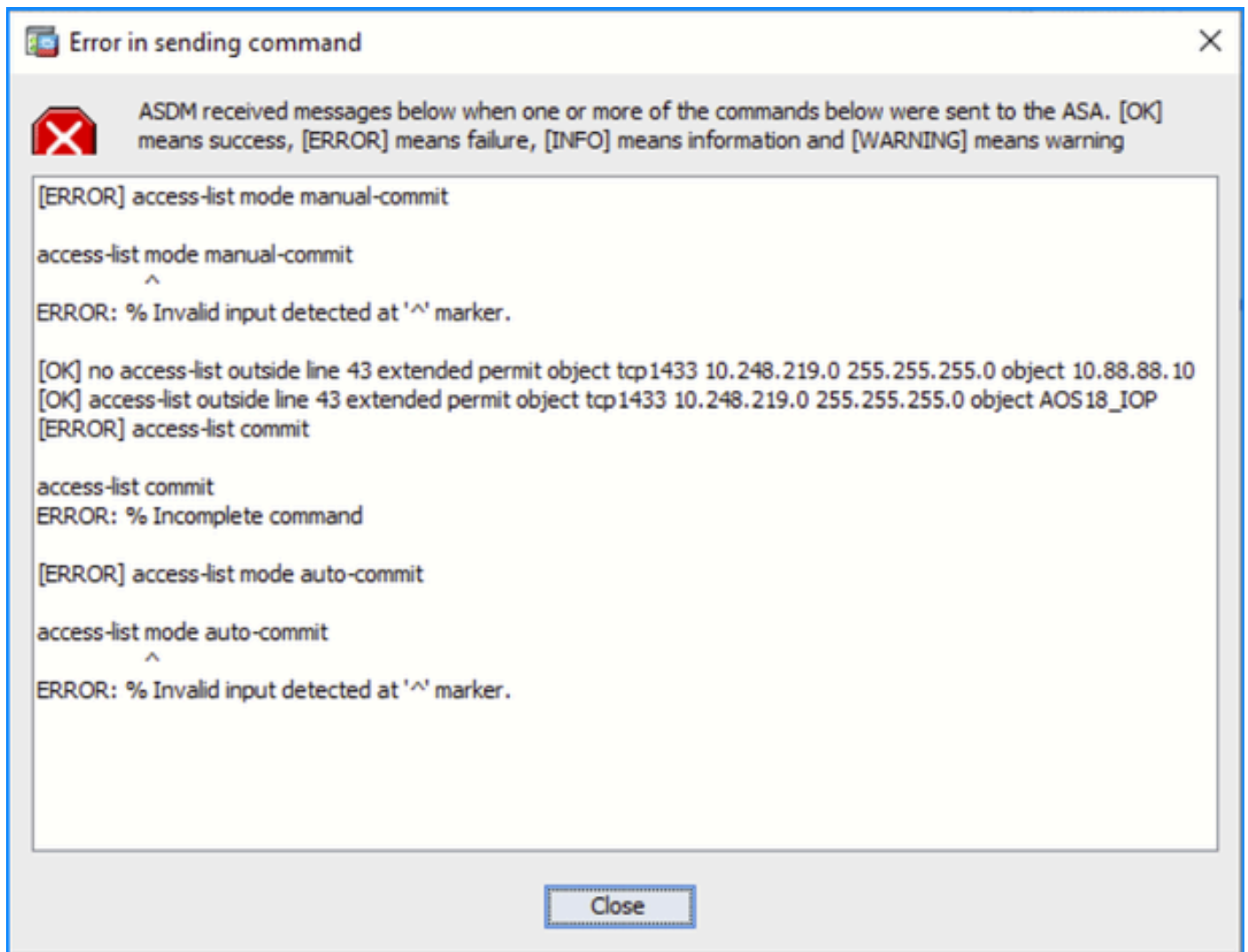
Cisco Bug ID [CSCtq38377](#) 「ENH: ASDMはASAでACLハッシュ計算を使用し、ローカルでは計算を使用しない」 およびCisco Bug ID [CSCtq38405](#) 「ENH: ASAはASDにACLハッシュ情報を提供するメカニズムが必要」を参照してください。

問題3. 「ERROR: % Invalid input detected at '^' marker.」というエラーメッセージ

が表示されます

ASDMでACLを編集すると、「ERROR: % Invalid input detected at '^' marker.」というエラーメッセージが表示されます。

```
[ERROR] access-list mode manual-commit access-list mode manual-commit
      ^
ERROR: % Invalid input detected at '^' marker.
[OK] no access-list ACL1 line 1 extended permit tcp object my-obj-1 object my-obj-2 eq 12345
[ERROR] access-list commit access-list commit
ERROR: % Incomplete command
[ERROR] access-list mode auto-commit access-list mode auto-commit
      ^
ERROR: % Invalid input detected at '^' marker.
```

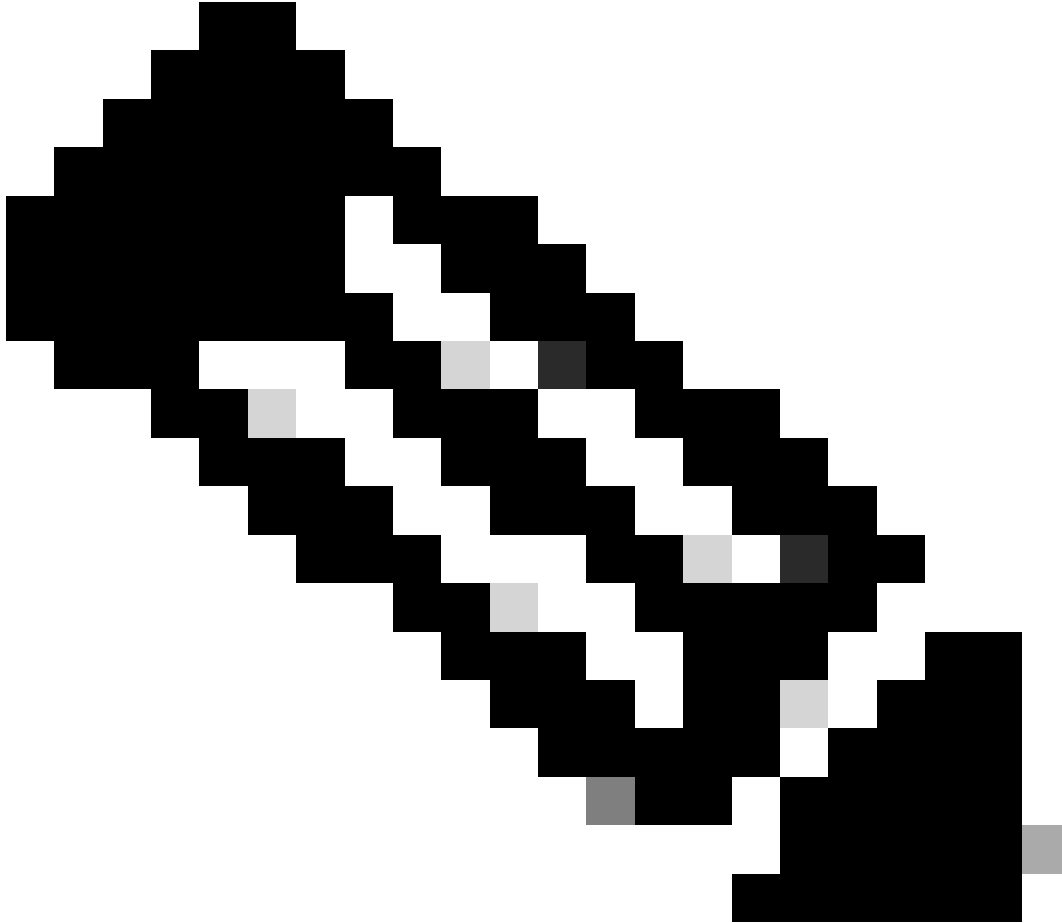


トラブルシューティング – 推奨処置

Cisco Bug ID [CSCvq05064](#) 「ASDMからのエントリ(ACL)の編集でエラーが発生する」を参照し

てください。OpenJRE/Oracleバージョン7.12.2を使用してASDMを使用する場合」およびCisco Bug ID [CSCvp88926](#)「アクセスリストの削除中に追加コマンドを送信する」を参照してください。

---



注：これらの不具合は、最近のASDMソフトウェアリリースで修正されています。詳細については、不具合の詳細を確認してください。

---

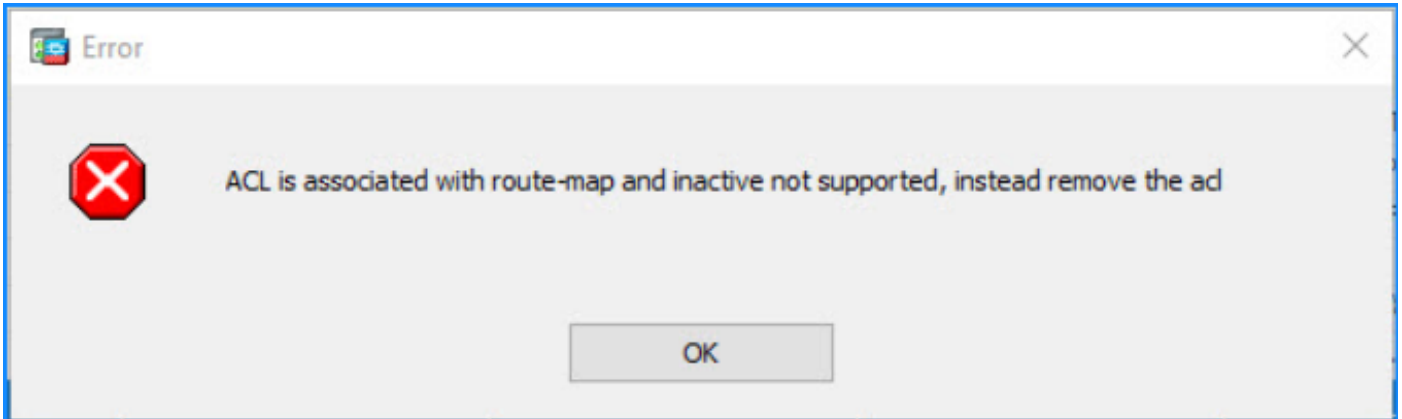
問題4：特定のケースで「ERROR: ACL is associated with route-map and inactive not supported, instead remove the acl」というエラーメッセージが表示される

「ERROR: ACL is associated with route-map and inactive not supported, instead remove the acl」というエラーメッセージが次のいずれかの場合に表示されます。

1. ポリシーベースルーティング設定で使用するASDMでACLを編集します。

```
firewall (config)# access-list pbr line 1 permit ip any host 192.0.2.1
```

エラー：ACLはルートマップに関連付けられていて、非アクティブはサポートされていません。  
代わりにaclを削除してください



2. ACL ASDMの編集>設定> リモートアクセスVPN > ネットワーク (クライアント) アクセス>  
ダイナミックアクセスポリシー

トラブルシューティング – 推奨処置

1. Cisco Bug ID [CSCwb57615](#) 「回線番号が失敗したpbrアクセスリストの設定」を参照してください。回避策は、設定から「line」パラメータを除外することです。
2. Cisco Bug ID [CSCwe34665](#) 「Unable to Edit the ACL objects if it is already in use, getting the exception」を参照してください。



注：これらの不具合は、最新のASAソフトウェアリリースで修正されています。詳細については、不具合の詳細を確認してください。

---

## 問題 5.暗黙的に拒否された接続に関するログがASDMリアルタイムログビューアに表示されない

ASDM Real-Time Log Viewerでは、暗黙的に拒否された接続のログは表示されません。

### トラブルシューティング – 推奨処置

アクセスリストの最後の暗黙的なdenyでは、syslogは生成されません。拒否されたトラフィックをすべて対象としてsyslogを生成する場合は、ACLの最後にlogキーワードを付けたルールを追加します。



## 問題 6. ネットワークオブジェクトまたはオブジェクトグループを変更しようとする とASDMがフリーズする

Configuration > Firewall > Access Rulesページ(Addressesタブ)からネットワークオブジェクトまたはオブジェクトグループを変更しようとする、ASDMがフリーズします。この問題が発生した場合、ユーザはネットワークオブジェクトウィンドウのパラメータを編集できません。

### トラブルシューティング – 推奨処置

Cisco Bug ID [CSCwj12250](#) 「ネットワークオブジェクトまたはネットワークオブジェクトグループの編集時にASDMがフリーズする」を参照してください。この問題を回避するには、topN host statistics collectionを無効にします。

```
<#root>
```

```
ASA(config)#
```

```
no hpm topN enable
```

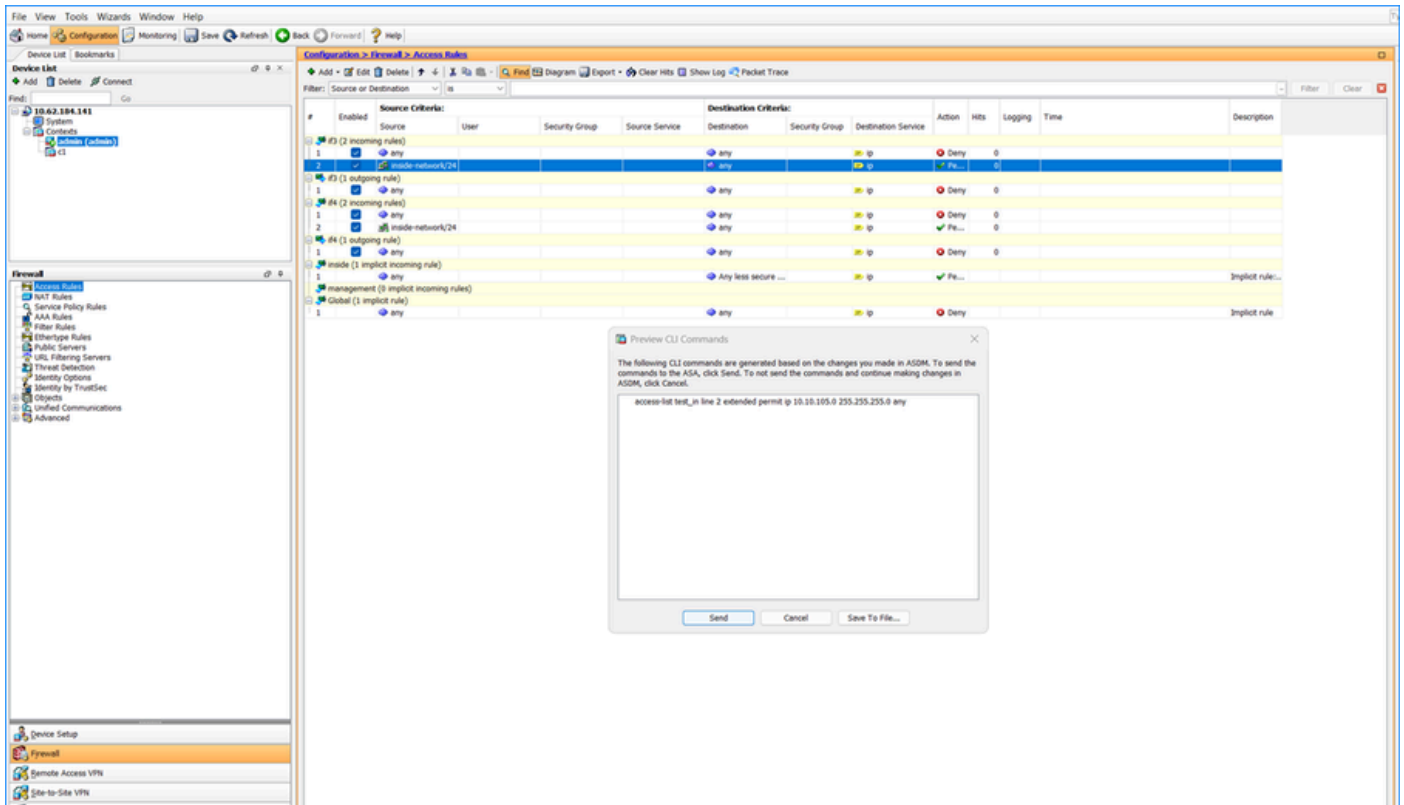


注：この不具合は、最近のASDMソフトウェアリリースで修正されています。詳細については、不具合の詳細を確認してください。

---

## 問題 7.ASDMでは、異なるインターフェイスのアクセスコントロールリスト(ACL)ルールを表示できません

ASDMでは、インターフェイスレベルのアクセスコントロールリスト(ACL)が変更された場合に、異なるインターフェイスの追加のアクセスコントロールリストのルールを表示できます。この例では、着信ルール#2がインターフェイスif3 ACLに追加されています。ASDMではインターフェイスif4の#2も表示されますが、このルールはユーザによって設定されていません。コマンドのプレビューには、保留中の変更が1つ正しく表示されます。これは、ユーザインターフェイスの表示の問題です。



## トラブルシューティング – 推奨処置

Cisco Bug ID [CSCwm71434](#) 「ASDMが重複したインターフェイスアクセスリストエントリを表示する場合があります」を参照してください。

## 問題 8.リアルタイムログはリアルタイムログビューアでは使用できません

リアルタイムログビューアにログが表示されない

## トラブルシューティング – 推奨処置

1. ロギングが設定されていることを確認します。『[ASDM Book 1: Cisco ASA Series General Operations ASDM Configuration Guide, 7.22](#)』の「[Chapter: Logging](#)」を参照してください。
2. Cisco Bug ID [CSCvf82966](#) 「ASDM – ロギング : リアルタイムログを表示できない」を参照してください。



注：この不具合は、最近のASDMソフトウェアリリースで修正されています。詳細については、不具合の詳細を確認してください。

## 参考資料

- [ASDMブック1: Cisco ASAシリーズの一般的な操作ASDM設定ガイド7.22、章：ログイン。](#)

## 問題 9. リアルタイムログビューアの日付と時刻の列が空です

Severity	Date	Time	Syslog ID	Source IP	Source Port	Destination IP	Destination Port	Description
6			611101					User authentication succeeded: IP address: 10.229.20.35, Username: admin
6			113008					AAA transaction status ACCEPT : user = admin
6			113004					AAA user authorization Successful : server = LOCAL : user = admin
6			113012					AAA user authentication Successful : local database : user = admin
6			302013					Built inbound TCP connection 3505 for management:10.229.20.35/55403 (10.229.20.35/55403) to rtp_int_tap:169.254.1.3/4122 (10.62.184.141/22) -1-1

## トラブルシューティング – 推奨処置

1. RFC5424ロギングタイムスタンプ形式が使用されているかどうかを確認します。

```
<#root>
```

```
#
```

```
show run logging
```

```
logging enable
```

```
logging timestamp rfc5424
```

2. RFC5424ロギングタイムスタンプ形式を使用する場合は、ソフトウェアのCisco Bug ID [CSCvs52212](#) 「ASDM ENH: capability for Event Log Viewer to display ASA syslog with rfc5424 timestamp format」を参照してください。回避策は、RFC5424形式の使用を避けることです。

```
<#root>
```

```
firewall(config)#
```

```
no logging timestamp rfc5424
```

```
firewall(config)#
```

```
logging timestamp
```

3. また、ソフトウェア不具合、Cisco Bug ID [CSCwh70323](#) 「Timestamp entry missing for some syslog messages sent to syslog server」も参照してください。

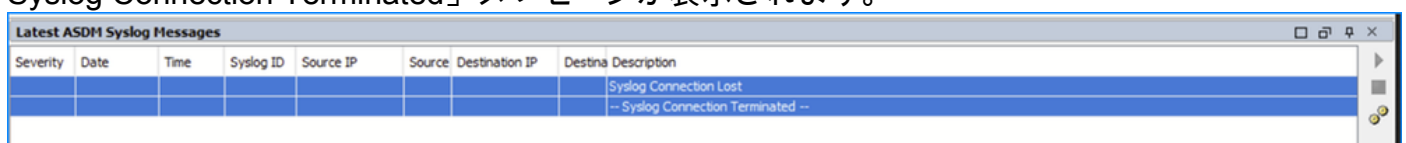
---

注：この不具合は、最近のASDMソフトウェアリリースで修正されています。詳細については、不具合の詳細を確認してください。

---

## 問題 10. マルチコンテキストASAで別のコンテキストに切り替えた後にASDMへのロギングが失敗する可能性がある

ホームページの最新のASDM syslogメッセージタブには、「Syslog Connection Lost」および「Syslog Connection Terminated」メッセージが表示されます。

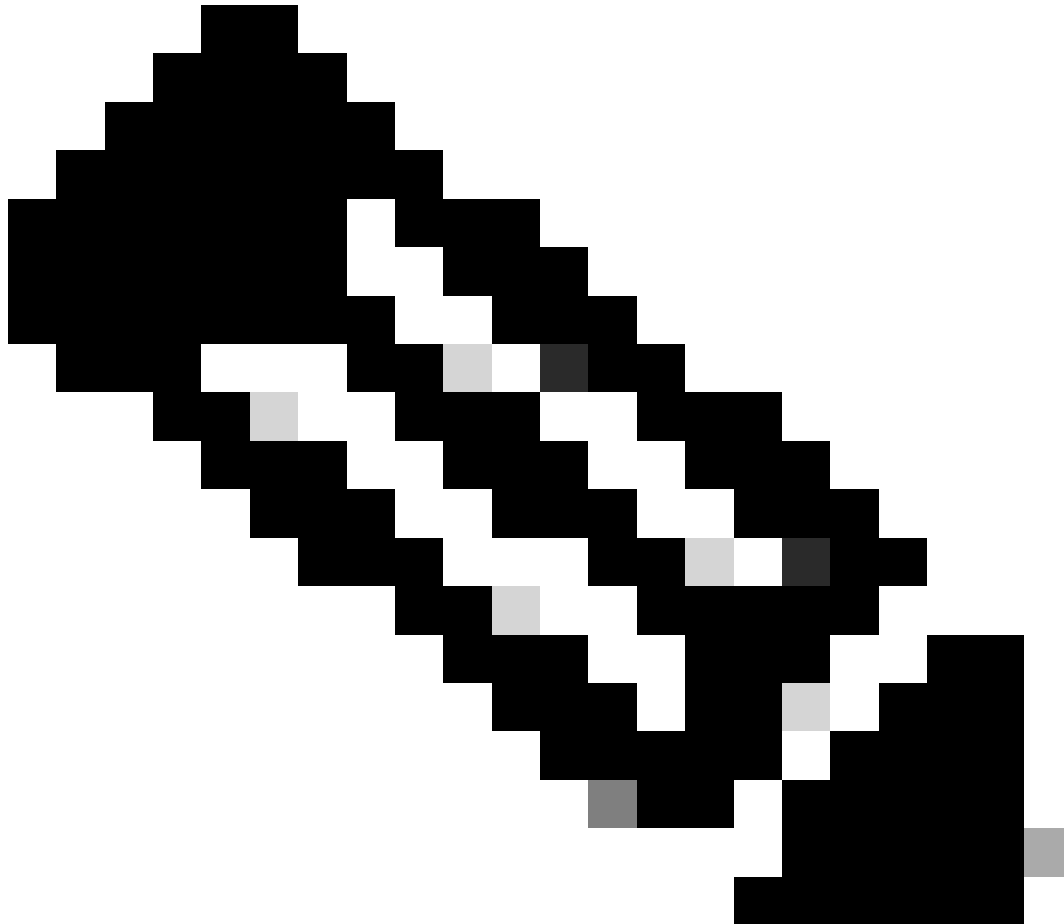


Severity	Date	Time	Syslog ID	Source IP	Source	Destination IP	Destina	Description
								Syslog Connection Lost
								-- Syslog Connection Terminated --

トラブルシューティング – 推奨処置

ロギングが設定されていることを確認します。Cisco Bug ID [CSCvz15404](#)「ASA : マルチコンテキストモード : ASDMロギングが停止し、別のコンテキストに切り替えられた場合」を参照してください。

---



注 : この不具合は、最近のASDMソフトウェアリリースで修正されています。詳細については、不具合の詳細を確認してください。

---

## 問題11:異なるコンテキスト間の切り替え時にASDMセッションが突然終了する

異なるコンテキスト間で切り替えを行うと、ASDMセッションが突然終了し、「The maximum number of management sessions for protocol http or user already exists.Please try again later」というメッセージが表示されます。syslogメッセージには次のログが表示されます。

```
%ASA-3-768004: QUOTA: management session quota exceeded for http protocol: current 5, protocol limit 5
```

%ASA-3-768004: QUOTA: management session quota exceeded for http protocol: current 5, protocol limit 5

## トラブルシューティング – 推奨処置

1. Current ASDMリソースの使用量が制限に達しているかどうかを確認します。この場合、Deniedカウンタが増加します。

```
<#root>
```

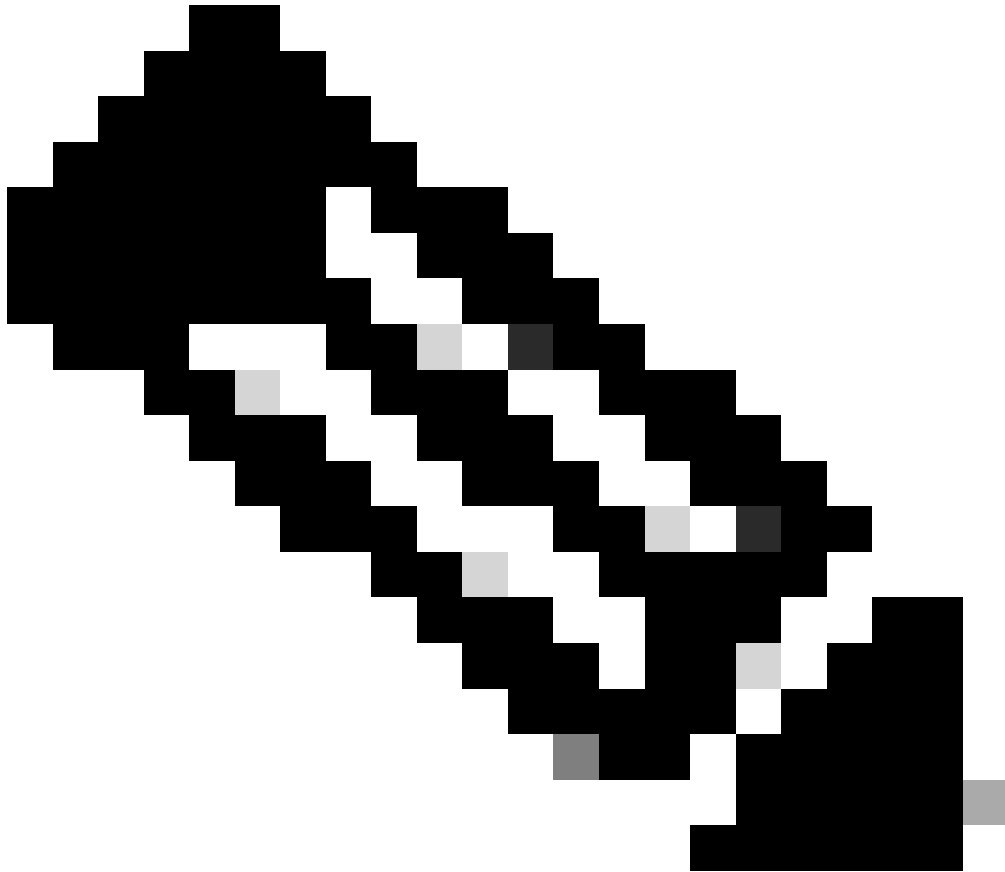
```
firewall #
```

```
show resource usage resource ASDM
```

Resource	Current	Peak	Limit	Denied Context
ASDM				
5				
	5			
5				
10				
admin				

2. Cisco Bug ID [CSCvs72378](#) 「異なるコンテキスト間での切り替え時に突然終了するASDMセッション」を参照してください。





注：この不具合は、最近のASAソフトウェアリリースで修正されています。詳細については、不具合の詳細を確認してください。

3. ソフトウェアバージョンでCisco Bug ID [CSCvs72378](#)の修正が取られており、現在のリソースが制限に達した場合は、既存のASDMセッションの一部を切断します。ASDMを閉じるか、またはASDMを実行しているホストのIPアドレスのHTTPS接続をクリアできます。この例では、ASDM上のHTTPサーバがデフォルトのHTTPSポート443で稼働していることを前提としています。

```
<#root>
```

```
#
```

```
show conn all protocol tcp port 443
```

```
TCP management 192.0.2.35:55281 NP Identity Ifc 192.0.2.1:443, idle 0:00:01, bytes 33634, flags UOB
```

```
TCP management 192.0.2.36:38844 NP Identity Ifc 192.0.2.1:443, idle 0:00:08, bytes 1629669, flags UOB
```

```
#
```

```
clear conn all protocol tcp port 443 address 192.0.2.35
```

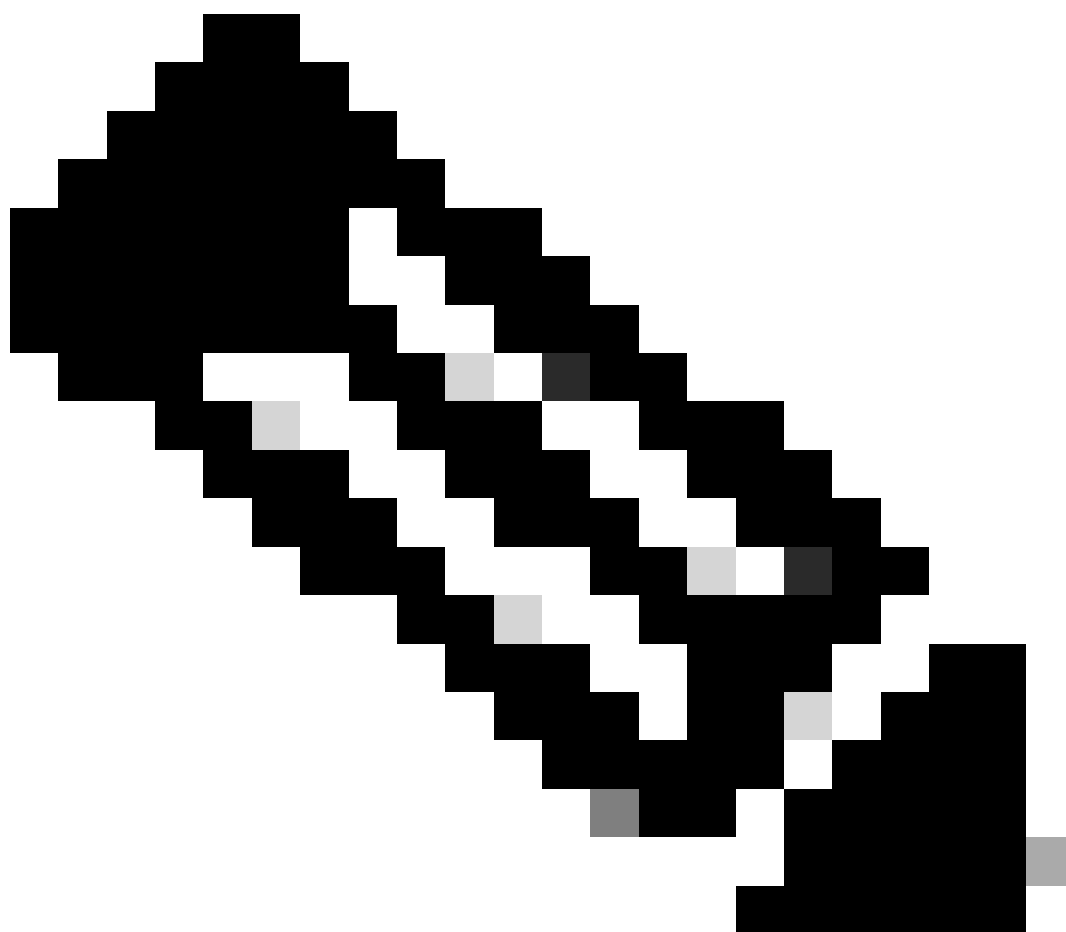
問題 12.ASDMがランダムに終了/終了し、「ASDM received a message from the ASA device to disconnect.ASDMを終了します。」

マルチコンテキストASAでは、ASDMがランダムに終了/終了し、「ASDM received a message from the ASA device to disconnect.ASDMを終了します。」

トラブルシューティング – 推奨処置

Cisco Bug ID [CSCwh04395](#)「ASDMアプリケーションが、マルチコンテキストセットアップでアラートメッセージを使用してランダムに終了する」のソフトウェア不具合を参照してください。

---

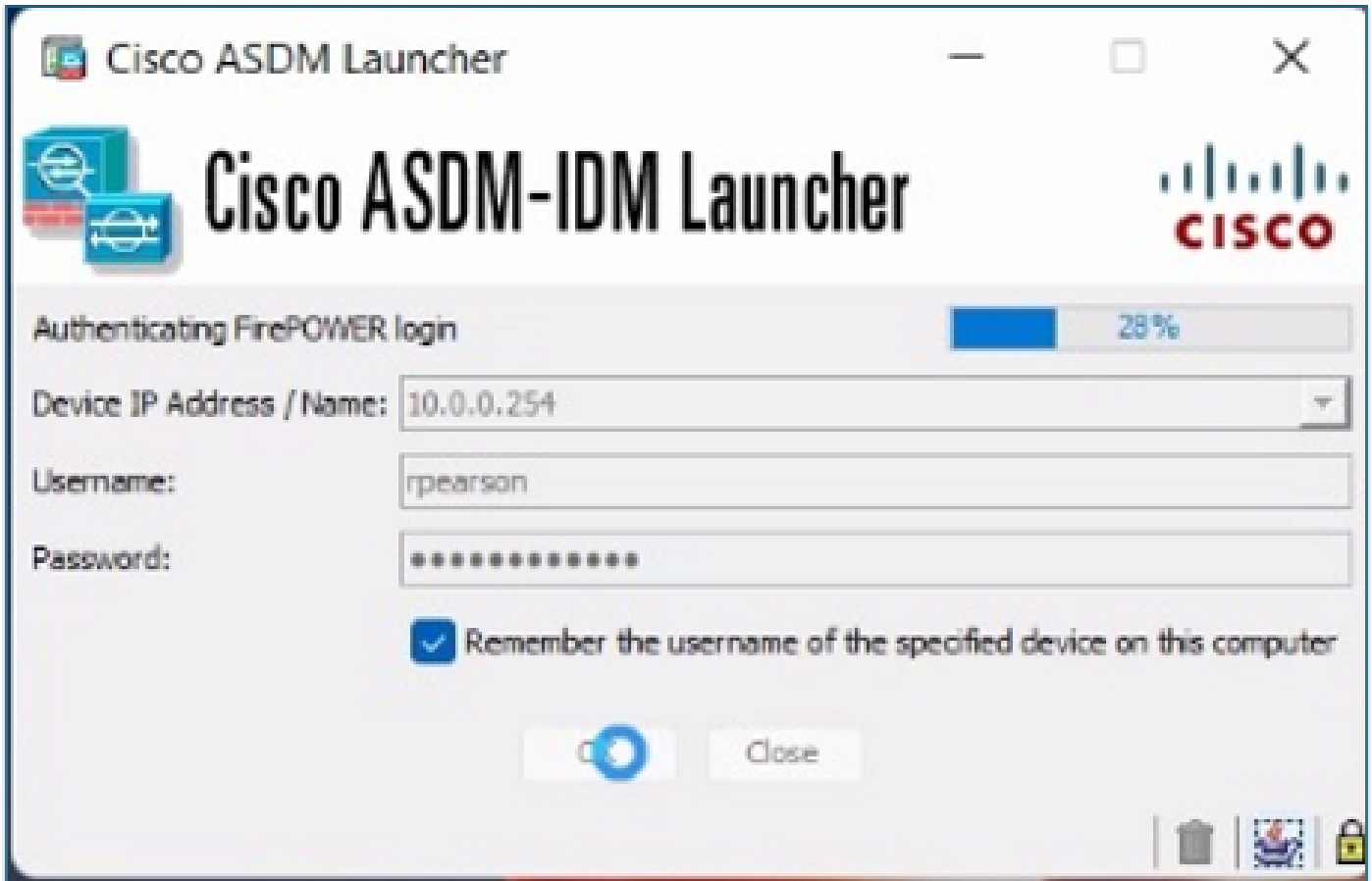


注：この不具合は、最近のASAソフトウェアリリースで修正されています。詳細については、不具合の詳細を確認してください。

---

## 問題 13.ASDMロードが「Authentication FirePOWER login」メッセージでハングする

ASDMロードが「Authentication FirePOWER login」メッセージでハングします。



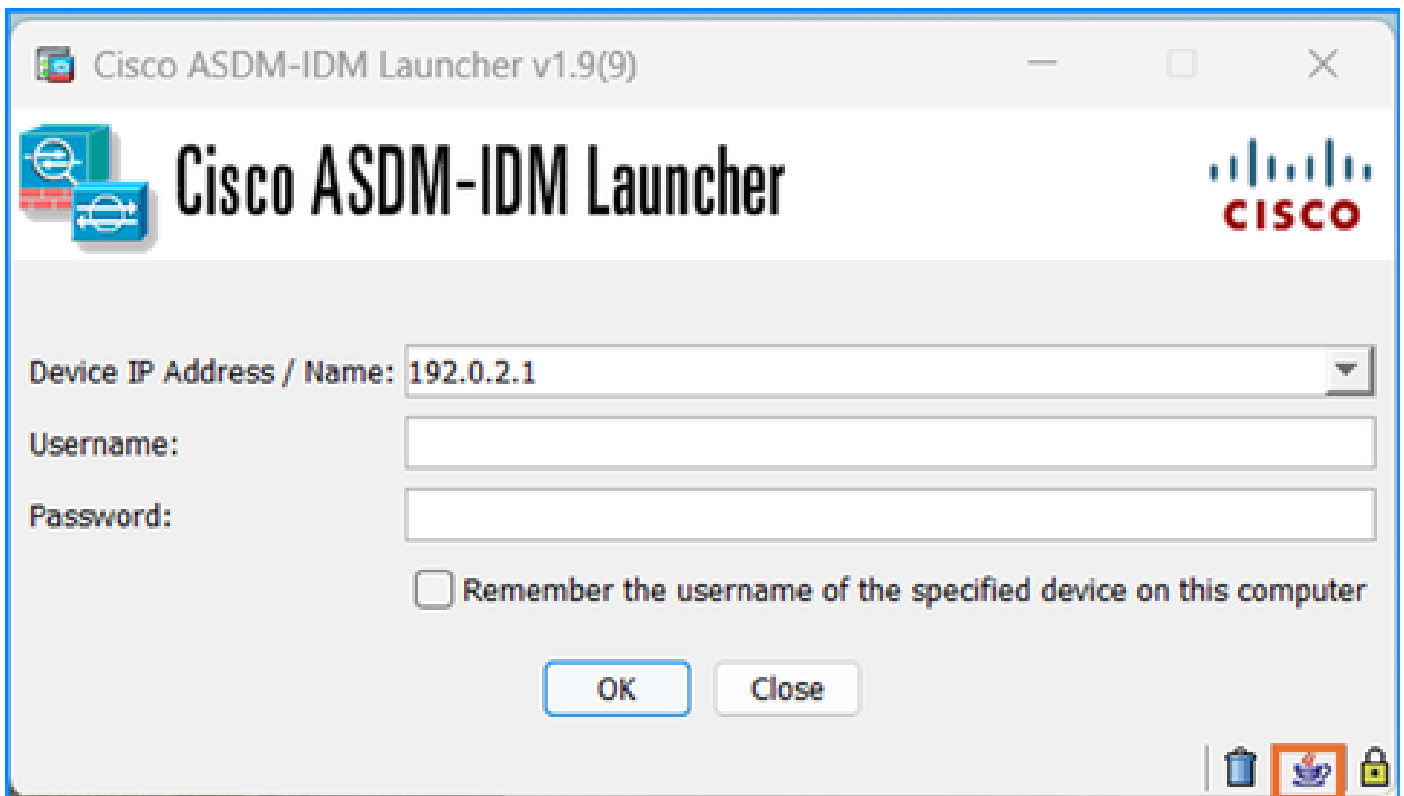
Javaコンソールログに「Failed to connect to FirePower, continue without it」というメッセージが表示されます。

<#root>

```
2023-05-08 16:55:10,564 [ERROR] CLI-PASSTHROUGH-DEBUG Inside doInitialProcessing:
0 [SGZ Loader: launchSgzApplet] ERROR com.cisco.pdm.headless.startup - CLI-PASSTHROUGH-DEBUG Inside doInitialProcessing:
CLI-PASSTHROUGH-DEBUG Inside doInitialProcessing:
2023-05-08 16:55:10,657 [ERROR] CLI-PASSTHROUGH-DEBUG Inside doInitialProcessing messenger: cp1@18c4cb7
93 [SGZ Loader: launchSgzApplet] ERROR com.cisco.pdm.headless.startup - CLI-PASSTHROUGH-DEBUG Inside doInitialProcessing messenger: cp1@18c4cb75
com.jidesoft.plaf.LookAndFeelFactory not loaded.
2023-05-08 17:15:31,419 [ERROR] Unable to login to DC-Lite. STATUS CODE IS 502
1220855 [SGZ Loader: launchSgzApplet] ERROR com.cisco.dmcommon.util.DMCommonEnv - Unable to login to
May 08, 2023 10:15:31 PM vd cx

INFO: Failed to connect to FirePower, continuing without it.
May 08, 2023 10:15:31 PM vd cx
INFO: If the FirePower is NATed, clear the cache (C:/Users/user1/.asdm/data/firepower.conf) and try again.
Env.isAsdmInHeadlessMode()----->false
java.lang.InterruptedExpection
    at java.lang.Object.wait(Native Method)
```

この症状を確認するには、Javaコンソールログを有効にします。

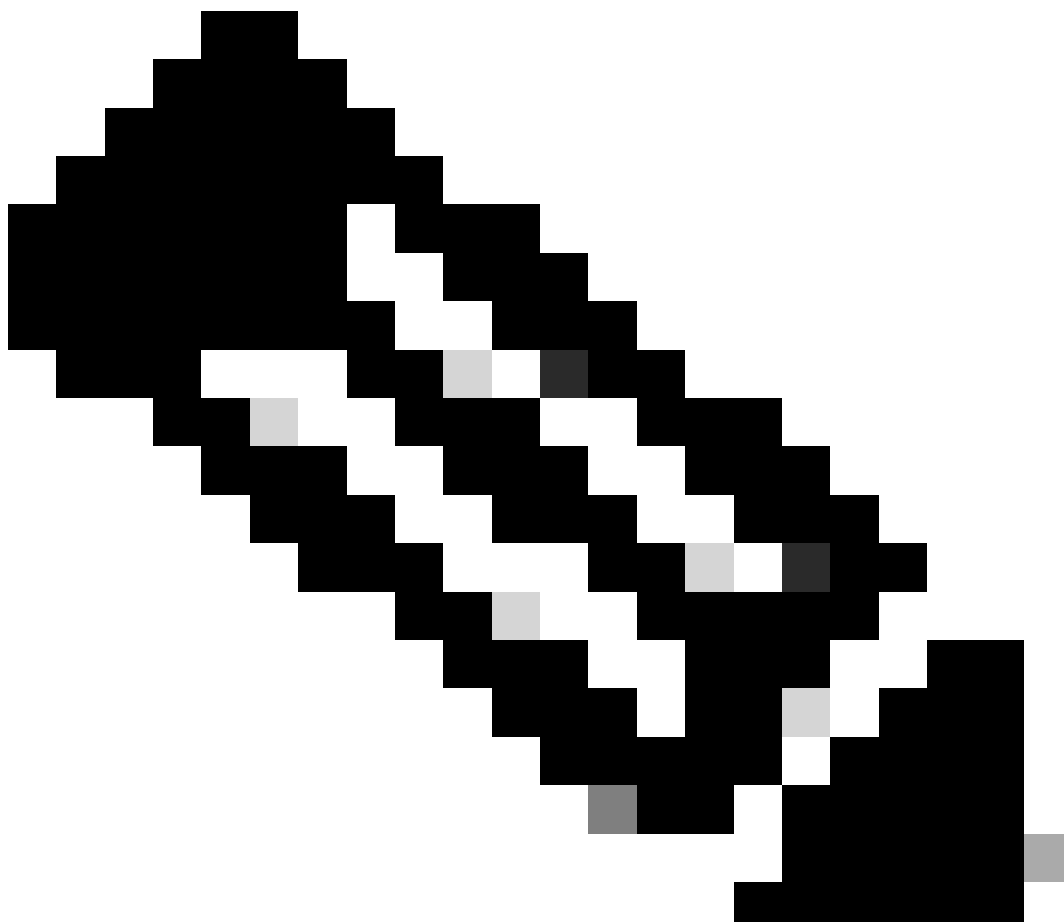


#### トラブルシューティング – 推奨処置

ソフトウェアのCisco Bug ID [CSCwe15164](#)「ASA: ASDMは、CLIを使用して「起動」されるまでSFRタブを表示できません」を参照してください。回避策の手順：

1. ASDMマネージャを閉じます。
2. SFRへのSSHアクセスを取得し、ユーザをルートに切り替えます(sudo su)。
3. 上記の手順を実行した後、ASDMを再起動すると、Firepower(SFR)タブをロードできるようになります。

---



注：この不具合は、最近のFirepowerソフトウェアリリースで修正されています。詳細については、不具合の詳細を確認してください。

---

## 問題 14.ASDMにFirepowerモジュールの管理/設定が表示されない

Firepowerモジュールの設定はASDMでは使用できません。

トラブルシューティング – 推奨処置

1. ASA、ASDM、Firepowerモジュール、およびオペレーティングシステムのバージョンに互換性があることを確認します。 詳細については、『[Cisco Secure Firewall ASAリリースノート](#)』、『[Cisco Secure Firewall ASDMリリースノート](#)』、『[Cisco Secure Firewall ASAの互換性](#)』:

  - ASA 9.14/ASDM 7.14/Firepower 6.6は、ASA 5525-X、5545-X、および5555-XでのASA

FirePOWERモジュールの最終バージョンです。

- ASA 9.12/ASDM 7.12/Firepower 6.4.0は、ASA 5515-Xおよび5585-X上のASA FirePOWERモジュールの最終バージョンです。
- ASA 9.9/ASDM 7.9(2)/Firepower 6.2.3は、ASA 5506-Xシリーズおよび5512-X上のASA FirePOWERモジュールの最終バージョンです。
- ASDMのバージョンには、特に記載がない限り、以前のすべてのASAバージョンとの下位互換性があります。たとえば、ASDM 7.13(1)では、ASA 9.10(1)上のASA 5516-Xを管理できます。
- ASDMは、ASA 9.8(4.45)+、9.12(4.50)+、9.14(4.14)+、および9.16(3.19)+を使用したFirePOWERモジュール管理ではサポートされていません。これらのリリースでは、モジュールを管理するためにFMCを使用する必要があります。これらのASAリリースにはASDM 7.18(1.152)以降が必要ですが、ASA FirePOWERモジュールに対するASDMのサポートは7.16で終了しています。
- ASDM 7.13(1)およびASDM 7.14(1)では、ASA 5512-X、5515-X、5585-XおよびASASMをサポートしていませんでした。ASDMサポートを復元するには、ASDM 7.13(1.101)または7.14(1.48)にアップグレードする必要があります。

2. バージョンに互換性がある場合は、モジュールが稼働しているかどうかを確認します。

```
<#root>
```

```
firewall#
```

```
show module sfr details
```

```
Getting details from the Service Module, please wait...
```

```
Card Type:          FirePOWER Services Software Module
Model:              ASA5508
Hardware version:   N/A
Serial Number:      AAAABBBB1111
Firmware version:   N/A
Software version:   7.0.6-236
MAC Address Range:  006b.f18e.dac6 to 006b.f18e.dac6
App. name:          ASA FirePOWER
```

```
App. Status:        Up
```

```
App. Status Desc:   Normal Operation
App. version:        7.0.6-236
```

```
Data Plane Status:  Up
```

```
Console session:    Ready
```

```
Status:             Up
```

```
DC addr:            No DC Configured
Mgmt IP addr:        192.0.2.1
Mgmt Network mask:   255.255.255.0
```

Mgmt Gateway: 192.0.2.254  
Mgmt web ports: 443  
Mgmt TLS enabled: true

モジュールがダウンしている場合は、sw-module module resetコマンドを使用して、モジュールをリセットしてから、モジュールソフトウェアをリロードできます。

#### 参考資料

- [Cisco Secure Firewall ASAリリースノート](#)
- [Cisco Secure Firewall ASDMリリースノート](#)
- [Cisco Secure Firewall ASAの互換性](#)

#### 問題 15.ASDMでセキュアクライアントプロファイルにアクセスできない

Javaコンソールログに「java.lang.ArrayIndexOutOfBoundsException: 3」エラーメッセージが表示されます。

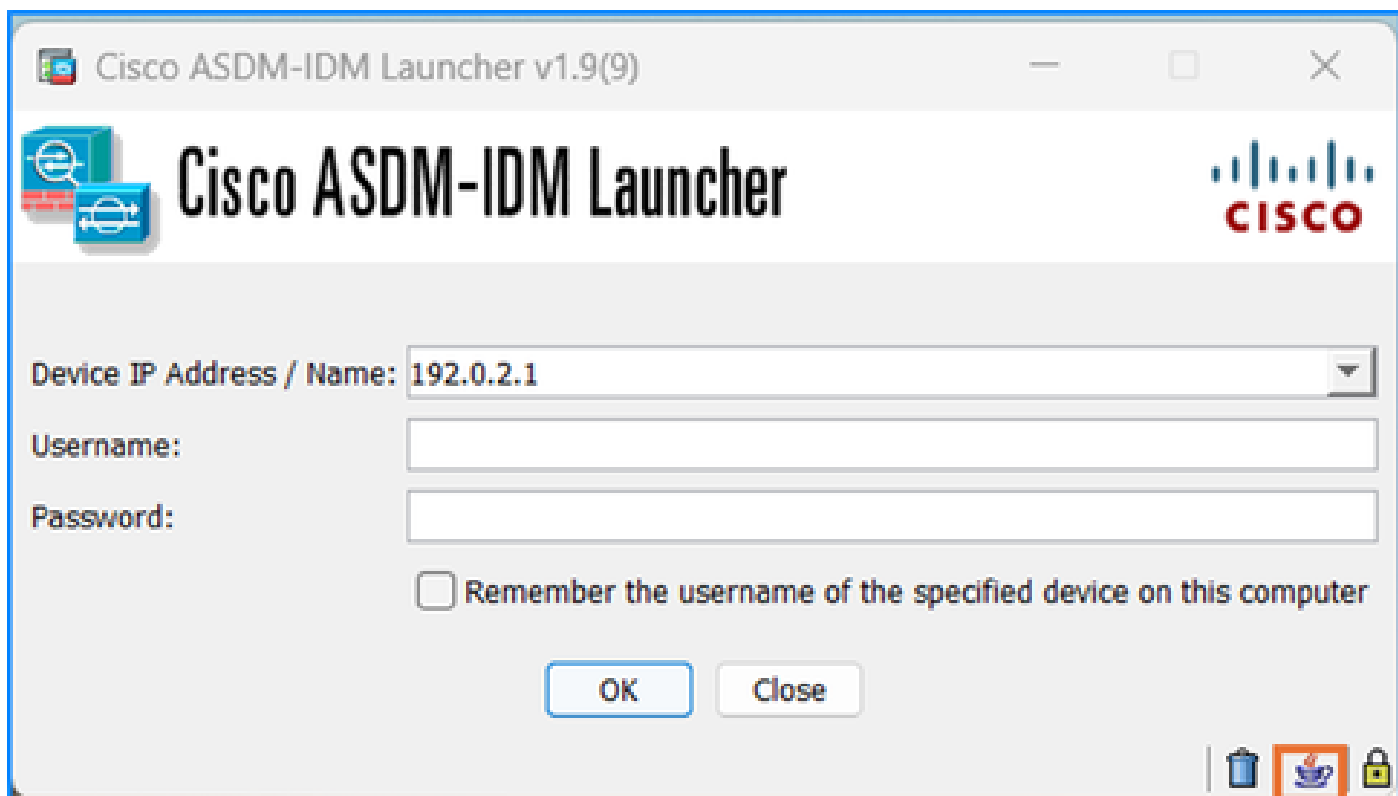
```
<#root>
```

```
LifeTime value : -1 HTTP Enable Status : nps-servers-ige
```

```
java.lang.ArrayIndexOutOfBoundsException: 3
```

```
at doz.a(doz.java:1256)  
at doz.a(doz.java:935)  
at doz.l(doz.java:1100)
```

この症状を確認するには、Javaコンソールログを有効にします。



トラブルシューティング – 推奨処置

Cisco Bug ID [CSCwi56155](#) 「Unable to access Secure Client Profile on ASDM」を参照してください。





注：この不具合は、最近のASDMソフトウェアリリースで修正されています。詳細については、不具合の詳細を確認してください。

---

## 問題16:ASDMでセキュアクライアントプロファイルXMLプロファイルを編集できない

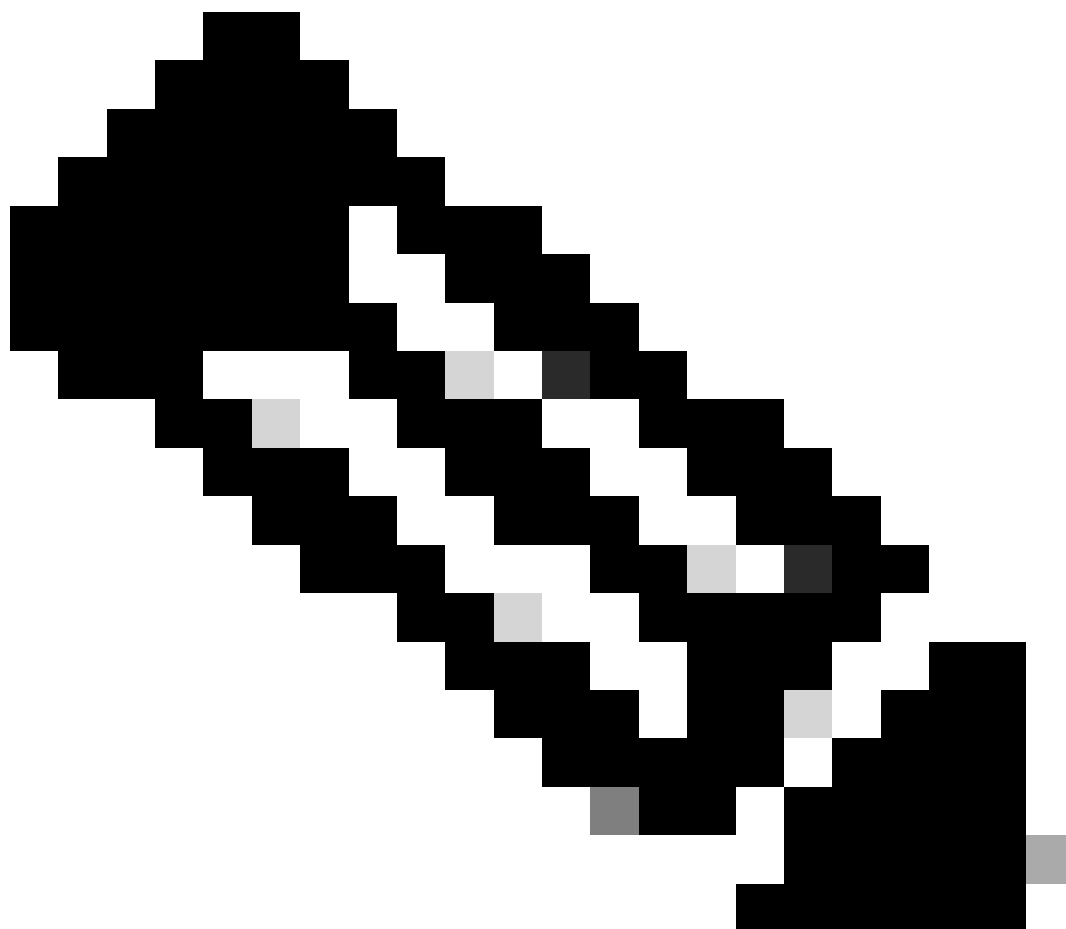
バージョン4.8より前のディスクにAnyConnectイメージが存在する場合、ASDMのConfiguration > Remote Access VPN > Network (Client) AccessのセキュアクライアントプロファイルXMLプロファイルはASAデバイスでは編集できません。

エラーメッセージ「There is no profile editor plugin in your Secure Client Image on the device.Please go to Network (Client) Access > Secure Client Software and install the Secure Client Image version 2.5 or later and then try again」が表示されます。

トラブルシューティング – 推奨処置

Cisco Bug ID [CSCwk64399](#) 「ASDM- Unable to edit Secure Client Profile」を参照してください。  
この問題を回避するには、プライオリティの低い別のAnyConnectイメージを設定します。

---



注：この不具合は、最近のASDMソフトウェアリリースで修正されています。詳細については、不具合の詳細を確認してください。

---

## 問題17. 設定を変更した後にセキュアクライアントのイメージが消失する

ASDM Configuration > Network (Client) Access > Secure Client Profileに変更を加えた後で、Configuration > Network (Client) Access > Secure Client Softwareの順に選択しても、イメージが見つからない。

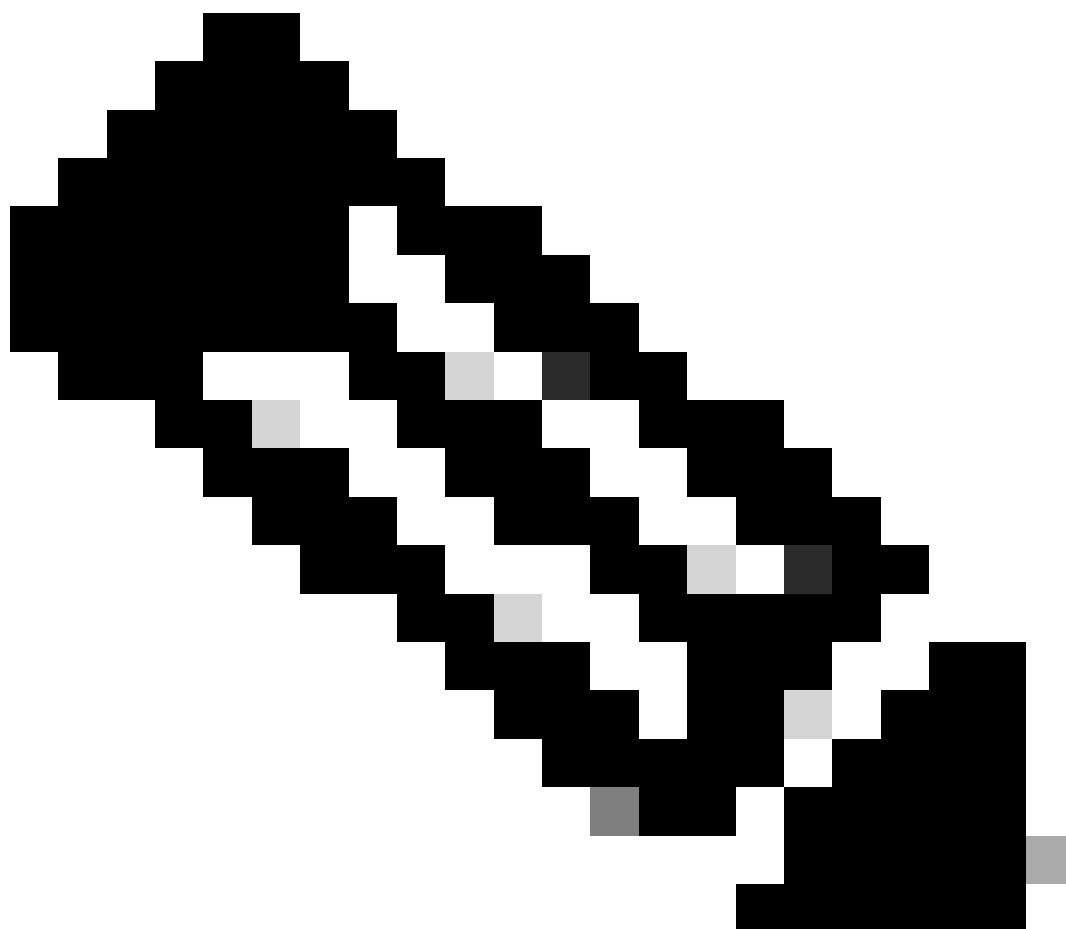
トラブルシューティング – 推奨処置

Cisco Bug ID [CSCwf23826](#) 「ASDMでSecure Client Profile Editorを変更した後、Secure Clientソフトウェアが表示されない」を参照してください。回避策のオプション：

- ASDMでRefreshアイコンをクリックします

または

- ASDMを閉じて再度開く
- 



注：この不具合は、最近のASDMソフトウェアリリースで修正されています。詳細については、不具合の詳細を確認してください。

---

問題18：無効なhttp server session-timeoutコマンドとhttp server idle-timeoutコマンド

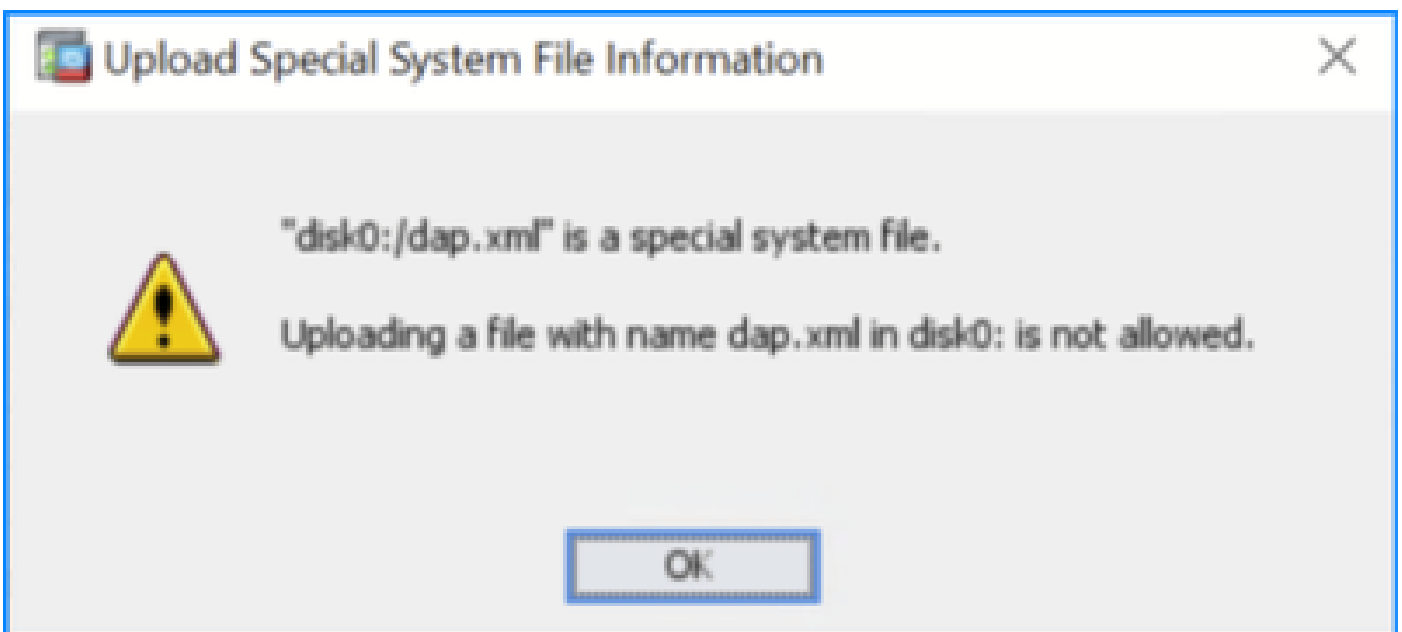
http server session-timeoutコマンドとhttp server idle-timeoutコマンドは、マルチコンテキストモードASAでは無効です。

トラブルシューティング – 推奨処置

Cisco Bug ID [CSCtx41707](#) 「マルチコンテキストモードでのhttp server timeoutコマンドのサポート」を参照してください。コマンドは設定可能ですが、値は影響しません。

#### 問題19: ASDMでのDap.xmlコピーの失敗

ASDMのFile Managementウィンドウを使用したASAへのdap.xmlのコピーが、エラー「disk0:/dap.xml is a special system file.disk0 : にdap.xmlという名前のファイルをアップロードすることは許可されていません。」



トラブルシューティング – 推奨処置

Cisco Bug ID [CSCvt62162](#) 「Cannot copy dap.xml using File Management in ASDM 7.13.1」を参照してください。回避策は、FTPやTFTPなどのプロトコルを使用して、ファイルを直接ASAにコピーすることです。



注：この不具合は、最近のASDMソフトウェアリリースで修正されています。詳細については、不具合の詳細を確認してください。

---

## 問題 20.ASDMにIKEポリシーとIPSECプロポーザルが表示されない

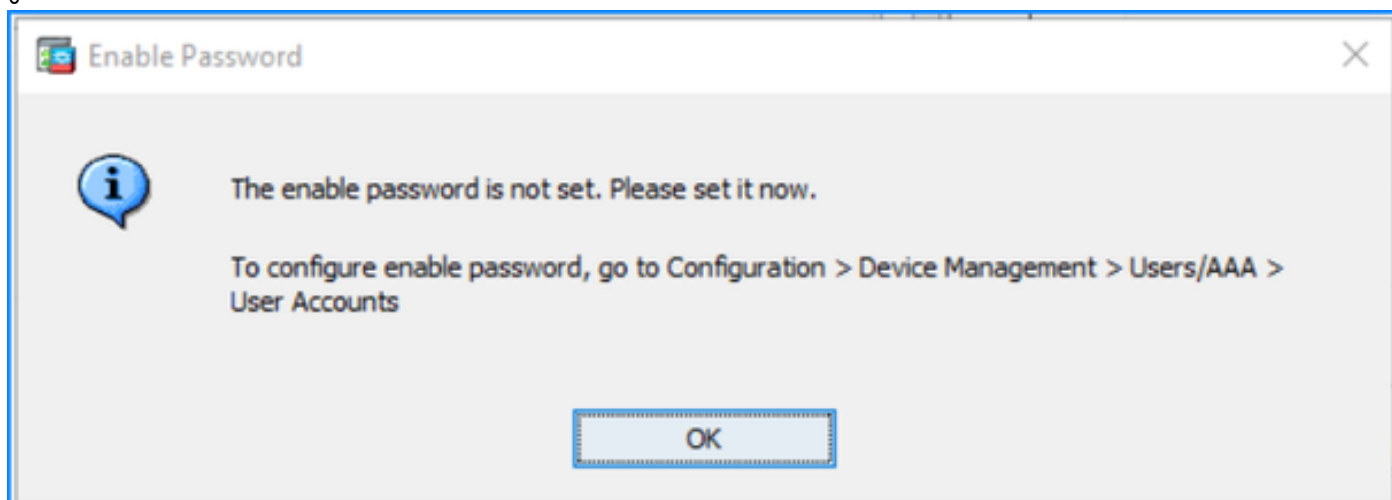
ASDMのConfigurations > Site-to-Site VPN ウィンドウにはIKEポリシーとIPSECプロポーザルが表示されません。

トラブルシューティング – 推奨処置

Cisco Bug ID [CSCwm42701](#) 「IKEポリシーとIPSECプロポーザルのタブでASDM display blankが表示される」を参照してください。

問題 21.ASDMでメッセージ「The enable password is not set.今すぐ設定してください。」

ASDMで「The enable password is not set.Please set it now.」というメッセージが表示されます。



トラブルシューティング – 推奨処置

ソフトウェアのCisco Bug ID [CSCvq42317](#) 「ASDM prompts to change enable password after it was set on CLI」を参照してください。

問題22: ASDM UIを更新した後にASDNオブジェクトが表示されない

既存のオブジェクトグループにオブジェクトグループとオブジェクトホストを追加し、ASDMをリフレッシュした後、そのオブジェクトグループがASDMリストから消えてしまう。この不具合を一致させるには、オブジェクト名を数字で始める必要があります。

トラブルシューティング – 推奨処置

Cisco Bug ID [CSCwf71723](#) 「ASDMで設定済みオブジェクト/オブジェクトグループが失われる」を参照してください。

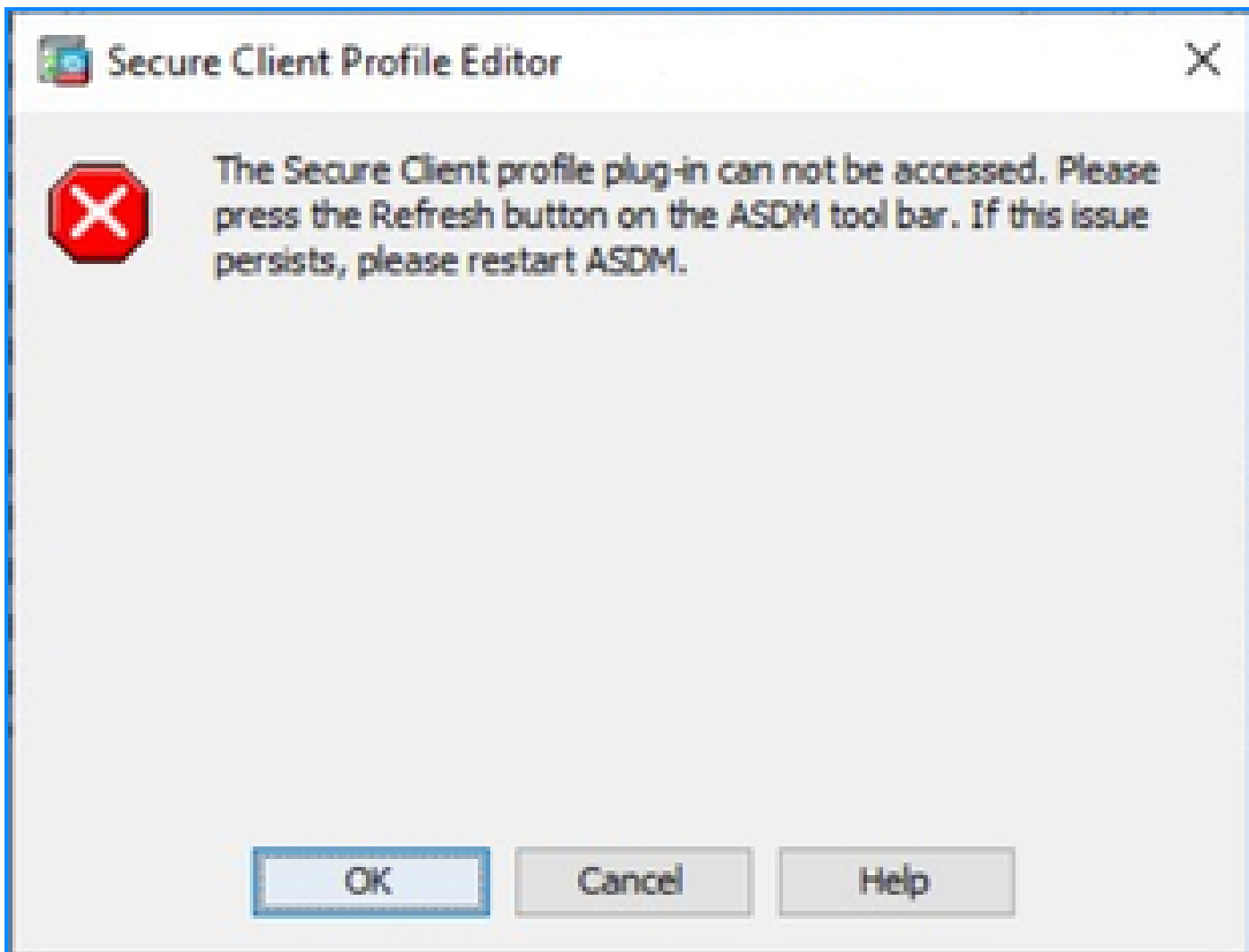


注：この不具合は、最近のASDMソフトウェアリリースで修正されています。詳細については、不具合の詳細を確認してください。

---

### 問題 23.4.5より前のバージョンのAnyConnectクライアントプロファイルを編集できない

バージョン4.5より前のAnyConnectプロファイルでは、AnyConnectクライアントプロファイルを編集できません。エラーメッセージは、「The Secure Client profile plug-in can not be accessed.ASDMツールバーのRefreshボタンを押してください。この問題が解決しない場合は、ASDMを再起動してください。



トラブルシューティング – 推奨処置

Cisco Bug ID [CSCwf16947](#) 「ASDM - Anyconnect Profile Editorをロードできない」を参照してください。



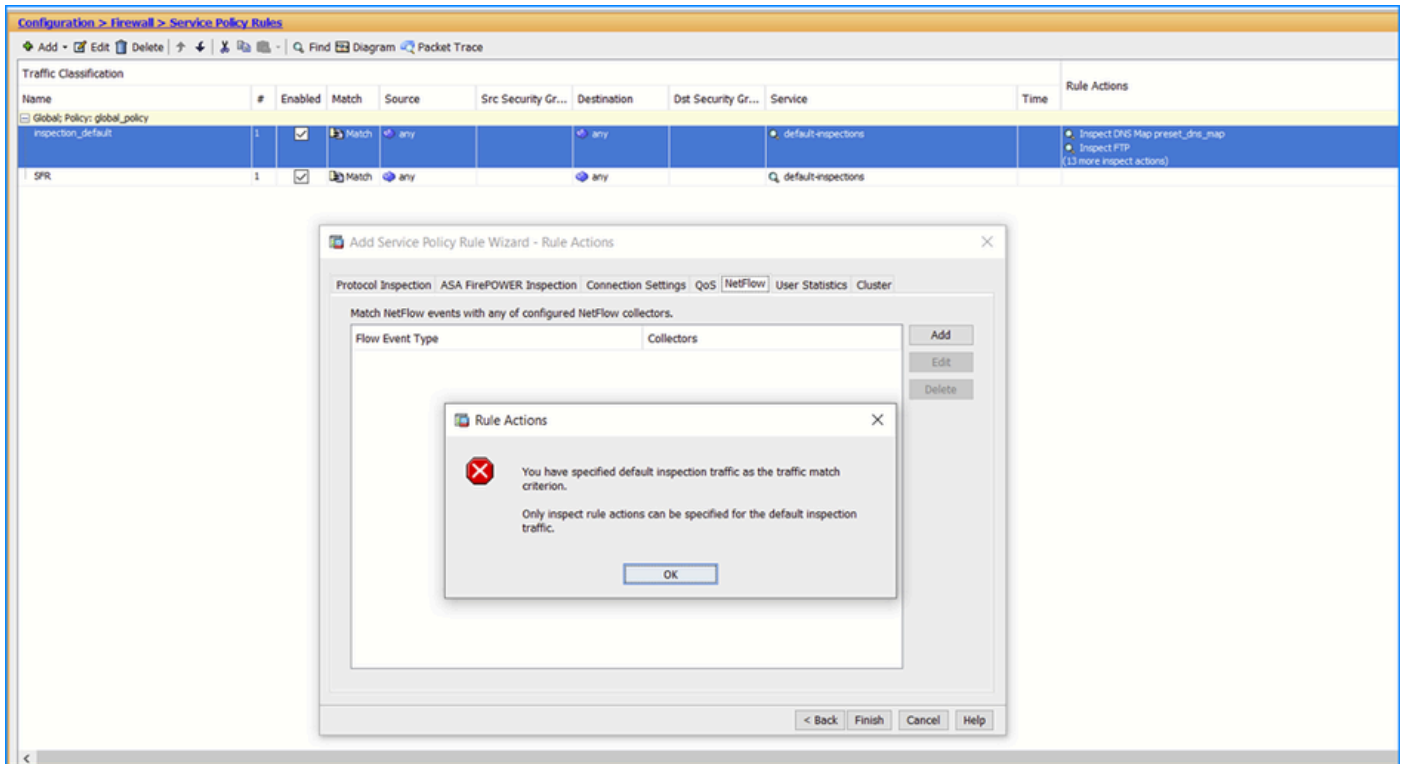


注：この不具合は、最近のASDMソフトウェアリリースで修正されています。詳細については、不具合の詳細を確認してください。

---

## 問題 24.Edit Service Policy > Rule Actions > ASA FirePOWER Inspectionタブに移動できない

ASDMバージョン7.8.2では、ユーザがEdit Service Policy > Rule Actions > ASA FirePOWER Inspectionタブに移動できず、エラー「You have specified default inspection traffic as the traffic match criterion.デフォルトのインスペクショントラフィックに指定できるのは、インスペクションルールアクションだけです。これは、ACLがリダイレクト用に選択されている場合でも発生します。



## トラブルシューティング – 推奨処置

Cisco Bug ID [CSCvg15782](#) 「ASDM – バージョン7.8(2)へのアップグレード後にSFRトラフィックリダイレクションの変更を表示できない」を参照してください。回避策は、CLIを使用してポリシーマップ設定を編集することです。



注：この不具合は、最近のASDMソフトウェアリリースで修正されています。詳細については、不具合の詳細を確認してください。

---

## 問題 25.ASDM上のAnyConnectイメージバージョン5.1およびAnyConnectプロファイルエディタ

Secure Clientソフトウェアバージョン5.1では、次の症状が見られます。

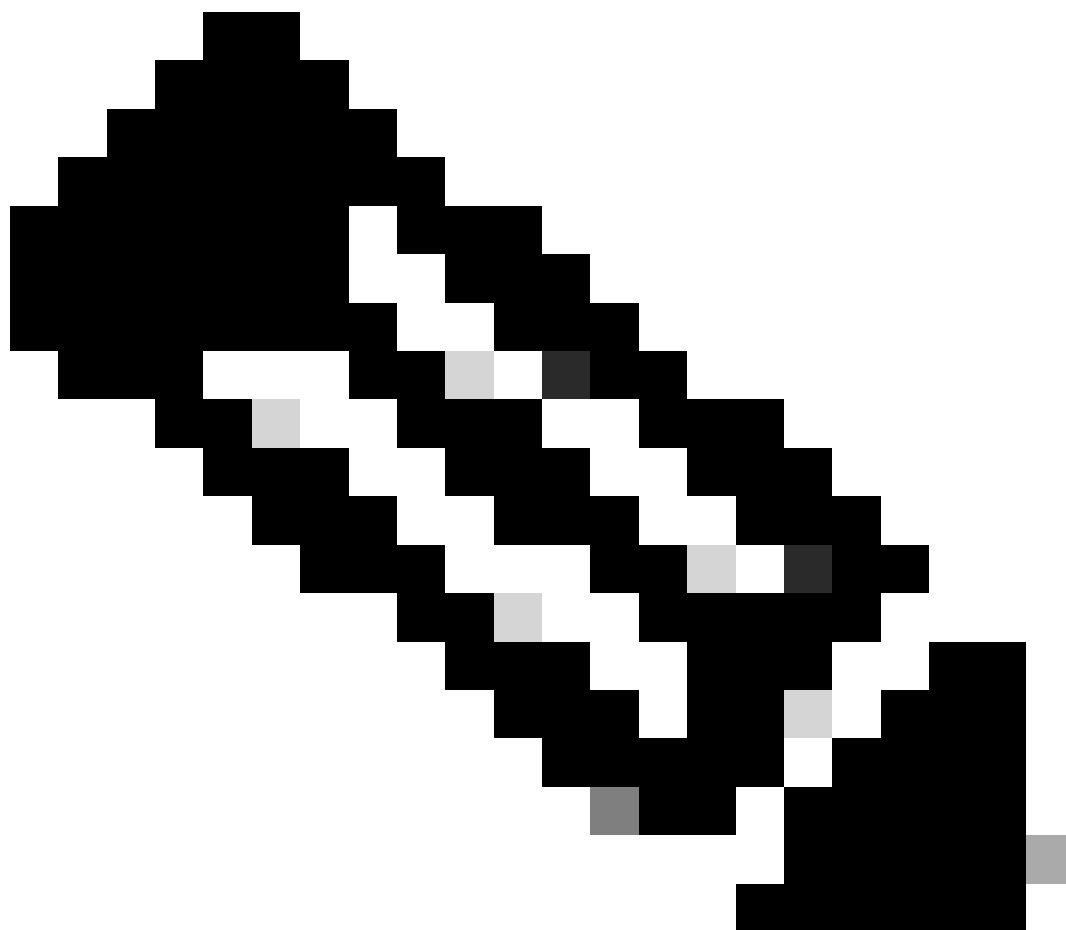
1. Win/Mac/Linuxパッケージの読み込み時にグループポリシーモジュール名が表示されない
2. ASDMでAnyConnect Profile Editorを開くことができない。

トラブルシューティング – 推奨処置

Cisco Bug ID [CSCwh74417](#) 「ASDM: AnyConnect Profile Editor and Group Policy cannot be loaded when using the CSC Image 5.1」を参照してください。この問題を回避するには、Secure

Clientの下位バージョンを使用します。

---

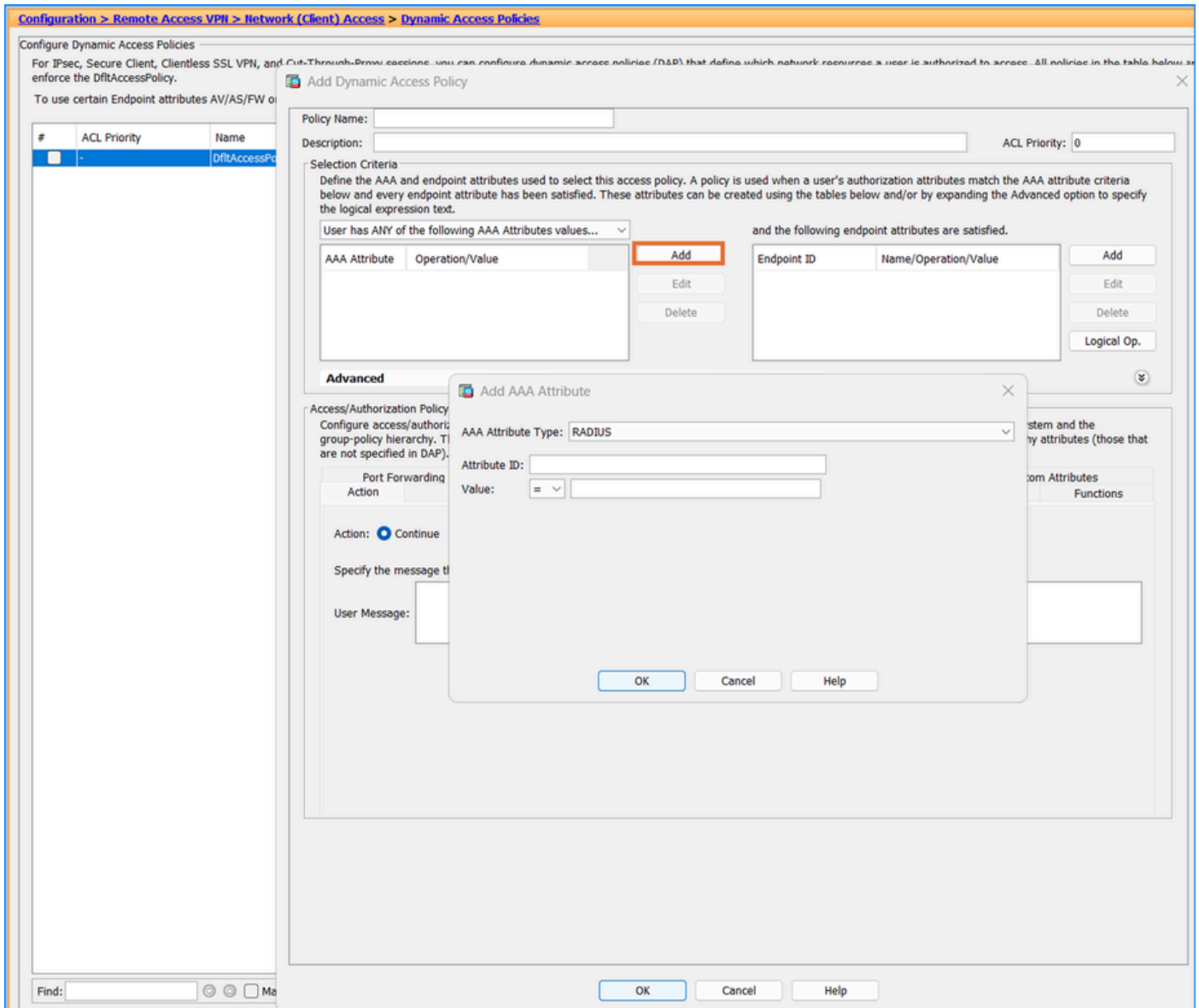


注：この不具合は、最近のASDMソフトウェアリリースで修正されています。詳細については、不具合の詳細を確認してください。

---

## 問題26:AAA属性タイプ(Radius/LDAP)がASDMに表示されない

AAA属性タイプ(Radius/LDAP)は、ASDM > Configuration > Remote Access VPN > Network (Client) Access > Dynamic Access Policies > Add > On AAA attribute field > Add > Select Radius or LDAPで表示されません。



## トラブルシューティング – 推奨処置

ソフトウェアのCisco Bug ID [CSCwa99370](#) 「ASDM : ASDM:DAP config missing AAA Attributes type (Radius/LDAP)」 およびCisco Bug ID [CSCwd16386](#) 「ASDM:DAP config missing AAA Attributes type (Radius/LDAP)」 を参照してください。

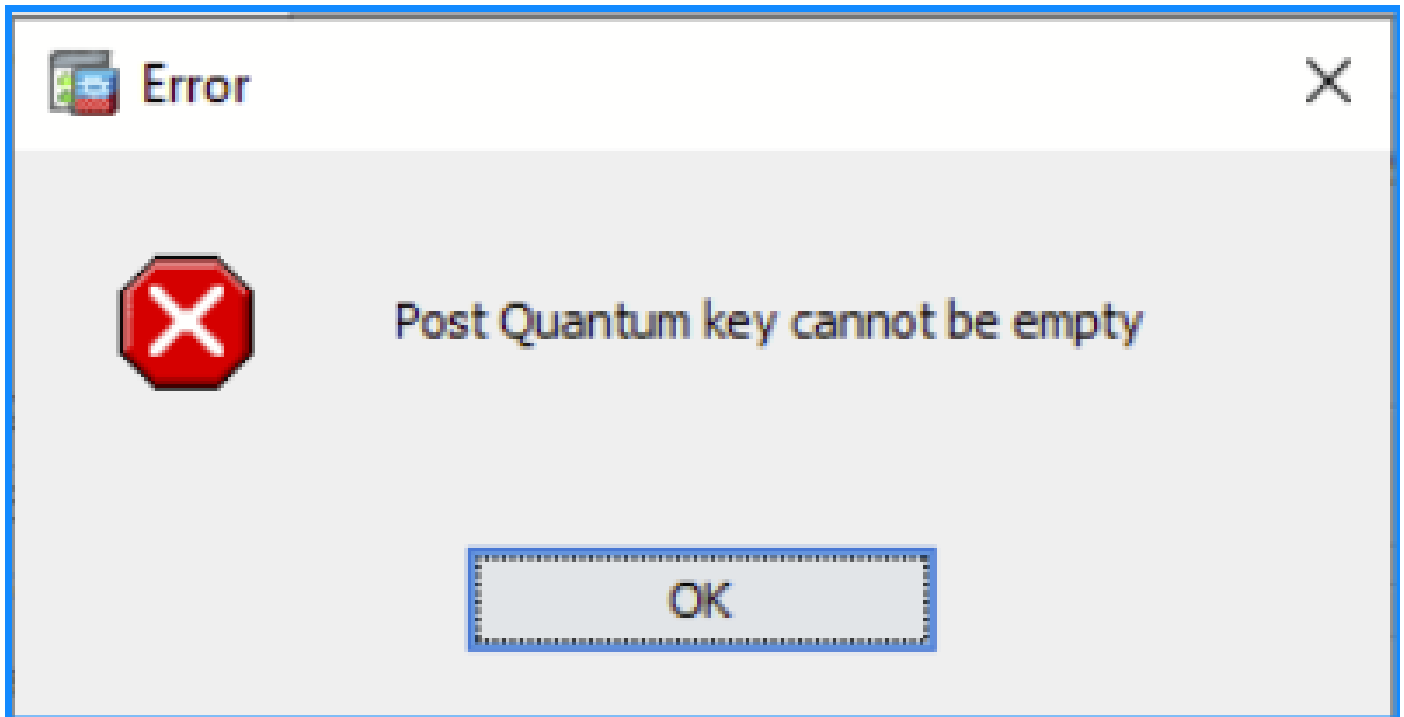


注：これらの不具合は、最近のASDMソフトウェアリリースで修正されています。詳細については、不具合の詳細を確認してください。

---

## 問題27:ASDMに「Post Quantum key cannot be empty」エラーが表示される

ASDM > Configuration > Remote Access VPN > Network (Client) Access > IPsec (IKEv2) Connection ProfilesのAdvancedセクションを編集すると、エラー「Post Quantum key cannot be empty」が表示される。



トラブルシューティング – 推奨処置

Cisco Bug ID [CSCwe58266](#) 「ASDM IKEv2 configuration - Post Quantum Key cannot be empty」  
エラーメッセージを参照してください。



注：この不具合は、最近のASDMソフトウェアリリースで修正されています。詳細については、不具合の詳細を確認してください。

---

## 問題28. ASDMで「where used」オプションを使用しても結果が表示されない

Configuration > Firewall > Objects > Network Objects/Groupsの順に移動し、Objectを右クリックして表示されるオプション「where used」を使用しても、ASDMで結果が表示されません。

トラブルシューティング – 推奨処置

Cisco Bug ID [CSCwd98702](#) 「ASDMの「使用された場所」オプションが機能しない」を参照してください。





注：この不具合は、最近のASDMソフトウェアリリースで修正されています。詳細については、不具合の詳細を確認してください。

---

## 問題29. ネットワークオブジェクトを削除する際に警告メッセージ「[Network Object] cannot be deleted because it is used in the following」が表示される

Configuration > Firewall > Objects > Network Objects/Groupsでネットワークグループで参照されるネットワークオブジェクトを削除する際に、「[Network Object] cannot be deleted because it is used in the following」という警告メッセージがASDMに表示されません。

トラブルシューティング – 推奨処置

Cisco Bug ID [CSCwe67056](#) 「[Network Object] cannot be deleted because it is used in the following」警告が表示されない」を参照してください。



注：この不具合は、最近のASDMソフトウェアリリースで修正されています。詳細については、不具合の詳細を確認してください。

### 問題30. ASDMのNetwork Objects/Groupタブの使い勝手の問題

次の症状が1つ以上見られます。

- 「オブジェクトグループの追加/編集ウィンドウ」の「新しいオブジェクトメンバーの作成」セクションの「名前」テキスト入力は「オプション」とマークされています。ただし、オブジェクトを作成して追加する[追加>>]ボタンは、名前を入力しない限り無効になります。
- 「使用場所」コンテキストメニューをクリックすると開く「使用状況」タブには、オブジェクトを直接参照するエンティティ（ACL、ルートマップ、オブジェクトグループ）のみが表示されます。また、2番目、3番目のように再帰的にリストする必要があります。順序参照（つまり、オブジェクトを含むオブジェクトグループを使用するACLは、オブジェクトの「使用」としてもリストする必要があります）。

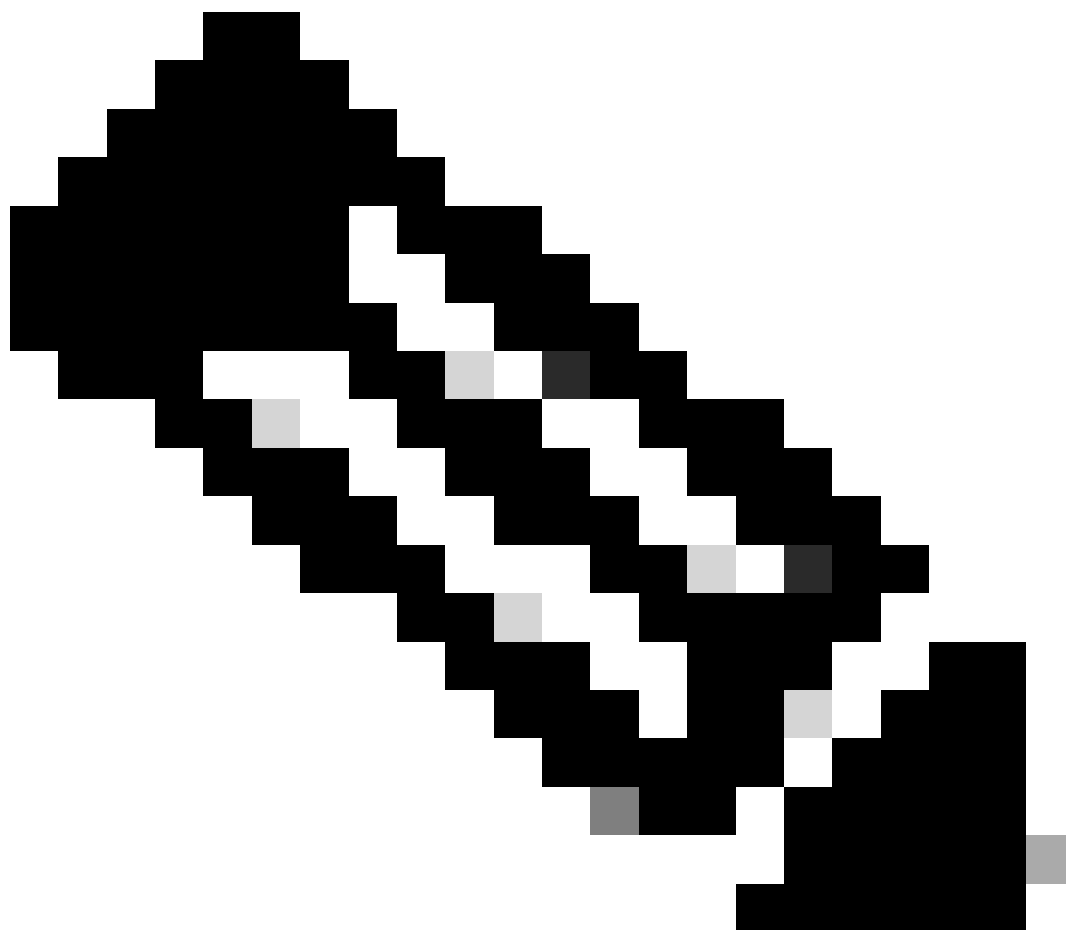
- 右クリックメニューの「削除」操作でも、この動作が表示されます。オブジェクトを直接参照するエンティティが自動的に削除されます（オブジェクトの削除時にエンティティが空になる場合）。2番目、3番目などの順序では、この方法は使用できません。オブジェクトと1番目の順序参照を削除すると、順序参照が空になります。

ユーザは、設定の残りの部分からオブジェクトが削除されたために空になるエンティティをASDMが防止していると考えることができます。しかし、これは必ずしも当てはまりません。

トラブルシューティング – 推奨処置

ソフトウェアのCisco Bug ID [CSCwe86257](#) 「ASDMでのネットワークオブジェクト/グループタブの使いやすさ」を参照してください。

---



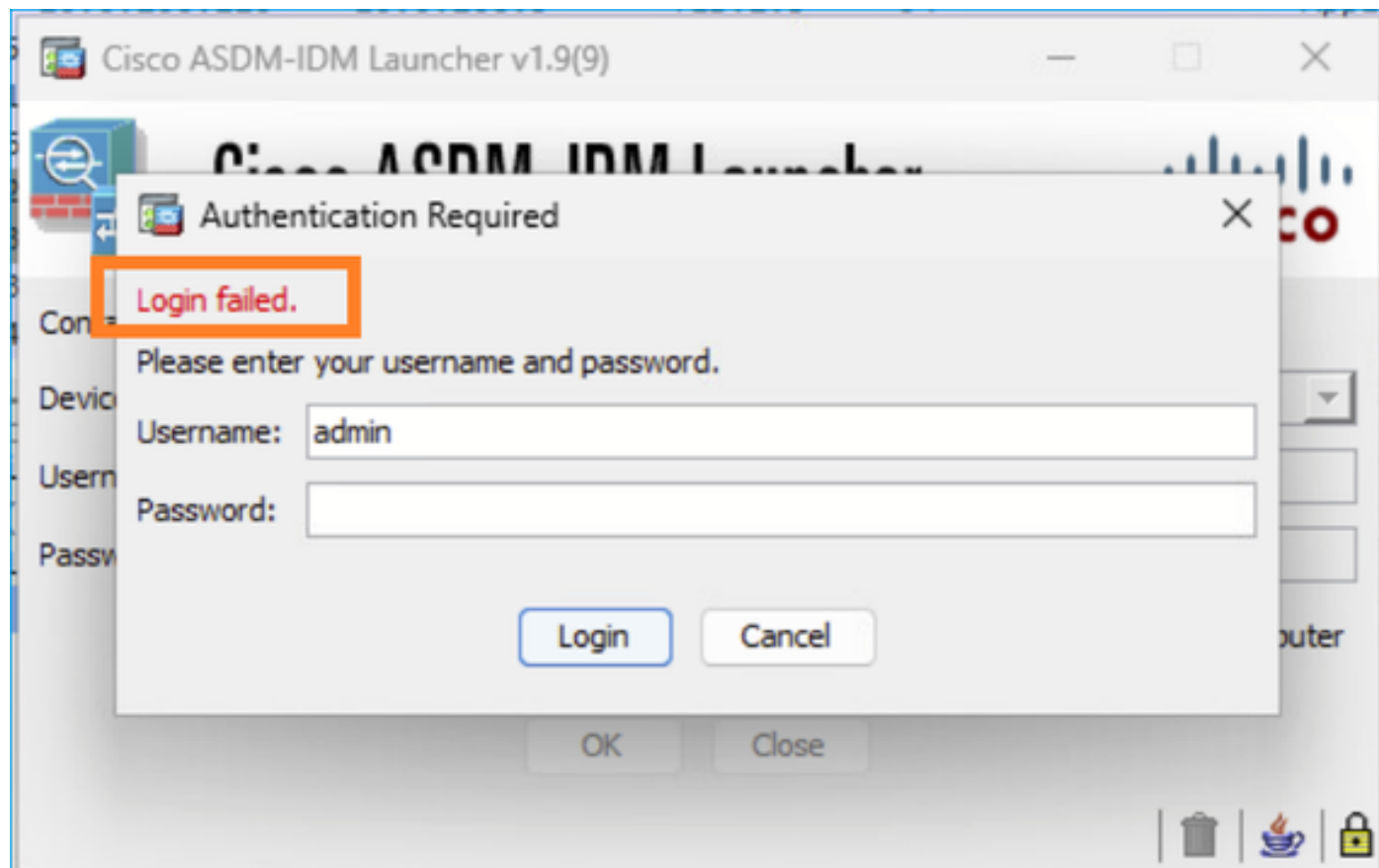
注：この不具合は、最近のASDMソフトウェアリリースで修正されています。詳細については、不具合の詳細を確認してください。

---

# ASDM認証問題のトラブルシューティング

## 問題 1.ASDMログインに失敗しました

ASDM UIに表示されるエラーは次のとおりです。



### トラブルシューティング – 推奨処置

このエラーは、同じインターフェイスでHTTPとWebvpnの両方のCisco Secure Client(AnyConnect)を有効にしている場合に発生する可能性があります。したがって、すべての条件を満たす必要があります。

1. インターフェイスでAnyConnect/Cisco Secure Clientが有効になっている
2. HTTPサーバがAnyConnect/Cisco Secure Clientと同じインターフェイスおよびポートで有効になっている

以下に例を挙げます。

```
<#root>
```

```
asa#
```

```
configure terminal
```

```
asa(config)#
```

webvpn

```
asa(config-webvpn)#
```

```
enable outside <-
```

```
default port in use (443)
```

```
and
```

```
asa(config)#
```

```
http server enable
```

```
<-
```

```
default port in use (443)
```

```
asa(config)#
```

```
http 0.0.0.0 0.0.0.0 outside
```

```
<- HTTP server configured on the same interface as Webvpn
```

トラブルシューティングのヒント : 「debug http 255」を有効にすると、ASDMとWebvpnの間の競合を確認できます。

```
<#root>
```

```
ciscoasa#
```

```
debug http 255
```

```
debug http enabled at level 255.
```

```
ciscoasa# ewaURLHookVCARedirect
```

```
...addr: 192.0.2.5
```

```
ewaURLHookHTTPRedirect: url = /+webvpn+/index.html
```

```
HTTP: ASDM request detected [ASDM/] for [/+webvpn+/index.html] <-----
```

```
webvpnhook: got '/+webvpn+' or '/+webvpn+/' : Sending back "/+webvpn+/index.html" <-----
```

```
HTTP 200 OK (192.0.2.110)HTTP: net_handle->standalone_client [1]
```

```
webvpn_admin_user_agent: buf: ASDM/ Java/1.8.0_431
```

```
ewsStringSearch: no buffer
```

```
Close 0
```

サイドノートとして、ログインが失敗したにもかかわらず、ASAのsyslogには認証が成功したことが表示されます。

```
<#root>
```

```
asa#
```

```
show logging
```

```
Oct 28 2024 07:42:44: %ASA-6-113012: AAA user authentication Successful : local database : user = user2  
Oct 28 2024 07:42:44: %ASA-6-113009: AAA retrieved default group policy (DfltGrpPolicy) for user = user2  
Oct 28 2024 07:42:44: %ASA-6-113008: AAA transaction status ACCEPT : user = user2  
Oct 28 2024 07:42:44: %ASA-6-605005: Login permitted from 192.0.2.110/60316 to NET50:192.0.2.5/https fo  
Oct 28 2024 07:42:44: %ASA-6-611101:
```

```
User authentication succeeded: IP address: 192.0.2.110, Uname: user2
```

## 回避策

### 回避策 1

いずれかのASA HTTPサーバのTCPポートを変更します。次に例を示します。

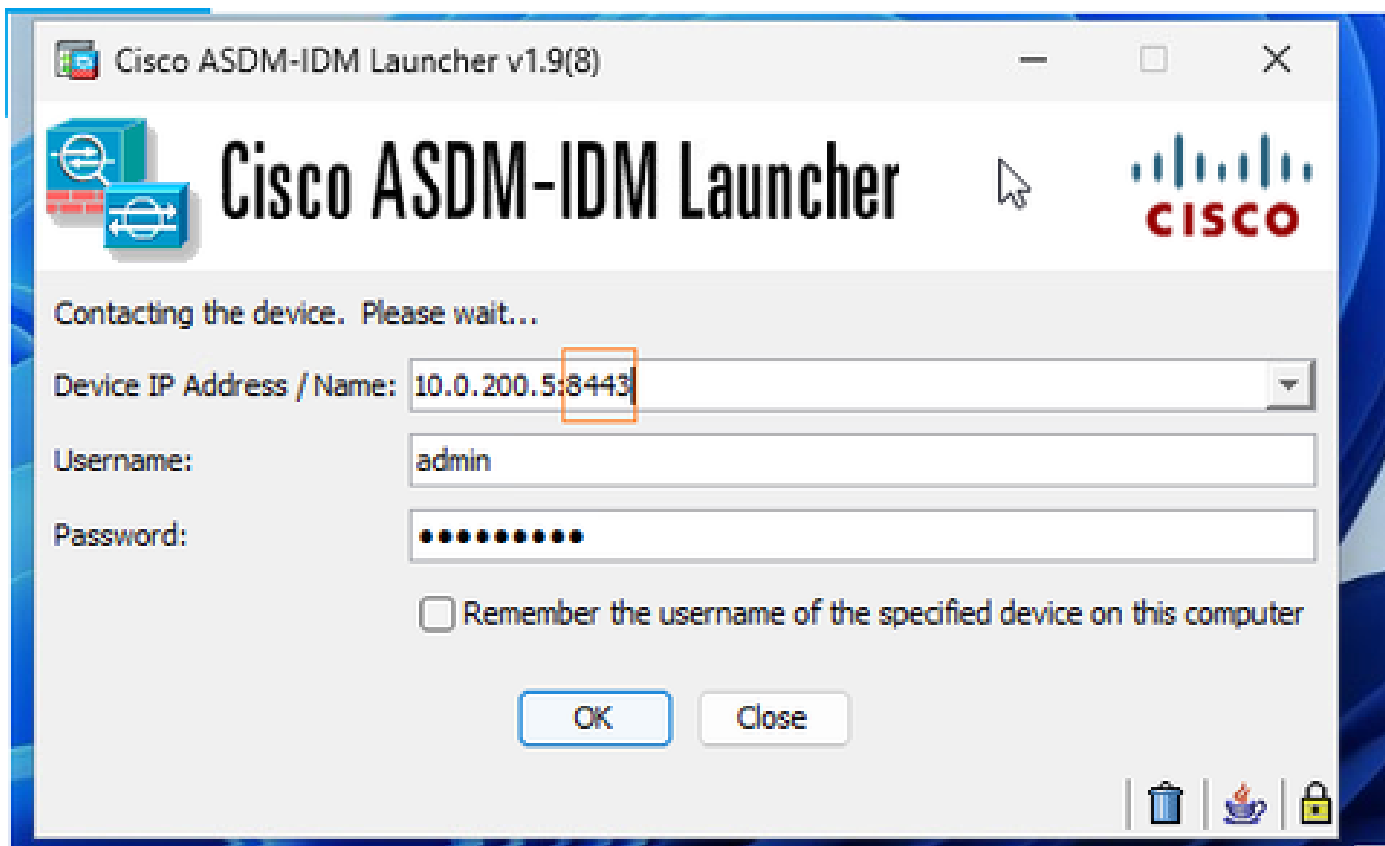
```
<#root>
```

```
ciscoasa#
```

```
configure terminal
```

```
ciscoasa(config)#
```

```
http server enable 8443
```



## 回避策 2

AnyConnect/Cisco Secure ClientのTCPポートを変更します。次に例を示します。

```
<#root>
```

```
ciscoasa#
```

```
configure terminal
```

```
ciscoasa(config)#
```

```
webvpn
```

```
ciscoasa(config-webvpn)#
```

```
no enable outside
```

```
<-- first you have disable WebVPN for all interfaces before changing the port
```

```
ciscoasa(config-webvpn)#
```

```
port 8443
```

```
ciscoasa(config-webvpn)#
```

```
enable outside
```

## 回避策 3

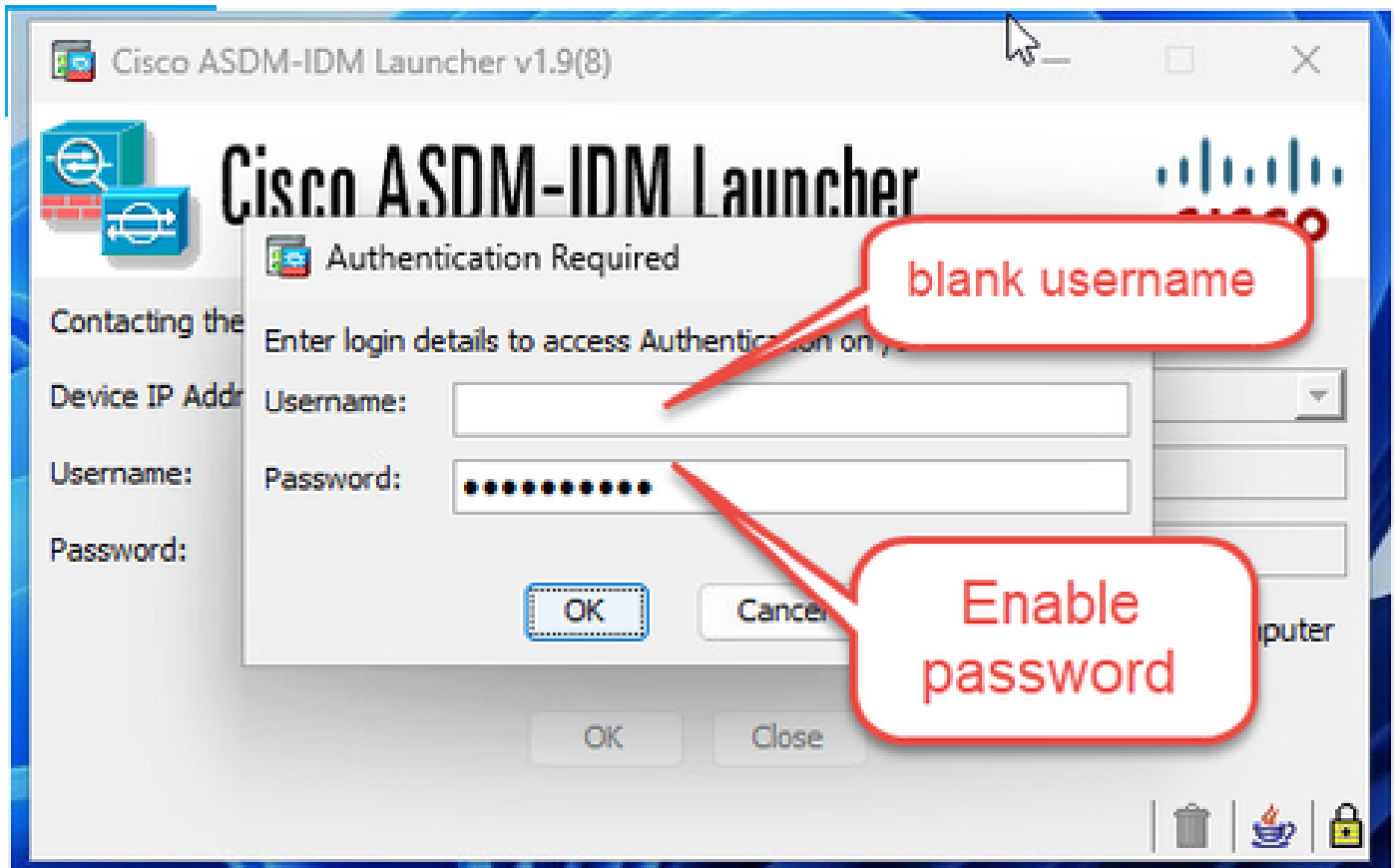
別の回避策は、「aaa authentication http console」設定を削除することです。

```
<#root>
```

```
ciscoasa(config)#
```

```
no aaa authentication http console LOCAL
```

この場合、イネーブルパスワードを使用するだけでASDMにログインできます。



関連する障害

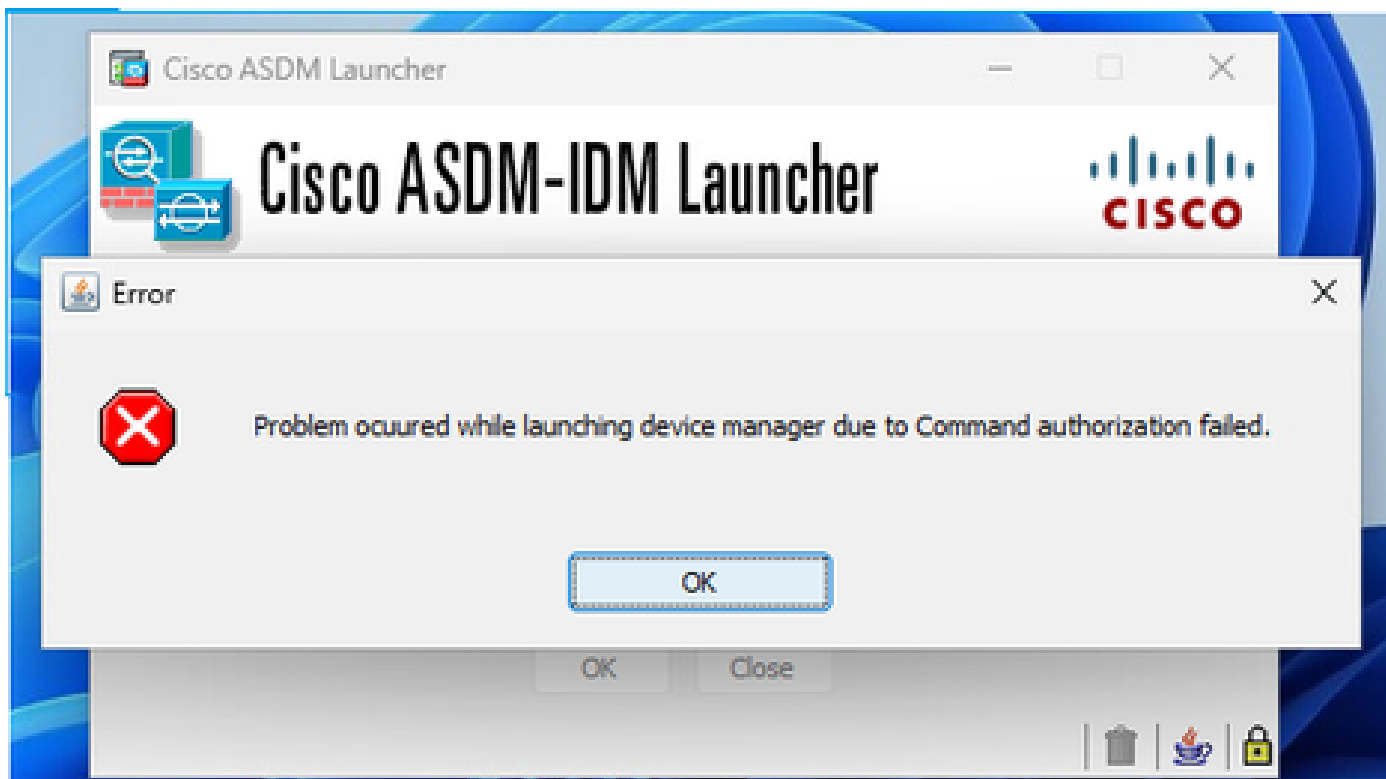
Cisco Bug ID [CSCwb67583](#)

同じインターフェイスでwebvpnとASDMが有効な場合に警告を追加

問題 2.ASDMコマンドの許可に失敗しました

ASDM UIに表示されるエラーは次のとおりです。





#### トラブルシューティング – 推奨手順

ASAのAAA設定をチェックして、次のことを確認します。

- aaa認証も設定されている。
- リモート認証サーバを使用する場合は、到達可能であり、コマンドを許可します。

#### 参考

<https://www.cisco.com/c/en/us/td/docs/security/asa/asa922/configuration/general/asa-922-general-config/aaa-local.html>

#### 問題3.ASDMの読み取り専用アクセスの設定

場合によっては、ASDMユーザに読み取り専用アクセスを提供する必要があります。

#### トラブルシューティング – 推奨手順

カスタム権限レベル(5)を持つ新規ユーザを作成します。次に例を示します。

```
<#root>  
asa(config)#  
username [username] password [password] privilege 5
```

このコマンドは、特権レベル5のユーザを作成します。特権レベルは「監視専用」レベルです。「[username]」と「[password]」は、目的のユーザ名とパスワードに置き換えます。

## 詳細

ローカルのコマンド許可を使用すると、16の特権レベル(0 ~ 15)のいずれかにコマンドを割り当てることができます。デフォルトでは、各コマンドは特権レベル0または15のいずれかに割り当てられます。各ユーザを特定の特権レベルに定義できます。各ユーザは、割り当てられた特権レベル以下で任意のコマンドを入力できます。ASAは、ローカルデータベース、RADIUSサーバ、またはLDAPサーバ ( LDAP属性をRADIUS属性にマッピングする場合 ) で定義されたユーザ権限レベルをサポートします。

## 手順

ステップ 1	Configuration > Device Management > Users/AAA > AAA Access > Authorizationの順に選択します。
ステップ 2	Enable authorization for ASA command access > Enableチェックボックスにチェックマークを付けます。
ステップ 3	Server Groupドロップダウンリストから、LOCALを選択します。
ステップ 4	<p>ローカルのコマンド許可を有効にする場合は、個々のコマンドまたはコマンドグループに特権レベルを手動で割り当てるか、事前定義されたユーザーアカウント特権を有効にするかを選択できます。</p> <ul style="list-style-type: none"><li>Set ASDM Defined User Rolesをクリックして、事前定義されたユーザーアカウント権限を使用します。</li></ul> <p>ASDMで定義されたユーザーロールの設定ダイアログボックスが表示されます。Yesをクリックすると、事前定義されたユーザーアカウント権限が使用されます。権限レベルはAdmin ( すべてのCLIコマンドにフルアクセスできる権限レベル15 )、読み取り専用 ( 権限レベル5の読み取り専用アクセス )、モニタ専用(権限レベル3のモニタリングセッションへのアクセスのみ)があります。</p> <ul style="list-style-type: none"><li>Configure Command Privilegesをクリックして、コマンドレベルを手動で設定します。</li></ul> <p>Command Privileges Setupダイアログボックスが表示されます。すべてのコマンドを表示するには、Command ModeドロップダウンリストからAll Modesを選択します。コンフィギュレーションモードを選択すると、そのモードで使用可能なコマンドが表示されます。たとえば、contextを選択すると、コンテキストコンフィギュレーションモードで使用可能なすべてのコマンドを表示できます。コンフィギュレーションモードに加えてユーザEXECモードまたは特権EXECモードでコマンドを入力でき、各モードでコマン</p>

	<p>ドが異なるアクションを実行する場合は、これらのモードの特権レベルを個別に設定できます。</p> <p>Variant列に、show、clear、またはcmdが表示されます。特権を設定できるのは、コマンドのshow、clear、またはconfigure形式に対してだけです。通常、このコマンドのconfigure形式は、設定変更を引き起こす形式です。変更されていないコマンド ( showまたはclear prefixなし ) またはno形式になります。</p> <p>コマンドのレベルを変更するには、コマンドをダブルクリックするか、Editをクリックします。レベルは0 ~ 15の間で設定できます。設定できるのは、mainコマンドの特権レベルだけです。たとえば、すべてのaaaコマンドのレベルは設定できますが、aaa authenticationコマンドとaaa authorization コマンドのレベルは個別に設定できません。</p> <p>表示されるすべてのコマンドのレベルを変更するには、Select All、Editの順にクリックします。</p> <p>OKをクリックして変更を確定します。</p>
ステップ5	<p>[APPLY] をクリックします。</p> <p>認証設定が割り当てられ、変更内容が実行コンフィギュレーションに保存されます。</p>

#### 参考

<https://www.cisco.com/c/en/us/td/docs/security/asa/asa922/asdm722/general/asdm-722-general-config/admin-management.html#ID-2111-00000650>

### 問題 4.ASDM多要素認証(MFA)

#### トラブルシューティング – 推奨手順

このドキュメントの作成時点では、ASDMはMFA ( または2FA ) をサポートしていません。この制限には、PingIDなどのソリューションを使用したMFAが含まれます。

#### 参考

Cisco Bug ID [CSCvs85995](#)

ENH : 二要素認証(MFA)によるASDMアクセス

### 問題 5.ASDM外部認証設定

#### トラブルシューティング – 推奨手順

ASDMで外部認証を設定するには、LDAP、RADIUS、RSA SecurID、またはTACACS+を使用できます。

#### 参考資料

- <https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/112967-acs-aaa-tacacs-00.html>
- <https://www.cisco.com/c/en/us/td/docs/security/asa/asa922/configuration/general/asa-922-general-config/aaa-radius.html>
- <https://www.cisco.com/c/en/us/td/docs/security/asa/asa922/configuration/general/asa-922-general-config/aaa-tacacs.html>
- <https://www.cisco.com/c/en/us/td/docs/security/asa/asa922/configuration/general/asa-922-general-config/aaa-ldap.html>

## 問題 6.ASDMローカル認証が失敗する

### トラブルシューティング – 推奨手順

外部認証とローカル認証をフォールバックとして使用する場合、ローカル認証は、外部サーバがダウンしているか動作していない場合にのみ動作します。このシナリオでのみ、ローカル認証が引き継がれ、ローカルユーザと接続できます。

これは、外部認証がローカル認証よりも優先されるためです。

以下に例を挙げます。

<#root>

```
asa(config)# aaa authentication ssh console RADIUS_AUTH LOCAL
```

### 参考

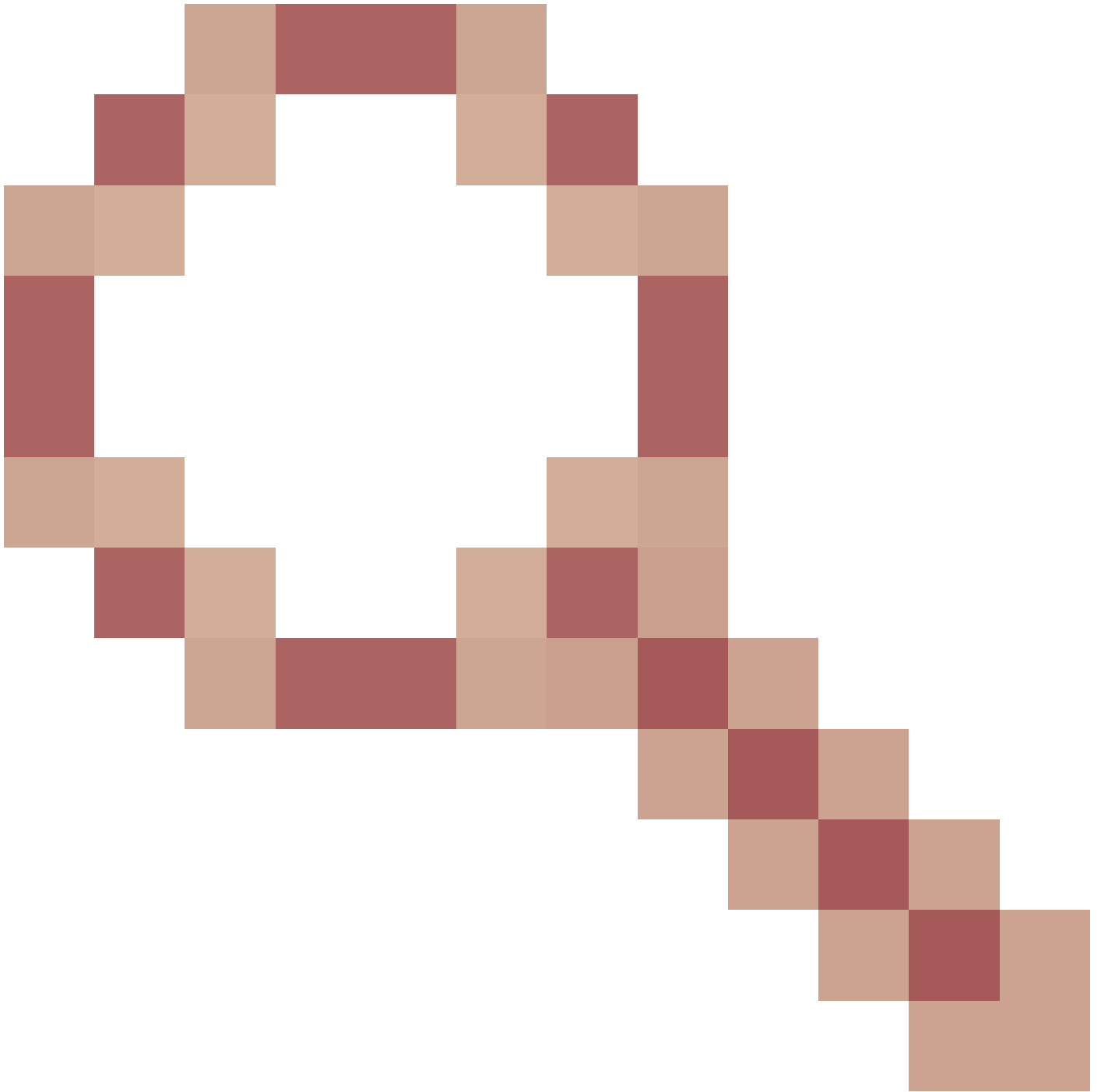
- <https://www.cisco.com/c/en/us/td/docs/security/asa/asa-cli-reference/A-H/asa-command-ref-A-H/aa-ac-commands.html#wp6184732320>

## 問題 7.ASDMワンタイムパスワード

### トラブルシューティング – 推奨手順

- ASDM OTP (ワンタイムパスワード) 認証のサポートは、シングルルーテッドモードのみでASAバージョン8.x ~ 9.xで追加されました。
- ASAファイアウォールトランスペアレントモードまたはマルチコンテキストモード (あるいはその両方) のASDM OTP認証は、このカテゴリには入りません。

Cisco Bug ID [CSCtf23419](#)



ENH : マルチコンテキストモードと透過モードでのASDM OTP認証のサポート

## 問題 8. 接続プロファイルにすべてのメソッドが表示されない

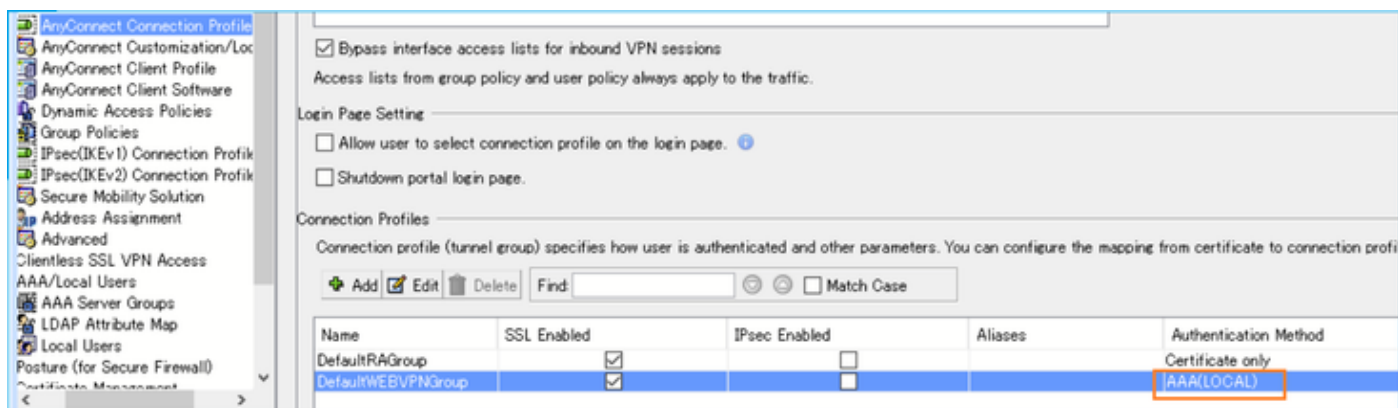
この場合の問題は、ASA CLI設定とASDM UIの間の不一致です。

具体的には、CLIには次の機能があります。

```
<#root>
```

```
tunnel-group DefaultWEBVPNGroup webvpn-attributes
 authentication aaa certificate
```

ASDM UIでは証明書方式について言及されませんが、次のようになります。



### トラブルシューティング – 推奨手順

これは表示の問題です。方式はASDMに表示されませんが、証明書認証が使用されます。

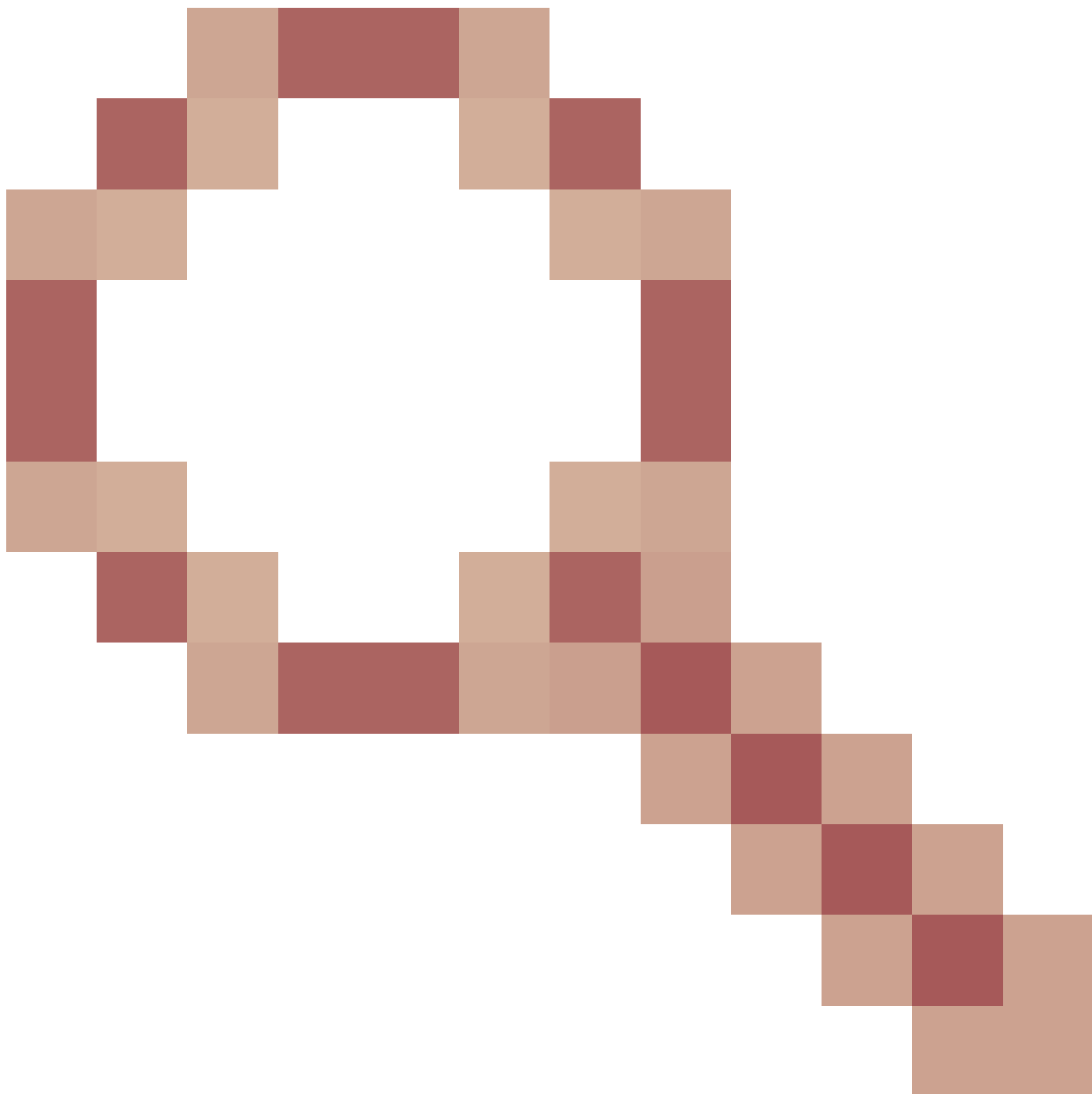
### 問題 9.ASDMセッションがタイムアウトしない

症状は、ASDM GUIのセッションタイムアウトが考慮されないことです。

### トラブルシューティング – 推奨手順

これは、管理対象ASAでコマンド「aaa authentication http console LOCAL」が設定されていない場合に発生します。

Cisco Bug ID [CSCwj70826](#)



ENH：警告を追加します。セッションのタイムアウトを設定します。「aaa authentication http console LOCAL」が必要です。

#### 回避策

管理対象ASAでコマンド「aaa authentication http console LOCAL」を設定します。

### 問題 10.ASDM LDAP認証が失敗する

#### トラブルシューティング – 推奨手順

##### 手順 1

設定が適切であることを確認します。次に例を示します。

```
<#root>
```

```
aaa-server ldap_server protocol ldap
aaa-server ldap_server (inside) host 192.0.2.1
  ldap-base-dn OU=ldap_ou,DC=example,DC=com
  ldap-scope subtree
  ldap-naming-attribute cn
  ldap-login-password *****
  ldap-login-dn CN=example, DC=example,DC=com
  server-type microsoft
asa(config)#

aaa authentication http console ldap_server LOCAL
```

## 手順 2

LDAPサーバのステータスを確認します。

```
<#root>
```

```
asa#
show aaa-server
```

良いシナリオ :

```
<#root>
```

```
Server status:
ACTIVE
, Last transaction at 11:45:23 UTC Tue Nov 19 2024
```

正しくないシナリオ :

```
<#root>
```

```
Server status:
FAILED
, Server disabled at 11:45:23 UTC Tue Nov 19 2024
```

## 手順 3

LDAP認証を一時的に無効にすることで、LOCAL認証が正しく動作することを確認します。



#### 手順 4

ASAでLDAPデバッグを実行し、ユーザの認証を試行します。

```
<#root>
```

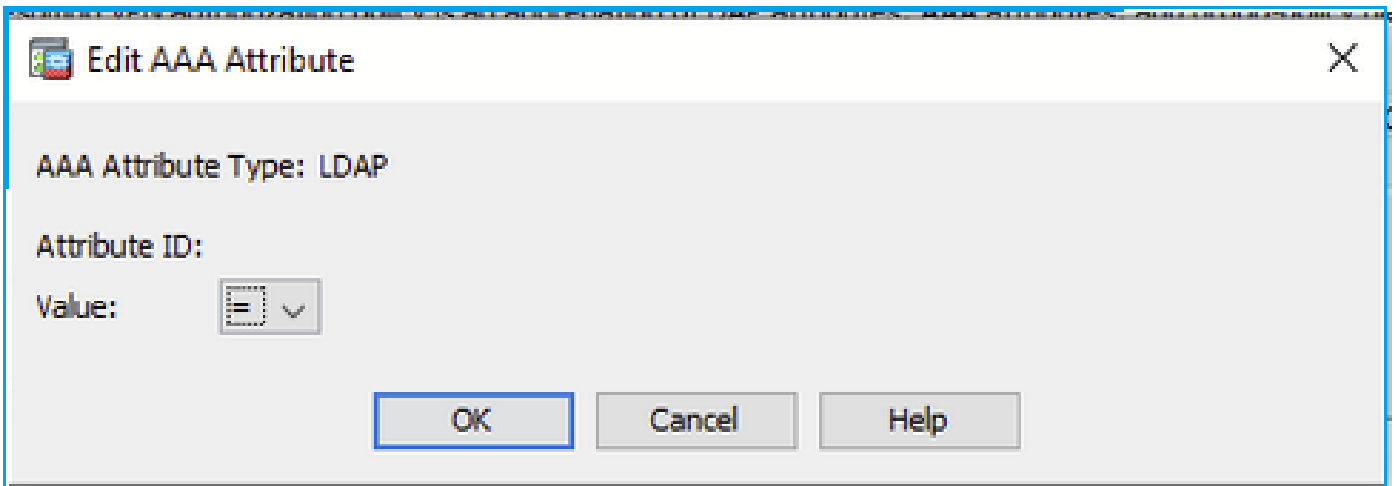
```
#
```

```
debug ldap 255
```

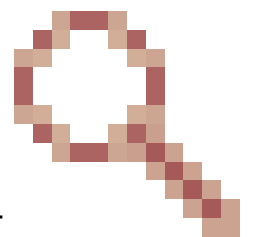
デバッグで、「Failed」のようなヒントを含む行を探します。

#### 問題 11.ASDM Webvpn DAP設定が欠落している

ASDMのDAP設定でAAA属性タイプ(Radius/LDAP)が表示されない(=および!=がドロップダウンに表示される)



#### トラブルシューティング – 推奨手順



これは、Cisco Bug ID [CSCwa99370](https://tools.cisco.com/bugcenter/bug/?bugID=CSCwa99370)によって追跡されるソフトウェア不具合です  
ASDM:DAP config missing AAA Attributes type(RADIUS/LDAP)



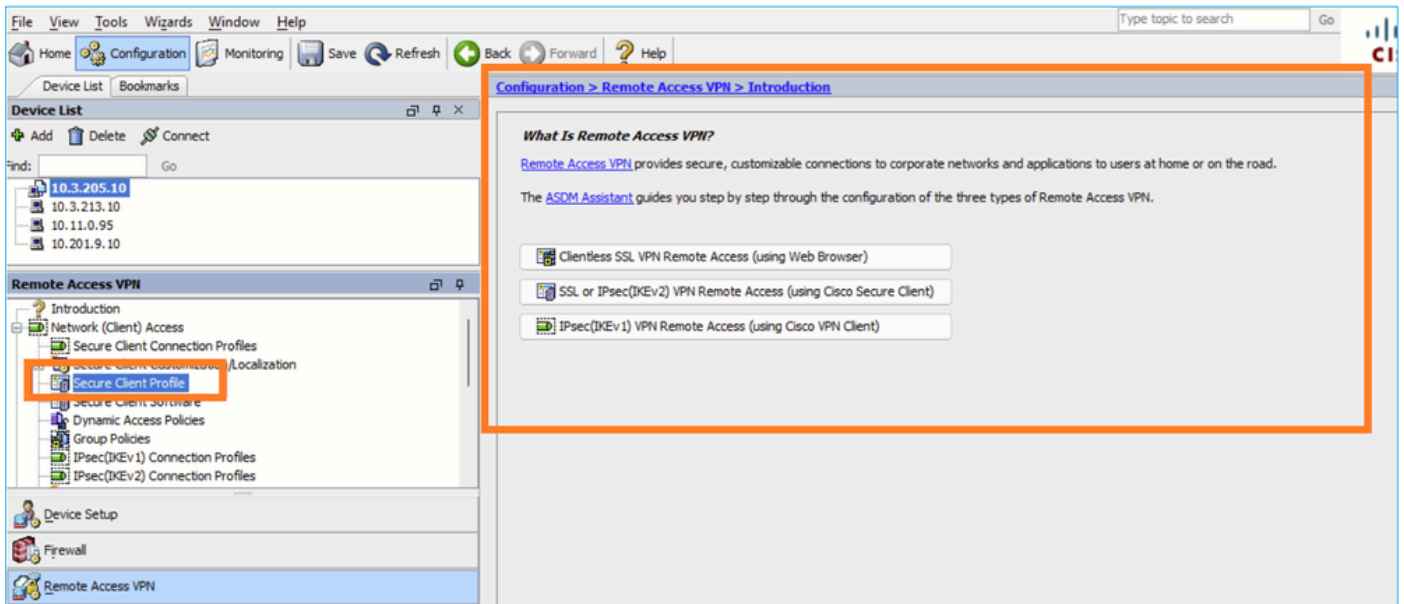
注：この不具合は、最近のASDMソフトウェアリリースで修正されています。詳細については、不具合の詳細を確認してください。

---

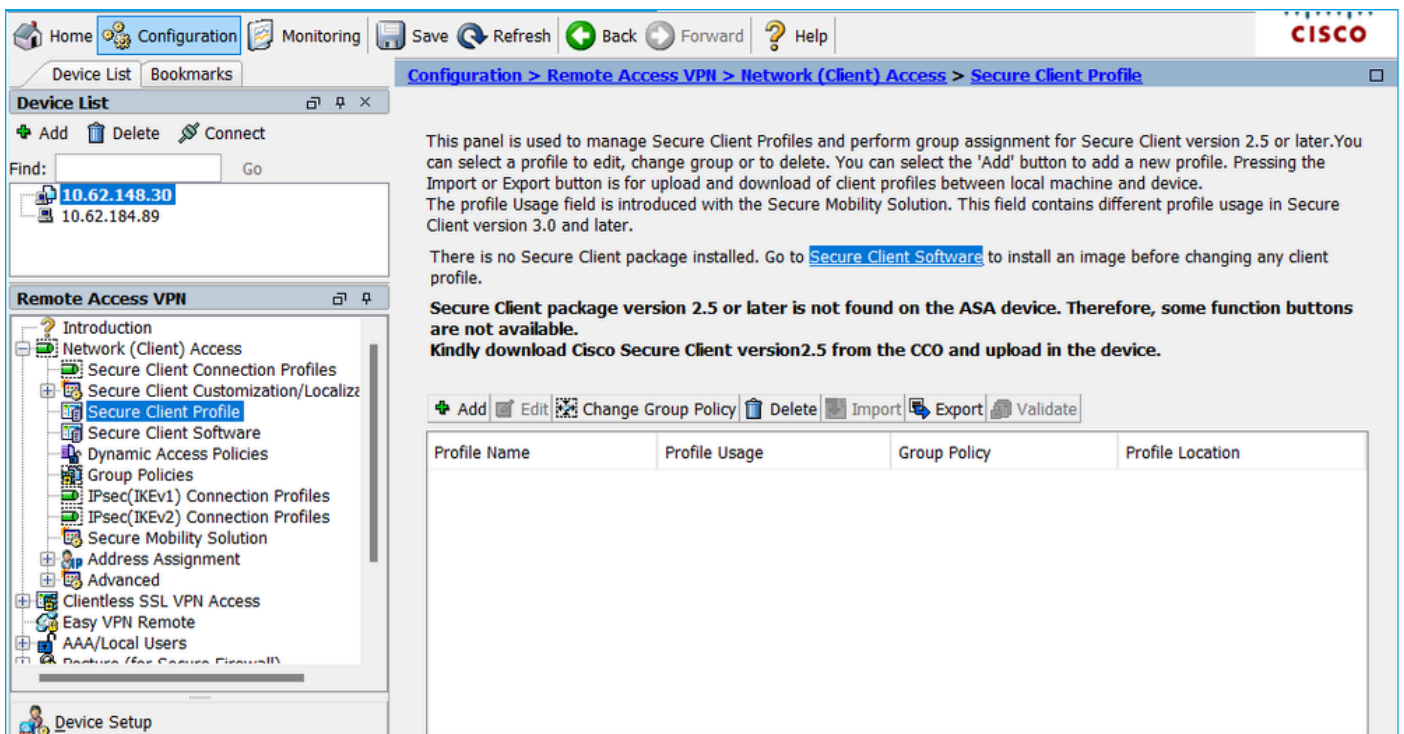
## ASDMのその他の問題のトラブルシューティング

### 問題 1.ASDMでセキュアクライアントプロファイルにアクセスできない

ASDM UIは次を表示します。



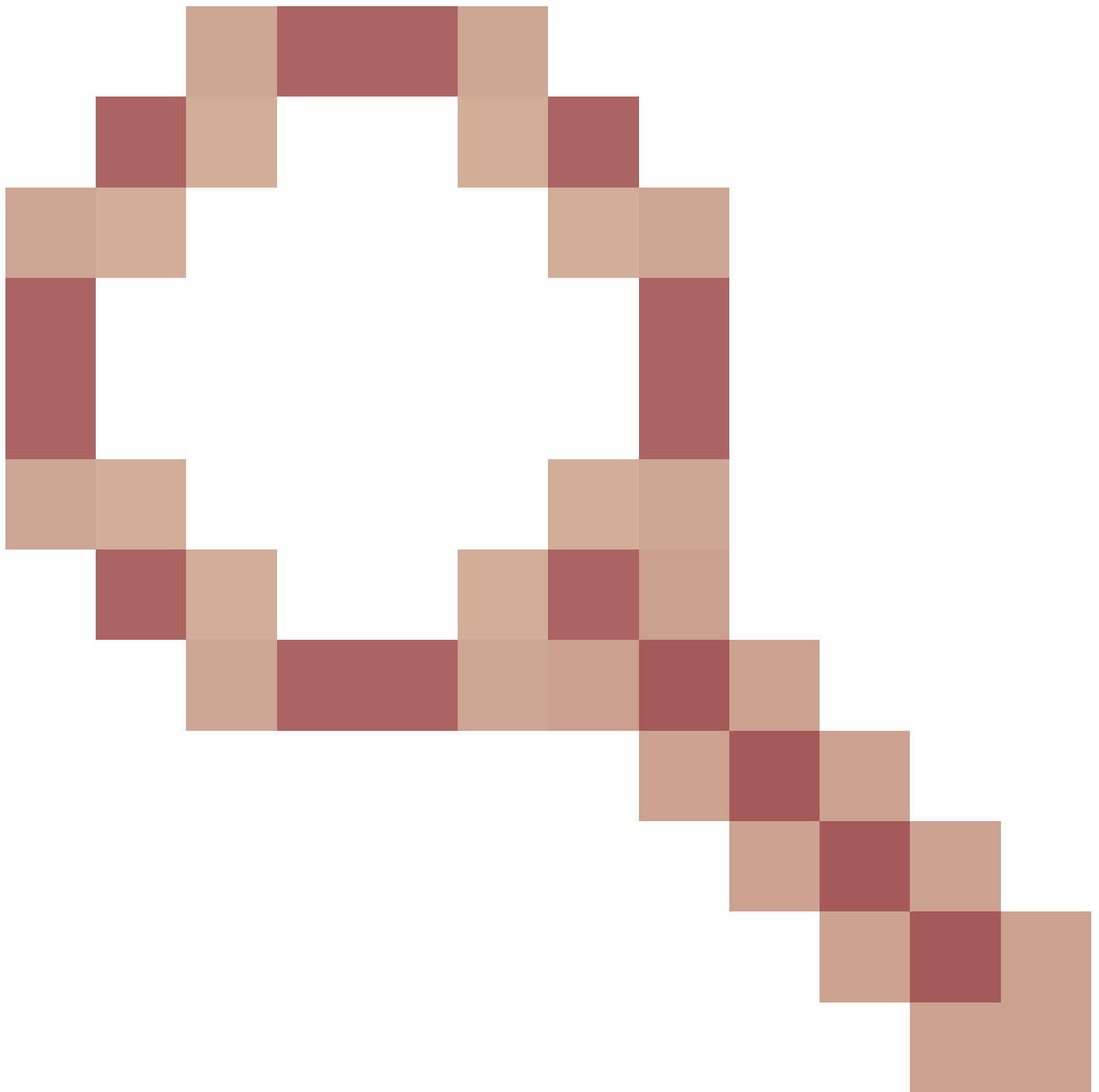
予想されるUI出力は次のとおりです。



トラブルシューティング – 推奨手順

これは既知の不具合です。

Cisco Bug ID [CSCwi56155](#)



ASDMでセキュアクライアントプロファイルにアクセスできない

回避策：

AnyConnectのダウングレード

または

ASDMのバージョン7.20.2へのアップグレード

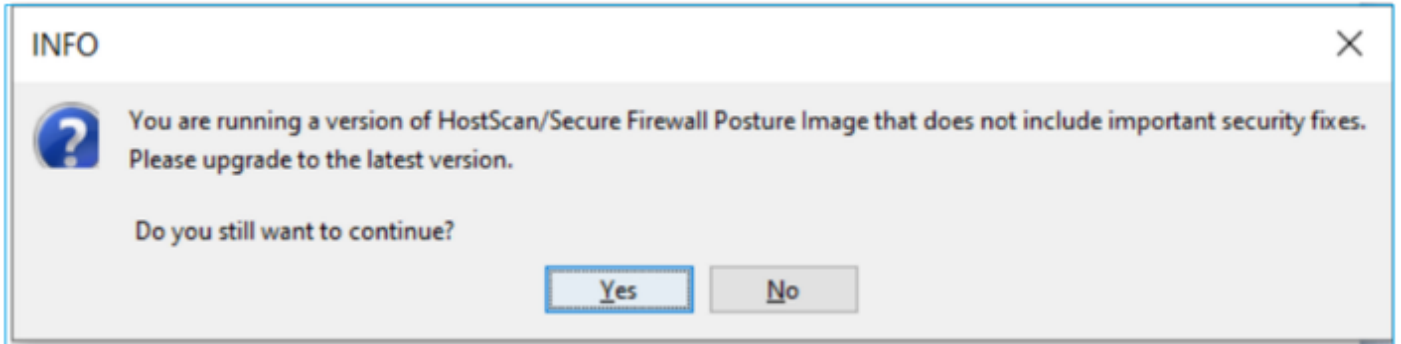
詳細については、不具合ノートを参照してください。また、不具合を購読して、不具合の更新に関する通知を受け取ることもできます。

問題 2.ASDMにホストスキャンのポップアップが表示される – イメージに重要なセ

セキュリティ修正が含まれていない

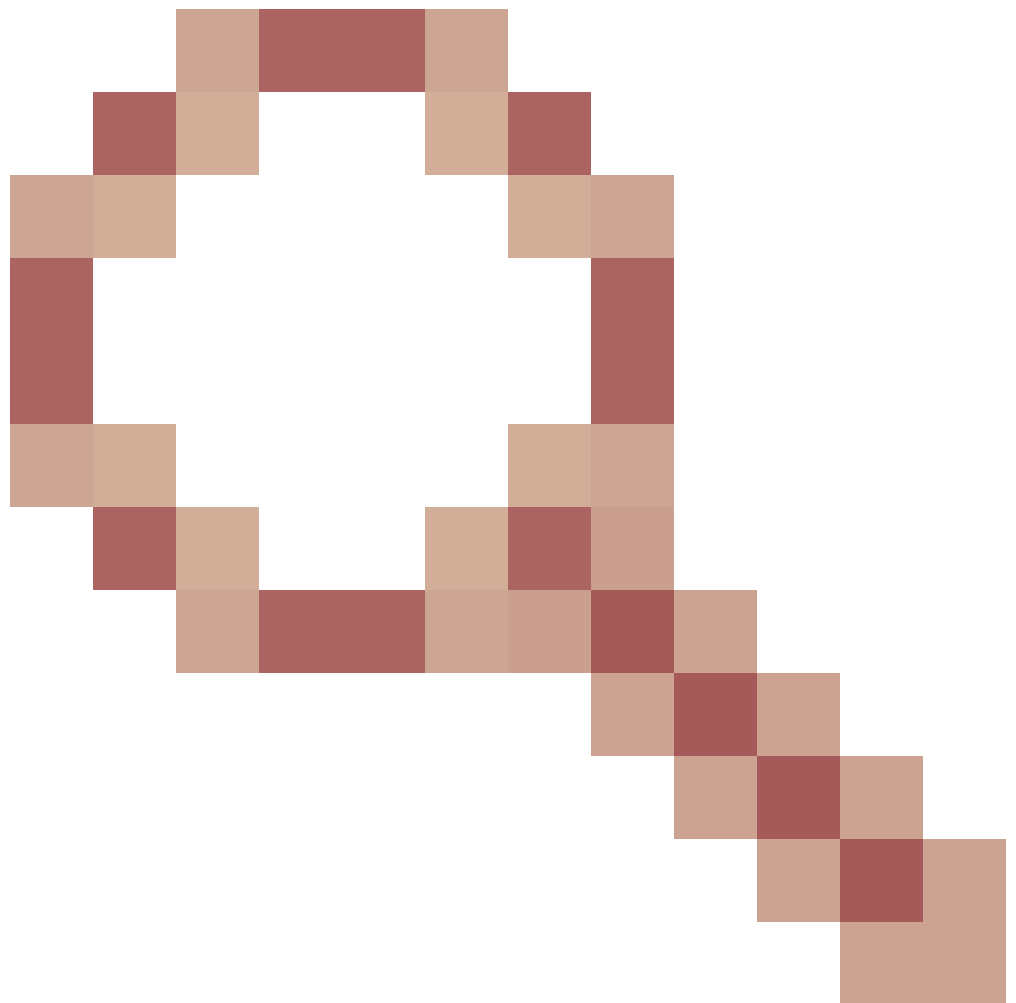
ASDM UIには次のように表示されます。

「重要なセキュリティ修正が含まれていないバージョンのHostScan/SecureFirewallポスタチャイメーجزを実行しています。最新バージョンにアップグレードしてください。続行しますか？」



トラブルシューティング – 推奨手順

これは既知の不具合です。



Cisco Bug ID [CSCwc62461](#)

ホストスキャンのためにASDMポップアップにログインすると、イメージに重要なセキュリティ修正が含まれない

---

注：この不具合は、最近のASDMソフトウェアリリースで修正されています。詳細については、不具合の詳細を確認してください。

---

回避策：

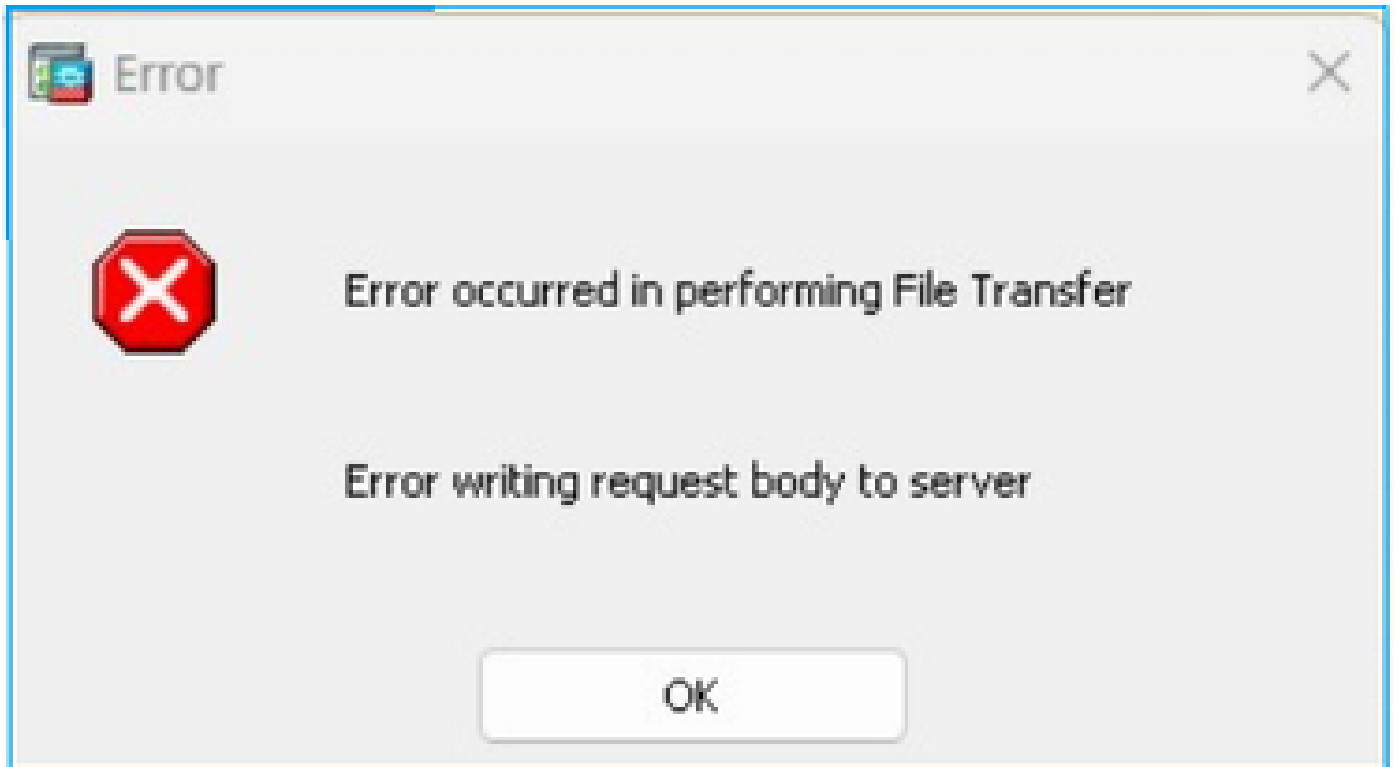
ポップアップメッセージボックスで[はい]をクリックして続行します。

**問題3.ASDM経由でイメージをコピーするときに「Error writing request body to server」が発生する**

ASDM UIには次のように表示されます。

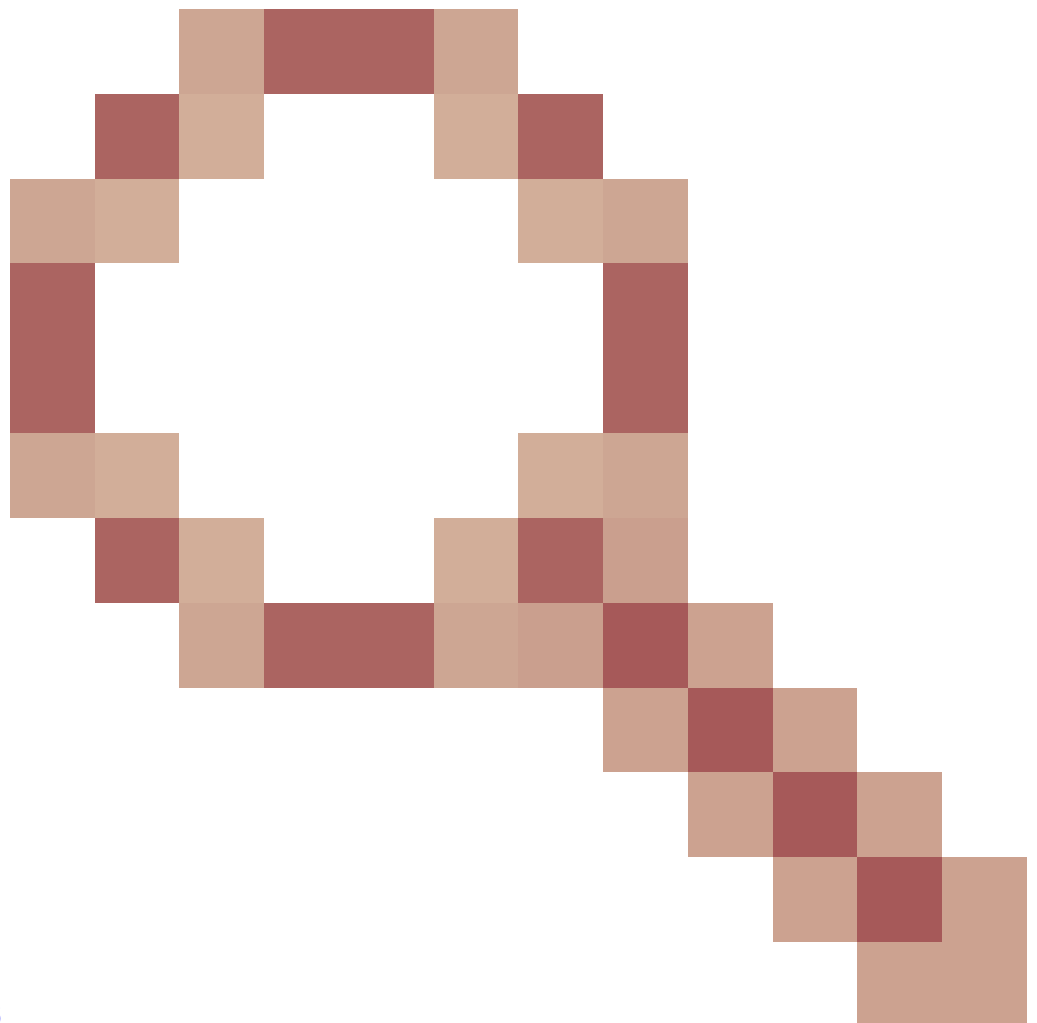
ファイル転送の実行中にエラーが発生しました

サーバーへの要求本文の書き込み中にエラーが発生しました



トラブルシューティング – 推奨処置

これは、次の項目によって追跡される既知の不具合です。



イメージのコピー時のASDMの「Error writing request body to server」

回避策

SCP/TFTPを使用してファイルを転送します。



## 翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。