Software Activation Configuration Guide, Cisco IOS XE Release 3S

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.

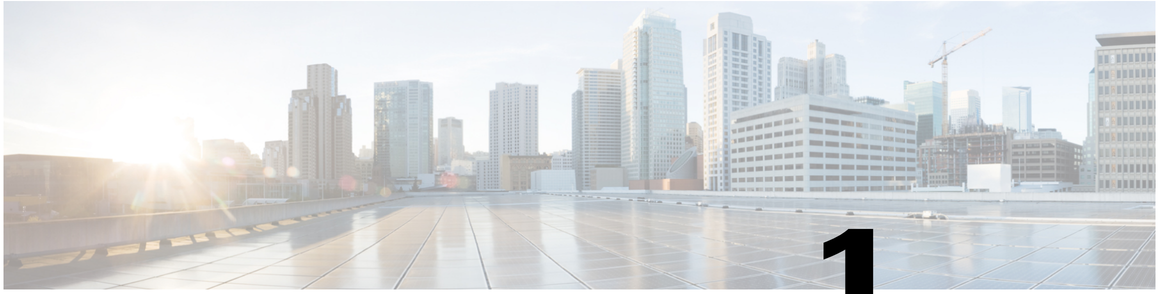
NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT 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.

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: http://www.cisco.com/go/trademarks. 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. (1110R)

CONTENTS



CHAPTER 1

Cisco IOS Software Activation Conceptual Overview

The Cisco IOS Software Activation feature is an orchestrated collection of processes and components to activate Cisco software feature sets by obtaining and validating Cisco software licenses. With this feature, you can enable licensed features and register licenses in these ways:

- By using the Cisco Product License Registration portal.
- By entering Cisco EXEC commands on the device.
- By using Cisco License Manager to register, obtain, and install licenses in a bulk fashion for network-wide deployments.

This document provides an overview of the Cisco software licensing processes and describes the role of the Cisco IOS Software Activation feature in those processes.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About the Cisco Software Licensing Process

Cisco Software Licensing Concepts

Cisco Product License Registration Portal

Use the Cisco Product License Registration portal at http://www.cisco.com/go/license to perform these licensing operations:

- Get a license through product authorization key (PAK) registration
- Register for a return merchandise authorization (RMA) replacement license
- Manage a license (look up a license and upload a rehost ticket)
- Migrate a license

You must have a Cisco.com account before you can access the portal.

Product Authorization Key

Interaction with the Cisco Product License Registration portals might require a PAK, which is provided when you order and purchase the right to use a feature set for a particular platform. The PAK serves as a receipt and is an important component in the process to obtain and upgrade a license.

You can also purchase a bulk PAK to fulfill multiple licenses on a device.

Unique Device Identifier

Cisco software performs license verification checks by comparing a stored unique device identifier (UDI)--a unique and unchangeable identifier assigned to all Cisco hardware devices--with the UDI of the device.

The UDI has two main components: the product ID (PID) and the serial number (SN). For most Cisco hardware devices, the UDI is printed on a label located on the back of the device and can be displayed by using the **show license udi** command.

Note When registering a license, you must use the correct UDI.

Cisco Software License Validation

Cisco software licensing uses a system of validation keys to provide a simple mechanism for deploying new feature sets that offers Cisco customers increased functionality for upgrading and maintaining their software.

Some feature sets on a Cisco device might need the license key before they can be enabled. You obtain the license key by using the Cisco licensing portal. The portal issues a license key for a specific Cisco software feature set, and the license is locked to the device UDI. (This is known as a node-locked license.)

Cisco License Manager

The Cisco License Manager, a client/server-based application that is available free to Cisco customers, can automatically discover Cisco devices on a network and can simplify the task of collecting the license key.

For more information, see the *User Guide for Cisco License Manager* at this URL: http://www.cisco.com/en/US/products/ps7138/products_user_guide_list.html .

Software End-User License Agreement

As part of the licensing process, you must accept terms and conditions set forth in the end-user license agreement. You implicitly accept the agreement when you first use a new device. However, you must explicitly accept the agreement before a feature set can be activated for evaluation and extension temporary licenses.

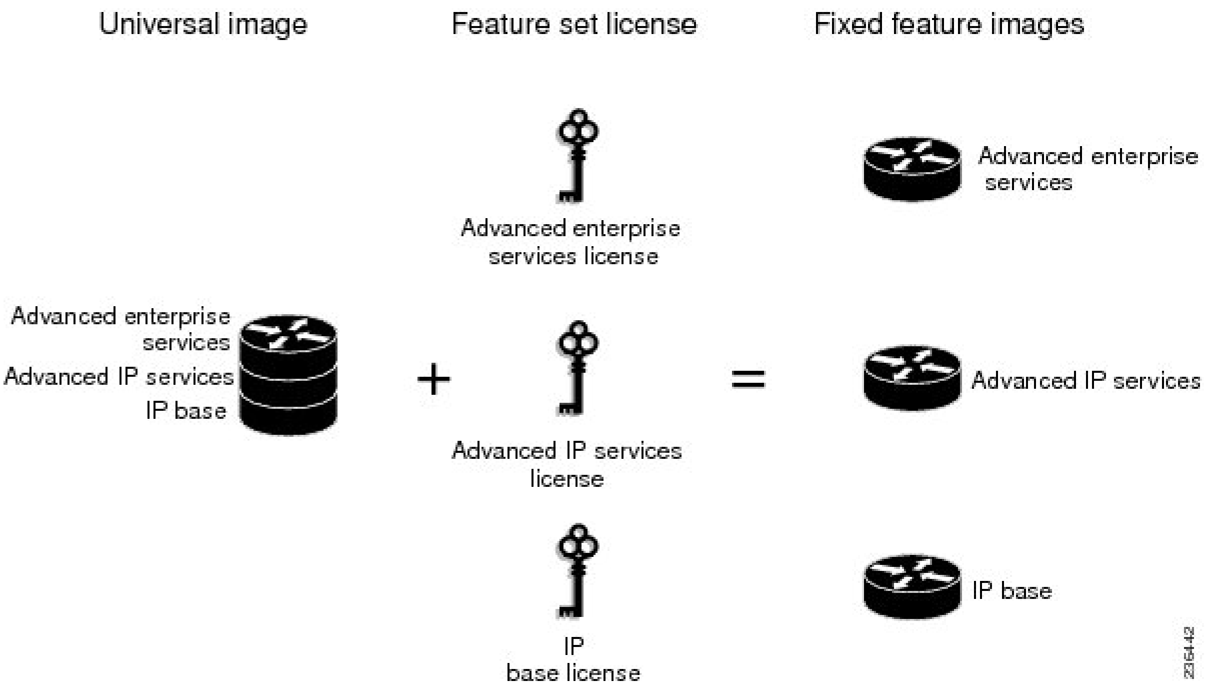
You can read the terms and conditions of the end-user license agreement at this URL: http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.html .

License Models for Images and Features

Cisco IOS Universal Image-Based Licenses

The Cisco IOS universal image contains *all* fixed feature images in one image. You can access the required functionality based on the license installed on the device. A higher-level feature-set license inherits the content of the lower-level feature sets it contains. The figure below shows an example of the feature sets and fixed feature images that can make the universal image.

Figure 1: Example of Universal Image Components



A platform can have a single universal image, which is a superset of all fixed feature images. Fixed feature images are an older packaging form in which the image contains only part of a systems capabilities. The fixed feature images supported by platform are predetermined and vary between platforms. A particular fixed feature image functionality is enabled based on license availability.

The software packaging simplifies the image selection process by consolidating the total number of packages and by using consistent package names across all hardware products.

The image-based license is used to help bring up all the subsystems that correspond to the image-level license that you purchase. Image licenses are enforced only during boot time.

The feature sets available for upgrading Cisco devices are listed on the Cisco IOS Software Packaging web page at this URL: http://www.cisco.com/en/US/products/sw/iosswrel/ps5460/index.html.

Feature-Based Licenses

Once the image-based license is used and the appropriate subsystems are activated, individual feature licenses are used to activate individual features.

License keys enable or disable individual features. Features check for their licenses before enabling themselves and adjust their behavior based on the following:

- Activation of a permanent license
- Expiration of a time-limited evaluation license

- Validity of a subscription license

License Types

Permanent Licenses

Permanent licenses are perpetual; that is, no usage period is associated with them. Once permanent licenses are installed, they provide all the permissions needed to access features in the software image. All permanent licenses are node locked and validated by the Cisco licensing infrastructure during software installation. Once a permanent license is installed, you do not need to upgrade for subsequent releases.

Cisco manufacturing preinstalls the appropriate permanent license on the ordered device for the purchased feature set. No customer interaction with the software activation processes is required to enable a license on new hardware.

Temporary Licenses

Temporary licenses are limited to a specific usage period (for example, 60 days). You must accept the end-user license agreement before the temporary licenses can be activated.

There are three types of temporary licenses: those embedded in Cisco images, evaluation licenses obtained from the Cisco Product License Registration portal, and extension licenses that are obtained from the Cisco Technical Assistant Center (TAC).

Although the embedded license can also be used for evaluation purposes, we recommend that you use the embedded license for emergency use only and obtain an evaluation license from the self-serve Cisco Product Licensing Registration portal.

These sections further define the types of temporary licenses:

Built-in Licenses for Emergencies

To avoid network downtime in the event of device failure and if the replaced device does not have the same licenses as the failed device, you can use a built-in license (an evaluation license) in the software image. Using it ensures that you can configure the needed features without requiring a license key. However, you must still accept an end-user license agreement and must acknowledge that there is a 60-day usage limit for this type of license.

Note You must go to the Cisco Product License Registration portal to obtain a permanent RMA replacement license.

Evaluation Licenses

Evaluation licenses are also temporary, and you use them to evaluate a feature set on new hardware.

You obtain evaluation licenses from the Cisco licensing portal: Licensing Portal for Demo Licenses

Note You must go to the Cisco Product License Registration portal prior to the expiration of the evaluation license to upgrade the license status.

Extension Licenses

When the time allowed for an evaluation licenses expires, you can work with TAC to obtain an extension license. Similar to an evaluation license, extension licenses are node locked and valid for a specific period (for example, 60 days) based on usage.

Note You must obtain approval to use an extension license.

Uncounted or Counted Licenses

Feature-based licenses are either uncounted licenses or counted licenses. Uncounted licenses do not have any count. Counted licenses have an attribute to fulfill for a certain number of counts. In other words, a count is associated with them that indicates the instances of that feature available for use in the system.

Pay as You Grow Model

The pay-as-you-grow model allows you to upgrade your hardware and software capacity by using a license key. You need not complete an RMA to add new hardware. You can purchase the upgrade, have it electronically delivered, and use the license key to enable increased capacity. The Cisco wireless controller is one example in which you can dynamically increase to 12, 25, 50, 100, or 250 access points for wireless services.

Subscription Licenses

The subscription license provides software enforcement for licensed features for a calendar period.

These node-locked license types are supported in a subscription license:

- Evaluation subscription license
- Extension subscription license
- Paid subscription license

Software Activation Processes

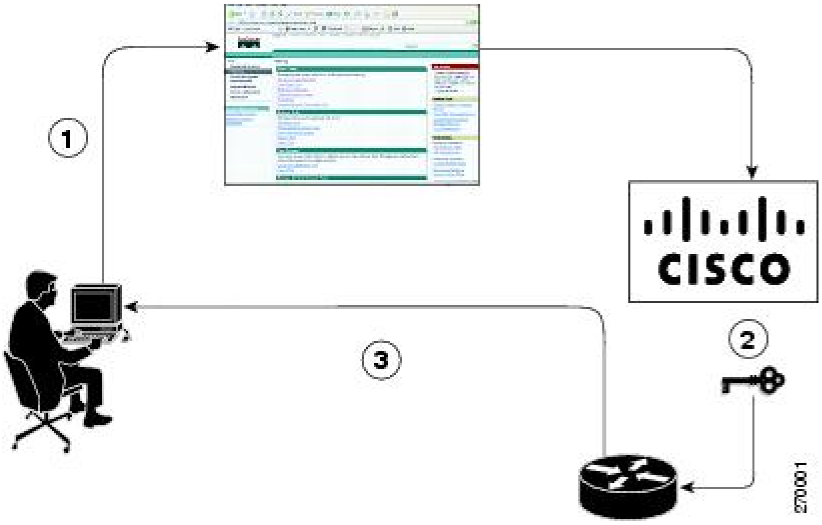
Software activation enables the various feature sets on a device by using license keys.

Note You can apply feature or maintenance upgrades to the software at any time. Maintenance upgrades do not require any interaction with the software activation process.

Manufacturing Preinstalled Licenses

The figure below shows the overall license work flow for manufacturing preinstalled licenses.

Figure 2: Manufacturing Preinstalled License Work Flow



The work flow for manufacturing preinstalled licensing involves these steps:

1. You place an order for a Cisco device through the Cisco sales ordering tool.
2. Manufacturing information technology systems pick up the order information and build the device. Manufacturing also retrieves a license key for the device being assembled by contacting a license server and then installing the code on the device. The device is shipped to you.
3. You install and configure the device, and place the device in production. There is no requirement to activate or register the software prior to use. A new device is ready for deployment upon receipt.

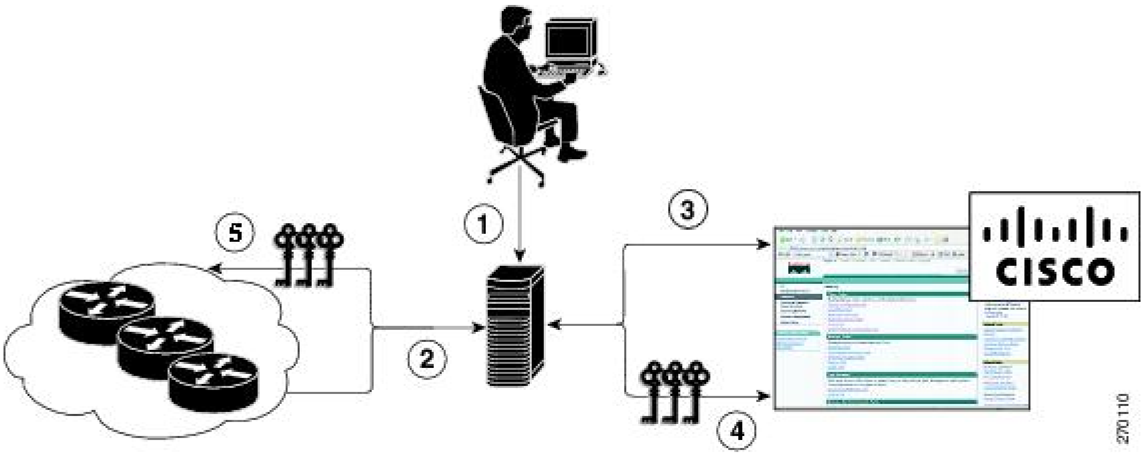
Automated Software Activation by Using Cisco License Manager

Cisco License Manager transparently interacts with the Cisco Product Licensing Registration portal for many devices. With the Cisco License Manager application deployed, you can automate many of the steps for upgrading and registering software licenses. For example, you can enter the PAK and select the device on which to install the license.

For a network-wide deployment, the Cisco License Manager can automate all license-related work flows by securely communicating to the licensing back-end fulfillment systems at Cisco.com and by deploying the obtained licenses to managed devices on a network-wide basis. The application also keeps an inventory of deployed licenses and generates license reports.

The figure below shows the license upgrade work flow for automated upgrades through Cisco License Manager.

Figure 3: License Upgrade Work Flow for Automated Upgrades through Cisco License Manager



The workflow for license upgrades for automated license transfers involves these steps:

1. Cisco License Manager identifies the source and destination devices and stock keeping units (SKUs) to transfer.
2. Cisco License Manager automatically determines the device credentials of the source device.
3. Cisco License Manager automatically communicates with Cisco.com to obtain the permissions ticket, which is used to start the rehost process. It applies the permissions ticket to the source device to obtain the rehost ticket.
4. Cisco License Manager automatically sends the rehost ticket along with the destination device UDI to automatically obtain the license keys from the Cisco Product Licensing Registration portal.
5. Cisco License Manager automatically installs the license key on the destination device.

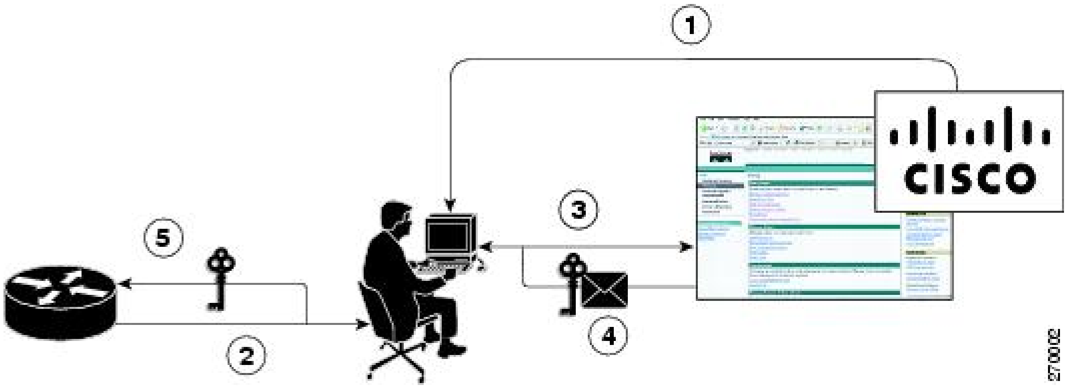
For more information, see the *User Guide for Cisco License Manager* at http://www.cisco.com/en/US/products/ps7138/products_user_guide_list.html.

License Software Activation by Using EXEC Commands

You install the license by using Cisco EXEC commands after receiving your license key electronically through e-mail or through paper and mail delivery.

The figure below shows the license upgrade process work flow for manual license fulfillment.

Figure 4: License Upgrade Work Flow for Manual License Fulfillment



The license upgrade process work flow for manual license fulfillment involves these steps:

1 You purchase the required PAKs for the desired type of license. Some licenses do not require a PAK, but they might need a contract instead.

2 You obtain the UDI from the device.

3 You enter the UDI and PAK into the Cisco Product License Registration portal. If it is a contract license, follow the links to non-PAK-based licenses and submit the UDI of the device.

4 The portal retrieves the SKUs associated with the PAK. You then select the SKU and enter the UDI, a unique and unchangeable identifier of the device where the license should be installed. A license key is then e-mailed to you, and you use that key to install the license.

5 You install the license file returned from the license portal to the device by using the CLI.

License Transfer Between Devices

Cisco supports two scenarios to transfer licenses between devices:

1 The first scenario has both the source and destination devices active and functional. In this scenario, the license is revoked on the source device, and a new permanent license is issued for the destination device.

2 The second is a failure scenario in which one of the devices is unavailable. In this scenario, the license from the failed device is transferred to the RMA or to the replaced device by using the RMA License Transfer process on the Cisco Product License Registration portal.

These scenarios are described in the following sections:

License Transfer Between Two Working Devices

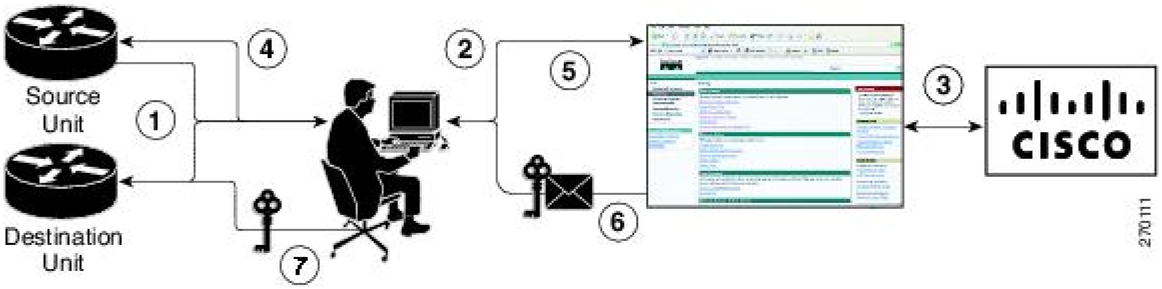
Cisco supports fully automated, customer-initiated, no-questions-asked transfer of licenses. Transferring a license between two working devices is accomplished by using a process known as *rehosting*. The rehosting process transfers a license from one UDI to another by revoking the license from the source device and installing it on a new device.

You perform a license transfer (rehosting) by using one of the following:

- Cisco Product License Registration portal
- Cisco IOS License Call Home commands
- Cisco License Manager application

The figure below shows the processes involved for rehosting (transferring) a license.

Figure 5: License Transfer Work Flow



The following summary is for a license transfer process by using the Cisco Product License Registration portal:

1. You obtain the UDI and device credentials from the source and destination devices by using the CLI.
2. You contact the Product License Registration page on Cisco.com, and you enter the source device credentials and the UDI into the license transfer portal tool.
3. The portal displays licenses that can be transferred from the source device.
4. Select the licenses that need to be transferred. A permission ticked is issued. You can use this permission ticket to start the rehost process by using the CLI.
5. You apply the permissions ticket to the source device by using the **license revoke** command. The source device then provides a rehost ticket indicating proof of revocation. A 60-day grace period license is also installed on the device to allow enough time to transfer the licenses to the destination device.
6. You enter the rehost ticket into the license transfer portal tool on Cisco.com along with the destination device UDI.
7. You receive the license key through e-mail.
8. You install the license key on the destination device.

After you execute the **license call-home resend** command, the source device contacts the Cisco Product License Registration portal and obtains a license key for the destination device after revoking it from the source device. The license key stored on the source device can then be installed on the destination device to complete the transfer.

By using Cisco License Manager, you can select the source and destination devices from a GUI wizard for automated processing.

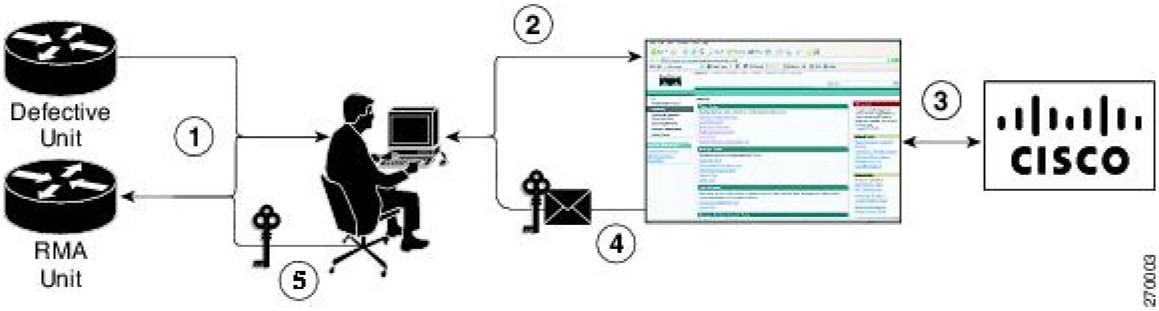
RMA License Transfer Between a Failed and a Working Device

Before you can transfer a software license from a failed device to a new device, you must enter UDI information from both devices into the Cisco Product License Registration portal. The portal issues the RMA replacement licenses (http://www.cisco.com/go/license).

If you need assistance to obtain a license, contact Cisco technical support at: http://www.cisco.com/cisco/web/support/index.html .

The figure below shows the license transfer work flow for RMA replacement licenses.

Figure 6: License Transfer Work Flow for RMA Replacement Licenses



The RMA replacement license process involves these steps:

1. You obtain the UDI of the defective and RMA devices.
2. You enter the UDI into the RMA license portal tool on Cisco.com.
3. The license portal determines licenses associated with the defective device.
4. The license portal issues replacement licenses.
5. You install the new license on the new device.

License Resend Request

If an original license is lost or misplaced, you can enter EXEC commands to request that all licenses for a specific UDI be re-sent. The command also stores the received license lines in a location that you specify.

Cisco License Manager also allows you to perform this function with an easy-to-use GUI.

Note You must have Internet access to place a license resend request.

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Master Commands List, All Releases
Software activation commands	*Software Activation Command Reference*
Software activation configuration	"Configuring the Cisco IOS Software Activation Feature" module

MIBs

MIB	MIBs Link
CISCO-LICENSE-MGMT-MIB	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use the Cisco MIB Locator at this URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Cisco IOS Software Activation

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1: Feature Information for Cisco IOS Software Activation

Feature Name	Releases	Feature Information
Cisco IOS Software Activation	12.4(15)XZ 12.4(20)T 15.0(1)M	The Cisco IOS Software Activation feature supports basic licensing processes. This feature is platform-independent. This feature module provides information about Cisco Software Activation: • "Configuring the Cisco IOS Software Activation Feature" module

Glossary

Cisco License Manager —Software tool that provides a GUI to track and manage licenses.

license file —File generated by Cisco licensing tools, which is used to install a license on a product. The license file contains of one or more license lines.

license key —A unique value that enables usage and entitlement for a set of Cisco software features.

license line —Characters arranged in a particular format that hold the license for a single feature within it. A line has all the necessary fields and attributes that make it a valid, tamperproof, and complete license. A single line can exist independently.

license manager —An application used to track and manage licenses for customers.

license server —Software tool at the hardware manufacturing site that generates product licenses.

license storage —File that stores a collection of license lines. A license file exists on a licensed device. This file exists in permanent storage.

node locked —The explicit binding of a unique license to a unique hardware platform. Node-locked licenses are locked to one of the UDIs in the system. Non-node locked licenses are not locked to any UDI.

PAK —Product authorization key, which is provided to you when you order and purchase the right to use a feature set for a particular platform. The PAK serves as a receipt and is used as part of the process to obtain a license.

permission ticket file —File generated by Cisco licensing that is used to get a rehost ticket during a manual rehosting process. The permission ticket file contains one or more adding and removing license operations for rehosting.

perpetual license —License where use rights are permanent. These licenses can be used as long as required.

persistence storage —File that lives for the lifetime of the device that has a license and survives image changes. This file should exist in a write once storage area. The persistence file holds the license history for that device, along with certain information about license removals, expiries, rehost, and so on.

rehost —Process where a valid license is transferred from one platform to another. This implies the license is no longer valid on the original platform.

removable storage —Portable device such as compact flash or USB used to store and access data.

RMA —Return Merchandise Authorization, which is the process whereby you can return a defective product.

signature server —Generates the licenses for products and is found at Cisco manufacturing sites. Also called a permission file generator.

SKU —Stock keeping unit. A unique, individual part number used to track and monitor inventory. A Cisco software licensing SKU maps to one or more software features.

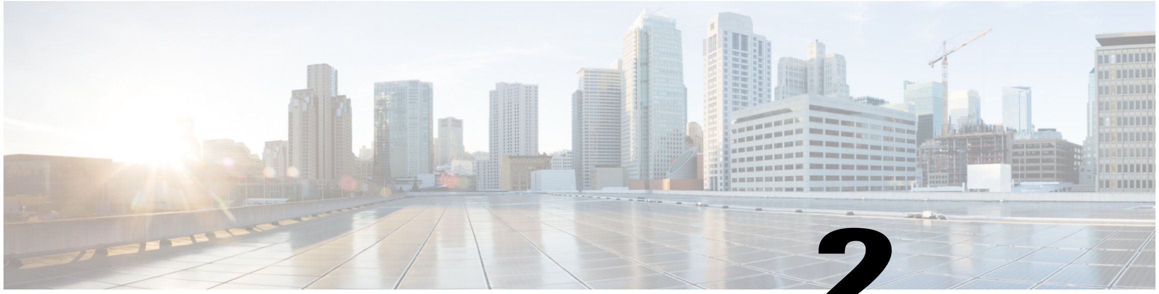
stack —A switch stack is a set of up to nine Catalyst 3750 switches connected through their StackWise ports.

subscription-based licenses —Time-based license that requires the subscriber to periodically renew or the license will expire after an agreed-upon time.

SWIFT —Software Infrastructure and Fulfillment Technology. The Cisco licensing infrastructure that is accessed through HTTPS over the Internet. The Cisco License Manager application interacts with the Cisco licensing infrastructure on behalf of many devices. You can interact directly with the Cisco licensing infrastructure service by using Cisco software commands.

UDI —Unique device identifier, which is a Cisco-wide schema to identify products. The UDI contains a product ID, version ID, and a serial number. The UDI does not change during deployment in the field. Note that when the term UDI is used in the context of licensing, it typically refers to only the product ID and serial number.

universal image —A single software image containing all Cisco functionality levels. These levels can be enabled by installing the appropriate license.



CHAPTER 2

Configuring the Cisco IOS Software Activation Feature

This document describes the tasks used to activate software by using the Cisco IOS Software Activation feature, license keys, and Cisco EXEC commands. When you activate software from a Cisco device, you can license software without the need for additional application software.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions for Cisco IOS Software Activation

Not all Cisco hardware platforms can use the Cisco IOS Software Activation feature. Use the Cisco Feature Navigator at http://www.cisco.com/go/cfn and the table in the Feature Information for Cisco IOS Software Activation section to determine which platforms and images support the Cisco IOS Software Activation feature.

For the stackable switches that support the Cisco IOS Software Activation feature, one switch must act as primary and the others as secondaries. The primary switch performs management and administrative operations on itself as well as on the secondary switches.

Information About the Cisco IOS Software Activation

License Activation MIB Support

The Cisco IOS Software Activation feature introduces the CISCO-LICENSE-MGMT-MIB to allow SNMP-based license management and administrative tasks. A description of this MIB can be found by using tools at this URL: http://tools.cisco.com/ITDIT/MIBS/servlet/index

Use the MIB Locator tool and the Search for MIB selection box to select CISCO-LICENSE-MGMT-MIB .

The unique device identifier (UDI) is also associated with the Entity Name and Product Description data elements for the management information base (MIB) system. The MIB nomenclature for Entity Name is entPhysicalName and for Product Description is entPhysicalDescr.

How to Activate Software from a Cisco IOS Device

Installing and Upgrading Licenses by Using Software Activation Commands

Before You Begin

Read and understand the license activation process concepts in the in the “Cisco IOS Software Activation Conceptual Overview” module.

To install or upgrade a license by using the **license install** command, you must have already received the license file from the Cisco Product License Registration portal at http://www.cisco.com/go/license (or you already backed up the license by using the **license save** command).

If you use Microsoft Entourage and receive the license file from Cisco in an e-mail attachment, the license file will contain UTF-8 marking. These extra bytes in the license file cause it to be unusable during license installation. To work around this issue, you can use a text editor to remove the extra characters and then install the license file. For more information about UTF-8 encoding, go to this URL: http://www.w3.org/International/questions/qa-utf8-bom.

Note The installation process does not install duplicate licenses. This message appears when duplicate licenses are detected:

```
Installing...Feature:xxx-xxx-xxx...Skipped:Duplicate
```

Note A standby device reboots twice when there is a mismatch of licenses.

SUMMARY STEPS

1. Obtain the PAK.
2. **enable**
3. **show license udi**
4. Convert the PAK to a license by entering the PAK and the UDI into the Cisco Product License Registration portal: http://www.cisco.com/go/license.
5. **license install** *stored-location-url*
6. **configure terminal**
7. **license boot level** {**metroaggrservices**}
8. **write memory**
9. **reload**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Obtain the PAK.	The PAK is provided to you when you order or purchase the right to use a feature set for a particular platform. • The PAK serves as a receipt and is used as part of the process to obtain a license.
Step 2	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 3	**show license udi** **Example:** `Device# show license udi`	Displays all the UDI values that can be licensed in a system. • You need the UDI of the device as part of the process to obtain a license.
Step 4	Convert the PAK to a license by entering the PAK and the UDI into the Cisco Product License Registration portal: http://www.cisco.com/go/license.	After entering the appropriate information, you will receive an e-mail containing the license information that you can use to install the license: • Copy the license file received from the Cisco Product License Registration portal to the appropriate file system on the device. or • Click the **Install** button on the web page.
Step 5	**license install** *stored-location-url*	Installs the license.

	Command or Action	Purpose
	Example: `Device# license install tftp://infra-sun/<user>/license/5400/38a.lic`	• Accept the end-user license agreement if prompted.
Step 6	**configure terminal** **Example:** `Device# configure terminal`	Enters the global configuration mode.

Step 7	**license boot level** {**metroaggrservices**}
	Example:
	`Device(config)# license boot level metroaggrservices`
		Activates the metroaggrservices license on the device upon the next reload.

Step 8	**write memory** **Example:** `Device# write memory`	Saves the running configuration to NVRAM.
Step 9	**reload** **Example:** `Device# reload`	(Optional) Restarts the device to enable the new feature set. **Note** A reload is not required when moving from an evaluation license to a permanent license of the same license level on ASR 903 routers.

Managing Licenses by Using Software Activation Commands

Adding a Comment to a License File

SUMMARY STEPS

1. **enable**
2. **license comment add** *feature-name comment* [**switch** *switch-num*]
3. **show license file** [**switch** *switch-num*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**license comment add** *feature-name comment* [**switch** *switch-num*] **Example:** `Device# license comment add gsmamrnb-codec-pack “Use this permanent license”`	Adds or deletes information about a specific license. • (Only on Cisco Catalyst 3750-E switch platforms) If a switch number is specified, this command is executed on the specified switch. • When the license is present in license storage and multiple license lines are stored, you are prompted to select a license line. To select the license, type the number at the Select Index to Add Comment prompt.
Step 3	**show license file** [**switch** *switch-num*] **Example:** `Device# show license file`	Displays comments added to a Cisco software license file. • If the device is a switch, this command obtains statistics from the specified switch.

Saving All Licenses to a Specified Storage Area

SUMMARY STEPS

1. **enable**
2. **license save** *file-sys://lic-location* [**switch** *switch-num*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**license save** *file-sys://lic-location* [**switch** *switch-num*] **Example:** `Device# license save flash:all_licenses.lic`	Saves copies of all licenses in a device and stores them in a format required by the command in the specified storage location. Saved licenses are restored by using the **license install** command. • *lic-location* : The license storage location can be a directory or a URL that points to a file system. Use the **?** command to see the storage locations supported by your device. • (Optional) **switch** *switch-num*: sends this request to a specific switch in a switch stack.

Saving License Credential Information Associated with a Device to a Specified Storage Area

Before You Begin

Before you can start the rehost or resend process, a device credential is required. Cisco software licensing requires that the license files generated by the Cisco back-end licensing system for its devices be secure and tamper-resistant. Security features are in place to authenticate a license by means of encrypted license credentials. If it becomes necessary to transfer a license from one device to another (which is called rehosting), a permission ticket is required. To generate the permission ticket, the Cisco back-end licensing system requires the device credential information.

SUMMARY STEPS

1. **enable**
2. **license save credential** *file-sys://lic-location* [**switch** *switch-num*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**license save credential** *file-sys://lic-location* [**switch** *switch-num*] **Example:** `Device# license save credential flash:cred.lic`	Saves credential information associated with a device to a specified URL. • *lic-location* : The license storage location can be a directory or a URL that points to a file system. Use the **?** command to see the storage locations supported by your device. • (Optional)**switch** *switch-num*: sends this request to a specific switch in a switch stack.

	Command or Action	Purpose

Displaying All Licenses in a Device

SUMMARY STEPS

1. **enable**
2. **show license all**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show license all** **Example:** `Device# show license all`	Displays information about all licenses in the device.

Displaying Detailed Information about Licensed Features

SUMMARY STEPS

1. **enable**
2. **show license detail** [*feature-name*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**show license detail** [*feature-name*] **Example:** `Device# show license detail`	Displays detailed information about all licensed features or the specified licensed feature.

Displaying Licensed Feature Sets Available in an Image

SUMMARY STEPS

1. **enable**
2. **show license feature**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show license feature** **Example:** `Device# show license feature`	Displays a list of licensed features available in an image.

Removing Licenses by Using Software Activation Commands

Removing a License Entry from a Permanent License File

Note

- The **license clear** command lists all licenses, but some licenses, such as built-in licenses, cannot be cleared.
- Only licenses that have been added by using the **license install** command are removed. Evaluation licenses are not removed.
- If a license is not in use, the **license clear** command displays all the licenses related to this feature and prompts you to make a selection. Different prompts are displayed, depending upon whether single or multiple licenses are available in the device. The selected licenses are removed from the device.
- If a license is in use, the **license clear** command might fail. However, depending on the application policy using the license, some licenses might be cleared.
- When a switch is specified, the **license clear** command is issued on that switch. When a mixed stack platform is used, the primary switch must have installed the minimum licensing features required to support the licensing operations of the secondary switches. When this command is issued from a primary switch, the switch number is required to clear a license on that switch.

SUMMARY STEPS

1. **enable**
2. **license clear** *feature-name* [**switch** *switch-num*]
3. **show license detail**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**license clear** *feature-name* [**switch** *switch-num*] **Example:** `Device# license clear gsmamrnb-codec-pack`	Removes a license entry from license storage once it has been verified that the license line is valid and was explicitly installed. • The optional **switch** *switch-num* keyword and argument send this request to a specific switch in a switch stack. • You must select the index number of the license to clear. Enter the number at the Select Index to Clear prompt.

	Command or Action	Purpose
Step 3	**show license detail** **Example:** `Device# show license detail`	Verifies that the license has been cleared.

Rehosting (Revoking and Transferring) a License

Before You Begin

Read and understand the license transfer between devices concepts in the "Cisco IOS Software Activation Conceptual Overview" module.

Cisco software licensing requires that the license files generated by the Cisco back-end licensing system for its devices be secure and tamper-resistant. Security features are in place to authenticate a license by means of encrypted license credentials. Rehosting requires a permission ticket. To generate the permission ticket, the Cisco back-end licensing system requires the device credential information. Use the **license save credential** command to save device credential information to a specified file system.

SUMMARY STEPS

1. **enable**
2. **license revoke revoke** *permission-file-url output-rehost-ticket-url*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**license revoke revoke** *permission-file-url output-rehost-ticket-url* **Example:** `Device# license revoke tftp://infra-sun/ramanp/pt.lic flash:rt.lic`	Revokes and transfers a license by using the permission ticket provided by the Cisco back-end licensing system. It removes the original, permanent license from the device and provides a license for the new device. • An end-user license agreement is displayed for all grace-period licenses in the permission ticket. • You must read and accept the agreement. If you do not accept the agreement, the rehost operation stops.

Troubleshooting License Operations by Using Software Activation Commands

SUMMARY STEPS

1. **enable**
2. **show license file** [**switch** *switch-num*]
3. **show license statistics**
4. **show license status** [**switch** *switch-num*]
5. **debug license** {**all** | **core** | **errors** | **events**}
6. **no debug license** {**all** | **core** | **errors** | **events**}

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show license file** [**switch** *switch-num*] **Example:** `Device# show license file`	Displays license entries and license details stored in a Cisco software license file. If the device is a switch, this command obtains statistics from the specified switch.
Step 3	**show license statistics** **Example:** `Device# show license statistics`	Displays license statistics information. The display includes relevant statistics for error counts and is useful for troubleshooting licensing-related problems.
Step 4	**show license status** [**switch** *switch-num*] **Example:** `Device# show license status`	Displays the status of licenses in the system. If the device is a switch, this command obtains status from the specified switch.

Step 5	**debug license** {**all** | **core** | **errors** | **events**}
	Example:
	`Device# debug license errors`
		Enables controlled software license debugging activity on a device.

Step 6	**no debug license** {**all** | **core** | **errors** | **events**}
	Example:
	`Device# no debug license errors`
		Disables license debugging activity on a device.

Configuring Examples for Software Licensing

Example: Installing and Upgrading Licenses

The following example shows how to use the **license install** command to install a license saved in TFTP on the device. The display is truncated for easier readability:

```
Device# license install tftp://infra-sun/<user>/license/5400/38a.lic
Installing licenses from "tftp://infra-sun/<user>/license/5400/38a.lic"
Loading <user>/license/5400/38a.lic from 172.19.211.47 (via GigabitEthernet0/0): !
[OK - 1192 bytes]
Extension licenses are being installed in the device with UDI "AS54XM-AC-RPS:JAE0948QXKD"
for the following features:
 Feature Name: gsmamrnb-codec-pack
PLEASE  READ THE  FOLLOWING TERMS  CAREFULLY. . .
ACCEPT? [yes/no]: yes
Issue 'license feature gsmamrnb-codec-pack' command to enable the license
Installing...Feature:gsmamrnb-codec-pack...Successful:Supported
```

Example: Adding a Comment to a License File

The following example shows how to use the **license comment** command to add or delete information about a specific license. The command checks that a license associated with the specified feature is present in license storage. If a switch number is specified, this command is executed on the specified switch.

As the example shows, when the license is present and multiple license lines are stored, you are prompted to select a license line. This action helps to distinguish licenses. Type the number at the Select Index to Add Comment prompt to select the license.

```
Device# license comment add gsmamrnb-codec-pack “Use this permanent license”
Feature: gsmamrnb-codec-pack
    1  License Type: Evaluation
 License State: Inactive
     Evaluation total period: 20 hours 0  minute
     Evaluation period left: 20 hours 0  minute
 License Addition: Additive
 Comment:
 Store Index: 0
 Store Name: Primary License Storage
    2  License Type: Permanent
 License State: Active, Not in Use
 License Addition: Exclusive
 Comment:
 Store Index: 1
 Store Name: Primary License Storage
Select Index to Add Comment [1-2]: 2
% Success: Adding comment "Use this permanent license" succeeded
Device# show license file
License Store: Primary License Storage
  Store Index: 0
    License: 11 gsmamrnb-codec-pack 1.0 LONG TRIAL DISABLED 20 DISABLED STANDA
             LONE ADD INFINITE_KEYS INFINITE_KEYS NEVER NEVER NiL SLM_CODE CL_
             ND_LCK NiL *1YCHJRBMWKZAED2400 NiL NiL NiL 5_MINS <UDI><PID>AS54X
             M-AC-RPS</PID><SN>JAE0948QXKD</SN></UDI> ,Jx8qaVf:iXWaH9PsXjkVnmz
             7gWh:cxdf9nUkzY6o8fRuQbu,7wTUz237Cz6g9VjfrCk,0a2Pdo,Ow6LWxcCRFL:x
             cTxwnffn9i,4,aUWv8rL50opDUdAsFnxLsvoFRkcAfm$<WLC>AQEBIQAB//9NA+1m
             Uwfs/lD0dmdF9kyX8wDrua1TZhnnAy6Mxs1dTboIcRaahKxJJdj4Oi1w3wscqvPiA
             mWSaEmUT56rstk6gvmj+EQKRfD9A0ime1czrdKxfILT0LaXT416nwmfp92Tya6vIQ
             4FnlBdqJ1sMzXeSq8PmVcTU9A4o9hil9vKur8N9F885D9GVF0bJHciT5M=</WLC>
    Comment: Use this permanent license.
       Hash: E1WjIQo4qsl9g8cpnpoogP/0DeY=
Device#
```

Example: Saving All Licenses to a Specified Storage Area

The following example shows how to use the **license save** command to save copies of all licenses to the flash file system:

```
Device# license save flash:all_licenses.lic
license lines saved ..... to flash:all_licenses.lic
```

Example: Removing Licenses

The following examples shows how to use the **license clear** command to remove a license entry from license storage once it has been verified that the license line is valid and was explicitly installed.

You must select the index number of the license to clear. Type the number at the Select Index to Clear prompt as shown in this example.

```
Device# license clear standard
Feature: standard
    1  License Type: Evaluation
 License State: Inactive
     Evaluation total period: 20 hours 0  minute
     Evaluation period left: 20 hours 0  minute
 License Addition: Additive
 Comment:
 Store Index: 0
 Store Name: Primary License Storage
    2  License Type: Permanent
 License State: Active, Not in Use
 License Addition: Exclusive
 Comment:
 Store Index: 1
 Store Name: Primary License Storage
Select Index to Clear [1-2]: 1
Are you sure you want to clear? (yes/[no]): yes
Device# show license detail
Feature: premium                Period left:  1 hour   0 minute
Index:  1       Feature: premium                           Version: 1.0
        License Type: Evaluation
        License State: Active, Not in Use, EULA not accepted
            Evaluation total period:  1 hour   0 minute
            Evaluation period left:  1 hour   0 minute
        License Count: Non-Counted
        License Priority: None
        Store Index: 0
        Store Name: Evaluation License Storage
```

Example: Rehosting (Revoking and Transferring) a License

The following example shows how to use the **license revoke** command to revoke a license stored in TFTP and how to transfer it to a license stored in flash memory. You might need to read and accept the terms and conditions of the license type being transferred. The following example is truncated for readability:

```
Device# license revoke tftp://infra-sun/ramanp/pt.lic flash:rt.lic
Following Permanent license(s) will be revoked from this device
 Feature Name: gsmamrnb-codec-pack
Following Extension license(s) will be installed in this device
 Feature Name: gsmamrnb-codec-pack
PLEASE  READ THE  FOLLOWING TERMS  CAREFULLY. . .
ACCEPT? [yes/no]: yes
Issue 'license feature gsmamrnb-codec-pack' command to enable the license
Rehost ticket saved ..... to flash:rt.lic
```

Example: Generic Command Enhanced with Licensing Information

The generic commands described in the following sections are enhanced with licensing information:

reload

The **reload** command shows the expired licenses, followed by expiring licenses sorted by the period left and end date:

```
Device# reload
The following license(s) are expiring or have expired.
Features with expired licenses may not work after Reload.
Feature: uc,Status: expiring, Period Left: 7  wks 5  days
Proceed with reload? [confirm]
```

show running-config

The **show running-config** command displays the unique device identifier (UDI) of a device. If the configuration file was copied from a different device, a warning is displayed upon reload. A UDI mismatch warning is also displayed during reload if the startup-config file has a different UDI than the platform UDI.

```
Device# show running-config
Building configuration...
Current configuration : 4772 bytes
!
version 12.4
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service internal
!
hostname csl-xfr-enhance-2951
!
...
...
license udi pid CISCO2951 sn FHH1211P037
license boot module c2951 technology-package securityk9 disable
license boot module c2951 technology-package uc
license boot module c2951 technology-package data
license call-home url https://tools-stage.cisco.com/SWIFT/Licensing
license agent listener http plaintext /lic-agent authenticate none
!
!
archive
 log config
  hidekeys
!
.
.
.
```

show tech-support

The **show tech-support** command displays the output of the **show license udi**, **show license file**, **show license detail**, **show license status**, and the **show license statistics** commands.

```
Device# show tech-support
------------------ show license udi ------------------
Device#   PID                   SN              UDI
-----------------------------------------------------------------------------
*0        CISCO2951             FHH1211P037     CISCO2951:FHH1211P037
------------------ show license feature ------------------
Feature name             Enforcement  Evaluation  Subscription   Enabled
ipbasek9                 no           no          no             no
securityk9               yes          yes         no             no
uc                       yes          yes         no             yes
data                     yes          yes         no             no
gatekeeper               yes          yes         no             no
LI                       yes          no          no             no
SSL_VPN                  yes          yes         no             no
ios-ips-update           yes          yes         yes            no
SNASw                    yes          yes         no             no
------------------ show license file ------------------
License Store: Primary License Storage
License Store: Evaluation License Storage
  Store Index: 0
    License: 11 securityk9 1.0 LONG TRIAL DISABLED 1440 DISABLED STANDALONE AD
             D INFINITE_KEYS INFINITE_KEYS NEVER NEVER NiL SLM_CODE DEMO NiL N
             iL Ni NiL NiL 5_MINS NiL GT5YVbrMAdt0NY50UcKGfvLTjQ17P2o3g84hE8Tq
             sOfu3Xph0N:2AmMdpMNxxKXSVG$<WLC>AQEBIQAB//+FugzZgqFJn/XhIxoyelg63
             YJD++i6Qx6vVp0MVqrX2EinbufbTfGzc7/GHNZaDZqRqwInXo3s+nsLU7rOtdOxoI
             xYZAo3LYmUJ+MFzsqlhKoJVlPyEvQ8H21MNUjVbhoN0gyIWsyiJaM8AQIkVBQFzhr
             10GYolVzdzfJfEPQIx6tZ++/Vtc/q3SF/5Ko8XCY=</WLC>
    Comment:
       Hash: CLWUVZgY84BMRTO3JIlYmIqwAQA=
------------------ show license detail ------------------
Index: 1        Feature: SNASw                            Version: 1.0
        License Type: Evaluation
        License State: Active, Not in Use, EULA not accepted
            Evaluation total period: 8  weeks 4  days
            Evaluation period left: 8  weeks 4  days
        Lock type: Non Node locked
        Vendor info:
        License Addition: Additive
        License Generation version: 0x8100000
        License Count: Non-Counted
        License Priority: None
        Store Index: 5
        Store Name: Evaluation License Storage
------------------ show license status ------------------
                License Type Supported
        permanent               Non-expiring node locked license
        extension               Expiring node locked license
        evaluation              Expiring non node locked license
        paid subscription       Expiring node locked subscription license
                                with valid end date
        extension subscription  Expiring node locked subscription license
        evaluation subscription Expiring node locked subscription license
...
```

```
...
------------------ show license statistics ------------------
                Administrative statistics
        Install success count:   0
        Install failure count:   0
        Install duplicate count: 0
        Comment add count:       0
        Comment delete count:    0
        Clear count:             0
        Save count:              0
        Save cred count:         1
                Client statistics
        Request success count:   1
        Request failure count:   3
        Release count:           0
        Global Notify count:     4
```

show version

The **show version** command displays the license UDI information:

```
Device> show version
Cisco IOS Software, C2951 Software (C2951-UNIVERSALK9-M), Experimental Version
12.4(20090326:052343)
 [rifu-xformers_3_25 130]
Copyright (c) 1986-2009 by Cisco Systems, Inc.
Compiled Thu 26-Mar-09 21:49 by rifu
ROM: System Bootstrap, Version 12.4(20090303:092436)
[BLD-xformers_dev.XFR_20090303-20090303_0101-53
 107], DEVELOPMENT SOFTWARE
csl-xfr-enhance-2951 uptime is 3 days, 4 hours, 28 minutes
System returned to ROM by reload at 18:48:45 PST Mon Nov 26 1956
System image file is "flash0:c2951-universalk9-mz.SSA"
Last reload reason: Reload Command
...
...
Cisco C2951 (revision 1.0) with 1005568K/43008K bytes of memory.
Processor board ID FHH1211P037
3 Gigabit Ethernet interfaces
1 terminal line
1 cisco Special Services Engine(s)
DRAM configuration is 72 bits wide with parity enabled.
255K bytes of non-volatile configuration memory.
250880K bytes of ATA System CompactFlash 0 (Read/Write)
License Info:
License UDI:
-------------------------------------------------
Device#   PID                   SN
-------------------------------------------------
*0        CISCO2951             FHH1211P037
Technology Package License Information for Module:'c2951'
----------------------------------------------------------------
Technology    Technology-package          Technology-package
              Current       Type          Next reboot
-----------------------------------------------------------------
ipbase        ipbasek9      None          ipbasek9
security      disable       None          disable
uc            uc            Evaluation    uc
data          None          None          None
Configuration register is 0x0
```

Additional References

Related Documents

Related Topic	Document Title
Cisco License Manager application	*User Guide for Cisco License Manager*
Software activation conceptual overview	"Cisco IOS Software Activation Conceptual Overview" module
Software activation commands	*Software Activation Command Reference*
Cisco IOS commands	Master Commands List, All Releases
Integrated Services Routers licensing	*Software Activation on Cisco Integrated Services Routers*

MIBs

MIB	MIBs Link
CISCO-LICENSE-MGMT-MIB	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

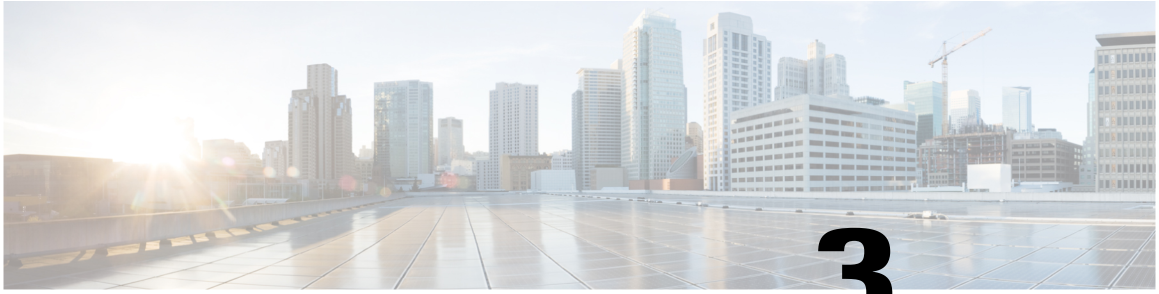
Feature Information for Cisco IOS Software Activation

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 2: Feature Information for Cisco IOS Software Activation

Feature Name	Releases	Feature Information
Cisco IOS Software Activation	12.4(15)XZ 12.4(20)T 15.0(1)M 15.4(1)S	Cisco IOS Software Activation EXEC commands support basic licensing processes. This feature is platform-independent. These commands were introduced or modified by this feature: **debug license**, **license clear**, **license comment**, **license install**, **license revoke**, **license save**, **license save credential**, **show license all**, **show license detail**, **show license feature**, **show license file**, **show license statistics**, **show license status**, **show license udi** In Cisco IOS Release 15.4(1)S, support was added for the Cisco ASR 901S series router.
CISL-SNMP support (MIB)	12.4(20)T 15.0(1)M	SNMP support for the CISCO-LICENSE-MGMT-MIB was added. These commands were introduced or modified by this feature: **snmp-server enable traps**, **snmp-server host**



CHAPTER 3

Configuring Call Home

The Call Home feature provides e-mail-based and web-based notification of critical system events. A versatile range of message formats are available for optimal compatibility with pager services, standard e-mail, or XML-based automated parsing applications. Common uses of this feature may include direct paging of a network support engineer, e-mail notification to a Network Operations Center, XML delivery to a support website, and utilization of Cisco Smart Call Home services for direct case generation with the Cisco Systems Technical Assistance Center (TAC).

This document describes how to configure the Call Home feature on Cisco ASR 1000 Series Aggregation Services Routers beginning with Cisco IOS XE Release 2.6.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Call Home

How you configure Call Home depends on how you intend to use the feature. Consider the following requirements before you configure Call Home:

- Obtain e-mail, phone, and street address information for the Call Home contact to be configured so that the receiver can determine the origin of messages received.
- Identify the name or IPv4 address of a primary Simple Mail Transfer Protocol (SMTP) server and any backup servers, if using e-mail message delivery.
- Verify IP connectivity from the router to the e-mail server(s) or the destination HTTP server.
- If Cisco Smart Call Home is used, an active service contract covering the device is required to provide full SCH service.

Information About Call Home

Call Home provides e-mail-based and web-based notification of critical system events. A versatile range of message formats are available for optimal compatibility with pager services, standard e-mail, or XML-based automated parsing applications. Common uses of this feature may include direct paging of a network support engineer, e-mail notification to a Network Operations Center, XML delivery to a support website, and utilization of Cisco Smart Call Home services for direct case generation with the Cisco Systems Technical Assistance Center (TAC).

The Call Home feature can deliver alert messages containing information on configuration, environmental conditions, inventory, syslog, and crash events.

The Call Home feature can deliver alerts to multiple recipients, referred to as *Call Home destination profiles* , each with configurable message formats and content categories. A predefined destination profile (CiscoTAC-1) is provided, and you also can define your own destination profiles. The CiscoTAC-1 profile is used to send alerts to the backend server of the Smart Call Home service, which can be used to create service requests to Cisco TAC, the service will depend on the Smart Call Home service support in place for your device and the severity of the alert.

Flexible message delivery and format options make it easy to integrate specific support requirements.

Benefits of Using Call Home

The Call Home feature offers the following benefits:

- Multiple message-format options:
  - Short Text—Suitable for pagers or printed reports.
  - Plain Text—Full formatted message information suitable for human reading.
  - XML—Matching readable format using Extensible Markup Language (XML) and Adaptive Markup Language (AML) document type definitions (DTDs). The XML format enables communication with the Cisco Smart Call Home server.
- Multiple concurrent message destinations.
- Multiple message categories, including configuration, environmental conditions, inventory, syslog, and crash events

  and diagnostics.
- Filtering of messages by severity and pattern matching.

- Scheduling of periodic message sending.

Obtaining Smart Call Home Services

If you have a service contract directly with Cisco, you can register for the Smart Call Home service. Smart Call Home analyzes Smart Call Home messages and provides background information and recommendations. For critical issues, Automatic Service Requests are generated with the Cisco TAC.

Smart Call Home offers the following features:

- Continuous device health monitoring and real-time alerts.
- Analysis of Smart Call Home messages and, if needed, Automatic Service Request generation routed to the correct TAC team, including detailed diagnostic information to speed problem resolution.
- Secure message transport directly from your device or through an HTTP proxy server or a downloadable Transport Gateway (TG). You can use a TG aggregation point to support multiple devices or in cases where security dictates that your devices may not be connected directly to the Internet.
- Web-based access to Smart Call Home messages and recommendations, inventory, and configuration information for all Smart Call Home devices provides access to associated field notices, security advisories, and end-of-life information.

You need the following items to register for Smart Call Home:

- SMARTnet contract number for your router.
- Your e-mail address
- Your Cisco.com username

For information about how to configure Call Home to work with the Smart Call Home service, see the How To Configure Call Home to Support the Smart Call Home Service.

Anonymous Reporting

Smart Call Home is a service capability included with many Cisco service contracts and is designed to assist customers resolve problems more quickly. In addition, the information gained from crash messages helps Cisco understand equipment and issues occurring in the field. If you decide not to use Smart Call Home, you can still enable Anonymous Reporting to allow Cisco to securely receive minimal error and health information from the device. If you enable Anonymous Reporting, your customer identity will remain anonymous, and no identifying information is sent.

Note When you enable Anonymous Reporting, you acknowledge your consent to transfer the specified data to Cisco or to vendors operating on behalf of Cisco (including countries outside the United States). Cisco maintains the privacy of all customers. For information about how Cisco treats personal information, see the Cisco Privacy Statement at Cisco Online Privacy Statement

When Call Home is configured in an anonymous way, only crash, inventory, and test messages are sent to Cisco. No identifying information is sent.

For more information about what is sent in these messages, see the Alert Group Trigger Events and Commands section.

Smart Licensing

Smart Call Home is required to use the Smart Licensing service.

The Smart Licensing service is an alternative licensing architecture to Cisco Software Licensing (CSL). Smart Call Licensing uses the Cisco Smart Software Manager as a backend tool for managing licenses. You must configure Cisco Smart Call Home before you can use Cisco Smart Licensing. For more information, see the Configuring and Enabling Smart Call Home section.

How to Configure Call Home

Configuring the Management Interface VRF

The Call Home feature on the Cisco ASR 1000 Series Routers requires use of the Gigabit Ethernet Management interface virtual routing and forwarding (VRF) instance. The Gigabit Ethernet Management interface is automatically part of its own VRF named “Mgmt-intf.”

To configure the Management interface VRF, complete the following steps:

or

ipv6 address {*X:X:X:X::X* **link-local** | *X:X:X:X::X/prefix* [**anycast** | **eui-64**] | **autoconfig** [**default**]}

SUMMARY STEPS

1. **configure terminal**
2. **interface GigabitEthernet 0**
3. **vrf forwarding Mgmt-intf**
4. Do one of the following:
   - **ip address** *ip-address mask* [**secondary** [**vrf** *vrf-name*]]
   -
   -
   - **ipv6 address** {*X:X:X:X::X* **link-local** | *X:X:X:X::X/prefix* [**anycast** | **eui-64**] | **autoconfig** [**default**]}

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device#` **configure terminal**	Enters global configuration mode.

	Command or Action	Purpose
Step 2	**interface GigabitEthernet 0** **Example:** `Router(config)# interface GigabitEthernet0`	(Required) Specifies the Gigabit Ethernet Management interface on the Cisco ASR 1000 Series Router.
Step 3	**vrf forwarding Mgmt-intf** **Example:** `Router(config-if)# vrf forwarding Mgmt-intf`	(Required) Associates the Mgmt-intf VRF with the Gigabit Ethernet Management interface. This command is configured by default.
Step 4	Do one of the following: • **ip address** *ip-address mask* [**secondary** [**vrf** *vrf-name*]] • • • **ipv6 address** {*X:X:X:X::X* **link-local** | *X:X:X:X::X/prefix* [**anycast** | **eui-64**] | **autoconfig** [**default**]} **Example:** `Router(config-if)# ip address 10.10.10.10 0.0.0.0`	(Required) Specifies the IPv4 or IPv6 addressing for the interface.

Configuring Smart Call Home (Single Command)

To enable all Call Home basic configurations using a single command, perform the following steps:

SUMMARY STEPS

1. **configure terminal**
2. **call-home reporting** {**anonymous** | **contact-email-addr** *email-address*} [**http-proxy** {*ipv4-address* | *ipv6-address* | **name**} **port** *port number*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 2	**call-home reporting** {**anonymous** | **contact-email-addr** *email-address*} [**http-proxy** {*ipv4-address* | *ipv6-address* | **name**} **port** *port number*] **Example:** `Device(config)#` **call-home reporting contact-email-addr email@company.com**	Enables all Call Home basic configurations using a single command. • **anonymous—**Enables Call-Home TAC profile to only send crash, inventory, and test messages and send the messages in an anonymous way. • **contact-email-addr—**Enables Smart Call Home service full reporting capability and sends a full inventory message from Call-Home TAC profile to Smart Call Home server to start full registration process. • **http-proxy** {*ipv4-address* | *ipv6-address* | **name—**An ipv4 or ipv6 address or server name. Maximum length is 64. • **port** *port number***—**Port number. Range is 1 to 65535. **Note** HTTP proxy option allows you to make use of your own proxy server to buffer and secure internet connections from your devices. **Note** After successfully enabling Call Home either in anonymous or full registration mode using the **call-home reporting** command, an inventory message is sent out. If Call Home is enabled in anonymous mode, an anonymous inventory message is sent out. If Call Home is enabled in full registration mode, a Full Inventory message for full registration mode is sent. For more information about what is sent in these messages, see the "Alert Group Trigger Events and Commands" section.

Configuring and Enabling Smart Call Home

SUMMARY STEPS

1. **configure terminal**
2. **call-home**
3. **profile CiscoTAC-1**
4. **destination transport-method http**
5. **active**
6. **exit**
7. **contact-email-addr** *email-address*
8. **exit**
9. service call-home
10. **exit**
11. copy running-config startup-config

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**call-home** **Example:** `Device(config)# call-home`	Enters call home configuration mode.
Step 3	**profile CiscoTAC-1** **Example:** `Device(config-call-home)# profile CiscoTAC-1`	Enters call home destination profile configuration mode for the CiscoTAC-1 destination profile.
Step 4	**destination transport-method http** **Example:** `Device(cfg-call-home-profile)# destination transport-method http`	(Required only if using HTTPS) Configures the message transport method for http.
Step 5	**active** **Example:** `Device(cfg-call-home-profile)# active`	Enables the destination profile.
Step 6	**exit** **Example:** `Device(cfg-call-home-profile)# exit`	Exits call home destination profile configuration mode and returns to call home configuration mode.
Step 7	**contact-email-addr** *email-address* **Example:** `Device(cfg-call-home)# contact-email-addr username@example.com`	Assigns the customer's e-mail address. Enter up to 200 characters in e-mail address format with no spaces.
Step 8	**exit** **Example:** `Device(cfg-call-home)# exit`	Exits call home configuration mode and returns to global configuration mode.

	Command or Action	Purpose
Step 9	service call-home **Example:** `Device(config)#` **service call-home**	Enables the Call Home feature.
Step 10	**exit** **Example:** `Device(config)#` **exit**	Exits global configuration mode and returns to privileged EXEC mode.
Step 11	copy running-config startup-config **Example:** `Device#` **copy running-config startup-config**	Saves the configuration to NVRAM.

Enabling and Disabling Call Home

To enable or disable the Call Home feature, complete the following steps:

SUMMARY STEPS

1. **configure terminal**
2. **service call-home**
3. **no service call-home**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Router#` **configure terminal**	Enters global configuration mode.
Step 2	**service call-home** **Example:** `Router(config)#` **service call-home**	Enables the Call Home feature.

	Command or Action	Purpose
Step 3	**no service call-home** **Example:** `Router(config)#` **no service call-home**	Disables the Call Home feature.

Configuring Contact Information

Each router must include a contact e-mail address. You can optionally include a phone number, street address, contract ID, customer ID, and site ID.

To assign the contact information, complete the following steps:

SUMMARY STEPS

1. **configure terminal**
2. **call-home**
3. **contact-email-addr** *email-address*
4. **phone-number** +*phone-number*
5. **street-address** *street-address*
6. **customer-id** *text*
7. **site-id** *text*
8. **contract-id** *text*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Router>` **configure terminal**	Enters global configuration mode.
Step 2	**call-home** **Example:** `Router(config)#` **call-home**	Enters call home configuration mode.

	Command or Action	Purpose
Step 3	**contact-email-addr** *email-address* **Example:** `Router(cfg-call-home)#` **contact-email-addr username@example.com**	Assigns the customer's e-mail address. Enter up to 200 characters in e-mail address format with no spaces.
Step 4	**phone-number** +*phone-number* **Example:** `Router(cfg-call-home)#` **phone-number +1-222-333-4444**	(Optional) Assigns the customer's phone number. **Note** The number must begin with a plus (+) prefix, and may contain only dashes (-) and numbers. Enter up to 16 characters. If you include spaces, you must enclose your entry within double quotation marks (" ").
Step 5	**street-address** *street-address* **Example:** `Router(cfg-call-home)#` **street-address "1234 Any Street, Any city, Any state, 12345"**	(Optional) Assigns the customer's street address where RMA equipment can be shipped. Enter up to 200 characters. If you include spaces, you must enclose your entry within double quotation marks (" ").
Step 6	**customer-id** *text* **Example:** `Router(cfg-call-home)#` **customer-id Customer1234**	(Optional) Identifies the customer ID. Enter up to 64 characters. If you include spaces, you must enclose your entry within double quotation marks (" ").
Step 7	**site-id** *text* **Example:** `Router(cfg-call-home)#` **site-id Site1ManhattanNY**	(Optional) Identifies the customer site ID. Enter up to 200 characters. If you include spaces, you must enclose your entry within double quotation marks (" ").
Step 8	**contract-id** *text* **Example:** `Router(cfg-call-home)#` **contract-id Company1234**	(Optional) Identifies the customer's contract ID for the router. Enter up to 64 characters. If you include spaces, you must enclose your entry within double quotation marks (" ").

Example

The following example shows the configuration of contact information:

```
Device# configure terminal
```

```
Enter configuration commands, one per line.  End with CNTL/Z.

Device(config)# call-home

Device(cfg-call-home)# contact-email-addr username@example.com

Device(cfg-call-home)# phone-number +1-222-333-4444

Device(cfg-call-home)# street-address "1234 Any Street, Any city, Any state, 12345"

Device(cfg-call-home)# customer-id Customer1234


Device(cfg-call-home)# site-id Site1ManhattanNY

Device(cfg-call-home)# contract-id Company1234


Device(cfg-call-home)# exit
```

Configuring a Destination Profile

A destination profile contains the required delivery information for an alert notification. You can configure multiple destination profiles of one or more type.

You can create and define a new destination profile or copy and use another destination profile. If you define a new destination profile, you must assign a profile name. If you define a new destination profile, you must assign a profile name.

You can control which profile to be used for Smart Licensing by enabling or disabling smart-licensing data of that profile. Only one active profile can have smart-license data enabled. For more information about Smart Licensing, see the "Managing Cisco CSR 1000V Licenses" section.

If you use the Cisco Smart Call Home service, the destination profile must use the XML message format.

Note The Call Home feature provides a predefined profile named CiscoTAC-1 that is inactive by default. The CiscoTAC-1 profile is intended for use with the Smart Call Home service, which requires certain additional configuration steps to enable the service with the Call Home feature. For more information about this profile, see the Using the Predefined CiscoTAC-1 Destination Profile.

Note

You can configure the following attributes for a destination profile:

- Profile name—String that uniquely identifies each user-defined destination profile. The profile name is limited to 31 characters and is not case-sensitive. You cannot use **all** as a profile name.
- Transport method—The transport mechanism, either e-mail or HTTP (including HTTPS), for delivery of alerts.
    - For user-defined destination profiles, e-mail is the default, and you can enable one or both transport mechanisms. If you disable both methods, e-mail is enabled.
    - For the predefined Cisco TAC profile, you can enable either transport mechanism, but not both.

- Destination address—The actual address related to the transport method by which the alert should be sent.
  In Call Home version 3, you can change the destination of the CiscoTAC-1 profile.
- Message formatting—The message format used for sending the alert. The format options for a user-defined destination profile are long-text, short-text, or XML. The default is XML. For the predefined Cisco TAC profile, only XML is allowed. If you use the Cisco Smart Call Home service, the destination profile must use the XML message format.
- Message size—The maximum destination message size. The valid range is 50 to 3,145,728 bytes and the default is 3,145,728 bytes.
- Reporting method—You can choose which data to report for a profile. You can report Smart Call Home data or Smart Licensing data for a profile. Only one active profile is allowed to report Smart Licensing data at a time.
- Anonymous reporting—You can choose for your customer identity to remain anonymous, and no identifying information is sent.
- Subscribing to interesting alert-groups—You can choose to subscribe to alert-groups highlighting your interests.

This section includes the following tasks:

Creating a New Destination Profile

To create and configure a new destination profile, complete the following steps:

SUMMARY STEPS

1. **configure terminal**
2. **call-home**
3. **profile** *name*
4. **destination transport-method email**
5. **destination address email** *email-address*
6. **destination preferred-msg-format** {**long-text** | **short-text** | **xml**}
7. **destination message-size** *bytes*
8. **active**
9. **exit**
10. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device#` **configure terminal**	Enters global configuration mode.

	Command or Action	Purpose
Step 2	**call-home** **Example:** `Device(config)#` **call-home**	Enters call home configuration mode.
Step 3	**profile** *name* **Example:** `Device(config-call-home)#` **profile profile1**	Enters call home destination profile configuration mode for the specified destination profile name. If the specified destination profile does not exist, it is created.
Step 4	**destination transport-method email** **Example:** `Device(cfg-call-home-profile)#` **destination transport-method email**	(Optional) Configures the message transport method for email. This is the default.
Step 5	**destination address email** *email-address* **Example:** `Device(cfg-call-home-profile)#` **destination address email myaddress@example.com**	(Required) Configures the destination e-mail address to which Call Home messages are sent.
Step 6	**destination preferred-msg-format** {**long-text** | **short-text** | **xml**} **Example:** `Device(cfg-call-home-profile)#` **destination preferred-msg-format xml**	(Optional) Configures a preferred message format. The default is XML.
Step 7	**destination message-size** *bytes* **Example:** `Device(cfg-call-home-profile)#` **destination message-size 3145728**	(Optional) Configures a maximum destination message size (from 50 to 3145728 bytes) for the destination profile. The default is 3145728 bytes.
Step 8	**active** **Example:** `Device(cfg-call-home-profile)#` **active**	(Optional) Enables the destination profile. By default, a user-defined profile is enabled when it is created.
Step 9	**exit** **Example:** `Device(cfg-call-home-profile)#` **exit**	Exits call home destination profile configuration mode and returns to call home configuration mode.

	Command or Action	Purpose
Step 10	**end** **Example:** `Device(cfg-call-home)#` **end**	Returns to privileged EXEC mode.

Setting Profiles to Anonymous Mode

To create a new destination profile by copying an existing profile, complete the following steps:

SUMMARY STEPS

1. **configure terminal**
2. **call-home**
3. **copy profile** *source-profile target-profile*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device#` **configure terminal**	Enters global configuration mode.
Step 2	**call-home** **Example:** `Device(config)#` **call-home**	Enters call home configuration mode.
Step 3	**copy profile** *source-profile target-profile* **Example:** `Device(cfg-call-home)#` **copy profile profile1 profile2**	Creates a new destination profile with the same configuration settings as the existing destination profile, where: • *source-profile* —Specifies the existing name of the profile. • *target-profile* —Specifies a name for the new copy of the profile.

Subscribing to Alert Groups

An alert group is a predefined subset of Call Home alerts supported in all routers. Different types of Call Home alerts are grouped into different alert groups depending on their type. The following alert groups are available:

- Configuration
- Diagnostic
- Environment
- Inventory
- Syslog
- Crash

The triggering events for each alert group are listed in the Alert Group Trigger Events and Commands, and the contents of the alert group messages are listed in the Message Contents.

You can select one or more alert groups to be received by a destination profile.

Note A Call Home alert is only sent to destination profiles that have subscribed to the alert group containing that Call Home alert. In addition, the alert group must be enabled.

Periodic Notification

When you subscribe a destination profile to either the Configuration or the Inventory alert group, you can choose to receive the alert group messages asynchronously or periodically at a specified time. The sending period can be one of the following:

- Daily—Specify the time of day to send, using an hour:minute format hh:mm, with a 24-hour clock (for example, 14:30).
- Weekly—Specify the day of the week and time of day in the format day hh:mm, where the day of the week is spelled out (for example, monday).
- Monthly—Specify the numeric date, from 1 to 31, and the time of day, in the format date hh:mm.

Message Severity Threshold

When you subscribe a destination profile to the Environment or Syslog alert group, you can set a threshold for the sending of alert group messages based on the message's level of severity. Any message with a severity lower than the specified threshold of the destination profile is not sent to the destination.

Note When syslog level is changed via IOS CLI, the new value is propagated to non-IOS processes as well, with the result that these processes no longer send syslog messages of lower priority to IOS to process, thus "saving" CPU cycles for IOS.

The table below lists the keywords used to configure the severity, which range from catastrophic (level 9, highest level of urgency) to debugging (level 0, lowest level of urgency). If no severity threshold is configured, the default is debugging (level 0). However, the default is not recommended due to the number of messages that will be triggered.

Note Call Home severity levels are not the same as system message logging severity levels.

Table 3: Severity and Syslog Level Mapping

Level	Keyword	Syslog Level	Description
9	**catastrophic**	N/A	Network-wide catastrophic failure.
8	**disaster**	N/A	Significant network impact.
7	**fatal**	Emergency (0)	System is unusable.
6	**critical**	Alert (1)	Critical conditions, immediate attention needed.
5	**major**	Critical (2)	Major conditions.
4	**minor**	Error (3)	Minor conditions.
3	**warning**	Warning (4)	Warning conditions.
2	**notification**	Notice (5)	Basic notification and informational messages. Possibly independently insignificant.
1	**normal**	Information (6)	Normal event signifying return to normal state.
0	**debugging**	Debug (7)	Debugging messages.

Configuring Snapshot Command List

To configure the snapshot command list, perform the following steps:

SUMMARY STEPS

1. **configure terminal**
2. **call-home**
3. [**no** | **default**] **alert-group-config snapshot**
4. [**no** | **default**] **add-command** *command string*
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device#` **configure terminal**	Enters global configuration mode.
Step 2	**call-home** **Example:** `Device(config)#` **call-home**	Enters Call Home configuration mode.
Step 3	[**no** | **default**] **alert-group-config snapshot** **Example:** `Device(cfg-call-home)#` **alert-group-config snapshot**	Enters snapshot configuration mode. The **no** or **default** command will remove all snapshot command.
Step 4	[**no** | **default**] **add-command** *command string* **Example:** `Device(cfg-call-home-snapshot)#` **add-command** *"show version"*	Adds the command to the Snapshot alert group. The **no** or **default** command will remove the corresponding command. • *command string*—IOS command. Maximum length is 128.
Step 5	**end** **Example:** `Device(cfg-call-home-snapshot)#` **exit**	Exits and saves the configuration.

Configuring General email Options

Configuring the Mail Server

To use the e-mail message transport, you must configure at least one Simple Mail Transfer Protocol (SMTP) e-mail server address. You can specify up to four backup e-mail servers, for a maximum of five total mail-server definitions.

Consider the following guidelines when configuring the mail server:

- Backup e-mail servers can be defined by repeating the **mail-server** command using different priority numbers.
- The **mail-server priority** *number* parameter can be configured from 1 to 100. The server with the highest priority (lowest priority number) is tried first.

To configure general email options, perform the following steps:

SUMMARY STEPS

1. **configure terminal**
2. **call-home**
3. **mail-server** {*ipv4-address* | *name*} **priority** *number*
4. **sender from** *email-address*
5. **sender reply-to** *email-address*
6. **source-interface** *interface-name*
7. **source-ip-address** *ipv4/ipv6 address*
8. **vrf***vrf-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device#` **configure terminal**	Enters global configuration mode.
Step 2	**call-home** **Example:** `Device(config)#` **call-home**	Enters call home configuration mode.
Step 3	**mail-server** {*ipv4-address* | *name*} **priority** *number*	Assigns an email server address and its relative priority among configured email servers.

	Command or Action	Purpose
	Example: `Device(cfg-call-home)#` **mail-server stmp.example.com priority 1**	Provide either of these: - The email server's IP address or - The email server's fully qualified domain name (FQDN) of 64 characters or less. Assign a priority number between 1 (highest priority) and 100 (lowest priority).
Step 4	**sender from** *email-address* **Example:** `Device(cfg-call-home)#` **sender from username@example.com**	(Optional) Assigns the e-mail address that will appear in the from field in Call Home e-mail messages. If no address is specified, the contact e-mail address is used.
Step 5	**sender reply-to** *email-address* **Example:** `Device(cfg-call-home)#` **sender reply-to username@example.com**	(Optional) Assigns the e-mail address that will appear in the reply-to field in Call Home e-mail messages.
Step 6	**source-interface** *interface-name* **Example:** `Device(cfg-call-home)#` **source-interface loopback1**	Assigns the source interface name to send call-home messages. *interface-name*—Source interface name. Maximum length is 64. **Note** For HTTP messages, use the **ip http client source-interface** *interface-name* command in global configuration mode to configure the source interface name. This allows all HTTP clients on the device to use the same source interface.
Step 7	**source-ip-address** *ipv4/ipv6 address* **Example:** `Device(cfg-call-home)#` **ip-address 209.165.200.226**	Assigns source IP address to send call-home messages. - *ipv4/ipv6 address*—Source IP (ipv4 or ipv6) address. Maximum length is 64.
Step 8	**vrf***vrf-name* **Example:** `Device(cfg-call-home)#` **vrf** *vpn1*	(Optional) Specifies the VRF instance to send call-home email messages. If no vrf is specified, the global routing table is used. **Note** For HTTP messages, if the source interface is associated with a VRF, use the **ip http client source-interface** *interface-name* command in global configuration mode to specify the VRF instance that will be used for all HTTP clients on the device.

Example: General email Options

The following example shows general email options:

```
Device# configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# call-home
Device(cfg-call-home)# mail-server smtp.example.com priority 1
Device(cfg-call-home)# mail-server 192.168.0.1 priority 2
Device(cfg-call-home)# exit
```

Specifying Rate Limit for Sending Call Home Messages

To specify the rate limit for sending Call Home messages, perform the following steps:

SUMMARY STEPS

1. **configure terminal**
2. **call-home**
3. **rate-limit** *number*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device#` **configure terminal**	Enters global configuration mode.
Step 2	**call-home** **Example:** `Device(config)#` **call-home**	Enters call home configuration mode.
Step 3	**rate-limit** *number* **Example:** `Device(cfg-call-home)#` **rate-limit 40**	Specifies a limit on the number of messages sent per minute. • *number*—Range 1 to 60. The default is 20.

Specifying HTTP Proxy Server

To specify an HTTP proxy server for sending Call Home HTTP(S) messages to a destination, perform the following steps:

SUMMARY STEPS

1. **configure terminal**
2. **call-home**
3. **http-proxy** {*ipv4-address* | *ipv6-address name*} *name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device#` **configure terminal**	Enters global configuration mode.
Step 2	**call-home** **Example:** `Device(config)#` **call-home**	Enters call home configuration mode.
Step 3	**http-proxy** {*ipv4-address* | *ipv6-address name*} *name* **Example:** `Device(config)#` **http-proxy 1.1.1.1 port 1**	Specifies the proxy server for the HTTP request.

Enabling AAA Authorization to Run IOS Commands for Call Home Messages

To enable AAA authorization to run IOS commands that enable the collection of output for a Call Home message, perform the following steps:

SUMMARY STEPS

1. **configure terminal**
2. **call-home**
3. **aaa-authorization**
4. **aaa-authorization** [**username** *username*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device#` **configure terminal**	Enters global configuration mode.
Step 2	**call-home** **Example:** `Device(config)#` **call-home**	Enters call home configuration mode.
Step 3	**aaa-authorization** **Example:** `Device(cfg-call-home)#` **aaa-authorization**	Enables AAA authorization. **Note** By default, AAA authorization is disabled for Call Home.
Step 4	**aaa-authorization** [**username** *username*] **Example:** `Device(cfg-call-home)#` **aaa-authorization username** *username*	Specifies the username for authorization. • **username** *user*—Default username is callhome. Maximum length is 64.

Configuring Syslog Throttling

To enable or disable Call Home syslog message throttling and avoid sending repetitive Call Home syslog messages, perform the following steps:

SUMMARY STEPS

1. **configure terminal**
2. **call-home**
3. [**no**] **syslog-throttling**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device#` **configure terminal**	Enters global configuration mode.

	Command or Action	Purpose
Step 2	**call-home** **Example:** `Device(config)#` **call-home**	Enters call home configuration mode.
Step 3	[**no**] **syslog-throttling** **Example:** `Device(cfg-call-home)#` **syslog-throttling**	Enables or disables Call Home syslog message throttling and avoids sending repetitive Call Home syslog messages. By default, syslog message throttling is enabled.

Configuring Call Home Data Privacy

The **data-privacy** command scrubs data, such as IP addresses, from running configuration files to protect the privacy of customers. Enabling the **data-privacy** command can affect CPU utilization when scrubbing a large amount of data. Currently, **show** command output is not being scrubbed except for configuration messages in the **show running-config** all and show startup-config data.

SUMMARY STEPS

1. **configure terminal**
2. **call-home**
3. **data-privacy** {**level** {**normal** | **high**} | **hostname**}

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device#` **configure terminal**	Enters global configuration mode.
Step 2	**call-home** **Example:** `Device(config)#` **call-home**	Enters call home configuration mode.
Step 3	**data-privacy** {**level** {**normal** | **high**} | **hostname**}	Scrubs data from running configuration file to protect the privacy of the user. The default data-privacy level is normal.

	Command or Action	Purpose
	Example: `Device(cfg-call-home)#` **data-privacy level high**	**Note** Enabling the data-privacy command can affect CPU utilization when scrubbing a large amount of data. • **normal—**Scrubs all normal-level commands. • **high—**Scrubs all normal-level commands plus the IP domain name and IP address commands. • **hostname—**Scrubs all high-level commands plus the hostname command. **Note** Scrubbing the hostname from configuration messages can cause Smart Call Home processing failure on some platforms.

Working With Destination Profiles

This section describes some of the tasks that you can complete with destination profiles:

Activating and Deactivating a Destination Profile

Except for the predefined CiscoTAC-1 profile, all Call Home destination profiles are automatically activated once you create them. If you do not want to use a profile right way, you can deactivate the profile. The CiscoTAC-1 profile is inactive by default and must be activated to be used.

To activate or deactivate a destination profile, complete the following steps:

SUMMARY STEPS

1. **configure terminal**
2. **call-home**
3. **profile** *name*
4. **active**
5. no active
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Router#` **configure terminal**	Enters global configuration mode.

	Command or Action	Purpose
Step 2	**call-home** **Example:** `Router(config)#` **call-home**	Enters call home configuration mode.
Step 3	**profile** *name* **Example:** `Router(config-call-home)#` **profile test**	Enters call home destination profile configuration mode for the specified destination profile. If the specified destination profile does not exist, it is created.
Step 4	**active** **Example:** `Router(cfg-call-home-profile)#` **active**	Enables the destination profile. By default, a new profile is enabled when it is created.
Step 5	no active **Example:** `Router(cfg-call-home-profile)#` **no active**	Disables the destination profile.
Step 6	**end** **Example:** `Router(cfg-call-home)#` **end**	Exits call home destination profile configuration mode and returns to privileged EXEC mode.

Renaming a Destination Profile

To change the name of an existing profile, complete the following steps:

SUMMARY STEPS

1. **configure terminal**
2. **call-home**
3. **rename profile** *source-profile target-profile*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 2	**call-home** **Example:** `Router(config)# call-home`	Enters call home configuration mode.
Step 3	**rename profile** *source-profile target-profile* **Example:** `Router(cfg-call-home)# rename profile2 testprofile`	Renames an existing source file, where: • *source-profile* —Specifies the existing name of the profile. • *target-profile* —Specifies a new name for the existing profile.

Using the Predefined CiscoTAC-1 Destination Profile

The CiscoTAC-1 profile is automatically configured in the Call Home feature for your use with the Cisco Smart Call Home service. This profile includes certain information, such as the destination e-mail address and HTTPS URL, and default alert groups for communication with the Smart Call Home service. Some of these attributes, such as the destination e-mail address, HTTPS URL, and message format cannot be modified.

You can use either email or http transport to communicate with the Smart Call Home service backend server. By default, the CiscoTAC-1 profile is inactive and uses email as the default transport method. To use email transport, you only need to enable the profile. However, to use this profile with the Cisco Smart Call Home service secure server (via HTTPS), you not only must enable the profile, but you must also change the transport method to HTTP as shown in the following example:

```
Router# configure terminal
Router(config)# call-home
Router(config-call-home)# profile CiscoTAC-1
Router(cfg-call-home-profile)# destination transport-method http
Router(cfg-call-home-profile)# active
```

For more information about additional requirements for Configuring the Smart Call Home service, see the How To Configure Call Home to Support the Smart Call Home Service section.

Verifying the Call Home Profile Configuration

To verify the profile configuration for Call Home, use the **show call-home profile** command. See Displaying Call Home Configuration Information for more information and examples.

Sending Call Home Communications Manually

You can manually send several types of Call Home communications. To send Call Home communications, complete the tasks in this section. This section contains the following subsections:

Sending a Call Home Test Message Manually

You can use the **call-home test** command to send a user-defined Call Home test message.

SUMMARY STEPS

1. **call-home test** [“*test-message*”] **profile** *name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**call-home test** [“*test-message*”] **profile** *name* **Example:** `Router#` **call-home test profile profile1**	Sends a test message to the specified destination profile. The user-defined test message text is optional, but must be enclosed in quotes (“ ”) if it contains spaces. If no user-defined message is configured, a default message is sent.

Sending Call Home Alert Group Messages Manually

You can use the **call-home send** command to manually send a specific alert group message.

Note the following guidelines when manually sending a Call Home alert group message:

- Configuration,
  diagnostic

  , and inventory alert groups can be sent manually.
- When you manually trigger an alert group message and you specify a destination profile name, a message is sent to the destination profile regardless of the active status, subscription status, or severity setting of the profile.
- When you manually trigger a configuration or inventory alert group message and do not specify a destination profile name, a message is sent to all active profiles that have either a normal or periodic subscription to the specified alert group.
- When you manually trigger a diagnostic alert group message and do not specify a destination profile name, a message is sent to all active profiles that have a lower severity subscription than the severity of the diagnostic results of the specified slot.

To manually trigger Call Home alert group messages, complete the following steps:

SUMMARY STEPS

1. **call-home send alert-group configuration** [**profile** *name*]
2. **call-home send alert-group diagnostic slot R0** [**profile** *name*]
3. **call-home send alert-group inventory** [**profile** *name*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**call-home send alert-group configuration** [**profile** *name*] **Example:** `Device#` **call-home send alert-group configuration profile CiscoTAC-1**	Sends a configuration alert group message to one destination profile if specified, or to all subscribed destination profiles.
Step 2	**call-home send alert-group diagnostic slot R0** [**profile** *name*] **Example:** `Device#` **call-home send alert-group diagnostic slot R0 profile CiscoTAC-1**	Sends a diagnostic alert group message to one destination profile if specified, or to all subscribed destination profiles with a lower severity subscription than the diagnostic result for route processor slot 0.
Step 3	**call-home send alert-group inventory** [**profile** *name*] **Example:** `Device#` **call-home send alert-group inventory**	Sends an inventory alert group message to one destination profile if specified, or to all subscribed destination profiles.

Submitting Call Home Analysis and Report Requests

You can use the **call-home request** command to submit information about your system to Cisco Systems to receive helpful analysis and report information specific to your system. You can request a variety of reports, including security alerts, known bugs, best practices, and command references.

Note the following guidelines when manually sending Call Home analysis and report requests:

- If a **profile** *name* is specified, the request is sent to the profile. If no profile is specified, the request is sent to the Cisco TAC profile. The recipient profile does not need to be enabled for the call-home request. The profile should specify the e-mail address where the transport gateway is configured so that the request message can be forwarded to the Cisco TAC and the user can receive the reply from the Smart Call Home service.
- The **ccoid** *user-id* is the registered identifier of the Smart Call Home user. If the *user-id* is specified, the response is sent to the e-mail address of the registered user. If no *user-id* is specified, the response is sent to the contact e-mail address of the device.
- Based on the keyword specifying the type of report requested, the following information is returned:

- ◦ **config-sanity—**Information on best practices as related to the current running configuration.
- ◦ **bugs-list—**Known bugs in the running version and in the currently applied features.
- ◦ **command-reference—**Reference links to all commands in the running configuration.
- ◦ **product-advisory—**Product Security Incident Response Team (PSIRT) notices, End of Life (EOL) or End of Sales (EOS) notices, or field notices (FN) that may affect devices in your network.

To submit a request for analysis and report information from the Cisco Output Interpreter tool, complete the following steps:

SUMMARY STEPS

1. **call-home request output-analysis** "*show-command*"
2. **call-home request** {**config-sanity** | **bugs-list** | **command-reference** | **product-advisory**}

DETAILED STEPS

	Command or Action	Purpose
Step 1	**call-home request output-analysis** "*show-command*" **Example:** [**profile** *name*] [**ccoid** *user-id*] **Example:** `Device#` **call-home request output-analysis "show diag" profile TG**	Sends the output of the specified **show** command for analysis. The **show** command must be contained in quotes ("").
Step 2	**call-home request** {**config-sanity** | **bugs-list** | **command-reference** | **product-advisory**} **Example:** [**profile** *name*] [**ccoid** *user-id*] **Example:** `Device#` **call-home request config-sanity profile TG**	Sends the output of a predetermined set of commands, such as the **show running-config all** and **show version** commands, for analysis. In addition, the **call home request product-advisory** subcommand includes all inventory alert group commands. The keyword specified after the **call-home request** command specifies the type of report requested.

Example

The following example shows a request for analysis of a user-specified **show** command:

```
Router# call-home request output-analysis "show diag" profile TG
```

Manually Sending Command Output Message for One Command or a Command List

You can use the **call-home send** command to execute a CLI command and e-mail the command output to Cisco or to an e-mail address that you specify.

Note the following guidelines when sending the output of a command:

- The specified IOS command or list of IOS commands can be any run command, including commands for all modules. The command must be contained in quotes (“”).
- If the email option is selected using the “email” keyword and an email address is specified, the command output is sent to that address. If neither the email nor the HTTP option is specified, the output is sent in long-text format with the specified service request number to the Cisco TAC (attach@cisco.com).
- If neither the “email” nor the “http” keyword is specified, the service request number is required for both long-text and XML message formats and is provided in the subject line of the email.
- If the HTTP option is specified, the CiscoTac-1 profile destination HTTP or HTTPS URL is used as the destination. The destination email address can be specified so that Smart Call Home can forward the message to the email address. The user must specify either the destination email address or an SR number but they can also specify both.

To execute a command and send the command output, complete the following step:

SUMMARY STEPS

1. **call-home send** {*cli command* | *cli list*} [**email** *email* **msg-format** {**long-text** | **xml**} | **http** {**destination-email-address***email*}][**tac-service-request SR#**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**call-home send** {*cli command* | *cli list*} [**email** *email* **msg-format** {**long-text** | **xml**} | **http** {**destination-email-address***email*}][**tac-service-request SR#** **Example:** `Router#` **call-home send “show version; show running-config show inventory” emailsupport@example.com msg-format xml**	Executes the CLI or CLI list and sends output via email or HTTP. • {*cli command* | *cli list*}—Specifies the IOS command or list of IOS commands (separated by ‘;’). It can be any run command, including commands for all modules. The commands must be contained in quotes (“”). • **email** *email* **msg-format** {**long-text** | **xml—**If the email option is selected, the command output will be sent to the specified email address in long-text or XML format with the service request number in the subject. The email address, the service request number, or both must be specified. The service request number is required if the email address is not specified (default is attach@cisco.com for long-text format and callhome@cisco.com for XML format). • **http** {**destination-email-address***email*—If the http option is selected, the command output will be sent to Smart Call Home backend server (URL specified in TAC profile) in XML format.

	Command or Action	Purpose
		destination-email-address*email* can be specified so that the backend server can forward the message to the email address. The email address, the service request number, or both must be specified. • **tac-service-request SR#—**Specifies the service request number. The service request number is required if the email address is not specified.

Example

The following example shows how to send the output of a CLI command to a user-specified email address:

```
Device# call-home send "show diag" email support@example.com
```

The following example shows the command output sent in long-text format to attach@cisco.com, with the SR number specified:

```
Device# call-home send "show version"; "show run tac-service-request 123456
```

The following example shows the command output sent in XML message format to callhome@cisco.com:

```
Device# call-home send "show diag" email callhome@example.com msg-format xml
```

Configuring Diagnostic Signatures

The Diagnostic Signatures feature downloads digitally signed signatures to devices. Diagnostic Signatures (DS) files are formatted files that collate knowledge of diagnostic events and provide methods to troubleshoot them without a need to upgrade the Cisco software. The aim of DS is to deliver flexible intelligence that can detect and collect troubleshooting information that can be used to resolve known problems in customer networks.

Prerequisites for Diagnostic Signatures

Before you download and configure diagnostic signatures (DS) on a device, you must ensure that the following conditions are met:

- You must assign a DS to the device. Refer to the “Diagnostic Signature Downloading” section for more information on how to assign DSes to devices.
- HTTP/Secure HTTP (HTTPS) transport is required for downloading DS files. You must install the certification authority (CA) certificate to enable the authentication of the destination HTTPS server.
- Target URLs must be one of the Cisco Technical Assistance Center (TAC) HTTPS URLs:
  - https://tools-stage.cisco.com/its/service/oddce/services/DDCEService
  - https://tools-dev.cisco.com/its/service/oddce/services/DDCEService

Information About Diagnostic Signatures

Diagnostic Signatures Overview

Diagnostic signatures (DS) subsystem is introduced within the call-home system to provide a flexible framework that allows the defining of new events and corresponding CLIs that can analyze these events without upgrading the Cisco software.

DS provides you the ability to define more types of events and trigger types to perform the required actions than the Call-Home feature. The DS subsystem downloads and processes files on a device as well as handles callbacks for diagnostic signature events.

The Diagnostic signature feature downloads digitally signed signatures that are in the form of files to devices. DS files are formatted files that collate the knowledge of diagnostic events and provide methods to troubleshoot these events.

DS files contain XML data to specify the event description, and these files include a CLI to perform required actions. These files are digitally signed by Cisco or a third party to certify its integrity, reliability, and security.

The structure of a DS file can be one of the following formats:

- Metadata-based simple signature that specifies event type and contains other information that can be used to match the event, perform actions such as collecting information by using the CLI or resetting the line card in the device if there is an event match.
- Embedded Event Manager (EEM) Tool Command Language (Tcl) script-based signature that specifies new events in the event register line and additional action in the Tcl script.
- Combination of both the formats mentioned above.

The following basic information is contained in a DS file:

- ID (unique string)—unique key that represents a DS file that can be used to search a DS.
- Name (ShortDescription)—unique description of the DS file that can be used in lists for selection.
- Description—long description about the signature.
- Revision—version number, which increments when the DS content is updated.
- ProductFamily
    - OsVersion (multiple values)—a list of operating system versions for each product family.
    - Technology—technology that the DS belongs to.

Diagnostic Signature Downloading

To download the diagnostic signature (DS) file, you require the secure HTTP (HTTPS) protocol. If you have already configured an email transport method to download files on your device, you must change your assigned profile transport method to HTTPS to download and use DS.

Cisco software uses a PKI Trustpool Management feature, which is enabled by default on devices, to create a scheme to provision, store, and manage a pool of certificates from known certification authorities (CAs). The trustpool feature installs the CA certificate automatically. The CA certificate is required for the authentication of the destination HTTPS servers. Therefore, to enable the HTTPS protocol, the firewall is bypassed to access the service call-home (SCH) HTTPS server. The target URLs, which are defined in the SCH HTTPS server, must be one of the Technical Assistance Center (TAC) HTTPS URLs:

- https://tools-stage.cisco.com/its/service/oddce/services/DDCEService
- https://tools-dev.cisco.com/its/service/oddce/services/DDCEService

.

There are two types of DS update requests to download DS files: regular and forced-download.

Regular download requests DS files that were recently updated. You can trigger a regular download request either by using a periodic configuration or by initiating an on-demand CLI. The regular download update happens only when the version of the requested DS is different from the version of the DS on the device. Periodic download is enabled by checking responses to periodic inventory messages. When an inventory message checks for any assigned DS on the device, the device sends a DS update request message that requests for an updated DS. In a DS update request message, the status and revision number of the DS is included such that only a DS with the latest revision number is downloaded.

Forced-download downloads a specific DS or a set of DSes. You can trigger the forced-download update request only by initiating an on-demand CLI. In a force-download update request, the latest version of the DS file is downloaded irrespective of the current DS file version on the device.

Diagnostic Signature Signing

The diagnostic signature (DS) files are digitally signed before they are made available for downloading. The following methods are used for digitally signing DS files:

- Signing algorithm (Rivest Shamir and Adleman [RSA] 2048 bits)
- Request keypairs to Abraxas system, which is the digital signing client
- DS signed via secure socket layer (SSL) through a code signing client, where the signature is embedded using XML tags
- Public keys are embedded in the DS subsystem (Cisco signed, partner signed, third-party signed) in the Cisco software. The digitally signed DS file contains the product name such as Diagnostic_Signatures (Cisco signed), Diagnostic_Signatures_Partner, Diagnostic_Signatures_3rd_Party. The product names are only used to sign the DS files.

The digital signing client can be found at https://abraxas.cisco.com/SignEngine/submit.jsp

These conditions that must be met to verify the digital signature in a DS file:

- Code sign component support must be available in Cisco software.
- Various public keys that verify the different kinds of diagnostic signatures must be included in platforms where DS is supported.
- After parsing and retrieving the DS, the DS must execute the verification application program interface (API) to verify that the DS is valid.

Diagnostic Signature Workflow

The Diagnostic Signature is enabled by default on the Cisco software.

- Use the **destination transport-method http** command to configure both email and HTTP data transfer methods to download DSes.
- Download all DS files or specific DS files either by using the on-demand or periodic download.
- Store the downloaded DS files on nonremovable disks, such as bootflash or harddisk, so that DS files can be read after a device reload. Syslog messages are displayed if the disk space is not sufficient.
- Use periodic download to verify if the same version of DS is already available on the device. If a different version of DS is available on the device, the older version is uninstalled and the newer version is installed. Service disruption may occur during this time because of the unavailability of the DS.
- Associate the DS on your device with only one profile. Associating a DS with two different profiles may lead to unexpected results.
- Use the severity and pattern of occurrence of events on the device to determine the CLI commands that must be included in the new DS to trigger actions. For events that have already been identified, the metadata of the DS is in a much simpler format.

The DS metadata is parsed and stored in a database for event registration and information collection. When an event occurs, the action specified in the DS is performed.

Diagnostic Signature Events and Actions

Diagnostic signature (DS) events and actions are defined while digitally signing a DS. The DS events and actions data are included after the administrator metadata and operational metadata in the DS.

Diagnostic Signature Event Detection

Event detection in DS is defined in two ways: single event detection and multiple event detection.

Single Event Detection

In single event detection, only one event detector is defined within a DS. The event specification format is one of the following two types:

- DS event specification type—syslog, environment, diagnostic, periodic, configuration, Online Insertion Removal (OIR), immediate, and call-home are the supported event types, where “immediate” indicates that these types of DSes do not contain any event detection part and “call-home” type modifies the existing CLI commands. After the registration of the event types, the DS performs the associated action immediately.
- Embedded Event Manager (EEM) specification type—supports all existing EEM event types. The EEM specification type also supports a new EEM event detector without having to modify the Cisco software.

Other than using EEM to detect events, DS is triggered when a Tool Command Language (Tcl) script is used to specify event detection types.

Multiple Event Detection

Multiple event detection involves defining two or more event detectors, two or more corresponding tracked object states, and a time period for the events to occur. The specification format for multiple event detection can include complex event correlation for tracked event detectors. For example, three event detectors—syslog, OIR, and IPSLA—are defined during the creation of a DS file. The correlation that is specified for these event detectors is that the DS will execute its action if both syslog and OIR events are triggered simultaneously, or if IPSLA is triggered alone.

Diagnostic Signature Actions and Variables

The diagnostic signature (DS) files consists of various actions that must be initiated when an event occurs. The action type indicates the kind of action that will be initiated in response to a certain event.

Variables are elements within a DS file that are used to customize the files.

Action Types

DS actions are categorized into the following four types:

- Call-home
- Command
- Emailto
- Script

DS action types call-home and emailto collect event data and send a message to call-home servers or to the defined email addresses. The message includes the following elements:

- Message type—diagnostic-signature
- Message subtype—ds-id
- Message description—event-id : ds name

The commands defined for the DS action type initiates CLI commands that can change configuration of the device. The DS action type script executes Tcl scripts.

Variables

Variables are referenced within a DS and are used to customize the DS file. All DS variable names have the prefix ds_ to separate them from other variables. In some situations, DS runs a set of commands simultaneously based on the last command result or a set of commands based on the variables defined within a DS. The following are the supported DS variable types:

- System variable—values assigned automatically by the device without any configuration changes. The Diagnostic Signatures feature supports two types of system variables: ds_hostname and ds_signature_id.
- Environment variable—values assigned manually by using the **environment** *variable-name variable-value* command in call-home diagnostic-signature configuration mode. Use the **show call-home diagnostic-signature** command to display the name and value of all DS environment variables.
- Prompt variable—values assigned manually by using the **call-home diagnostic-signature install** *ds-id* command in privileged EXEC mode. If you do not set this value, the status of the DS indicates pending.
- Regular expression variable—values assigned from a regular expression pattern match with predefined CLI command outputs.
- Syslog event variable—values assigned during an event detection in the DS file. This variable is valid only for syslog event detection.

How to Configure Diagnostic Signatures

Configuring Service Call-Home for Diagnostic Signatures

Configure the service call-home feature to set attributes such as the contact email address where notifications regarding diagnostic signature (DS) downloads are sent and destination HTTP/secure HTTP (HTTPS) URL to download the DS files from. These attributes are set for the call-home profile user1. For periodic downloads, schedule the time when the diagnostic signature files must be downloaded.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **service call-home**
4. **call-home**
5. **contact-email-addr** *email-address*
6. **mail-server** {*ipv4-addr* | *name*} **priority** *number*
7. **profile** *profile-name*
8. **destination transport-method** {**email** | **http**}
9. **destination address** {**email** *address* | **http** *url*}
10. **subscribe-to-alert-group inventory** [**periodic** {**daily** *hh:mm* | **monthly** *day hh:mm* | **weekly** *day hh:mm*}]
11. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**service call-home** **Example:** `Device(config)# service call-home`	Enables call-home service on a device.
Step 4	**call-home** **Example:** `Device(config)# call-home`	Enters call-home configuration mode for the configuration of call-home settings.

	Command or Action	Purpose
Step 5	**contact-email-addr** *email-address* **Example:** `Device(cfg-call-home)# contact-email-addr userid@example.com`	(Optional) Assigns an email address to be used for call-home customer contact.
Step 6	**mail-server** {*ipv4-addr* | *name*} **priority** *number* **Example:** `Device(cfg-call-home)# mail-server 10.1.1.1 priority 4`	Configures a Simple Mail Transfer Protocol (SMTP) email server address for call-home.
Step 7	**profile** *profile-name* **Example:** `Device(cfg-call-home)# profile user1`	Configures a destination profile for call-home and enters call-home profile configuration mode.

Step 8	**destination transport-method** {**email** | **http**}
	Example:
	`Device(cfg-call-home-profile)# destination transport-method http`
		Specifies a transport method for a destination profile in the call-home.

Step 9	**destination address** {**email** *address* | **http** *url*}
	Example:
	`Device(cfg-call-home-profile)# destination address http https://tools-stage.cisco.com/its/service/oddce/services/DDCEService`
		Configures the address type and location to which call-home messages are sent.

Step 10	**subscribe-to-alert-group inventory** [**periodic** {**daily** *hh:mm* | **monthly** *day hh:mm* | **weekly** *day hh:mm*}] **Example:** `Device(cfg-call-home-profile)# subscribe-to-alert-group inventory periodic daily 14:30`	Configures a destination profile to receive messages for the Inventory alert group for call-home. • This command is used only for the periodic downloading of DS files.
Step 11	**exit** **Example:** `Device(cfg-call-home-profile)# exit`	Exits call-home profile configuration mode and returns to call-home configuration mode.

What to Do Next

Configure DS with profile user1 as described in the “Configuring Diagnostic Signatures” section. The attributes set for the call-home profile user1 apply to DS.

Configuring Diagnostic Signatures

Before You Begin

Configure the Service Call-Home feature to set attributes for the call-home profile user1 as described in the "Configuring Service Call-Home for Diagnostic Signatures" section. When you configure diagnostic signatures (DSes), define the same profile name user1. DS then uses the attributes set for user1.

SUMMARY STEPS

1. **diagnostic-signature**
2. **profile** *ds-profile-name*
3. **environment ds_** *env-varname ds-env-varvalue*
4. **end**
5. **call-home diagnostic-signature** {{**deinstall** | **download**} {*ds-id* | **all**} | **install** *ds-id*}
6. **show call-home diagnostic-signature** [*ds-id* [**actions** | **events** | **prerequisite** | **prompt** | **variables**] | **failure** | **statistics** [**download**]]
7. **debug call-home diagnostic-signature** {**action** | **all** | **api** | **cli** | **download** | **event-registration** | **parsing**}

DETAILED STEPS

	Command or Action	Purpose
Step 1	**diagnostic-signature** **Example:** `Device(cfg-call-home)# diagnostic-signature`	Enters call-home diagnostic signature mode.
Step 2	**profile** *ds-profile-name* **Example:** `Device(cfg-call-home-diag-sign)# profile user1`	Specifies the destination profile on a device that DS uses.
Step 3	**environment ds_** *env-varname ds-env-varvalue* **Example:** `Device(cfg-call-home-diag-sign)# environment ds_env1 envarval`	Sets the environment variable value for DS on a device.

Step 4	**end**
	Example:
	`Device(cfg-call-home-diag-sign)# end`
		Exits call-home diagnostic signature mode and returns to privileged EXEC mode.

Step 5	**call-home diagnostic-signature** {{**deinstall** | **download**} {*ds-id* | **all**} | **install** *ds-id*}
	Example:
	`Device# call-home diagnostic-signature download 6030`
		Downloads, installs, and uninstalls diagnostic signature files on a device.

	Command or Action	Purpose
Step 6	**show call-home diagnostic-signature** [*ds-id* [**actions** | **events** | **prerequisite** | **prompt** | **variables**] | **failure** | **statistics** [**download**]] **Example:** `Device# show call-home diagnostic-signature`	Displays the attributes and statistics of a call-home diagnostic signature file on a device.

Step 7	**debug call-home diagnostic-signature** {**action** | **all** | **api** | **cli** | **download** | **event-registration** | **parsing**}
	Example:
	`Device# debug call-home diagnostic-signature all`
		Displays debugging of one or all of the call-home diagnostic signature flags on a device.

Configuration Examples for Diagnostic Signatures

Examples: Configuring Diagnostic Signatures

The following example shows how to enable the periodic downloading request for diagnostic signature (DS) files. This configuration will send download requests to the service call-home server daily at 2:30 p.m. to check for updated DS files. The transport method is set to HTTP.

```
Device> enable
Device# configure terminal
Device(config)# service call-home
Device(config)# call-home
Device(cfg-call-home)# contact-email-addr userid@example.com
Device(cfg-call-home)# mail-server 10.1.1.1 priority 4
Device(cfg-call-home)# profile user-1
Device(cfg-call-home-profile)# destination transport-method http
Device(cfg-call-home-profile)# destination address http
https://tools-dev.cisco.com/its/service/oddce/services/DDCEService
Device(cfg-call-home-profile)# subscribe-to-alert-group inventory periodic daily 14:30
Device(cfg-call-home-profile)# exit
Device(cfg-call-home)# diagnostic-signature
Device(cfg-call-home-diag-sign)# profile user1
Device(cfg-call-home-diag-sign)# environment ds_env1 envarval
Device(cfg-call-home-diag-sign)# end
```

The following is sample output from the **show call-home diagnostic-signature** command for the configuration displayed above:

```
Device# show call-home diagnostic-signature

Current diagnostic-signature settings:
Diagnostic-signature: enabled
Profile: user1 (status: ACTIVE)
Environment variable:
ds_env1: abc
Downloaded DSes:
DS ID    DS Name                          Revision Status     Last Update (GMT+00:00)
-------- -------------------------------- -------- ---------- -------------------
6015     CronInterval                     1.0      registered 2013-01-16 04:49:52
6030     ActCH                            1.0      registered 2013-01-16 06:10:22
```

```
6032     MultiEvents                     1.0      registered 2013-01-16 06:10:37
6033     PureTCL                         1.0      registered 2013-01-16 06:11:48
```

Configuring Call Home

The Call Home feature provides e-mail-based and web-based notification of critical system events. A versatile range of message formats are available for optimal compatibility with pager services, standard e-mail, or XML-based automated parsing applications. Common uses of this feature may include direct paging of a network support engineer, e-mail notification to a Network Operations Center, XML delivery to a support website, and utilization of Cisco Smart Call Home services for direct case generation with the Cisco Systems Technical Assistance Center (TAC).

This document describes how to configure the Call Home feature on Cisco ASR 1000 Series Aggregation Services Routers beginning with Cisco IOS XE Release 2.6.

How To Configure Call Home to Support the Smart Call Home Service

This section provides an overview of the minimum steps required to configure the Call Home feature on a Cisco device, and other required supporting configuration to communicate securely with the Smart Call Home service using HTTPS:

Prerequisites

Before you configure and use the Smart Call Home Service, be sure that you have completed the following prerequisites:

- Verify that you have an active Cisco Systems service contract for the device being configured.
- Verify that you have IP connectivity to the Cisco HTTPS server.
- Obtain the latest Cisco Systems server security certificate. In Cisco IOS XE Release 2.6.0, the following shows the latest text for the Cisco Systems server security certificate:

```
MIIDAjCCAmsCEH3Z/gfPqB63EHln+6eJNMYwDQYJKoZIhvcNAQEFBQAwgcExCzAJ
BgNVBAYTAlVTMRcwFQYDVQQKEw5WZXJpU2lnbiwgSW5jLjE8MDoGA1UECxMzQ2xh
c3MgMyBQdWJsaWMgUHJpbWFyeSBDZXJ0aWZpY2F0aW9uIEF1dGhvcml0eSAtIEcy
MTowOAYDVQQLEzEoYykgMTk5OCBWZXJpU2lnbiwgSW5jLiAtIEZvciBhdXRob3Jp
emVkIHVzZSBvbmx5MR8wHQYDVQQLExZWZXJpU2lnbiBUcnVzdCBOZXR3b3JrMB4X
DTk4MDUxODAwMDAwMFoXDTI4MDgwMTIzNTk1OVowgcExCzAJBgNVBAYTAlVTMRcw
FQYDVQQKEw5WZXJpU2lnbiwgSW5jLjE8MDoGA1UECxMzQ2xhc3MgMyBQdWJsaWMg
UHJpbWFyeSBDZXJ0aWZpY2F0aW9uIEF1dGhvcml0eSAtIEcyMTowOAYDVQQLEzEo
YykgMTk5OCBWZXJpU2lnbiwgSW5jLiAtIEZvciBhdXRob3JpemVkIHVzZSBvbmx5
MR8wHQYDVQQLExZWZXJpU2lnbiBUcnVzdCBOZXR3b3JrMIGfMA0GCSqGSIb3DQEB
AQUAA4GNADCBiQKBgQDMXtERXVxp0KvTuWpMmR9ZmDCOFoUgRm1HP9SFIIThbbP4
pO0M8RcPO/mn+SXXwc+EY/J8Y8+iR/LGWzOOZEAEaMGAuWQcRXfH2G71lSk8UOg0
13gfqLptQ5GVj0VXXn7F+8qkBOvqlzdUMG+7AUcyM83cV5tkaWH4mx0ciU9cZwID
AQABMA0GCSqGSIb3DQEBBQUAA4GBAFFNzb5cy5gZnBWyATl4Lk0PZ3BwmcYQWpSk
U01UbSuvDV1Ai2TT1+7eVmGSX6bEHRBhNtMsJzzoKQm5EWR0zLVznxxIqbxhAe7i
F6YM40AIOw7n60RzKprxaZLvcRTDOaxxp5EJb+RxBrO6WVcmeQD2+A2iMzAo1KpY
oJ2daZH9
```

Declare and Authenticate a CA Trustpoint

To establish communication with the Cisco HTTPS server for Smart Call Home service, you must declare and authenticate the Cisco server security certificate.

SUMMARY STEPS

1. **configure terminal**
2. **crypto pki trustpoint** *name*
3. **enrollment terminal**
4. **exit**
5. **crypto pki authenticate** *name*
6. At the prompt, paste the security certificate text.
7. **quit**
8. **yes**
9. **end**
10. copy running-config startup-config

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Router#` **configure terminal**	Enters global configuration mode.
Step 2	**crypto pki trustpoint** *name* **Example:** `Router(config)#` **crypto pki trustpoint cisco**	Declares a CA trustpoint on your router and enters CA trustpoint configuration mode.
Step 3	**enrollment terminal** **Example:** `Router(ca-trustpoint)#` **enrollment terminal**	Specifies a manual cut-and-paste method of certificate enrollment.
Step 4	**exit** **Example:** `Router(ca-trustpoint)#` **exit**	Exits CA trustpoint configuration mode and returns to global configuration mode.
Step 5	**crypto pki authenticate** *name* **Example:** `Router(config)#` **crypto pki authenticate cisco**	Authenticates the named CA. **Note** The CA name should match the *name* specified in the **crypto pki trustpoint** command.

	Command or Action	Purpose

Step 6	At the prompt, paste the security certificate text.
	Example:
	`Enter the base 64 encoded CA certificate.`
	Example:
	`End with a blank line or the word "quit" on a line by itself`
	Example:
	`<Paste certificate text here>`
		Specifies the security certificate text.

Step 7	**quit** **Example:** **quit**	Specifies the end of the security certificate text.
Step 8	**yes** **Example:** **% Do you accept this certificate? [yes/no]: yes**	Confirms acceptance of the entered security certificate.
Step 9	**end** **Example:** `Router#` **end**	Exits global configuration mode and returns to privileged EXEC mode.
Step 10	copy running-config startup-config **Example:** `Router#` **copy running-config startup-config**	Saves the configuration to NVRAM.

Examples

The following example shows the configuration for declaring and authenticating the Cisco server security certificate:

```
Router# configure terminal
Router(config)# crypto pki trustpoint cisco
Router(ca-trustpoint)# enrollment terminal
Router(ca-trustpoint)# exit
Router(config)# crypto pki authenticate cisco
Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself
MIIDAjCCAmsCEH3Z/gfPqB63EHln+6eJNMYwDQYJKoZIhvcNAQEFBQAwgcExCzAJ
BgNVBAYTAlVTMRcwFQYDVQQKEw5WZXJpU2lnbiwgSW5jLjE8MDoGA1UECxMzQ2xh
c3MgMyBQdWJsaWMgUHJpbWFyeSBDZXJ0aWZpY2F0aW9uIEF1dGhvcml0eSAtIEcy
MTowOAYDVQQLEzEoYykgMTk5OCBWZXJpU2lnbiwgSW5jLiAtIEZvciBhdXRob3Jp
emVkIHVzZSBvbmx5MR8wHQYDVQQLExZWZXJpU2lnbiBUcnVzdCBOZXR3b3JrMB4X
DTk4MDUxODAwMDAwMFoXDTI4MDgwMTIzNTk1OVowgcExCzAJBgNVBAYTAlVTMRcw
```

```
FQYDVQQKEw5WZXJpU2lnbiwgSW5jLjE8MDoGA1UECxMzQ2xhc3MgMyBQdWJsaWMg
UHJpbWFyeSBDZXJ0aWZpY2F0aW9uIEF1dGhvcml0eSAtIEcyMTowOAYDVQQLEzEo
YykgMTk5OCBWZXJpU2lnbiwgSW5jLiAtIEZvciBhdXRob3JpemVkIHVzZSBvbmx5
MR8wHQYDVQQLExZWZXJpU2lnbiBUcnVzdCBOZXR3b3JrMIGfMA0GCSqGSIb3DQEB
AQUAA4GNADCBiQKBgQDMXtERXVxp0KvTuWpMmR9ZmDCOFoUgRm1HP9SFIIThbbP4
pO0M8RcPO/mn+SXXwc+EY/J8Y8+iR/LGWzOOZEAEaMGAuWQcRXfH2G71lSk8UOg0
13gfqLptQ5GVj0VXXn7F+8qkBOvqlzdUMG+7AUcyM83cV5tkaWH4mx0ciU9cZwID
AQABMA0GCSqGSIb3DQEBBQUAA4GBAFFNzb5cy5gZnBWyATl4Lk0PZ3BwmcYQWpSk
U01UbSuvDV1Ai2TT1+7eVmGSX6bEHRBhNtMsJzzoKQm5EWR0zLVznxxIqbxhAe7i
F6YM40AIOw7n60RzKprxaZLvcRTDOaxxp5EJb+RxBrO6WVcmeQD2+A2iMzAo1KpY
oJ2daZH9
quit
Certificate has the following attributes:
       Fingerprint MD5: A2339B4C 747873D4 6CE7C1F3 8DCB5CE9
      Fingerprint SHA1: 85371CA6 E550143D CE280347 1BDE3A09 E8F8770F
% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
% Certificate successfully imported
Router(config)# end
Router# copy running-config startup-config
```

Start Smart Call Home Registration

To start the Smart Call Home registration process, manually send an inventory alert-group message to the CiscoTAC-1 profile.

SUMMARY STEPS

1. **call-home send alert-group inventory profile CiscoTAC-1**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**call-home send alert-group inventory profile CiscoTAC-1** **Example:** `Device#` **call-home send alert-group inventory profile CiscoTAC-1**	Sends an inventory alert group message to the CiscoTAC-1 destination profile.

What To Do Next

To receive an email from Cisco Systems and follow the instructions to complete the device registration in the Smart Call Home web application:

- Launch the Smart Call Home web application at the following URL:

https://tools.cisco.com/sch/

- Accept the Legal Agreement.
- Confirm device registration for Call Home devices with pending registration.

For more information about using the Smart Call Home web application, see *Smart Call Home User Guide* . This user guide also includes configuration examples for sending Smart Call Home messages directly from your device or through a transport gateway (TG) aggregation point. You can use a TG aggregation point in cases requiring support for multiple devices or in cases where security requirements mandate that your devices must not be connected directly to the Internet.

Displaying Call Home Configuration Information

You can use variations of the **show call-home** command to display Call Home configuration information.

To display the configured Call Home information, use one or more of the following commands:

SUMMARY STEPS

1. **show call-home**
2. **show call-home detail**
3. **show call-home alert-group**
4. **show call-home mail-server status**
5. **show call-home profile** {**all** | *name*}
6. **show call-home statistics**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**show call-home** **Example:** `Device# show call-home`	Displays the Call Home configuration in summary.
Step 2	**show call-home detail** **Example:** `Device# show call-home detail`	Displays the Call Home configuration in detail.
Step 3	**show call-home alert-group** **Example:** `Device# show call-home alert-group`	Displays the available alert groups and their status.
Step 4	**show call-home mail-server status** **Example:** `Device# show call-home mail-server status`	Checks and displays the availability of the configured e-mail server(s).

Step 5	**show call-home profile** {**all** | *name*}
	Example:
	`Device# show call-home profile all`
		Displays the configuration of the specified destination profile. Use the **all** keyword to display the configuration of all destination profiles.

	Command or Action	Purpose
Step 6	**show call-home statistics** **Example:** `Device#` **show call-home statistics**	Displays the statistics of Call Home events.

Configuration Examples for Call Home

The following examples show the sample output when using different options of the **show call-home** command.

Example: Call Home Information in Summary

```
Device# show call-home
Current call home settings:
    call home feature : disable
    call home message's from address: username@example.com
    call home message's reply-to address: username@example.com
    vrf for call-home messages: Mgmt-intf
    contact person's email address: username@example.com
    contact person's phone number: +14085551234
    street address: 1234 Any Street Any city Any state 12345
    customer ID: customer@example.com
    contract ID: 123456789
    site ID: example.com
    Mail-server[1]: Address: smtp.example.com Priority: 1
    Mail-server[2]: Address: 192.168.0.1 Priority: 2
    Rate-limit: 20 message(s) per minute
Available alert groups:
    Keyword                  State   Description
    ------------------------ ------- -------------------------------
    configuration            Enable  configuration info
    diagnostic               Enable  diagnostic info
    environment              Enable  environmental info
    inventory                Enable  inventory info
    syslog                   Enable  syslog info
Profiles:
    Profile Name: campus-noc
    Profile Name: CiscoTAC-1
```

Example: Configured Call Home Information in Detail

```
Device# show call-home detail
Current call home settings:
   call home feature: enable
   call home message's from address: router@example.com
   call home message's reply-to address: support@example.com
   vrf for call-home messages: Not yet set up
   contact person's email address: technical@example.com
   contact person's phone number: +1-408-555-1234
   street address: 1234 Picaboo Street, Any city, Any state, 12345
   customer ID: ExampleCorp
   contract ID: X123456789
   site ID: SantaClara
   source ip address: Not yet set up
   source interface: GigabitEthernet1
   Mail-server[1]: Address: 192.168.2.1 Priority: 1
   Mail-server[2]: Address: 223.255.254.254 Priority: 2
   http proxy: 192.168.1.1:80
   aaa-authorization: disable
   aaa-authorization username: callhome (default)
   data-privacy: normal
   syslog throttling: enable
   Rate-limit: 20 message(s) per minute
   Snapshot command[0]: show version
   Snapshot command[1]: show clock
Available alert groups:
   Keyword State Description
   ------------------------ ------- -------------------------------
   configuration Enable configuration info
   crash Enable crash and traceback info
   inventory Enable inventory info
   snapshot Enable snapshot info
   syslog Enable syslog info
Profiles:
   Profile Name: campus-noc
   Profile status: ACTIVE
   Preferred Message Format: xml
   Message Size Limit: 3145728 Bytes
Transport Method: email
   Email address(es): noc@example.com
   HTTP address(es): Not yet set up
   Alert-group Severity
   ------------------------ ------------
   configuration            normal
   crash                    normal
   inventory                normal
   Syslog-Pattern           Severity
   ------------------------ ------------
   .*CALL_LOOP.* debug
Profile Name: CiscoTAC-1
   Profile status: INACTIVE
   Profile mode: Full Reporting
   Preferred Message Format: xml
   Message Size Limit: 3145728 Bytes
   Transport Method: email
   Email address(es): callhome@cisco.com
   HTTP address(es): https://tools.cisco.com/its/service/oddce/services/DDCEService
   Periodic configuration info message is scheduled every 14 day of the month at 11:12
   Periodic inventory info message is scheduled every 14 day of the month at 10:57
   Alert-group Severity
   ------------------------ ------------
   crash                    normal
   Syslog-Pattern           Severity
   ------------------------ ------------
   .*CALL_LOOP.*            debug
```

Example: Available Call Home Alert Groups

```
Device# show call-home alert-group
Available alert groups:
   Keyword State Description
   ------------------------ ------- -------------------------------
   configuration Enable configuration info
   crash Enable crash and traceback info
   inventory Enable inventory info
   snapshot Enable snapshot info
   syslog Enable syslog info
```

Example: Email Server Status Information

```
Device# show call-home mail-server status
Please wait. Checking for mail server status ...
     Mail-server[1]: Address: 192.168.2.1 Priority: 1 [Not Available]
     Mail-server[2]: Address: 223.255.254.254 Priority: 2 [Available]
```

Examples: Information for All Destination Profiles

```
Device# show call-home profile all
     Profile Name: campus-noc
     Profile status: ACTIVE
     Preferred Message Format: xml
     Message Size Limit: 3145728 Bytes
     Transport Method: email
     Email address(es): noc@example.com
     HTTP address(es): Not yet set up
     Alert-group Severity
     ------------------------ ------------
     configuration               normal
     crash                       normal
     inventory                   normal
     Syslog-Pattern              Severity
     ------------------------ ------------
     .*CALL_LOOP.* debug
Profile Name: CiscoTAC-1
     Profile status: INACTIVE
     Profile mode: Full Reporting
     Preferred Message Format: xml
     Message Size Limit: 3145728 Bytes
     Transport Method: email
     Email address(es): callhome@cisco.com
     HTTP address(es): https://tools.cisco.com/its/service/oddce/services/DDCEService

     Periodic configuration info message is scheduled every 14 day of the month at 11:12

     Periodic inventory info message is scheduled every 14 day of the month at 10:57
     Alert-group                 Severity
     ------------------------ ------------
     crash                       normal
     Syslog-Pattern              Severity
     ------------------------ ------------
     .*CALL_LOOP.*               debug
```

Example: Information for a User-Defined Destination Profile

```
Device# show call-home profile campus-noc
Profile Name: campus-noc
    Profile status: ACTIVE
    Preferred Message Format: xml
    Message Size Limit: 3145728 Bytes
    Transport Method: email
    Email address(es): noc@example.com
    HTTP address(es): Not yet set up
    Alert-group                Severity
    ------------------------ ------------
    configuration              normal
    crash                      normal
    inventory                  normal
    Syslog-Pattern             Severity
    ------------------------ ------------
    .*CALL_LOOP.*              debug
```

Example: Call Home Statistics

```
Device# show call-home statistics
Message Types   Total                Email                HTTP
-------------   -------------------- -------------------- ------------------
Total Success   3                    3                    0
    Config      3                    3                    0
    Diagnostic  0                    0                    0
    Environment 0                    0                    0
    Inventory   2                    2                    0
    SysLog      0                    0                    0
    Test        0                    0                    0
    Request     0                    0                    0
    Send-CLI    0                    0                    0
Total In-Queue  0                    0                    0
    Config      0                    0                    0
    Diagnostic  0                    0                    0
    Environment 0                    0                    0
    Inventory   0                    0                    0
    SysLog      0                    0                    0
    Test        0                    0                    0
    Request     0                    0                    0
    Send-CLI    0                 0                 0
Total Failed    0                 0                 0
    Config      0                 0                 0
    Diagnostic  0                 0                 0
    Environment 0                 0                 0
    Inventory   0                 0                 0
    SysLog      0                 0                 0
    Test        0                 0                 0
    Request     0                 0                 0
    Send-CLI    0                 0                 0
Total Ratelimit
      -dropped  0                 0                 0
    Config      0                 0                 0
    Diagnostic  0                 0                 0
    Environment 0                 0                 0
    Inventory   0                 0                 0
    SysLog      0                 0                 0
    Test        0                 0                 0
    Request     0                 0                 0
    Send-CLI    0                 0                 0
Last call-home message sent time: 2010-01-11 18:32:32 GMT+00:00
```

Default Settings

Lists of default Call Home settings.

Parameters	Default
Call Home feature status	Disabled
User-defined profile status	Active
Predefined Cisco TAC profile status	Inactive
Transport method	E-mail
Message format type	XML
Destination message size for a message sent in long text, short text, or XML format	3,145,728
Alert group status	Enabled
Call Home message severity threshold	0 (debugging)
Message rate limit for messages per minute	20
AAA Authorization	Disabled
Call Home syslog message throttling	Enabled
Data privacy level	Normal

Alert Group Trigger Events and Commands

Call Home trigger events are grouped into alert groups, with each alert group assigned CLI commands to execute when an event occurs. The CLI command output is included in the transmitted message. Table 4: Call Home Alert Groups, Events, and Actions , on page 81 lists the trigger events included in each alert group, including the severity level of each event and the executed CLI commands for the alert group.

Table 4: Call Home Alert Groups, Events, and Actions

Alert Group	Call Home Trigger Event	Syslog Event	Severity	Description and CLI Commands Executed
Crash	SYSTEM_CRASH	—	—	Events related to system crash. Commands executed: **show version show logging show region show stack**
—	TRACEBACK	—	—	Detects software traceback events. Commands executed: **show version show logging show region show stack**
Configuration	—	—	—	User-generated request for configuration. (Sent to TAC.) CLI commands executed: **show platform show inventory show running-config all show startup-config show version**
Diagnostic	—	—	—	CLI commands executed: **show platform show diagnostic result slot x detail show version show inventory show buffers show logging show diagnostic result slot all show diagnostic events slot all**

Alert Group	Call Home Trigger Event	Syslog Event	Severity	Description and CLI Commands Executed
Environmental	—	—	—	Events related to power, fan, and environment sensing elements, such as temperature alarms. (Sent to TAC.) CLI commands executed: **show platform show environment show inventory show logging**
Inventory	—	—	—	Inventory status should be provided whenever a unit is cold-booted, or when FRUs are inserted or removed. This is considered a noncritical event, and the information is used for status and entitlement. (Sent to TAC.) CLI commands executed: **show diag all eeprom detail | include MAC show license all show platform show platform hardware qfp active infrastructure chipset 0 capabilities show platform software vnic-if interface-mapping show version**
Syslog	—	—	—	Event logged to syslog. CLI commands executed: **show logging**

Message Contents

The following tables display the content formats of alert group messages:

- The **Format for a Short Text Message** table describes the content fields of a short text message.

- The **Common Fields for All Long Text and XML Messages** table describes the content fields that are common to all long text and XML messages. The fields specific to a particular alert group message are inserted at a point between the common fields. The insertion point is identified in the table.
- The **Inserted Fields for a Reactive or Proactive Event Message** table describes the inserted content fields for reactive messages (system failures that require a TAC case) and proactive messages (issues that might result in degraded system performance).
- The **Inserted Fields for an Inventory Event Message** table describes the inserted content fields for an inventory message.

This section also includes the following subsections that provide sample messages:

Table 5: Format for a Short Text Message

Data Item	Description
Device identification	Configured device name
Date/time stamp	Time stamp of the triggering event
Error isolation message	Plain English description of triggering event
Alarm urgency level	Error level such as that applied to a system message

Table 6: Common Fields for All Long Text and XML Messages

Data Item (Plain Text and XML)	Description (Plain Text and XML)	MML Tag (XML Only)
Time stamp	Date and time stamp of event in ISO time notation: *YYYY-MM-DD HH:MM:SS GMT+HH:MM*.	CallHome/EventTime
Message name	Name of message. Specific event names are listed in the **Alert Group Trigger Events and Commands** section.	For short text message only
Message type	Specifically “Call Home”.	CallHome/Event/Type
Message subtype	Specific type of message: full, delta, test	CallHome/Event/SubType
Message group	Specifically “reactive”. Optional, because default is “reactive”.	Not applicable. For long-text message only
Severity level	Severity level of message.	Body/Block/Severity
Source ID	Product type for routing through the workflow engine. This is typically the product family name.	For long-text message only

Data Item (Plain Text and XML)	Description (Plain Text and XML)	MML Tag (XML Only)
Device ID	Unique device identifier (UDI) for end device generating message. This field should be empty if the message is nonspecific to a fabric switch. The format is *type@Sid@seria* l. • *type* is the product model number from backplane IDPROM. • @ is a separator character. • *Sid* is C, identifying the serial ID as a chassis serial number. • *serial* is the number identified by the Sid field. Example: ASR1006@C@FOX105101DH	CallHome/CustomerData/ ContractData/DeviceId
Customer ID	Optional user-configurable field used for contract information or other ID by any support service.	CallHome/CustomerData/ ContractData/CustomerId
Contract ID	Optional user-configurable field used for contract information or other ID by any support service.	CallHome/CustomerData/ ContractData/ContractId
Site ID	Optional user-configurable field used for site IDs supplied by Cisco Systems or other data meaningful to alternate support services.	CallHome/CustomerData/ ContractData/SiteId
Server ID	If the message is generated from the fabric switch, this is the unique device identifier (UDI) of the switch. The format is *type@Sid@seria* l. • *type* is the product model number from backplane IDPROM. • @ is a separator character. • *Sid* is C, identifying the serial ID as a chassis serial number. • *serial* is the number identified by the Sid field. Example: ASR1006@C@FOX105101DH	For long text message only
Message description	Short text describing the error.	CallHome/MessageDescription
Device name	Node that experienced the event. This is the host name of the device.	CallHome/CustomerData/ SystemInfo/NameName

Data Item (Plain Text and XML)	Description (Plain Text and XML)	MML Tag (XML Only)	
Contact name	Name of person to contact for issues associated with the node experiencing the event.	CallHome/CustomerData/ SystemInfo/Contact	
Contact e-mail	E-mail address of person identified as contact for this unit.	CallHome/CustomerData/ SystemInfo/ContactEmail	
Contact phone number	Phone number of the person identified as the contact for this unit.	CallHome/CustomerData/ SystemInfo/ContactPhoneNumber	
Street address	Optional field containing street address for RMA part shipments associated with this unit.	CallHome/CustomerData/ SystemInfo/StreetAddress	
Model name	Model name of the router. This is the “specific model as part of a product family name.	CallHome/Device/Cisco_Chassis/ Model	
Serial number	Chassis serial number of the unit.	CallHome/Device/Cisco_Chassis/ SerialNumber	
Chassis part number	Top assembly number of the chassis.	CallHome/Device/Cisco_Chassis/ AdditionalInformation/AD@name= “PartNumber”	
System object ID	System Object ID that uniquely identifies the system.	CallHome/Device/Cisco_Chassis/ AdditionalInformation/AD@name= “sysObjectID”	
System description	System description for the managed element.	CallHome/Device/Cisco_Chassis/ AdditionalInformation/AD@name= “sysDescr”	
Fields specific to a particular alert group message are inserted here.	The following fields may be repeated if multiple CLI commands are executed for this alert group.		
	Command output name	The exact name of the issued CLI command.	/aml/Attachments/Attachment/Name
	Attachment type	Attachment type. Usually “inline”.	/aml/Attachments/Attachment@type
	MIME type	Normally “text” or “plain” or encoding type.	/aml/Attachments/Attachment/ Data@encoding
	Command output text	Output of command automatically executed.	/mml/attachments/attachment/atdata

Table 7: Inserted Fields for a Reactive or Proactive Event Message

Data Item (Plain Text and XML)	Description (Plain Text and XML)	MML Tag (XML Only)
Chassis hardware version	Hardware version of chassis.	CallHome/Device/Cisco_Chassis/HardwareVersion
Supervisor module software version	Top-level software version.	CallHome/Device/Cisco_Chassis/AdditionalInformation/AD@name= “SoftwareVersion”
Affected FRU name	Name of the affected FRU generating the event message.	CallHome/Device/Cisco_Chassis/Cisco_Card/Model
Affected FRU serial number	Serial number of affected FRU.	CallHome/Device/Cisco_Chassis/Cisco_Card/SerialNumber
Affected FRU part number	Part number of affected FRU.	CallHome/Device/Cisco_Chassis/Cisco_Card/PartNumber
FRU slot	Slot number of FRU generating the event message.	CallHome/Device/Cisco_Chassis/Cisco_Card/LocationWithinContainer
FRU hardware version	Hardware version of affected FRU.	CallHome/Device/Cisco_Chassis/Cisco_Card/HardwareVersion
FRU software version	Software version(s) running on affected FRU.	CallHome/Device/Cisco_Chassis/Cisco_Card/SoftwareIdentity/VersionString

Table 8: Inserted Fields for an Inventory Event Message

Data Item (Plain Text and XML)	Description (Plain Text and XML)	MML Tag (XML Only)
Chassis hardware version	Hardware version of chassis.	CallHome/Device/Cisco_Chassis/HardwareVersion
Supervisor module software version	Top-level software version.	CallHome/Device/Cisco_Chassis/AdditionalInformation/AD@name= “SoftwareVersion”
FRU name	Name of the affected FRU generating the event message.	CallHome/Device/Cisco_Chassis/Cisco_Card/Model
FRU s/n	Serial number of FRU.	CallHome/Device/Cisco_Chassis/Cisco_Card/SerialNumber
FRU part number	Part number of FRU.	CallHome/Device/Cisco_Chassis/Cisco_Card/PartNumber

Data Item (Plain Text and XML)	Description (Plain Text and XML)	MML Tag (XML Only)
FRU slot	Slot number of FRU.	CallHome/Device/Cisco_Chassis/ Cisco_Card/LocationWithinContainer
FRU hardware version	Hardware version of FRU.	CallHome/Device/Cisco_Chassis/ CiscoCard/HardwareVersion
FRU software version	Software version(s) running on FRU.	CallHome/Device/Cisco_Chassis/ Cisco_Card/SoftwareIdentity/ VersionString

Sample Syslog Alert Notification in XML Format

The following example shows a sample syslog alert notification in XML format:

```
<?xml version="1.0" encoding="UTF-8"?>
<soap-env:Envelope xmlns:soap-env="http://www.w3.org/2003/05/soap-envelope">
<soap-env:Header>
<aml-session:Session xmlns:aml-session="http://www.cisco.com/2004/01/aml-session"
soap-env:mustUnderstand="true"
soap-env:role="http://www.w3.org/2003/05/soap-envelope/role/next">
<aml-session:To>http://tools.cisco.com/neddce/services/DDCEService</aml-session:To>
<aml-session:Path>
<aml-session:Via>http://www.cisco.com/appliance/uri</aml-session:Via>
</aml-session:Path>
<aml-session:From>http://www.cisco.com/appliance/uri</aml-session:From>
<aml-session:MessageId>M8:9S1NMSF22DW:51AEAC68</aml-session:MessageId>
</aml-session:Session>
</soap-env:Header>
<soap-env:Body>
<aml-block:Block xmlns:aml-block="http://www.cisco.com/2004/01/aml-block">
<aml-block:Header>
<aml-block:Type>http://www.cisco.com/2005/05/callhome/syslog</aml-block:Type>
<aml-block:CreationDate>2013-06-05 03:11:36 GMT+00:00</aml-block:CreationDate>
<aml-block:Builder>
<aml-block:Name>CSR1000v</aml-block:Name>
<aml-block:Version>2.0</aml-block:Version>
</aml-block:Builder>
<aml-block:BlockGroup>
<aml-block:GroupId>G9:9S1NMSF22DW:51AEAC68</aml-block:GroupId>
<aml-block:Number>0</aml-block:Number>
<aml-block:IsLast>true</aml-block:IsLast>
<aml-block:IsPrimary>true</aml-block:IsPrimary>
<aml-block:WaitForPrimary>false</aml-block:WaitForPrimary>
</aml-block:BlockGroup>
<aml-block:Severity>2</aml-block:Severity>
</aml-block:Header>
<aml-block:Content>
<ch:CallHome xmlns:ch="http://www.cisco.com/2005/05/callhome" version="1.0">
<ch:EventTime>2013-06-05 03:11:36 GMT+00:00</ch:EventTime> <ch:MessageDescription>*Jun 5
03:11:36.041: %CLEAR-5-COUNTERS: Clear counter on all interfaces by
console</ch:MessageDescription> <ch:Event> <ch:Type>syslog</ch:Type>
<ch:SubType></ch:SubType> <ch:Brand>Cisco Systems</ch:Brand> <ch:Series>CSR1000v Cloud
Services Router</ch:Series> </ch:Event> <ch:CustomerData> <ch:UserData>
<ch:Email>weijuhua@cisco.com</ch:Email>
</ch:UserData>
<ch:ContractData>
<ch:CustomerId></ch:CustomerId>
<ch:SiteId></ch:SiteId>
<ch:ContractId></ch:ContractId>
<ch:DeviceId>CSR1000V@C@9S1NMSF22DW</ch:DeviceId>
</ch:ContractData>
```

```
<ch:SystemInfo>
<ch:Name>qiang-vm</ch:Name>
<ch:Contact></ch:Contact>
<ch:ContactEmail>weijuhua@cisco.com</ch:ContactEmail>
<ch:ContactPhoneNumber></ch:ContactPhoneNumber>
<ch:StreetAddress></ch:StreetAddress>
</ch:SystemInfo>
<ch:CCOID></ch:CCOID>
<ch:IdToken></ch:IdToken>
</ch:CustomerData>
<ch:Device>
<rme:Chassis xmlns:rme="http://www.cisco.com/rme/4.0">
<rme:Model>CSR1000V</rme:Model>
<rme:HardwareVersion></rme:HardwareVersion>
<rme:SerialNumber>9S1NMSF22DW</rme:SerialNumber>
<rme:AdditionalInformation>
<rme:AD name="PartNumber" value="" />
<rme:AD name="SoftwareVersion" value="15.4(20130604:093915)" /> <rme:AD
name="SystemObjectId" value="1.3.6.1.4.1.9.1.1537" /> <rme:AD name="SystemDescription"
value="Cisco IOS Software, CSR1000V Software (X86_64_LINUX_IOSD-ADVENTERPRISEK9-M),
Experimental Version 15.4(20130604:093915) [mcp_dev-qiazhou-ultra_ut 100] Copyright (c)
1986-2013 by Cisco Systems, Inc.
Compiled Tue 04-Jun-13 02:39 by jsmith" /> <rme:AD name="ServiceNumber" value="" />
<rme:AD name="ForwardAddress" value="" /> </rme:AdditionalInformation> </rme:Chassis>
</ch:Device> </ch:CallHome> </aml-block:Content> <aml-block:Attachments>
<aml-block:Attachment type="inline"> <aml-block:Name>show logging</aml-block:Name>
<aml-block:Data encoding="plain"> <![CDATA[show logging Syslog logging: enabled (0
messages dropped, 1 messages rate-limited, 0 flushes, 0 overruns, xml disabled, filtering
disabled)
No Active Message Discriminator.
No Inactive Message Discriminator.
Console logging: level debugging, 391 messages logged, xml disabled,
filtering disabled
Monitor logging: level debugging, 0 messages logged, xml disabled,
filtering disabled
Buffer logging: level debugging, 391 messages logged, xml disabled,
filtering disabled
Exception Logging: size (4096 bytes)
Count and timestamp logging messages: disabled
Persistent logging: disabled
No active filter modules.
Trap logging: level informational, 56 message lines logged
Logging Source-Interface: VRF Name:
Log Buffer (4096 bytes):
*Jun 5 03:11:18.295: %SYS-5-CONFIG_I: Configured from console by console
qiang-vm#]]></aml-block:Data> </aml-block:Attachment> </aml-block:Attachments>
</aml-block:Block> </soap-env:Body> </soap-env:Envelope>
```

Sample Smart Licensing Alert Notification in XML Format

The following example shows a Smart Licensing alert notification in XML format:

```
<?xml version="1.0" encoding="UTF-8"?>
<soap-env:Envelope xmlns:soap-env="http://www.w3.org/2003/05/soap-envelope">
<soap-env:Header>
<aml-session:Session xmlns:aml-session="http://www.cisco.com/2004/01/aml-session"
soap-env:mustUnderstand="true"
soap-env:role="http://www.w3.org/2003/05/soap-envelope/role/next">
<aml-session:To>http://tools.cisco.com/neddce/services/DDCEService</aml-session:To>
<aml-session:Path>
<aml-session:Via>http://www.cisco.com/appliance/uri</aml-session:Via>
</aml-session:Path>
<aml-session:From>http://www.cisco.com/appliance/uri</aml-session:From>
<aml-session:MessageId>M2:98I1W09R72W:5136E366</aml-session:MessageId>
</aml-session:Session>
</soap-env:Header>
<soap-env:Body>
<aml-block:Block xmlns:aml-block="http://www.cisco.com/2004/01/aml-block">
<aml-block:Header>
<aml-block:Type>http://www.cisco.com/2005/05/callhome/license</aml-block:Type>
```

```
<aml-block:CreationDate>2013-03-06 06:34:14 GMT+00:00</aml-block:CreationDate>
<aml-block:Builder>
<aml-block:Name>CSR1000v</aml-block:Name>
<aml-block:Version>2.0</aml-block:Version>
</aml-block:Builder>
<aml-block:BlockGroup>
<aml-block:GroupId>G3:98I1W09R72W:5136E366</aml-block:GroupId>
<aml-block:Number>0</aml-block:Number>
<aml-block:IsLast>true</aml-block:IsLast>
<aml-block:IsPrimary>true</aml-block:IsPrimary>
<aml-block:WaitForPrimary>false</aml-block:WaitForPrimary>
</aml-block:BlockGroup>
<aml-block:Severity>1</aml-block:Severity>
</aml-block:Header>
<aml-block:Content>
<ch:CallHome xmlns:ch="http://www.cisco.com/2005/05/callhome" version="1.0">
<ch:EventTime>2013-04-10 07:47:28 GMT+08:00</ch:EventTime>
<ch:MessageDescription>Smart Licensing </ch:MessageDescription>
<ch:Event>
<ch:Type>License</ch:Type>
<ch:SubType>Register</ch:SubType> <!maybe other values like certificate_renewal,
id_certificate_ack, poll_for_data, license_disable, license_usage, entitlement_request>
<ch:Brand>Cisco Systems</ch:Brand>
<ch:Series>CSR1000v Cloud Services Router</ch:Series>
</ch:Event>
<ch:CustomerData>
<ch:UserData>
<ch:Email>test@cisco.com</ch:Email>
</ch:UserData>
<ch:ContractData>
<ch:CustomerId></ch:CustomerId>
<ch:SiteId></ch:SiteId>
<ch:ContractId></ch:ContractId>
<ch:DeviceId>CSR1000V@C@98I1W09R72W</ch:DeviceId>
</ch:ContractData>
<ch:SystemInfo>
<ch:Name>router</ch:Name>
<ch:Contact></ch:Contact>
<ch:ContactEmail>test@cisco.com</ch:ContactEmail>
<ch:ContactPhoneNumber></ch:ContactPhoneNumber>
<ch:StreetAddress></ch:StreetAddress>
</ch:SystemInfo>
<ch-inv:CCOID>xxxx</ch-inv:CCOID>
<ch:IdToken>yyyy</ch:IdToken> <!either CCOID or IdToken needs to be specified when
subtype is Register>
</ch:CustomerData>
<ch:Device>
<rme:Chassis xmlns:rme="http://www.cisco.com/rme/4.0">
<rme:Model>CSR1000V</rme:Model>
<rme:HardwareVersion>1.4</rme:HardwareVersion>
<rme:SerialNumber>98I1W09R72W</rme:SerialNumber>
<rme:AdditionalInformation>
<rme:AD name="PartNumber" value="68-3376-01" />
<rme:AD name="SoftwareVersion" value="15.3(20130303:013635)" />
<rme:AD name="SystemObjectId" value="1.3.6.1.4.1.9.1.1537" />
<rme:AD name="SystemDescription" value="Cisco IOS Software, IOS-XE Software
(X86_64_LINUX_IOSD-ADVENTERPRISEK9-M), Experimental Version 15.3(20130303:013635)
[mcp_dev-BLD-BLD_MCP_DEV_LATEST_20130303_000028-ios 171]
Copyright (c) 1986-2013 by Cisco Systems, Inc.
Compiled Sat 02-Mar-13 20:49 by mcpre" />
<rme:AD name="ServiceNumber" value="" />
<rme:AD name="ForwardAddress" value="" />
</rme:AdditionalInformation>
</rme:Chassis>
</ch:Device>
</ch:CallHome>
</aml-block:Content>
<aml-block:Attachments>
<aml-block:Attachment type="inline">
<aml-block:Name>smart_licensing_data</aml-block:Name>
<aml-block:Data encoding="plain">
<![CDATA[…licensing data… ]]></aml-block:Data>
</aml-block:Attachment>
```

```
</aml-block:Attachments>
</aml-block:Block>
</soap-env:Body>
</soap-env:Envelope>
<response><![CDATA[{"signature":{"type":"SHA_1","value":"SIG_SIGNED_VALUE"},"response":"{\
"header\":null,\"status_code\":\"ERROR\",\"status_message\":\"Failed to process the
request.\",\"response_data\":\"\"}"}]]></response>
        <email>xxx@yyy.com</email><result xmlns="">succeeded</result>
    </soapenv:Body>
</soapenv:Envelope>
```

Additional References

The following sections provide references related to the Call Home feature.

Related Documents

Related Topic	Title
Cisco IOS XE commands	Cisco IOS Master Commands List, All Releases
Explains how the Smart Call Home service offers web-based access to important information on select Cisco devices and offers higher network availability, and increased operational efficiency by providing proactive diagnostics and real-time alerts.	Smart Call Home User Guide
Smart Call Home site page on Cisco.com for access to all related product information.	Cisco Smart Call Home site
Public Key Infrastructure (PKI) and Certificate Authority configuration in Cisco IOS XE software	Cisco IOS XE Security Configuration Guide: Secure Connectivity

Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

MIB	MIBs Link
CISCO-CALLHOME-MIB	To locate and download MIBs for selected platforms, Cisco IOS XE software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	—

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

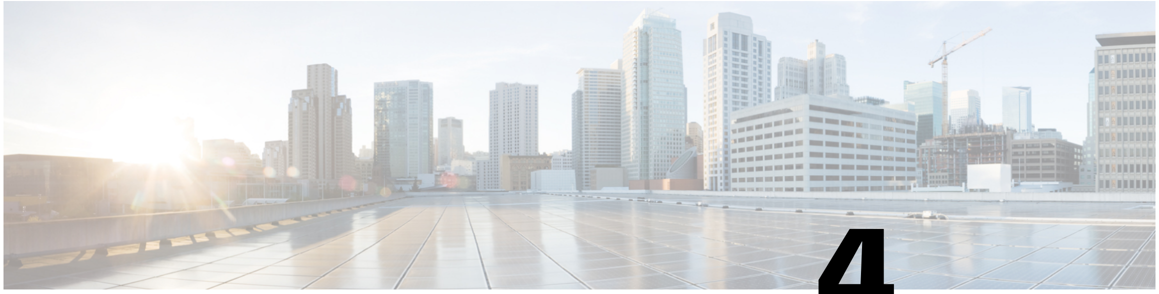
Feature Information for Call Home

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS XE software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn . An account on Cisco.com is not required.

Note The Feature Information table below lists only the Cisco IOS XE software release that introduced support for a given feature in a given Cisco IOS XE software release train. Unless noted otherwise, subsequent releases of that Cisco IOS XE software release train also support that feature.

Table 9: Feature Information for Call Home

Feature Name	Releases	Feature Information
Call Home	Cisco IOS XE Release 3.13S	The Call Home feature provides e-mail-based and web-based notification of critical system events. A versatile range of message formats are available for optimal compatibility with pager services, standard e-mail, or XML-based automated parsing applications. In Cisco IOS XE Release 2.6, support was added for the Cisco ASR 1000 Series Aggregation Services Routers. The following commands were introduced or modified: None **show diagnostic** commands
Smart Licensing	Cisco IOS XE Release 3.12S, 3.13S	The Smart Call Home feature is required to use the Smart Licensing service. The Smart Licensing service is an alternative licensing architecture to Cisco Software Licensing (CSL). Smart Call Licensing uses the Cisco Smart Software Manager as a backend tool for managing licenses. Smart Licensing support has been provided on the Cisco CSR 1000V on a controlled-availability basis beginning with Cisco IOS XE Release 3.12S. The following commands are new or modified: **show diagnostic** commands.



CHAPTER 4

Cisco Smart Licensing Client

Smart Licensing Client feature is a standardized licensing platform that simplifies the Cisco software experience and helps you to understand how Cisco software is used across your network. Smart Licensing is the next generation licensing platform for all Cisco software products.

This document provides an overview of the Cisco Smart Licensing Client feature and describes the several tools and processes required to complete the products registration and authorization.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Cisco Smart Licensing Client

- Ensure that Call Home is not disabled before using the Smart Licensing Client feature.

- Ensure that Cisco One Suites is configured before enabling Smart Licensing on the device.

Restrictions for Cisco Smart Licensing Client

- Only Cisco One Suites is supported in Cisco Smart Licensing for the current release.
- Only one licensing mode, either the Classical Licensing (CISL) or the Smart Licensing mode is supported at one point in time.

Information About Cisco Smart Licensing Client

Cisco Smart Licensing - An Overview

A new licensing model, based on a single technology, has been designed for Cisco called Smart Licensing that is intended to provide Enterprise Level Agreement-like capabilities for all of Cisco's products.

Smart Licensing is software based licensing end-to-end platform that consists of several tools and processes to authorize customers the usage and reporting of the Cisco products. The feature has the capability to capture the customers order and communicates with Cisco Cloud License Service through Smart Call Home transport media to complete the products registration and authorization on desired performance and technology level.

The Smart Licensing feature is aimed at giving users an experience of a single, standardized licensing solution for all Cisco products.

To know more about Smart Call Home, please refer to Smart Call Home.

Transitioning from CISL to Smart Licensing

In the Smart Licensing Model, customers can activate licensed objects without the use of a special software key or upgrade license file. The customers simply activate the new functionality using the appropriate product commands and configurations and the functionality is activated. A software reboot may or may not be required depending on the product capabilities and requirements.

Similarly, downgrading or removing an advanced feature, performance, or functionality would require a removal of the configuration or command.

Once either of these actions has been taken, the change in license state is noted by the Smart Software Manager upon next synchronization and an appropriate action is then taken.

Cisco One Suites

Cisco ONE Suites is a new way for customers to purchase infrastructure software. Cisco ONE offers a simplified purchasing model, centered on common customer scenarios in the data center, wide area network, and local access networks. To know more about Cisco One Suites, please refer to Cisco ONE Suites.

How to Activate Cisco Smart Licensing Client

Enable Smart Licensing

Before You Begin

Before you enable Smart Licensing, ensure that Cisco One Suites is already enabled on your device. To know how to enable Cisco One Suites, please refer to Activating Cisco One Suite License.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **license smart enable**
4. **exit**
5. **write memory**
6. **reload**
7. **show license all**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**license smart enable** **Example:** `Device# license smart enable`	Activates Smart Licensing on the device. **Note** When you enable Smart Licensing, the Cisco Software License (CSL) and all licensing calls pass through the Smart Agent. For the ‘no’ case, if Smart Licensing is already registered, the Smart Agent performs the ”license smart deregister” operation that deactivates Smart Licensing. Reload the device to activate the CSL on the device.
Step 4	**exit** **Example:** `Device# exit`	Exits the global configuration mode.

	Command or Action	Purpose
Step 5	**write memory** **Example:** `Device# write memory`	Saves the running configuration to NVRAM.
Step 6	**reload** **Example:** `Device# reload`	(Optional) Restarts the device to enable the new feature set. **Note** Reload the device if you have not reloaded the device after configuring the Cisco One Suites.
Step 7	**show license all** **Example:** `Device# show license all`	(Optional) Displays summary information about all licenses.

Smart License Disable

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **no license smart enable**
4. **license accept end user agreement**
5. **exit**
6. **write memory**
7. **reload**
8. **show license all**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**no license smart enable** **Example:** `Device(config)# no license smart enable`	Deactivates Smart Licensing on the device. **Note** When you disable Smart Licensing, the Cisco Software License (CSL) and all licensing calls pass through the Smart Agent. For the ‘no’ case, if Smart Licensing is already registered, the Smart Agent performs the ”license smart deregister” operation that deactivates Smart Licensing. Reload the device to activate the CSL on the device.
Step 4	**license accept end user agreement** **Example:** `Device(config)# license accept end user agreement`	Uses the **license accept end user agreement** command to configure a one-time acceptance of the EULA for all Cisco IOS software packages and features. **Note** After the **license accept end user agreement** command is issued and the EULA accepted, the EULA is automatically applied to all Cisco IOS software licenses. For more information, refer to the “Configuring the EULA” section in the Software Activation on Cisco ISR, Cisco ISR G2, and Cisco ISR NG Guide.
Step 5	**exit** **Example:** `Device(config)# exit`	Exits the global configuration mode.
Step 6	**write memory** **Example:** `Device# write memory`	Saves the running configuration to NVRAM.
Step 7	**reload** **Example:** `Device# reload`	(Optional) Restarts the device to enable the new feature set. **Note** Reload the device if you have not reloaded the device after configuring the Cisco One Suites.
Step 8	**show license all** **Example:** `Device# show license all`	(Optional) Displays summary information about all licenses.

Device Registration

SUMMARY STEPS

1. **enable**
2. **license smart register idtoken***idtoken*[**force**]
3. **license smart deregister**
4. **license smart renew**[**ID** | **auth**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**license smart register idtoken***idtoken*[**force**] **Example:** `Device# license smart register idtoken 123`	Registers the device with the back-end server. Token id can be obtained from your virtual a/c in the Smart Licensing server. • **force**: To forcefully register your device irrespective of either the device is registered or not. **Note** The device supplies the token ID to the Cisco server, which sends back a "Device Certificate" that is valid for 365 days.
Step 3	**license smart deregister** **Example:** `Device# license smart deregister`	Deregisters the device from the backend server.
Step 4	**license smart renew**[**ID** | **auth**] **Example:** `Device# license smart renew ID`	(Optional) Manually renews the ID certification or authorization.

Troubleshooting for Cisco Smart Licensing Client

You can troubleshoot Smart Licensing enabling issues using the following commands on the device:

- **show version**
- **show running-config**

- **show license tech support**
- **show license entitlement**
- **show license feature**
- **show license certificate**
- **debug smart_lic error**
- **debug smart_lic trace**

Configuration Examples for Cisco Smart Licensing Client

Example: Displays summary information about all licenses

The following example shows how to use the **show license all** command to display summary information about all licenses.

```
Device# show license all
Cisco Smart Licensing Agent, Version 1.0.0_development

Smart Licensing Enabled: Yes

UDI:
PID:CISCO2911/K9,SN:FTX1643AJFR

Compliance Status: In Compliance

Assigned License Pool: ISR_G2_Cisco_One

Grace period: Not in use

Entitlement:
    Tag: regid.2014-06.com.cisco.ISR_2900_FS_ENT,1.0_71846b6b-db2a-46f3-9c8e-ce0fc68882fc,
 Version: 1.0, Enforce Mode: Authorized
    Requested Time: Wed Oct 29 23:34:58.011,  Requested Count: 1
    Vendor String:

Smart Licensing State: authorized (4)

Licensing Certificates:
    ID Cert Info:
        Start Date: Oct 29 23:42:33 2014 UTC. Expiry Date: Oct 29 23:42:33 2015 UTC
        Serial Number: 97879
        Version: 3
        Subject/SN: 241e4492-9582-4f0a-9b01-221fdecc2a1b
        Common Name: 1A4BF5460E0939AED4D14B2E3C7CD809A98CFCC9::1,2
    Signing Cert Info:
        Start Date: Jun 14 20:18:52 2013 UTC. Expiry Date: Apr 24 21:55:42 2033 UTC
        Serial Number: 3
        Version: 3

Upcoming Scheduled Jobs:
   Certificate Renewal: Apr 27 23:45:24 2015 UTC (179 days, 23 hours, 59 minutes, 47 seconds
 remaining)
    Certificate Expiration: Oct 29 23:42:39 2015 UTC (364 days, 23 hours, 57 minutes, 2
seconds remaining)
    Authorization Renewal: Nov 28 23:45:35 2014 UTC (29 days, 23 hours, 59 minutes, 58
seconds remaining)
    Authorization Expiration: Jan 27 23:42:54 2015 UTC (89 days, 23 hours, 57 minutes, 17
seconds remaining)
    Daily Job: Oct 30 23:28:04 2014 UTC (23 hours, 42 minutes, 27 seconds remaining)
```

Example: Enabling Smart Licensing

The following example shows how to use the **license smart enable** command to confirm if the Cisco ONE Suite is enabled.

```
Device# license smart enable
Currently only Cisco ONE license suites are supported by Smart Licensing.
Please make sure your Cisco ONE suites are enabled before turning on Smart Licensing. Any
other licenses outside of Cisco ONE suites would be disabled and made unusable in Smart
Licensing. If you have any questions, please get in touch with your Cisco representative
before using this mmode.
Please confirm Cisco ONE suites are enabled? [yes/no]: yes
```

Additional References for Cisco Smart Licensing Client

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Cisco License Manager Application	*User Guide for Cisco License Manager*
Software Activation Conceptual Overview	"Cisco IOS Software Activation Conceptual Overview" module
Software Activation Commands	*Software Activation Command Reference*
Integrated Services Routers Licensing	*Software Activation on Cisco Integrated Services Routers*

Standards and RFCs

MIBs

MIB	MIBs Link
CISCO-LICENSE-MGMT-MIB	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Cisco Smart Licensing Client

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 10: Feature Information for Cisco Smart Licensing

Feature Name	Releases	Feature Information
Cisco Smart Licensing Client	Cisco IOS Release XE 3S	The Smart Licensing feature is a standardized licensing platform that simplifies the Cisco software experience and helps you understand how Cisco software is used across your network. Smart Licensing is the next generation licensing platform for all Cisco software products. This feature is platform-independent. The following commands were introduced or modified by this feature: **license smart enable**, **show license all**