Software Activation Configuration Guide, Cisco IOS XE Fuji 16.8.x

CONTENTS

CHAPTER 6 **Configuring Cisco License Call Home 97**

Read Me First

Important Information about Cisco IOS XE 16

Effective Cisco IOS XE Release 3.7.0E for Catalyst Switching and Cisco IOS XE Release 3.17S (for Access and Edge Routing) the two releases evolve (merge) into a single version of converged release—the Cisco IOS XE 16—providing one release covering the extensive range of access and edge products in the Switching and Routing portfolio.

Feature Information

Use Cisco Feature Navigator to find information about feature support, platform support, and Cisco software image support. An account on Cisco.com is not required.

Related References

- Cisco IOS Command References, All Releases

Obtaining Documentation and Submitting a Service Request

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.

- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.

- To submit a service request, visit Cisco Support.

- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.

- To obtain general networking, training, and certification titles, visit Cisco Press.

- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

CHAPTER 2

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.

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
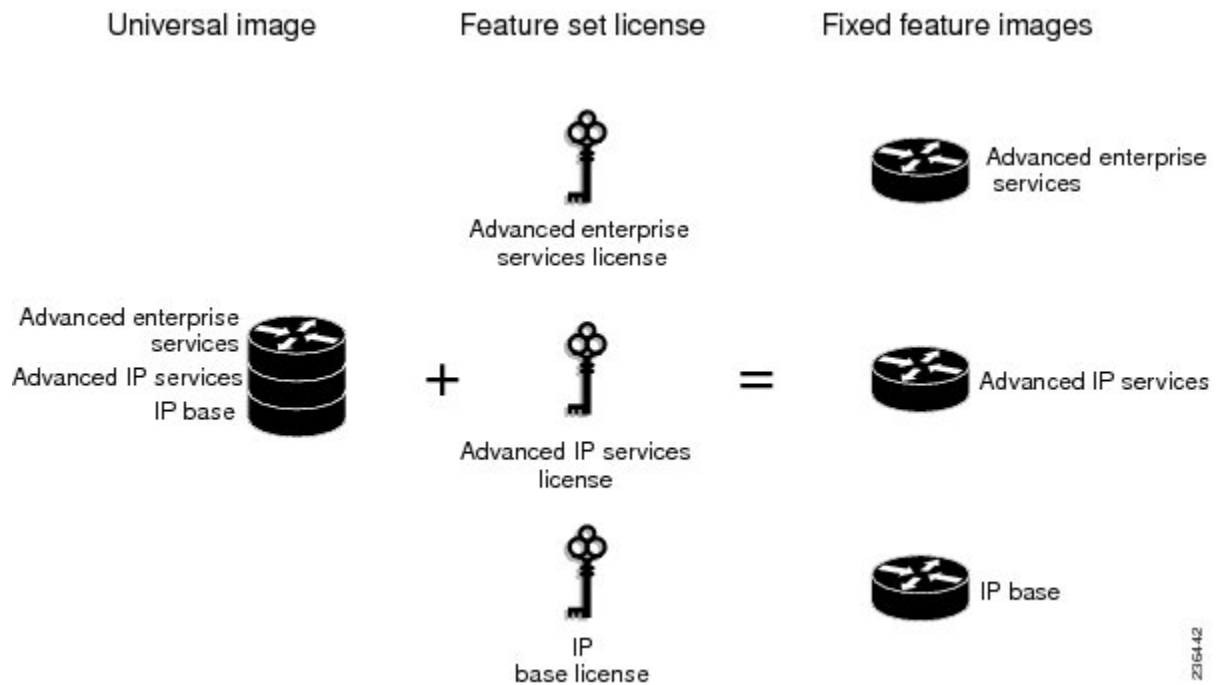
A platform can have a single universal image, which is a superset of all fixed feature images. Fixed feature images are an older packaging form in which the image contains only part of a systems capabilities. The fixed

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
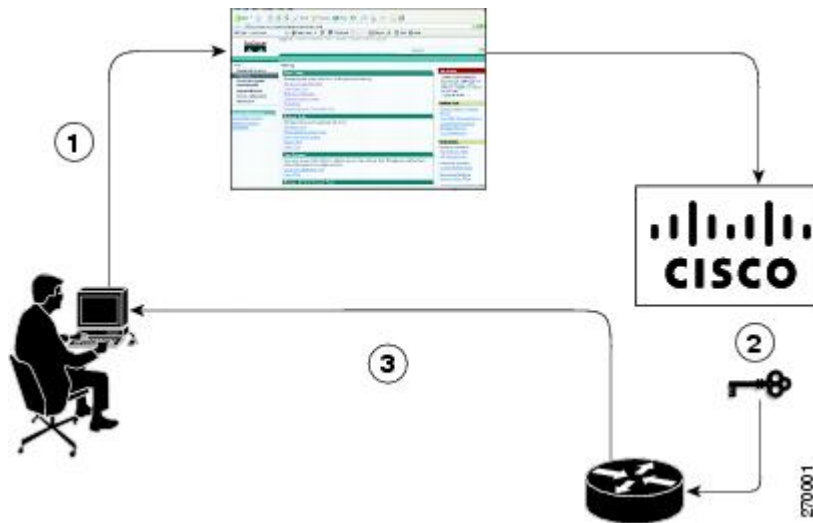
The work flow for manufacturing preinstalled licensing involves these steps:

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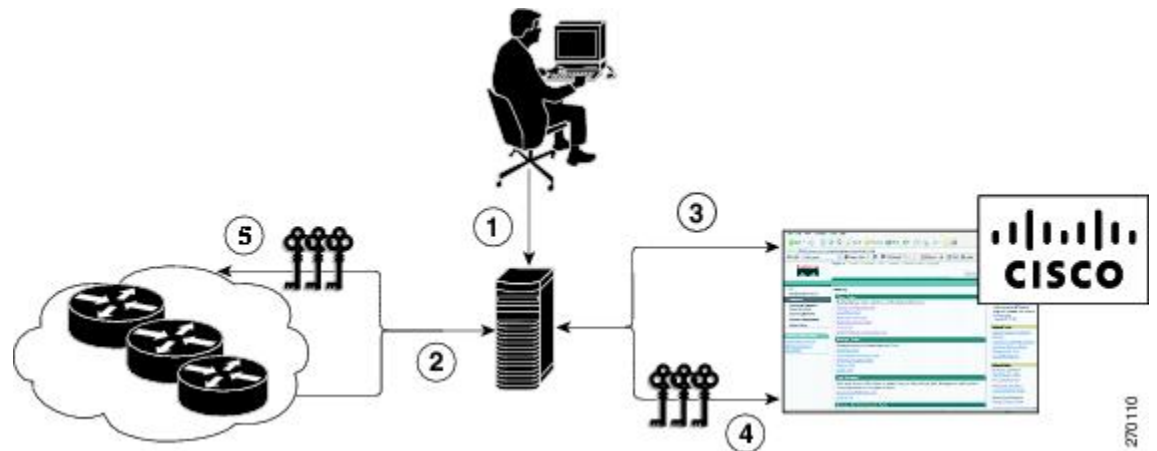
The workflow for license upgrades for automated license transfers involves these steps:

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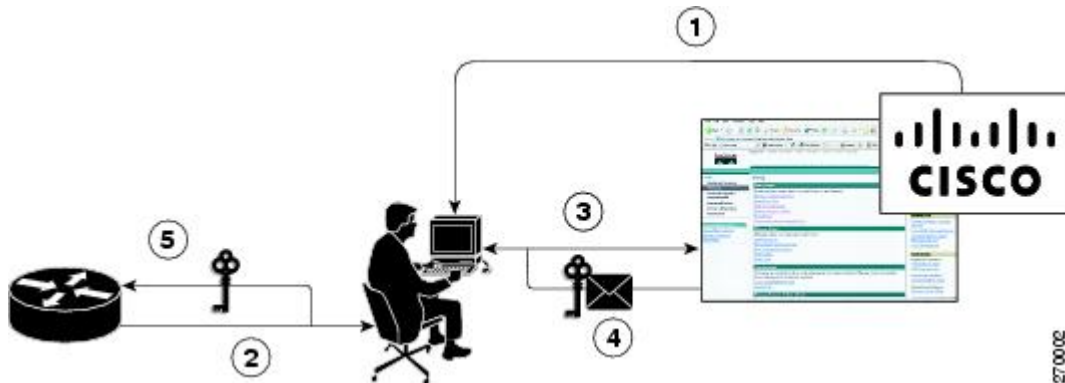
The license upgrade process work flow for manual license fulfillment involves these steps:

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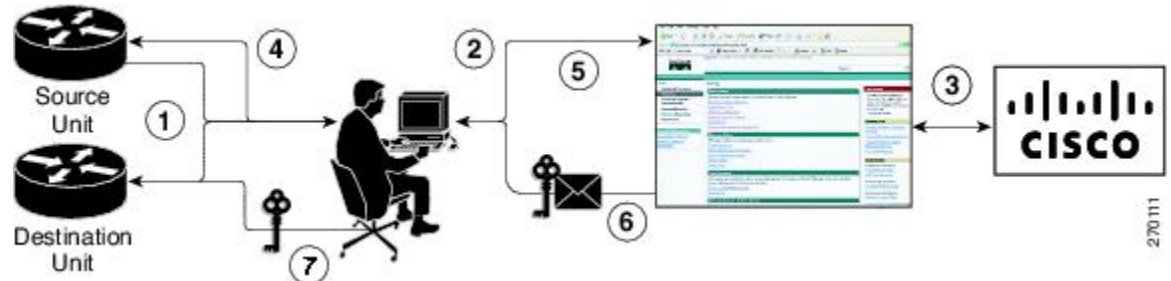
The following summary is for a license transfer process by using the Cisco Product License Registration portal:

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
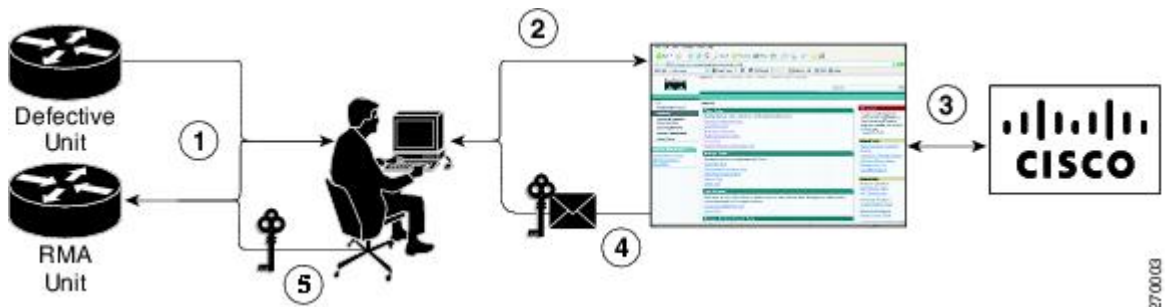
The RMA replacement license process involves these steps:

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.

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.

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*
	
	Example:
	
	`Device# license install`
	`tftp://infra-sun/<user>/license/5400/38a.lic`
		Installs the license.
		
		• Accept the end-user license agreement if prompted.

Step 6	**configure terminal** **Example:**	Enters the global configuration mode.

	Command or Action	Purpose
	`Device# configure terminal`	

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.

	Command or Action	Purpose
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.
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.

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.
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.
Step 3	**show license detail** **Example:**	Verifies that the license has been cleared.

Command or Action	Purpose
Device# show license detail	

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 : 1764 bytes
!
! Last configuration change at 15:20:26 IST Thu Aug 1 2019
! NVRAM config last updated at 15:36:45 IST Mon Jul 22 2019
!
version 16.9
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no platform punt-keepalive disable-kernel-core
platform bfd-debug-trace 1
platform xconnect load-balance-hash-algo mac-ip-instanceid
platform tcam-parity-error enable
platform tcam-threshold alarm-frequency 1
platform shell
!
hostname ASR920
!
boot-start-marker
boot-end-marker
!
!
vrf definition Mgmt-intf
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family
!
!
no aaa new-model
clock timezone IST 5 30
!
!
!
```

```
                   !
                   !
                   !
                   !
                   !
                   !
                   !
                   !
                   !
                   !
                   !
                   !
                   !
                   !
                   multilink bundle-name authenticated
                   !
                   !
                   !
                   license udi pid ASR-920-4SZ-D sn CAT2211U7WD
                   no license smart enable
                   file prompt quiet
                   !
                   !
                   spanning-tree extend system-id
                   sdm prefer default
                   diagnostic bootup level minimal
                   !
                   !
                   !
                   redundancy
```

show tech-support

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

```
Device# show tech-support
----------------- show license udi -----------------

SlotID   PID       SN         UDI
-------------------------------------------------------------------------------
*0   ASR-920-4SZ-D       CAT2211U7WD    ASR-920-4SZ-D:CAT2211U7WD


----------------- show license udi standby -----------------



----------------- show license status -----------------

 License Type Supported
permanent               Non-expiring node locked license
extension               Expiring node locked license
evaluation              Expiring non node locked license
evalRightToUse          Right to use evaluation non node locked license
rightToUse              Right to use non node locked license

 License Operation Supported
install    Install license
clear      Clear license
annotate   Comment license
save       Save license
revoke     Revoke license
```

```
 Device status
 Device Credential type: IMAGE
 Device Credential Verification: PASS
 Rehost Type: DC_OR_IC


----------------- show license status standby -----------------



----------------- show license feature -----------------


Feature name               Enforcement  Evaluation  Subscription  Enabled  RightToUse
advancedmetroipaccess      yes          yes         no            yes      no
metroipaccess              yes          yes         no            no       no
metroaccess                no           yes         no            no       no
1588                       yes          yes         no            no       no
10GEupgradelicense         yes          no          no            no       no
2portGE-4ports10GE         yes          no          no            yes      no


----------------- show license feature standby -----------------



----------------- show license file -----------------

License Store: Primary License Storage
  Store Index: 0
    License: 11 2portGE-4ports10GE 1.0 LONG NORMAL STANDALONE EXCL INFINITE_KE
             YS INFINITE_KEYS NEVER NEVER NiL SLM_CODE CL_ND_LCK NiL *17FU47V3
             CUF3HEZ400 NiL NiL NiL 5_MINS <UDI><PID>ASR-920-4SZ-D</PID><SN>CA
             T2211U7WD</SN></UDI> VQogQJa91F3yuYf3g:aWf9qOXg0bRnKs25ZhhWXQ6vfa
             wtSiGCTcJ6UX0Wsc5SdJV:aGsY56VDTPALe9s5h7maVC7WPHrQG9hDQBB1NUiiJTL
             pyzm4CCG3xA8H6w8Ujj7GVA$<WLC>AQEBISAB///ePuFEFLa1WYTTBsUwysYIlwUT
             u4NOSAmnH54EqMR+ddrdmYvQIWIKvh/Ta02F6X3ePuFEFLa1WYTTBsUwysYIlwUTu
             4NOSAnIcMf6vWuUuI1lxR4RgKX59uDYrlsEJot7Qno/vtYl8B0vN08xyEcTl52bmL
             3dfDsAumQ+9NeEXWOHMixGAsjTr+jONlkzusU=</WLC>
    Comment:
       Hash: M6TSnLClnXd4krgImjtXxTWRmcQ=
  Store Index: 1
    License: 11 advancedmetroipaccess 1.0 LONG NORMAL STANDALONE EXCL INFINITE
             _KEYS INFINITE_KEYS NEVER NEVER NiL SLM_CODE CL_ND_LCK NiL *17FU4
             7V3CUF3HEZ400 NiL NiL NiL 5_MINS <UDI><PID>ASR-920-4SZ-D</PID><SN
             >CAT2211U7WD</SN></UDI> BfkkXOhIiIUBcTUrSQLif:aZz0Kyvtju4rD7lMmvK
             mLytEIMPkuNEY3dSawv,OHtVUP3zh,qGeYcsPmpi3tGL2V8kxRbVvJXV,wrXJ3O6o
             us3,P7EQtt,Ho,9wCO2BwDbpfz$<WLC>AQEBISAB///ePuFEFLa1WYTTBsUwysYIl
             wUTu4NOSAkSLhrKyrLBd3+nroEfw8/8Av4nEYBFF/nePuFEFLa1WYTTBsUwysYIlw
             UTu4NOSAnIcMf6vWuUuI1lxR4RgKX59uDYrlsEJot7Qno/vtYl8B0vN08xyEcTl52
             bmL3dfDsAumQ+9NeEXWOHMixGAsjTr+jONlkzusU=</WLC>
    Comment:
       Hash: cuBh2U4PcOLuo1aYMZLYQ5MeBMw=
License Store: Built-In License Storage
  Store Index: 0
    License: 11 advancedmetroipaccess 1.0 LONG TRIAL DISABLED 1440 DISABLED ST
             ANDALONE ADD INFINITE_KEYS INFINITE_KEYS NEVER NEVER NiL SLM_CODE
              DEMO NiL NiL Ni NiL NiL 5_MINS NiL q7AiZERv7M3asfmTNiBq3AIfzXaMn
             771WFbW0QLSFTf8XRd,uBSGsOh5VadJXolSVH$<WLC>AQEBIf8B//+GAlABZF9TUb
             kV9DfLeeIHyU2S2mDnooo9JUxWfflSYbGg+v4MuWI3L+D6KJGVjyyRqwInXo3s+ns
             LU7rOtdOxoIxYZAo3LYmUJ+MFzsqlhKoJVlPyEvQ8H21MNUjVbhoN0gyIWsyiJaM8
             AQIkVBQFzhr10GYolVzdzfJfEPQIx6tZ++/Vtc/q3SF/5Ko8XCY=</WLC>
    Comment:
```

```
              Hash: 5J2d3ZfjOzgP5xlaiJQSlaiGh5s=
  Store Index: 1
    License: 11 metroipaccess 1.0 LONG TRIAL DISABLED 1440 DISABLED STANDALONE
             ADD INFINITE_KEYS INFINITE_KEYS NEVER NEVER NiL SLM_CODE DEMO Ni
             L NiL Ni NiL NiL 5_MINS NiL IAWD3vd7KQItmcShIC,OfF3GzO4u8QWwFBsvd
             Sb:hJ37cc9g9tgFm5xuhx8xlkEYVn$<WLC>AQEBIf8B//9ryCDjMpbNbltG4CTDc9
             WNRCMQWn9rrxz5QrHYihBHk4fxDPzR1Gd7iVy5zb+iA/+RqwInXo3s+nsLU7rOtdO
             xoIxYZAo3LYmUJ+MFzsqlhKoJVlPyEvQ8H21MNUjVbhoN0gyIWsyiJaM8AQIkVBQF
             zhr10GYolVzdzfJfEPQIx6tZ++/Vtc/q3SF/5Ko8XCY=</WLC>
    Comment:
        Hash: CLI5/I7/N6UcLXt3j/1AejmDR6k=
  Store Index: 2
    License: 11 metroaccess 1.0 LONG TRIAL DISABLED 1440 DISABLED STANDALONE A
             DD INFINITE_KEYS INFINITE_KEYS NEVER NEVER NiL SLM_CODE DEMO NiL
             NiL Ni NiL NiL 5_MINS NiL Tc5IK2dLk8:24bhasctP3uWtPe9GRDccbeQIO7f
             aqBVjFFz3A9YK6ZNpXbSE4lknLI$<WLC>AQEBIf8B//+w2jF8oVWArFb7oStekvG+
             x8aEAlunD5s0KOQ9r9p1tUnWCR7/QRzS8kYzXtPMYKSRqwInXo3s+nsLU7rOtdOxo
             IxYZAo3LYmUJ+MFzsqlhKoJVlPyEvQ8H21MNUjVbhoN0gyIWsyiJaM8AQIkVBQFzh
             r10GYolVzdzfJfEPQIx6tZ++/Vtc/q3SF/5Ko8XCY=</WLC>
    Comment:
        Hash: kKMjObqq6eiTdHduukDWLPZub/k=


------------------ show license file standby ------------------



------------------ show license detail ------------------

Index: 1  Feature: 2portGE-4ports10GE           Version: 1.0
 License Type: Permanent
 License State: Active, In Use
 License Count: Non-Counted
 License Priority: Medium
 Store Index: 0
 Store Name: Primary License Storage
Index: 2  Feature: advancedmetroipaccess         Version: 1.0
 License Type: Permanent
 License State: Active, In Use
 License Count: Non-Counted
 License Priority: Medium
 Store Index: 1
 Store Name: Primary License Storage
Index: 3  Feature: advancedmetroipaccess         Version: 1.0
 License Type: Evaluation
 License State: Inactive
    Evaluation total period: 8  weeks 4  days
    Evaluation period left: 0  minute  0  second
    Period used: 8  weeks 4  days
 License Count: Non-Counted
 License Priority: Low
 Store Index: 0
 Store Name: Built-In License Storage
Index: 4  Feature: metroaccess                   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
    Period used: 0  minute  0  second
 License Count: Non-Counted
 License Priority: None
 Store Index: 2
 Store Name: Built-In License Storage
Index: 5  Feature: metroipaccess                 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
     Period used: 0  minute  0  second
 License Count: Non-Counted
 License Priority: None
 Store Index: 1
 Store Name: Built-In License Storage


----------------- show license detail standby -----------------

% Error: No license for standby found - License feature not found

----------------- 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:         0

 Client statistics
Request success count:   2
Request failure count:   0
Release count:           0
Global Notify count:     1



----------------- show license statistics standby -----------------
```

show license udi

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

```
Device> show license udi
SlotID  PID                     SN                      UDI
-------------------------------------------------------------------------------
0       ASR-920-4SZ-D           CAT2211U7WD     ASR-920-4SZ-D:CAT2211U7WD
```

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*

Related Topic	Document Title
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**

Configuring a Cisco Right-To-Use License

This guide provides an overview and guidance for configuring the Cisco® ASR 1000 Series Aggregation Services Routers with Right-To-Use License (RTU).

Feature Information for Cisco Right-To-Use License

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.

Prerequisites for RTU

- You must obtain the device certificate from the Cisco licensing infrastructure before you start the installation process.
- You must have a Cisco user login account.

Information About Cisco RTU License

Overview of the Cisco Licensing Mechanism

The Cisco licensing mechanism provides flexibility to run a device at different technology package levels. This mechanism is referred to as technology package licensing and leverages the universal technology package based licensing solution. A universal image containing all levels of a software package is loaded on to the

device. During startup, the device determines the highest level of license and loads the corresponding software features or subsystems.

The Cisco ASR 1001 Router and ASR 1002-X Router support technology package-based licenses that are not node locked. Technology packages and feature licenses are activated using evaluation licenses that are built in. Evaluation licenses are limited period-metered licenses that are valid for 60 days. When the time allowed for an evaluation license expires, the license is automatically upgraded to RTU license. After all the RTU licenses are activated, there is no expiration of license and are valid for a lifetime.

To enable an evaluation license, you have to accept the global end user license agreement (EULA).

RTU Supported Software Licenses

This section describes the various RTU-supported software licenses.

| **Note** | Permanent licenses are not affected by Cisco IOS XE release upgrades. |

An evaluation license is required to activate the licensed features. When a router enters the configuration mode, a check is performed to verify the license. Feature configurations are allowed only valid licenses are available. If a permanent license does not exist, Cisco IOS activates an RTU license when you accept the EULA agreement and the corresponding Cisco IOS functionalities will be available. The RTU license supports the following software features:

- Inter chassis redundancy

- Lawful intercept

- Software redundancy

- IPsec

- Throughput

Accept the EULA to activate the corresponding feature. Migration of a permanent license from previous versions of the software images are seamless. For information on accepting the EULA, see Example: Accepting the Global EULA, page 10-6.

Evaluation licenses and RTU licenses available on the Cisco ASR 1000 Series Routers

Evaluation and RTU Licenses	**Evaluation and RTU Licenses**	**License Name**	**License Description Evaluation License**
FLS-ASR1001-5G	FLS-ASR1001-5G	Upgrade from 2.5G to 5G license for Cisco ASR1001 Router	Yes
FLSASR1-IOSRED	Software redundancy license for Cisco ASR1000 Series Aggregation Services Routers	Yes	Yes

Evaluation and RTU Licenses	Evaluation and RTU Licenses	License Name	License Description Evaluation License
FLSASR1-IPSEC IPSEC	License for Cisco ASR1000 Series Aggregation Services Routers	Yes	Yes
FLSASR1-FW FW	License for Cisco ASR1000 Series Aggregation Services Routers	Yes	Yes
FLSASR1-FPI	Flex. Pack. Insp License for Cisco ASR1000 Series Aggregation Services Routers	Yes	Yes
FLSASR1-FWNAT-R	Firewall and NAT Stateful Inter-Chassis Redundancy License	Yes	Yes
FLSASR1-LI	Lawful Intercept License for Cisco ASR1000 Series Aggregation Services Routers	Yes	Yes
FLSASR1-BB	Broadband License for Cisco ASR1000 Series Aggregation Services Routers	Yes	Yes
FLSASR1-BB-4K	Broadband 4K Sessions for Cisco ASR1000 Series Aggregation Services Routers	Yes	Yes
FLSASR1-BB-16K	Broadband 16K Sessions for Cisco ASR1000 Series Aggregation Services Routers	Yes	Yes
FLSASR1-BB-32K	Broadband 32K Sessions for Cisco ASR1000 Series Aggregation Services Routers	Yes	Yes
FLSASR1-CS-250P	CUBE(SP) 250Session License for Cisco ASR1000 Series Aggregation Services Routers	Yes	Yes

Evaluation and RTU Licenses	Evaluation and RTU Licenses	License Name	License Description Evaluation License
FLSASR1-CS-2KP	CUBE(SP) 2K Session License for Cisco ASR1000 Series Aggregation Services Routers	Yes	Yes
FLSASR1-CS-4KP	CUBE(SP) 4K Session License for Cisco ASR1000 Series Aggregation Services Routers	Yes	Yes
FLSASR1-CS-16KP	CUBE(SP) 16K Session License for Cisco ASR1000 Series Aggregation Services Routers	Yes	Yes
FLSASR1-CS-32KP	CUBE(SP) 32K Session License for Cisco ASR1000 Series Aggregation Services Routers	Yes	Yes
FLSASR1-CS-LAB	CUBE(SP) Lab Use Only Lic for Cisco ASR1000 Series Aggregation Services Routers	Yes	Yes
FLSASR1-CS-TPEX	CUBE(SP) License for ASR1000 in Video/B2BTP Ex	Yes	Yes
SLASR1-AIS	Cisco ASR 1000 Advanced IP Services License	Yes	Yes
SLASR1-AES	Cisco ASR 1000 Advanced Enterprise Services License	Yes	Yes
SLASR1-IPB	Cisco ASR 1000 IP BASE License		
FLS-ASR1001-5G	Throughput performance upgrade from 2.5G to 5G license for ASR1001	Yes	Yes

How to Activate an Evaluation License

Note	Evaluation RTU licenses automatically changes to RTU licenses after an evaluation period of 60 days.

Evaluation licenses can be activated using the license boot level {adventerprise | advipservices |ipbase} command.

SUMMARY STEPS

1. enable
2. configure terminal
3. license boot level {adventerprise | advipservices |ipbase}
4. exit
5. copy running-config startup-config
6. reload

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable **Example:** `Router> enable`	Enables the privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal **Example:** `Router#configure terminal`	Enters the global configuration mode.
Step 3	license boot level {adventerprise | advipservices |ipbase} **Example:** `Router(config)#license boot level adventerprise`	Enables the evaluation license. **Note** Use the ? command with the technology-package command to see the software packages and features supported on your router.
Step 4	exit **Example:** `Router(config)#exit`	Exits the global configuration mode.
Step 5	copy running-config startup-config **Example:** `Router#copy running-config startup-config`	Saves the configuration.
Step 6	reload **Example:** `Router#reload`	Reloads the router. A reload is required to activate the software package.

Example

The following example shows how to activate an evaluation license:

```
Router>enable
Router#configure terminal
Router(config)#license boot level adventerprise
% use 'write' command to make license boot config take effect on next boot
Router(config)#exit
Router#copy running-config startup-config
Router#reload
```

Configuring Throughput

For information on configuring throughput on the Cisco ASR 1001 Router, see Cisco ASR 1001 Router Quick Start Guide. For information on configuring throughput on the Cisco ASR 1002-X Router, see Cisco ASR 1001 Router Quick Start Guide.

Example: IPSec

Configure map or tunnels to the interface to trigger the EULA. Perform the following actions when required:

```
step1:
Device#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)#crypto isakmp policy 1
Device(config-isakmp)#encryption aes
Device(config-isakmp)#hash md5
Device(config-isakmp)#group 2
Device(config-isakmp)#lifetime 86400
Device(config-isakmp)#authentication pre-share
Device(config-isakmp)#exit

step2:
Device(config)#crypto isakmp key cisco address 10.10.0.0

step3:
Device(config)#crypto ipsec transform-set trans esp-aes esp-md5-hmac
Device(cfg-crypto-trans)#mode transport
Device(cfg-crypto-trans)#exit

step4:
Device(config)#crypto map map1 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
Device(config-crypto-map)#set transform-set trans
Device(config-crypto-map)#set peer 10.10.0.0
Device(config-crypto-map)#match address 101
Device(config-crypto-map)#exit

step5:
Device(config)#access-list 101 permit ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255
Device(config)#access-list 102 permit ip 100.100.100.0 0.0.0.255 100.100.100.0 0.0.0.255
Device(config)#exit

step6:
Device#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)#int GigabitEthernet0/0/1
```

```
Device(config-if)#crypto map map1
Device(config-if)#end
```

Example: Accepting an EULA for Software Redundancy License

The following example shows the acceptance of an EULA for the software redundancy feature:

```
Router(config)#redundancy
Router(config-red)#mode
Router(config-red)#mode sso

PLEASE  READ THE  FOLLOWING TERMS  CAREFULLY. INSTALLING THE LICENSE OR LICENSE  KEY
PROVIDED FOR  ANY CISCO  PRODUCT  FEATURE  OR  USING SUCH PRODUCT  FEATURE  CONSTITUTES
YOUR  FULL ACCEPTANCE  OF  THE FOLLOWING TERMS. YOU MUST NOT PROCEED FURTHER IF YOU ARE NOT
 WILLING TO  BE BOUND BY ALL THE TERMS SET FORTH HEREIN.

Use of this product feature requires  an additional license from Cisco, together with an
additional  payment.  You may use this product feature on an evaluation basis, without
payment to Cisco, for 60 days. Your use of the  product,  including  during the 60 day
evaluation  period,  is subject to the Cisco end user license agreement
http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.html If you use the product
 feature beyond the 60 day evaluation period, you must submit the appropriate payment to
Cisco for the license. After the 60 day  evaluation  period,  your  use of the  product
feature will be governed  solely by the Cisco  end user license agreement (link above),
together  with any supplements  relating to such product  feature.  The above  applies
even if the evaluation  license  is  not  automatically terminated  and you do  not receive
 any notice of the expiration of the evaluation  period.  It is your  responsibility  to
determine when the evaluation  period is complete and you are required to make  payment to
 Cisco for your use of the product feature beyond the evaluation period.

Your  acceptance  of  this agreement  for the software  features on one product  shall be
deemed  your  acceptance  with  respect  to all  such software  on all Cisco  products  you
 purchase  which includes the same software.  (The foregoing  notwithstanding, you must
purchase a license for each software  feature you use past the 60 days evaluation  period,
 so  that  if you enable a software  feature on  1000  devices, you must purchase 1000
licenses for use past  the 60 day evaluation period.)

Activation  of the  software command line interface will be evidence of your acceptance of
 this agreement.

ACCEPT? (yes/[no]): yes

Router(config)#
```

Example: Accepting an EULA for the Inter-Chassis Redundancy License

The following example shows the acceptance of an EULA for the application redundancy feature:

```
Router(config-red)#application redundancy

PLEASE  READ THE  FOLLOWING TERMS  CAREFULLY. INSTALLING THE LICENSE OR LICENSE  KEY
PROVIDED FOR  ANY CISCO  PRODUCT  FEATURE  OR  USING SUCH PRODUCT  FEATURE  CONSTITUTES
YOUR  FULL ACCEPTANCE  OF  THE FOLLOWING TERMS. YOU MUST NOT PROCEED FURTHER IF YOU ARE NOT
 WILLING TO  BE BOUND BY ALL THE TERMS SET FORTH HEREIN.

Use of this product feature requires  an additional license from Cisco, together with an
additional  payment.  You may use this product feature on an evaluation basis, without
payment to Cisco, for 60 days. Your use of the  product,  including  during the 60 day
evaluation  period,  is subject to the Cisco end user license agreement
http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.html If you use the product
 feature beyond the 60 day evaluation period, you must submit the appropriate payment to
```

Cisco for the license. After the 60 day evaluation period, your use of the product
feature will be governed solely by the Cisco end user license agreement (link above),
together with any supplements relating to such product feature. The above applies
even if the evaluation license is not automatically terminated and you do not receive
 any notice of the expiration of the evaluation period. It is your responsibility to
determine when the evaluation period is complete and you are required to make payment to
 Cisco for your use of the product feature beyond the evaluation period.

Your acceptance of this agreement for the software features on one product shall be
deemed your acceptance with respect to all such software on all Cisco products you
 purchase which includes the same software. (The foregoing notwithstanding, you must
purchase a license for each software feature you use past the 60 days evaluation period,
 so that if you enable a software feature on 1000 devices, you must purchase 1000
licenses for use past the 60 day evaluation period.)

Activation of the software command line interface will be evidence of your acceptance of
 this agreement.
ACCEPT? (yes/[no]): yes

Example: IPSec

Configure map or tunnels to the interface to trigger the EULA. Perform the following actions when required:

```
step1:
Device#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)#crypto isakmp policy 1
Device(config-isakmp)#encryption aes
Device(config-isakmp)#hash md5
Device(config-isakmp)#group 2
Device(config-isakmp)#lifetime 86400
Device(config-isakmp)#authentication pre-share
Device(config-isakmp)#exit

step2:
Device(config)#crypto isakmp key cisco address 10.10.0.0

step3:
Device(config)#crypto ipsec transform-set trans esp-aes esp-md5-hmac
Device(cfg-crypto-trans)#mode transport
Device(cfg-crypto-trans)#exit

step4:
Device(config)#crypto map map1 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
Device(config-crypto-map)#set transform-set trans
Device(config-crypto-map)#set peer 10.10.0.0
Device(config-crypto-map)#match address 101
Device(config-crypto-map)#exit

step5:
Device(config)#access-list 101 permit ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255
Device(config)#access-list 102 permit ip 100.100.100.0 0.0.0.255 100.100.100.0 0.0.0.255
Device(config)#exit

step6:
Device#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)#int GigabitEthernet0/0/1
Device(config-if)#crypto map map1
Device(config-if)#end
```

Example: Accepting an EULA for the Lawful Intercept License

The following example shows the acceptance of an EULA for the lawful intercept feature. The following MIBs are required to activate lawful intercept license:

- snmp-server view INTERCEPT_VIEW ciscoIpTapMIB

- snmp-server view INTERCEPT_VIEW cisco802TapMIB

- snmp-server view INTERCEPT_VIEW ciscoTap2MIB

```
Router(config-red)#snmp-server view INTERCEPT_VIEW ciscoIpTapMIB included

PLEASE  READ THE  FOLLOWING TERMS  CAREFULLY. INSTALLING THE LICENSE OR LICENSE  KEY
PROVIDED FOR  ANY CISCO  PRODUCT  FEATURE  OR  USING SUCH PRODUCT  FEATURE  CONSTITUTES
YOUR  FULL ACCEPTANCE  OF  THE FOLLOWING TERMS. YOU MUST NOT PROCEED FURTHER IF YOU ARE NOT
 WILLING TO  BE BOUND BY ALL THE TERMS SET FORTH HEREIN.

Use of this product feature requires  an additional license from Cisco, together with an
additional  payment.  You may use this product feature on an evaluation basis, without
payment to Cisco, for 60 days. Your use of the  product,  including  during the 60 day
evaluation  period,  is subject to the Cisco end user license agreement
http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.html If you use the product
 feature beyond the 60 day evaluation period, you must submit the appropriate payment to
Cisco for the license. After the 60 day  evaluation  period,  your  use of the  product
feature will be governed  solely by the Cisco  end user license agreement (link above),
together  with any supplements  relating to such product  feature.  The above  applies
even if the evaluation  license  is  not  automatically terminated  and you do  not receive
 any notice of the expiration of the evaluation  period.  It is your  responsibility  to
determine when the evaluation  period is complete and you are required to make  payment to
 Cisco for your use of the product feature beyond the evaluation period.

Your  acceptance  of  this agreement  for the software  features on one product  shall be
deemed  your  acceptance  with  respect  to all  such software  on all Cisco  products  you
 purchase  which includes the same software.  (The foregoing  notwithstanding, you must
purchase a license for each software  feature you use past the 60 days evaluation  period,
 so  that  if you enable a software  feature on  1000  devices, you must purchase 1000
licenses for use past  the 60 day evaluation period.)

Activation  of the  software command line interface will be evidence of your acceptance of
 this agreement.
ACCEPT? (yes/[no]): yes
```

Sample Output for show Commands

Sample Output for the show license EULA Command

```
Router#show license EULA
Feature name            EULA Accepted
------------            -------------
adventerprise           yes
advipservices           no
ipbase                  n/a
avc                     n/a
broadband               n/a
broadband_4k            n/a
cube_250                n/a
cube_250_red            n/a
```

```
cube_ent_100           n/a
cube_ent_100_red       n/a
cube_lab               n/a
cube_video_b2btp       n/a
cube_video_b2btp_red   n/a
firewall               n/a
fpi                    n/a
fwnat_red              no
gtp_addon_aic          n/a
internal_service       n/a
ipsec                  no
lawful_intr            no
lisp                   n/a
nat64_stateful_2m      n/a
otv                    n/a
sgt_fw                 n/a
sw_redundancy          yes
throughput_10g         no
throughput_20g         no
throughput_36g         no
vpls                   n/a
```

```
PLEASE  READ THE  FOLLOWING TERMS  CAREFULLY. INSTALLING THE LICENSE OR
LICENSE  KEY  PROVIDED FOR  ANY CISCO  PRODUCT  FEATURE  OR  USING SUCH
PRODUCT  FEATURE  CONSTITUTES  YOUR  FULL ACCEPTANCE  OF  THE FOLLOWING
TERMS. YOU MUST NOT PROCEED FURTHER IF YOU ARE NOT WILLING TO  BE BOUND
BY ALL THE TERMS SET FORTH HEREIN.

Use of this product feature requires  an additional license from Cisco,
together with an additional  payment.  You may use this product feature
on an evaluation basis, without payment to Cisco, for 60 days. Your use
of the  product,  including  during the 60 day  evaluation  period,  is
subject to the Cisco end user license agreement
http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.html
If you use the product feature beyond the 60 day evaluation period, you
must submit the appropriate payment to Cisco for the license. After the
60 day  evaluation  period,  your  use of the  product  feature will be
governed  solely by the Cisco  end user license agreement (link above),
together  with any supplements  relating to such product  feature.  The
above  applies  even if the evaluation  license  is  not  automatically
terminated  and you do  not receive any notice of the expiration of the
evaluation  period. It is your  responsibility  to  determine when the
evaluation  period is complete and you are required to make  payment to
Cisco for your use of the product feature beyond the evaluation period.

Your  acceptance  of  this agreement  for the software  features on one
product  shall be deemed  your  acceptance  with  respect  to all  such
software  on all Cisco  products  you purchase  which includes the same
software.  (The foregoing  notwithstanding, you must purchase a license
for each software  feature you use past the 60 days evaluation  period,
so  that  if you enable a software  feature on  1000  devices, you must
purchase 1000 licenses for use past  the 60 day evaluation period.)

Activation  of the  software command line interface will be evidence of
your acceptance of this agreement.
```

Sample Output for the show license all Command

```
Router#show license all
License Store: Primary License Storage
License Store: Built-In License Storage
StoreIndex: 0   Feature: adventerprise                 Version: 1.0
        License Type: EvalRightToUse
```

```
                    License State: Active, In Use
                        Evaluation total period: 8  weeks 4  days
                        Evaluation period left: 6  weeks 2  days
                        Period used: 2  weeks 1  day
                        Transition date: Aug 24 2012 05:14:39
                    License Count: Non-Counted
                    License Priority: Low
StoreIndex: 1   Feature: advipservices               Version: 1.0
                    License Type: EvalRightToUse
                    License State: Active, Not in Use, EULA not accepted
                        Evaluation total period: 8  weeks 4  days
                        Evaluation period left: 8  weeks 4  days
                        Period used: 0  minute  0  second
                    License Count: Non-Counted
                    License Priority: None
StoreIndex: 2   Feature: fwnat_red                    Version: 1.0
                    License Type: EvalRightToUse
                    License State: Active, Not in Use, EULA not accepted
                        Evaluation total period: 8  weeks 4  days
                        Evaluation period left: 8  weeks 4  days
                        Period used: 0  minute  0  second
                    License Count: Non-Counted
                    License Priority: None
StoreIndex: 3   Feature: ipsec                        Version: 1.0
                    License Type: EvalRightToUse
                    License State: Active, Not in Use, EULA not accepted
                        Evaluation total period: 8  weeks 4  days
                        Evaluation period left: 8  weeks 4  days
                        Period used: 0  minute  0  second
                    License Count: Non-Counted
                    License Priority: None
StoreIndex: 4   Feature: lawful_intr                  Version: 1.0
                    License Type: EvalRightToUse
                    License State: Active, Not in Use, EULA not accepted
                        Evaluation total period: 8  weeks 4  days
                        Evaluation period left: 8  weeks 4  days
                        Period used: 0  minute  0  second
                    License Count: Non-Counted
                    License Priority: None
StoreIndex: 5   Feature: sw_redundancy                Version: 1.0
                    License Type: RightToUse
                    License State: Active, In Use
                    License Count: Non-Counted
                    License Priority: Low
StoreIndex: 6   Feature: throughput_10g               Version: 1.0
                    License Type: EvalRightToUse
                    License State: Active, Not in Use, EULA not accepted
                        Evaluation total period: 8  weeks 4  days
                        Evaluation period left: 8  weeks 4  days
                        Period used: 0  minute  0  second
                    License Count: Non-Counted
                    License Priority: None
StoreIndex: 7   Feature: throughput_20g               Version: 1.0
                    License Type: EvalRightToUse
                    License State: Active, Not in Use, EULA not accepted
                        Evaluation total period: 8  weeks 4  days
                        Evaluation period left: 8  weeks 4  days
                        Period used: 0  minute  0  second
                    License Count: Non-Counted
                    License Priority: None
StoreIndex: 8   Feature: throughput_36g               Version: 1.0
                    License Type: EvalRightToUse
                    License State: Active, Not in Use, EULA not accepted
                        Evaluation total period: 8  weeks 4  days
```

```
                    Evaluation period left: 8  weeks 4  days
                    Period used: 0  minute  0  second
              License Count: Non-Counted
              License Priority: None
```

•

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.

Smart Licensing supports Smart License Cisco ONE suite level licenses and image licenses, such as ipbase, Advanced IP Services (AIS), Advanced Enterprise Services (AES) and feature license and throughput performance, crypto throughput and port licensing on ASR 1000 Aggregation Series Routers.

To know more about Cisco One Suites, please refer to Cisco ONE Suites.

How to Activate Cisco One Suite License

SUMMARY STEPS

1. enable
2. configure terminal
3. license boot suite suite-name
4. exit
5. reload

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable **Example:** `Router> enable`	Enables the privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal **Example:** `Router#configure terminal`	Enters the global configuration mode.

Step 3	license boot suite suite-name
	Example:
	`Router(config)# license boot suite`
	`FoundationSuiteK9`
		Enables the suite license.
		Note This command is required for activating both the evaluation and permanent licenses.

Step 4	exit **Example:** `Router(config)#exit`	Exits the global configuration mode.

	Command or Action	**Purpose**
Step 5	reload **Example:** Router# reload	Reloads the router. A reload is required to activate the software suite.

Example

The following example shows how to activate an suite license:

```
Router>enable
Router#configure terminal
Router(config)#license boot suite FoundationSuiteK9

PLEASE READ THE FOLLOWING TERMS CAREFULLY. INSTALLING THE LICENSE OR
LICENSE KEY PROVIDED FOR ANY CISCO PRODUCT FEATURE OR USING SUCH
PRODUCT FEATURE CONSTITUTES YOUR FULL ACCEPTANCE OF THE FOLLOWING
TERMS. YOU MUST NOT PROCEED FURTHER IF YOU ARE NOT WILLING TO BE BOUND
BY ALL THE TERMS SET FORTH HEREIN.

Use of this product feature requires an additional license from Cisco,
together with an additional payment. You may use this product feature
on an evaluation basis, without payment to Cisco, for 60 days. Your use
of the product, including during the 60 day evaluation period, is
subject to the Cisco end user license agreement
http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.html
If you use the product feature beyond the 60 day evaluation period, you
must submit the appropriate payment to Cisco for the license. After the
60 day evaluation period, your use of the product feature will be
governed solely by the Cisco end user license agreement (link above),
together with any supplements relating to such product feature. The
above applies even if the evaluation license is not automatically
terminated and you do not receive any notice of the expiration of the
evaluation period. It is your responsibility to determine when the
evaluation period is complete and you are required to make payment to
Cisco for your use of the product feature beyond the evaluation period.

Your acceptance of this agreement for the software features on one
product shall be deemed your acceptance with respect to all such
software on all Cisco products you purchase which includes the same
software. (The foregoing notwithstanding, you must purchase a license
for each software feature you use past the 60 days evaluation period,
so that if you enable a software feature on 1000 devices, you must
purchase 1000 licenses for use past the 60 day evaluation period.)

Activation of the software command line interface will be evidence of
your acceptance of this agreement.


ACCEPT? [yes/no]: yes
% use 'write' command to make license boot config take effect on next boot

Router(config)#
*Nov 6 01:48:34.023: %LICENSE-6-EULA_ACCEPTED: EULA for feature FoundationSuiteK9 1.0 has
been accepted. UDI=C3900-SPE100/K9:FOC14440KXB; StoreIndex=3:Built-In License Storage
Router(config)#exit
Router#write
Router#reload
```

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 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.	http://www.cisco.com/cisco/web/support/index.html
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.	

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 3: 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. The following commands were introduced or modified: **show diagnostic** commands

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).

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.

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

- 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 on how to configure and register a Cisco ASR 1000 Series Router for Smart Call Home, see the Smart Call Home Quick Start Configuration Guide

Anonymous Reporting

Smart Call Home is a service capability that is included with many Cisco service contracts and is designed to assist you help resolve problems quickly. In addition, the information gained from crash messages helps Cisco understand equipment and issues occurring in the field. You can enable Anonymous Reporting without Smart Call Home. Anonymous Reporting allows Cisco to securely receive minimal error and health information from the device. If you enable Anonymous Reporting, your identity remains anonymous, and no identifying information is sent.

Note
When you enable Anonymous Reporting, you acknowledge your consent to transfer specified data. The data is shared with 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.

How to Configure Call Home

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.
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.

	Command or Action	**Purpose**
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.
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.
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 email 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:**	Enters call home configuration mode.

	Command or Action	Purpose
	Router(config)# **call-home**	
Step 3	**contact-email-addr** *email-address* **Example:** Router(cfg-call-home)# **contact-email-addr username@example.com**	Assigns the customer's email address. Enter up to 200 characters in email 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 start 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.

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.

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.
Step 2	**call-home** **Example:** Device(config)# **call-home**	Enters call home configuration mode.

	Command or Action	Purpose
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.
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:

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
- 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 4: 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.

Level	Keyword	Syslog Level	Description
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 removes the 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 removes the corresponding command. • *command string*—Cisco 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 email message transport, you must configure at least one Simple Mail Transfer Protocol (SMTP) email server address. You can specify up to four backup email servers, for a maximum of five total mail-server definitions.

Consider the following guidelines when configuring the mail server:

- Backup email 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* **Example:** Device(cfg-call-home)# **mail-server stmp.example.com priority 1**	Assigns an email server address and its relative priority among configured email servers. Provide either of the following: • The email server's IP address or • The email server's fully qualified domain name (FQDN) of 64 characters or less.

	Command or Action	**Purpose**
		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 email address that appears in the from field in Call Home email messages. If no address is specified, the contact email address is used.
Step 5	**sender reply-to** *email-address* **Example:** Device(cfg-call-home)# **sender reply-to username@example.com**	(Optional) Assigns the email address that appears in the reply-to field in Call Home email 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 command 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. This command would specify the VRF instance that is 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 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 Cisco IOS Commands for Call Home Messages

To enable AAA authorization to run Cisco 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:**	Enters global configuration mode.

	Command or Action	Purpose
	Device# **configure terminal**	
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**} **Example:** Device(cfg-call-home)# **data-privacy level high**	Scrubs data from running configuration file to protect the privacy of the user. The default data-privacy level is normal. **Note** Enabling the data-privacy command can affect CPU utilization when scrubbing a large amount of data. • **normal**—Scrubs all normal-level commands.

Command or Action	Purpose
	• **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.
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.

	Command or Action	Purpose
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, , 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 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 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

The **call-home request** command allows you to submit the system information to Cisco Systems. The report provides helpful analysis and information specific to your system. You can request various reports, including security alerts, known bugs, recommendations, and the 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 Call-home request can have a recipient profile that is not enabled. The recipient profile specifies the email address where the transport gateway is configured. The recipient profile allows the request message to be forwarded to the Cisco TAC and you 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 email address of the registered user. If no *user-id* is specified, the response is sent to the contact email address of the device.

- Based on the keyword specifying the type of report that is requested, the following information is returned:

  - **config-sanity**—Information on the recommendations for 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. The PSIRT includes 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 that is 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

Command or Action	Purpose
	Smart Call Home backend server (URL specified in TAC profile) in XML format.
	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 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).

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.

	Command or Action	**Purpose**
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.
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.

Example: Declaring and authenticating the Cisco server security certificate

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
AQABMA0GCSqGSIb3DQEBBQUAA4GBAFFNzb5cy5gZnBWyAT14Lk0PZ3BwmcYQWpSk
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.

	Command or Action	**Purpose**
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.
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 5: Call Home Alert Groups, Events, and Actions , on page 87 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 5: 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**

Alert Group	Call Home Trigger Event	Syslog Event	Severity	Description and CLI Commands Executed
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**
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 6: Format for a Short Text Message

Data Item	Description
Device identification	Configured device name

Data Item	Description
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 7: 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
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

Data Item (Plain Text and XML)	Description (Plain Text and XML)	MML Tag (XML Only)
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
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

Data Item (Plain Text and XML)	Description (Plain Text and XML)	MML Tag (XML Only)	
Model name	Model name of the router. This is the "specific model as part of a product family name.	CallHomeDeviceCisco_Chassis/ Model	
Serial number	Chassis serial number of the unit.	CallHomeDeviceCisco_Chassis/ SerialNumber	
Chassis part number	Top assembly number of the chassis.	CallHomeDeviceCisco_Chassis/ AdditionalInformation/AD@name= "PartNumber"	
System object ID	System Object ID that uniquely identifies the system.	CallHomeDeviceCisco_Chassis/ AdditionalInformation/AD@name= "sysObjectID"	
System description	System description for the managed element.	CallHomeDeviceCisco_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 8: 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

Data Item (Plain Text and XML)	Description (Plain Text and XML)	MML Tag (XML Only)
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 9: 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
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>
```

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 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 10: 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. The following commands were introduced or modified: **show diagnostic** commands

CHAPTER **6**

Configuring Cisco License Call Home

The Cisco License Call Home feature provides a robust set of commands that communicate with the Cisco licensing infrastructure, makes connections and data transfers, and provides interactive prompts to help you install and maintain software licenses. This module describes the tasks and the commands used to activate software by using the Cisco License Call Home 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.

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 License Call Home

- You must obtain the device certificate from the Cisco licensing infrastructure before starting.

- You must have a CCO user login account.

Restrictions for Cisco License Call Home

- The device must have an Internet connection and use HTTPS to connect to the Cisco licensing infrastructure. To set up a secure HTTP connection, see the HTTP 1.1 Web Server and Client chapter in the *Cisco IOS Network Management Configuration Guide*.

- Only certain platforms support the Cisco License Call Home feature, and these devices must be running a Cisco IOS crypto K9 image. For information about platform support, see the "Feature Information for Cisco License Call Home" section.
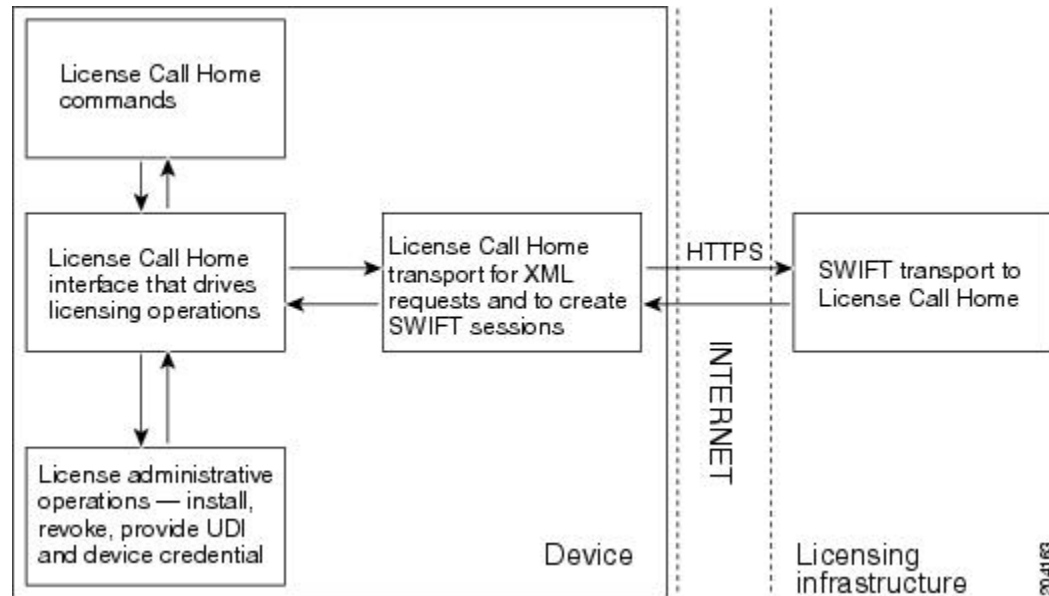
Information About Cisco License Call Home

Cisco License Call Home Interface

The Cisco License Call Home feature allows a Cisco device to communicate with the Cisco licensing infrastructure that provides license generation, fulfillment, and support. The Cisco License Call Home feature uses a secured Internet connection to retrieve licensing information. This feature provides a robust set of commands that makes connections, transfers data, and provides interactive prompts to help you install and maintain software licenses. Once you purchase a product authorization key (PAK), Cisco License Call Home commands enable you to easily perform these tasks:

- Install or upgrade a license.

- Transfer a license.

- Request that a license be resent.

The figure below shows how the Cisco License Call Home feature interfaces to the Cisco licensing back-end system. The architecture shown in the figure below allows the use of the License Call Home EXEC commands to communicate with the Cisco licensing infrastructure and to perform administrative license operations.

Figure 7: Cisco License Call Home Interface

The Cisco License Call Home feature works as a client-server model with each transaction completed as a separate connection to the Cisco licensing infrastructure. The Cisco License Call Home feature displays prompts to obtain required information and then connects to the Cisco licensing back end to interact with the Cisco licensing infrastructure. A Cisco License Call Home EXEC command initiates a request, and the Cisco licensing infrastructure provides the response. The processes designed into the Cisco License Call Home architecture manage the transport of information that provides the URL required to connect to the Cisco licensing infrastructure over the Internet and to create a session.

How to Configure Cisco License Call Home

Installing Licenses or Upgrading Software by Using Cisco License Call Home

SUMMARY STEPS

1. Obtain the PAK.
2. **enable**
3. **show license call-home pak** *pak-id*
4. **license call-home install pak** *pak-id*
5. **show license feature**

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

	Command or Action	Purpose
		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 call-home pak** *pak-id* **Example:** `Device# show license call-home pak 3XPXR9E7D30`	Displays the stock keeping unit (SKU) list and features available for the PAK provided.
Step 4	**license call-home install pak** *pak-id* **Example:** `Device# license call-home install pak 3XPXR9E7D30`	Installs a license by using the Cisco License Call Home feature. • Respond to the prompts in the command display.
Step 5	**show license feature** **Example:** `Device# show license feature`	Displays the list of licensed features.

Rehosting a License by Using Cisco License Call Home

SUMMARY STEPS

1. **enable**
2. **license call-home revoke udi** *target-udi output-of-rehosted-license-url*
3. **show license detail**
4. **license install** *stored-location-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 call-home revoke udi** *target-udi* *output-of-rehosted-license-url* **Example:** `Device# license call-home revoke udi`	Revokes and transfers a license by using source and target UDIs. Sends the rehost ticket to the Cisco licensing infrastructure with the target unique device identifier (UDI), converts it to a license file, and stores it in the URL specified.

	Command or Action	Purpose
	`AS54XM-AC-RPS:JAE0948QT6R` `flash:licensetargetudi.xml`	• Select from multiple SKUs for rehosting when you are prompted, and supply information when required.
Step 3	**show license detail** **Example:** `Device# show license detail`	Verifies that the license has been transferred.
Step 4	**license install** *stored-location-url*	(Optional) Installs the revoked license. • For details about installing and upgrading licenses, see the "Configuring the Cisco IOS Software Activation Feature" module.

Requesting a License Resend by Using Cisco License Call Home

SUMMARY STEPS

1. **enable**
2. **license call-home resend** *dest-lic-location*
3. **license install** *stored-location-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 call-home resend** *dest-lic-location*
	
	Example:
	
	`Device# license call-home resend`
	`flash:licenseresend.lic`
		Obtains all licenses this device owns and stores them in the specified location.

Step 3	**license install** *stored-location-url*	(Optional) Installs the revoked license. • For details about installing and upgrading licenses, see the "Configuring the Cisco IOS Software Activation Feature" module.

Configuration Examples for Cisco License Call Home

Example: Installing Licenses or Upgrading Software by Using Cisco License Call Home

The following example shows how to use the **license license call-home install pak** command to install a license by using the Cisco License Call Home feature. The command also displays prompts for mandatory information. The **show license feature** command is used to verify the installation.

```
Device# license call-home install pak 3XPXR9E7D30
CCO User name: User1
CCO password : ************
Pak Number          : 3XPXR9E7D30
Pak Fulfillment type: SINGLE
    1. SKU Name            : Gatekeeper
       SKU Type            : Product
       Description         : Gatekeeper
       Ordered Qty         : 1
       Available Qty       : 1
       Feature List        :
           Feature name:        gatekeeper Count: Uncounted
       Platform Supported : N/A
                            5400
                            5350
                            2800
                            3800
Do you want to install the above listed SKU(s)? [yes/no]: yes
Please enter the user's detail:
First Name : First-name
Last Name : Last-name
Title : Software Engineer
Company Name : Cisco Systems
Address1 : 510 McCarthy Blvd.
Address2  [Optional]:
City : Milpitas
State : CA
Province  [Optional]:
Zipcode : 95134
Country : USA
Phone : 408 526-4000
Fax  [Optional]:
Email : User1@cisco.com
Installing...Feature:gatekeeper...Successful

Device# show license feature
Feature name            Enforcement  Evaluation  Subscription  Enabled
gsmamrnb-codec-pack     yes          yes         no            no
Device#
```

Example: Rehosting a License by Using Cisco License Call Home

The following example shows how to use the **license call-home revoke udi** command to revoke and transfer a license by using source and target UDIs. The command also displays prompts for mandatory information. The **show license detail** command is used to verify that the license has been transferred.

```
Device# license call-home revoke udi AS54XM-AC-RPS:JAE0948QT6R flash:licensetargetudi.xml
CCO User name: User1
CCO password : ************
Retrieving the sku from swift ...........................
     1. SKU Name            : Gatekeeper
        SKU Type            : Product
        Description         :
        Ordered Qty         : 1
        Available Qty       : 1
        Feature List        :
            Feature name:        gatekeeper Count: Uncounted
        Platform Supported : N/A
                             5400
                             5350
                             2800
                             3800
     3. SKU Name            : Gatekeeper
        SKU Type            : Product
        Description         :
        Ordered Qty         : 1
        Available Qty       : 1
        Feature List        :
            Feature name:        gatekeeper Count: Uncounted
        Platform Supported : N/A
                             5400
                             5350
                             2800
                             3800
4. SKU Name            : GSMAMRNB
        SKU Type            : Product
        Description         : Transfer this feature set
        Ordered Qty         : 1
        Available Qty       : 1
        Feature List        :
            Feature name: gsmamrnb-codec-pac Count: Uncounted
        Platform Supported : 5400
                             5350
5. All of the above
Please select the sku number you want to revoke : 4
Retrieving the permission ticket from swift .............
Installing permission ticket and retrieving rehost ticket........Done


Device# show license detail
Index: 1  Feature: gsmamrnb-codec-pack   Version: 1.0
 License Type: Evaluation
 License State: Active, Not in Use, EULA 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 135266304
 License Priority: Low
 Store Index: 0
 Store Name: Evaluation License Storage
```

Example: Requesting a License Resend by Using Cisco License Call Home

The following examples shows how to use the **license call-home resend** command to obtain all licenses this device owns and store them in the specified location:

```
Device# license call-home resend flash:licenseresend.lic
CCO User name: User1
CCO password : ************
Email Address: User1@cisco.com
Getting Licenses from SWIFT ..........
Saving it to flash:licenseresend.lic.....Done
```

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*

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 License Call Home

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 11: Feature Information for Cisco License Call Home

Feature Name	Releases	Feature Information
Cisco License Call Home	12.4(15)XZ 12.4(20)T 15.1(1)SG Cisco IOS XE Release 3.3SG	The Cisco License Call Home feature provides a robust set of commands that communicate with the Cisco licensing infrastructure, makes connections and data transfers, and provides interactive prompts to help you install and maintain software licenses. In 12.4(15)XZ, this feature was introduced on the Cisco AS5300, AS5350, AS5350XM, AS5400, AS5400HPX, AS5400XM, 2800, 2851, 2821, 2811, 3800, 3825, and 3845 platforms. The following commands were introduced or modified by this feature: **license call-home install**, **license call-home resend**, **license call-home revoke**, **license call-home url**, **show license call-home**.