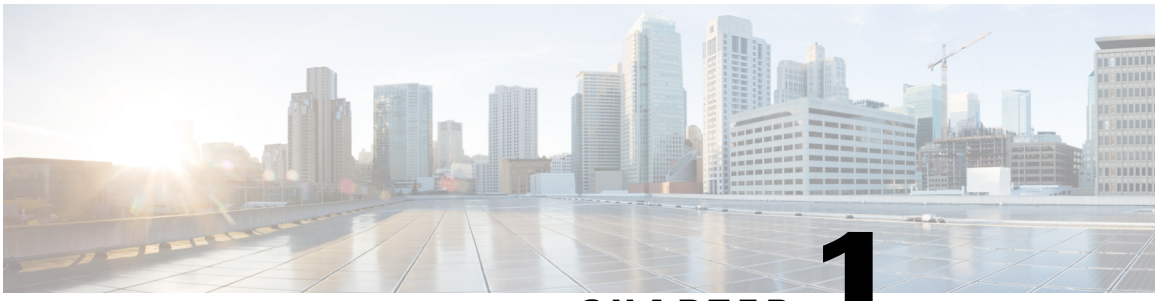
Software Activation Configuration Guid (Cisco ASR 920 Series)

First Published: 2014-07-28

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

CONTENTS



CHAPTER 1

Cisco IOS Software Activation Conceptual Overview

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

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

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

Finding Feature Information

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

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

Information About the Cisco Software Licensing Process

Cisco Software Licensing Concepts

Cisco Product License Registration Portal

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

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

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

Product Authorization Key

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

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

Unique Device Identifier

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

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

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

Cisco Software License Validation

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

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

Cisco License Manager

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

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

Software End-User License Agreement

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

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

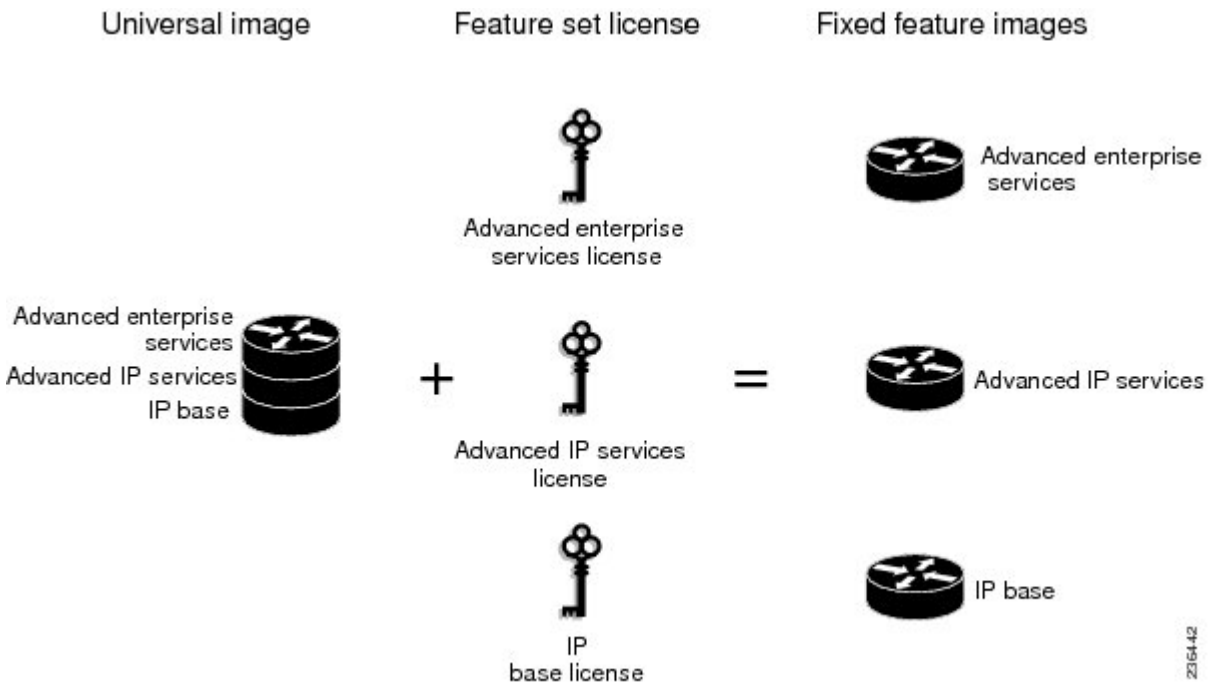
License Models for Images and Features

Cisco IOS Universal Image-Based Licenses

The Cisco IOS universal image contains *all* fixed feature images in one image. You can access the required functionality based on the license installed on the device. A higher-level feature-set license inherits the content

of the lower-level feature sets it contains. The figure below shows an example of the feature sets and fixed feature images that can make the universal image.

Figure 1: Example of Universal Image Components



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

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

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

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

Feature-Based Licenses

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

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

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

- Validity of a subscription license

License Types

Permanent Licenses

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

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

Temporary Licenses

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

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

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

These sections further define the types of temporary licenses:

Built-in Licenses for Emergencies

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

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

Evaluation Licenses

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

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

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

Extension Licenses

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

Note You must obtain approval to use an extension license.

Uncounted or Counted Licenses

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

Pay as You Grow Model

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

Subscription Licenses

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

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

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

Software Activation Processes

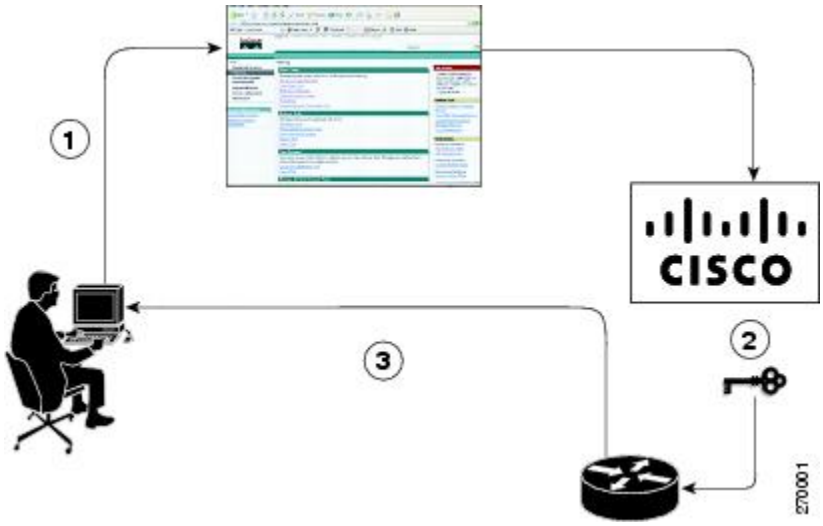
Software activation enables the various feature sets on a device by using license keys.

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

Manufacturing Preinstalled Licenses

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

Figure 2: Manufacturing Preinstalled License Work Flow



The work flow for manufacturing preinstalled licensing involves these steps:

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

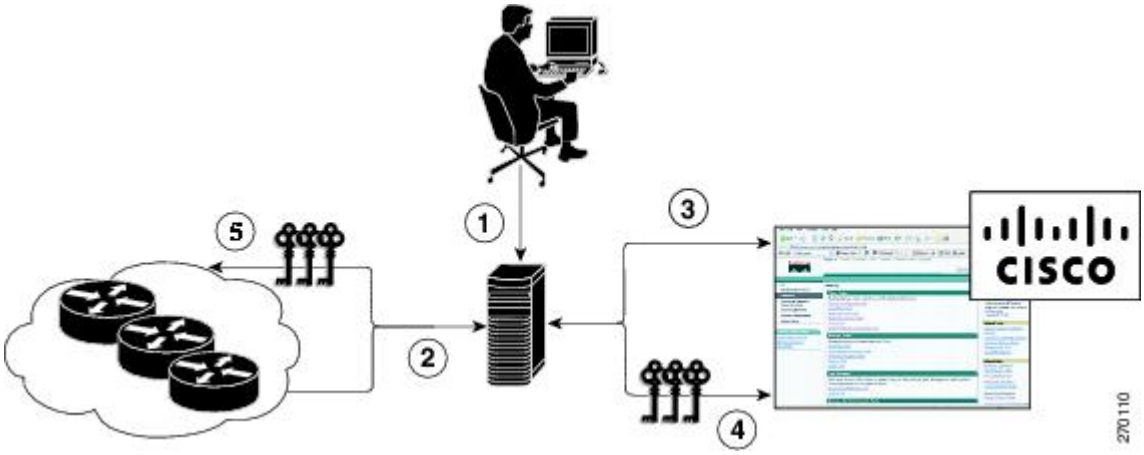
Automated Software Activation by Using Cisco License Manager

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

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

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

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



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

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

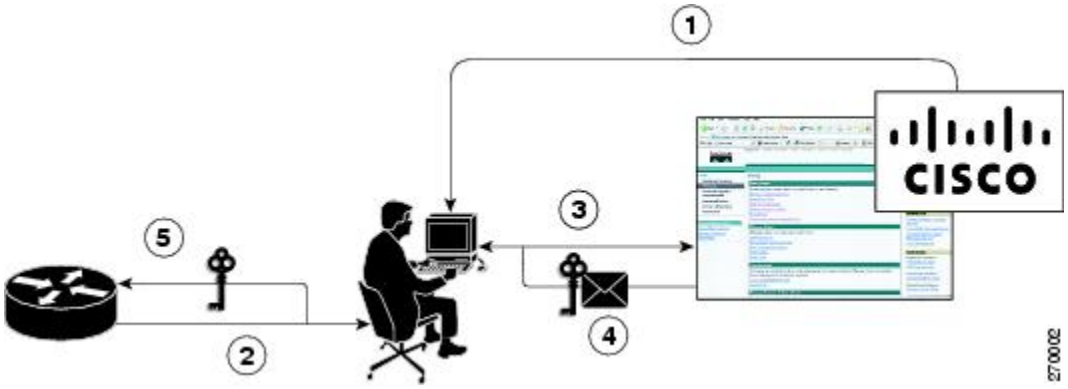
For more information, see the *User Guide for Cisco License Manager* at http://www.cisco.com/en/US/products/ps7138/products_user_guide_list.html.

License Software Activation by Using EXEC Commands

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

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

Figure 4: License Upgrade Work Flow for Manual License Fulfillment



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

1. You purchase the required PAKs for the desired type of license. Some licenses do not require a PAK, but they might need a contract instead.
2. You obtain the UDI from the device.
3. You enter the UDI and PAK into the Cisco Product License Registration portal. If it is a contract license, follow the links to non-PAK-based licenses and submit the UDI of the device.
4. The portal retrieves the SKUs associated with the PAK. You then select the SKU and enter the UDI, a unique and unchangeable identifier of the device where the license should be installed. A license key is then e-mailed to you, and you use that key to install the license.
5. You install the license file returned from the license portal to the device by using the CLI.

License Transfer Between Devices

Cisco supports two scenarios to transfer licenses between devices:

1. The first scenario has both the source and destination devices active and functional. In this scenario, the license is revoked on the source device, and a new permanent license is issued for the destination device.
2. The second is a failure scenario in which one of the devices is unavailable. In this scenario, the license from the failed device is transferred to the RMA or to the replaced device by using the RMA License Transfer process on the Cisco Product License Registration portal.

These scenarios are described in the following sections:

License Transfer Between Two Working Devices

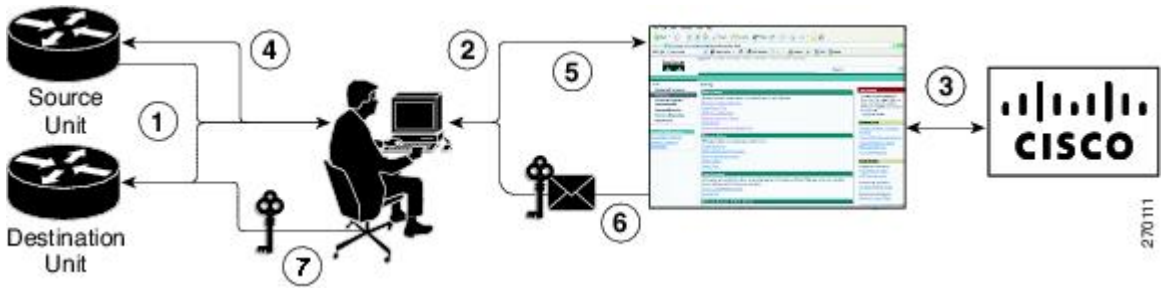
Cisco supports fully automated, customer-initiated, no-questions-asked transfer of licenses. Transferring a license between two working devices is accomplished by using a process known as *rehosting*. The rehosting process transfers a license from one UDI to another by revoking the license from the source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

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

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

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

Figure 5: License Transfer Work Flow



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

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

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

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

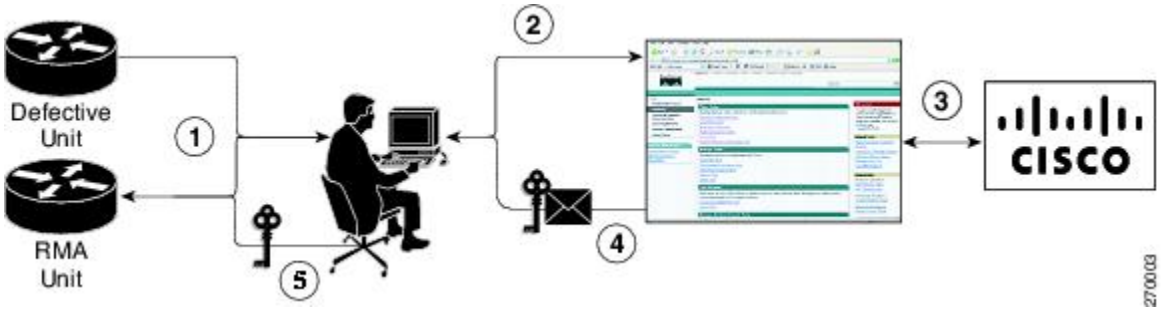
RMA License Transfer Between a Failed and a Working Device

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

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

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

Figure 6: License Transfer Work Flow for RMA Replacement Licenses



The RMA replacement license process involves these steps:

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

License Resend Request

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

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

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

Additional References

Related Documents

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

MIBs

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

Technical Assistance

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

Feature Information for Cisco IOS Software Activation

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

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

Table 1: Feature Information for Cisco IOS Software Activation

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

Glossary

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

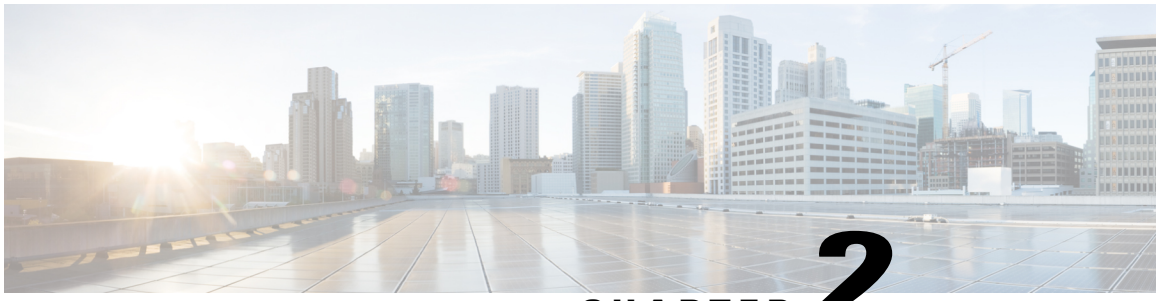
stack —A switch stack is a set of up to nine Catalyst 3750 switches connected through their StackWise ports.

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

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

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

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



CHAPTER 2

Configuring the Cisco IOS Software Activation Feature

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

Finding Feature Information

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

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

Restrictions for Cisco IOS Software Activation

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

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

Information About the Cisco IOS Software Activation

License Activation MIB Support

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

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

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

How to Activate Software from a Cisco IOS Device

Installing and Upgrading Licenses by Using Software Activation Commands

Before You Begin

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

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

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

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

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

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

SUMMARY STEPS

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

DETAILED STEPS

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

	Command or Action	Purpose
	Example: `Device# license install tftp://infra-sun/<user>/license/5400/38a.lic`	• Accept the end-user license agreement if prompted.
Step 6	**configure terminal** **Example:** `Device# configure terminal`	Enters the global configuration mode.
Step 7	**license boot level** {**metroaggrservices**} **Example:** `Device(config)# license boot level metroaggrservices`	Activates the metroaggrservices license on the device upon the next reload.
Step 8	**write memory** **Example:** `Device# write memory`	Saves the running configuration to NVRAM.
Step 9	**reload** **Example:** `Device# reload`	(Optional) Restarts the device to enable the new feature set. **Note** A reload is not required when moving from an evaluation license to a permanent license of the same license level on Cisco ASR 920 Series Routers.

Managing Licenses by Using Software Activation Commands

Adding a Comment to a License File

SUMMARY STEPS

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

DETAILED STEPS

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

Saving All Licenses to a Specified Storage Area

SUMMARY STEPS

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

DETAILED STEPS

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

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

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

Before You Begin

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

SUMMARY STEPS

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

DETAILED STEPS

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

	Command or Action	Purpose

Displaying All Licenses in a Device

SUMMARY STEPS

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

DETAILED STEPS

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

Displaying Detailed Information about Licensed Features

SUMMARY STEPS

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

DETAILED STEPS

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

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

Displaying Licensed Feature Sets Available in an Image

SUMMARY STEPS

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

DETAILED STEPS

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

Removing Licenses by Using Software Activation Commands

Removing a License Entry from a Permanent License File

Note

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

SUMMARY STEPS

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

DETAILED STEPS

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

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

Rehosting (Revoking and Transferring) a License

Before You Begin

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

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

SUMMARY STEPS

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

DETAILED STEPS

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

Troubleshooting License Operations by Using Software Activation Commands

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show license file** [**switch** *switch-num*] **Example:** `Device# show license file`	Displays license entries and license details stored in a Cisco software license file. If the device is a switch, this command obtains statistics from the specified switch.
Step 3	**show license statistics** **Example:** `Device# show license statistics`	Displays license statistics information. The display includes relevant statistics for error counts and is useful for troubleshooting licensing-related problems.
Step 4	**show license status** [**switch** *switch-num*] **Example:** `Device# show license status`	Displays the status of licenses in the system. If the device is a switch, this command obtains status from the specified switch.
Step 5	**debug license** {**all**	**core**	**errors**	**events**} **Example:** `Device# debug license errors`	Enables controlled software license debugging activity on a device.
Step 6	**no debug license** {**all**	**core**	**errors**	**events**} **Example:** `Device# no debug license errors`	Disables license debugging activity on a device.

Configuring Examples for Software Licensing

Example: Installing and Upgrading Licenses

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

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

Example: Adding a Comment to a License File

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

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

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

```
            cTxwnffn9i,4,aUWv8rL50opDUdAsFnxLsvoFRkcAfm$<WLC>AQEBIQAB//9NA+1m
            Uwfs/lD0dmdF9kyX8wDrua1TZhnnAy6Mxs1dTboIcRaahKxJJdj4Oi1w3wscqvPiA
            mWSaEmUT56rstk6gvmj+EQKRfD9A0ime1czrdKxfILT0LaXT416nwmfp92Tya6vIQ
            4FnlBdqJ1sMzXeSq8PmVcTU9A4o9hil9vKur8N9F885D9GVF0bJHciT5M=</WLC>
    Comment: Use this permanent license.
       Hash: E1WjIQo4qsl9g8cpnpoogP/0DeY=
Device#
```

Example: Saving All Licenses to a Specified Storage Area

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

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

Example: Removing Licenses

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

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

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

Example: Rehosting (Revoking and Transferring) a License

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

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

Example: Generic Command Enhanced with Licensing Information

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

reload

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

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

Note During the reload of Cisco ASR-920-24SZ-IM, ASR-920-24SZ-M, ASR-920-24TZ-M Series Router, there could be a IDPROM Access failure for Fan. To recover from this error, the router needs to be reloaded again.

show running-config

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

```
Device# show running-config
Building configuration...
Current configuration : 4772 bytes
!
version 12.4
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service internal
!
hostname csl-xfr-enhance-2951
```

```
!
...
...
license udi pid CISCO2951 sn FHH1211P037
license boot module c2951 technology-package securityk9 disable
license boot module c2951 technology-package uc
license boot module c2951 technology-package data
license call-home url https://tools-stage.cisco.com/SWIFT/Licensing
license agent listener http plaintext /lic-agent authenticate none
!
!
archive
 log config
  hidekeys
!
.
.
.
```

show tech-support

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

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

```
        permanent               Non-expiring node locked license
        extension               Expiring node locked license
        evaluation              Expiring non node locked license
        paid subscription       Expiring node locked subscription license
                                with valid end date
        extension subscription  Expiring node locked subscription license
        evaluation subscription Expiring node locked subscription license
...
...
------------------ show license statistics ------------------
               Administrative statistics
        Install success count:   0
        Install failure count:   0
        Install duplicate count: 0
        Comment add count:       0
        Comment delete count:    0
        Clear count:             0
        Save count:              0
        Save cred count:         1
               Client statistics
        Request success count:   1
        Request failure count:   3
        Release count:           0
        Global Notify count:     4
```

show version

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

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

Additional References

Related Documents

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

MIBs

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

Technical Assistance

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

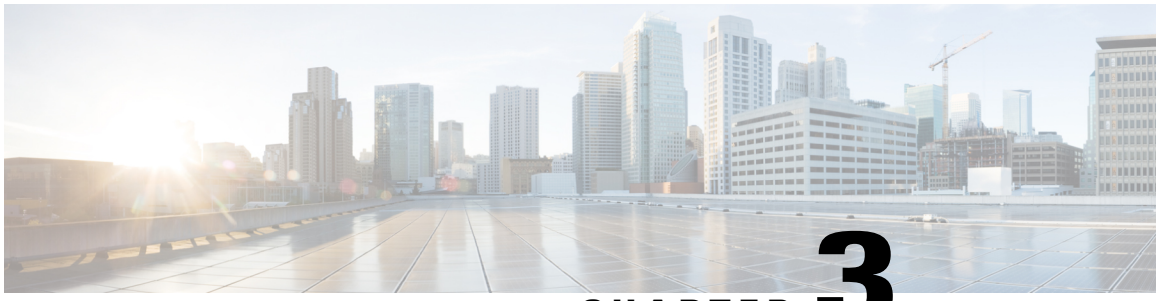
Feature Information for Cisco IOS Software Activation

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

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

Table 2: Feature Information for Cisco IOS Software Activation

Feature Name	Releases	Feature Information
Cisco IOS Software Activation	Cisco IOS XE Release 3.13.0S	This feature was introduced on the Cisco ASR 920 Series Aggregation Services Router (ASR-920-12CZ-A, ASR-920-12CZ-D, ASR-920-4SZ-A, ASR-920-4SZ-D).



CHAPTER 3

Configuring Call Home

Revised: July 9, 2014

The Call Home feature provides e-mail-based and web-based notification of critical system events. A versatile range of message formats are available for optimal compatibility with pager services, standard e-mail, or XML-based automated parsing applications. Common uses of this feature may include direct paging of a network support engineer, e-mail notification to a Network Operations Center, XML delivery to a support website, and utilization of Cisco Smart Call Home services for direct case generation with the Cisco Systems Technical Assistance Center (TAC). This document describes how to configure the Call Home feature on Cisco ASR 920 Series Routers beginning with Cisco IOS XE 3.13.0S.

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, see *Feature Information for Call Home*.

Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

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

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.
- Configure a trustpoint certificate authority (CA) if using secure HTTP (HTTPS) message delivery. For example, this procedure is required if you are using the HTTPS server for Cisco Smart Call Home Service in the CiscoTAC-1 profile for Call Home.
- Verify IP connectivity from the router to the e-mail server(s) or the destination HTTP server.
- If Cisco Smart Call Home is used, verify an active service contract exists for the device being configured.

Information About Call Home

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

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

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

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

Benefits of Using Call Home

The Call Home feature offers the following benefits:

- Multiple message-format options:

- Short Text—Suitable for pagers or printed reports.
- Plain Text—Full formatted message information suitable for human reading.
- XML—Matching readable format using Extensible Markup Language (XML) and Adaptive Markup Language (AML) document type definitions (DTDs). The XML format enables communication with the Cisco Smart Call Home server.

- Multiple concurrent message destinations.
- Multiple message categories, including configuration, environmental conditions, inventory, syslog, and crash events

  and diagnostics.
- Filtering of messages by severity and pattern matching.
- Scheduling of periodic message sending.

Obtaining Smart Call Home Services

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

Smart Call Home offers the following features:

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

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

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

For information 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

How to Configure Call Home

Configuring the Management Interface VRF

The Call Home feature requires use of the Gigabit Ethernet Management interface virtual routing and forwarding (VRF) instance. The Gigabit Ethernet Management interface is automatically part of its own VRF named "Mgmt-intf."

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

or

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Router#` **configure terminal**	Enters global configuration mode.
Step 2	**interface GigabitEthernet 0** **Example:** `Router(config)#` **interface GigabitEthernet0**	(Required) Specifies the Gigabit Ethernet Management interface on the router.
Step 3	**vrf forwarding Mgmt-intf** **Example:** `Router(config-if)#` **vrf forwarding Mgmt-intf**	(Required) Associates the Mgmt-intf VRF with the Gigabit Ethernet Management interface. This command is configured by default.

	Command or Action	Purpose
Step 4	Do one of the following: • **ip address** *ip-address mask* [**secondary** [**vrf** *vrf-name*]] • • • **ipv6 address** {*X:X:X:X::X* **link-local** | *X:X:X:X::X/prefix* [**anycast** | **eui-64**] | **autoconfig** [**default**]} **Example:** `Router(config-if)#` **ip address 10.10.10.10 0.0.0.0**	(Required) Specifies the IPv4 or IPv6 addressing for the interface.

What To Do Next

To find out more about the Gigabit Ethernet Management interface on the Cisco ASR 920 Series Routers or perform additional related configuration tasks on the management interface, see the Using the Management Ethernet Interface .

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.

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, on page 48.

You can configure the following attributes for a destination profile:

- Profile name—A 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 to which the alert should be sent.
- 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.

This section includes the following tasks:

Configuring a Destination Profile to Send Email Messages

To configure Call Home to send email messages, complete the following tasks:

Configuring the Mail Server

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

Consider the following guidelines when configuring the mail server:

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

SUMMARY STEPS

1. **configure terminal**
2. **call-home**
3. **mail-server** {*ipv4-address* | *name*} **priority** *number*

DETAILED STEPS

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

	Command or Action	Purpose
Step 3	**mail-server** {*ipv4-address* | *name*} **priority** *number* **Example:** `Router(cfg-call-home)#` **mail-server stmp.example.com priority 1**	Specifies an e-mail server and its relative priority among configured e-mail servers, where: • *ipv4-address* —Specifies the IPv4 address of the mail server. • *name* —Specifies the mail server's fully qualified domain name (FQDN) of 64 characters or less. • *number* —Assigns a number between 1 (highest priority) and 100 (lowest priority).

What to Do Next

Example:

The following example shows the configuration of a primary mail server (named "smtp.example.com") and secondary mail server at IP address 192.168.0.1:

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

Associating the Management Interface VRF With Call Home

The Call Home feature requires the management interface VRF (Mgmt-intf) to provide e-mail messaging support. If you have not configured the management interface VRF, see the Configuring the Management Interface VRF, on page 36.

To associate the management interface VRF with Call Home, complete the following steps:

SUMMARY STEPS

1. **configure terminal**
2. **call-home**
3. **vrf Mgmt-intf**

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	**vrf Mgmt-intf** **Example:** `Router(cfg-call-home)#` **vrf Mgmt-intf**	(Required) Associates the Mgmt-intf VRF for the email transport method using Call Home.

Configuring a Destination Profile for E-mail

To configure a destination profile for e-mail transport, 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:** `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 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:** `Router(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:** `Router(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:** `Router(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:** `Router(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:** `Router(cfg-call-home-profile)#` **active**	(Optional) Enables the destination profile. By default, a user-defined profile is enabled when it is created.

	Command or Action	Purpose
Step 9	**exit** **Example:** `Router(cfg-call-home-profile)#` **exit**	Exits call home destination profile configuration mode and returns to call home configuration mode.
Step 10	**end** **Example:** `Router(cfg-call-home)#` **end**	Returns to privileged EXEC mode.

Configuring Other Email Options

For the e-mail transport method, you can also configure the from and reply-to e-mail addresses by completing the following steps:

SUMMARY STEPS

1. **configure terminal**
2. **call-home**
3. **sender from** *email-address*
4. **sender reply-to** *email-address*

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	**sender from** *email-address* **Example:** `Router(cfg-call-home)#` **sender from username@example.com**	(Optional) Assigns the e-mail address that will appear in the from field in Call Home e-mail messages. If no address is specified, the contact e-mail address is used.

	Command or Action	Purpose
Step 4	**sender reply-to** *email-address* **Example:** `Router(cfg-call-home)#` **sender reply-to username@example.com**	(Optional) Assigns the e-mail address that will appear in the reply-to field in Call Home e-mail messages.

Configuring a Destination Profile to Send HTTP Messages

To configure Call Home to send HTTP (or HTTPS) messages, complete the following tasks:

Configuring the HTTP Source Interface

If you are using HTTP or HTTPS to send Call Home messages, then you must configure the VRF management interface as the HTTP client source interface.

SUMMARY STEPS

1. **configure terminal**
2. **ip http client source-interface** *type number*
3. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Router#` **configure terminal**	Enters global configuration mode.
Step 2	**ip http client source-interface** *type number* **Example:** `Router(config)#` **ip http client source-interface gigabitethernet 0**	Configures the source interface for the HTTP client. **Note** This interface should be the VRF management interface.
Step 3	**end** **Example:** `Router(cfg-call-home)#` **end**	Returns to privileged EXEC mode.

Configuring a Destination Profile for HTTP

To configure a destination profile for http transport, complete the following steps:

SUMMARY STEPS

1. **configure terminal**
2. **call-home**
3. **profile** *name*
4. **destination transport-method http**
5. **destination address http** *url*
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:** `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.
Step 4	**destination transport-method http** **Example:** `Router(cfg-call-home-profile)#` **destination transport-method http**	Enables the HTTP message transport method.

	Command or Action	Purpose
Step 5	**destination address http** *url* **Example:** `Router(cfg-call-home-profile)#` **destination address http https://example.url.com**	Configures the destination URL to which Call Home messages are sent. **Note** When entering a destination URL, include either **http://** or **https://**, depending on whether the server is a secure server. If the destination is a secure server, you must also configure a trustpoint CA.
Step 6	**destination preferred-msg-format** {**long-text** | **short-text** | **xml**} **Example:** `Router(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:** `Router(cfg-call-home-profile)#` **destination message-size 3,145,728**	(Optional) Configures a maximum destination message size for the destination profile.
Step 8	**active** **Example:** `Router(cfg-call-home-profile)#` **active**	Enables the destination profile. By default, a profile is enabled when it is created.
Step 9	**exit** **Example:** `Router(cfg-call-home-profile)#` **exit**	Exits call home destination profile configuration mode and returns to call home configuration mode.
Step 10	**end** **Example:** `Router(cfg-call-home)#` **end**	Returns to privileged EXEC mode.

Configuring a Trustpoint Certificate Authority

If you are using the HTTP transport method and specifying an HTTPS destination URL, then you will also need to configure a trustpoint certificate authority (CA).

For more information about how to configure a trustpoint CA, see the Declare and Authenticate a CA Trustpoint. That section describes how to configure a CA trustpoint for a secure Cisco server to use with the Smart Call Home service, but can be applied to other secure server configuration as needed by your site using the required certificate for your secure server.

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.
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.

	Command or Action	Purpose
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.

Copying a Destination Profile

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

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.

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 on the router:

- Configuration
- Diagnostic
- Environment
- Inventory
- Syslog

The triggering events for each alert group are listed in the Alert Group Trigger Events and Commands, on page 71, and the contents of the alert group messages are listed in the Message Contents, on page 74.

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

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

Periodic Notification

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

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

Message Severity Threshold

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

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

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

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

Table 3: Severity and Syslog Level Mapping

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

Syslog Pattern Matching

When you subscribe a destination profile to the Syslog alert group, you can optionally specify a text pattern to be matched within each syslog message. If you configure a pattern, a Syslog alert group message is sent only if it contains the specified pattern and meets the severity threshold. If the pattern contains spaces, you must enclose it within double quotation marks(“ ”) when configuring it. You can specify up to five patterns for each destination profile.

To subscribe a destination profile to one or more alert groups, complete the following steps:

SUMMARY STEPS

1. **configure terminal**
2. **call-home**
3. **alert-group** {**all** | **configuration** | **environment** | **inventory** | **syslog**}
4. **profile** *name*
5. **subscribe-to-alert-group all**
6. **subscribe-to-alert-group configuration** [**periodic** {**daily** *hh:mm* | **monthly** *date hh:mm* | **weekly** *day hh:mm*}]
7. **subscribe-to-alert-group diagnostic** [**severity** {**catastrophic** | **critical** | **debugging** | **disaster** | **fatal** | **major** | **minor** | **normal** | **notification** | **warning**}]
8. **subscribe-to-alert-group environment** [**severity** {**catastrophic** | **critical** | **debugging** | **disaster** | **fatal** | **major** | **minor** | **normal** | **notification** | **warning**}]
9. **subscribe-to-alert-group inventory** [**periodic** {**daily** *hh:mm* | **monthly** *date hh:mm* | **weekly** *day hh:mm*}]
10. **subscribe-to-alert-group syslog** [**severity** {**catastrophic** | **critical** | **debugging** | **disaster** | **fatal** | **major** | **minor** | **normal** | **notification** | **warning**}][**pattern** *string*]

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	**alert-group** {**all** | **configuration** | **environment** | **inventory** | **syslog**} **Example:** `Device(cfg-call-home)#` **alert-group all**	Enables the specified alert group. Use the all keyword to enable all alert groups. By default, all alert groups are enabled.
Step 4	**profile** *name* **Example:** `Device(cfg-call-home)#` **profile profile1**	Enters call home destination profile configuration mode for the specified destination profile.
Step 5	**subscribe-to-alert-group all** **Example:** `Device(cfg-call-home-profile)#` **subscribe-to-alert-group all**	(Optional) Subscribes this destination profile to all available alert groups. **Note** Alternatively, you can also subscribe to alert groups individually by specific type as described in steps 6 through 9.
Step 6	**subscribe-to-alert-group configuration** [**periodic** {**daily** *hh:mm* | **monthly** *date hh:mm* | **weekly** *day hh:mm*}] **Example:** `Device(cfg-call-home-profile)#` **subscribe-to-alert-group configuration periodic daily 12:00**	Subscribes this destination profile to the Configuration alert group, with an optional **periodic** value.
Step 7	**subscribe-to-alert-group diagnostic** [**severity** {**catastrophic** | **critical** | **debugging** | **disaster** | **fatal** | **major** | **minor** | **normal** | **notification** | **warning**}] **Example:** `Device(cfg-call-home-profile)#` **subscribe-to-alert-group diagnostic severity critical**	Subscribes this destination profile to the Diagnostic alert group, with an optional **severity** level.
Step 8	**subscribe-to-alert-group environment** [**severity** {**catastrophic** | **critical** | **debugging** | **disaster** | **fatal** | **major** | **minor** | **normal** | **notification** | **warning**}] **Example:** `Device(cfg-call-home-profile)#` **subscribe-to-alert-group environment severity major**	Subscribes this destination profile to the Environment alert group, with an optional **severity** level.
Step 9	**subscribe-to-alert-group inventory** [**periodic** {**daily** *hh:mm* | **monthly** *date hh:mm* | **weekly** *day hh:mm*}] **Example:** `Device(cfg-call-home-profile)#` **subscribe-to-alert-group inventory periodic monthly 1 12:00**	Subscribes this destination profile to the Inventory alert group, with an optional **periodic** value.

	Command or Action	Purpose
Step 10	**subscribe-to-alert-group syslog** [**severity** {**catastrophic** | **critical** | **debugging** | **disaster** | **fatal** | **major** | **minor** | **normal** | **notification** | **warning**}][**pattern** *string*] **Example:** `Device(cfg-call-home-profile)#` **subscribe-to-alert-group syslog**	Subscribes this destination profile to the Syslog alert group, with an optional **severity** level. You can specify a pattern to be matched in the syslog message, up to a maximum of five patterns per profile. If the pattern contains spaces, you must enclose it within double quotation marks (“ ”).

Configuring Contact Information

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

To assign the contact information, complete the following steps:

SUMMARY STEPS

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

DETAILED STEPS

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

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

Example

The following example shows the configuration of contact information:

```
Device# configure terminal
```

```
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# call-home
Device(cfg-call-home)# contact-email-addr username@example.com
Device(cfg-call-home)# phone-number +1-222-333-4444
Device(cfg-call-home)# street-address "1234 Any Street, Any city, Any state, 12345"
Device(cfg-call-home)# customer-id Customer1234

Device(cfg-call-home)# site-id Site1ManhattanNY
Device(cfg-call-home)# contract-id Company1234

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

Configuring the Number of Call Home Messages Sent Per Minute

The Call Home feature defaults to a maximum of 20 messages per minute. If you want to change that value, complete the following steps:

SUMMARY STEPS

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

DETAILED STEPS

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

Sending Call Home Communications Manually

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

Sending a Call Home Test Message Manually

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

SUMMARY STEPS

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

DETAILED STEPS

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

Sending Call Home Alert Group Messages Manually

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

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

- Configuration,
  diagnostic

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

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

SUMMARY STEPS

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

DETAILED STEPS

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

Submitting Call Home Analysis and Report Requests

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

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

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

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

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

SUMMARY STEPS

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

DETAILED STEPS

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

Example

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

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

Sending the Output of a Command to Cisco or an E-Mail Address

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 CLI command can be any run command, including commands for all modules. The command must be contained in quotes (“”).
- If an e-mail address is specified, the command output is sent to that address. If no e-mail address is specified, the output is sent to the Cisco TAC (attach@cisco.com). The e-mail is sent in long text format with the service number, if specified, in the subject line.
- The service number is required only if no e-mail address is specified, or if a Cisco TAC e-mail address is specified.

To execute a CLI command and e-mail the command output, complete the following step:

SUMMARY STEPS

1. **call-home send** “*command*”

DETAILED STEPS

	Command or Action	Purpose
Step 1	**call-home send** “*command*” **Example:** {**email** *email-addr* [**tac-service-request** *request-number*] | **tac-service-request** *request-number* [**email** *email-addr*]} **Example:** Router# **call-home send “show call-home” email support@example.com**	Executes the specified CLI command and e-mails the output, where: • **email** *email-addr* —Specifies the email address to which the command output should be sent. This keyword is optional if used after entering the **tac-service-request** option. • **tac-service-request** *request-number* —Specifies the TAC service request number that will appear in the subject line of the email. This keyword is optional if used after entering the **email** option.

Example

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

Router# **call-home send "show diag" email support@example.com**

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
```

Configure and Enable Call Home

To establish the Cisco Smart Call Home service, there are certain steps that must be performed to configure and enable the Call Home feature on the router.

The CiscoTAC-1 profile is predefined in the Call Home feature to communicate using email to the back-end server for the Smart Call Home service. The URL to the Cisco HTTPS back-end server is also predefined. This profile is inactive by default.

However, unlike other profiles that you can configure in Call Home to support both transport methods, the CiscoTAC-1 profile can only use one transport method at a time. Therefore, to use this profile with the Cisco Smart Call Home HTTPS server, you must change the transport method from email to HTTP and enable the profile. In addition, you must minimally specify a contact e-mail address and enable the Call Home feature.

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:** `Router#` **configure terminal**	Enters global configuration mode.
Step 2	**call-home** **Example:** `Router(config)#` **call-home**	Enters call home configuration mode.
Step 3	**profile CiscoTAC-1** **Example:** `Router(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:** `Router(cfg-call-home-profile)#` **destination transport-method http**	(Required only if using HTTPS) Configures the message transport method for http.
Step 5	**active** **Example:** `Router(cfg-call-home-profile)#` **active**	Enables the destination profile.

	Command or Action	Purpose
Step 6	**exit** **Example:** `Router(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:** `Router(cfg-call-home)#` **contact-email-addr username@example.com**	Assigns the customer's e-mail address. Enter up to 200 characters in e-mail address format with no spaces.
Step 8	**exit** **Example:** `Router(cfg-call-home)#` **exit**	Exits call home configuration mode and returns to global configuration mode.
Step 9	service call-home **Example:** `Router(config)#` **service call-home**	Enables the Call Home feature.
Step 10	**exit** **Example:** `Router(config)#` **exit**	Exits global configuration mode and returns to privileged EXEC mode.
Step 11	copy running-config startup-config **Example:** `Router#` **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.

Declare and Authenticate a CA Trustpoint

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

SUMMARY STEPS

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

DETAILED STEPS

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

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.

	Command or Action	Purpose
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
AQABMA0GCSqGSIb3DQEBBQUAA4GBAFFNzb5cy5gZnBWyATl4Lk0PZ3BwmcYQWpSk
U01UbSuvDVlAi2TT1+7eVmGSX6bEHRBhNtMsJzzoKQm5EWR0zLVznxxIqbxhAe7i
F6YM40AIOw7n60RzKprxaZLvcRTDOaxxp5EJb+RxBrO6WVcmeQD2+A2iMzAo1KpY
oJ2daZH9
quit
Certificate has the following attributes:
       Fingerprint MD5: A2339B4C 747873D4 6CE7C1F3 8DCB5CE9
      Fingerprint SHA1: 85371CA6 E550143D CE280347 1BDE3A09 E8F8770F
% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
% Certificate successfully imported
Router(config)# end
Router# copy running-config startup-config
```

Start Smart Call Home Registration

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

SUMMARY STEPS

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

DETAILED STEPS

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

What To Do Next

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

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

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

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

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

Displaying Call Home Configuration Information

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

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**show call-home** **Example:** `Device#` **show call-home**	Displays the Call Home configuration in summary.
Step 2	**show call-home detail** **Example:** `Device#` **show call-home detail**	Displays the Call Home configuration in detail.
Step 3	**show call-home alert-group** **Example:** `Device#` **show call-home alert-group**	Displays the available alert groups and their status.
Step 4	**show call-home mail-server status** **Example:** `Device#` **show call-home mail-server status**	Checks and displays the availability of the configured e-mail server(s).
Step 5	**show call-home profile** {**all**	*name*} **Example:** `Device#` **show call-home profile all**	Displays the configuration of the specified destination profile. Use the **all** keyword to display the configuration of all destination profiles.
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.

Examples

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

Configured Call Home Information in Summary

```
Router# 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
```

Configured Call Home Information in Detail

```
Router# show call-home detail
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 status: ACTIVE
    Preferred Message Format: long-text
    Message Size Limit: 3145728 Bytes
    Transport Method: email
```

```
    Email address(es): username@example.com
    HTTP  address(es): Not yet set up
    Alert-group               Severity
    ------------------------  ------------
    inventory                 normal
    Syslog-Pattern            Severity
    ------------------------  ------------
    N/A                       N/A
Profile Name: CiscoTAC-1
    Profile status: INACTIVE
    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 23 day of the month at 10:28
    Periodic inventory info message is scheduled every 23 day of the month at 10:13
    Alert-group               Severity
    ------------------------  ------------
    diagnostic                minor
    environment               minor
    inventory                 normal
    Syslog-Pattern            Severity
    ------------------------  ------------
    .*                        major
```

Available Call Home Alert Groups

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

E-Mail Server Status Information

```
Router# show call-home mail-server status
Please wait. Checking for mail server status ...
Translating "smtp.example.com"
    Mail-server[1]: Address: smtp.example.com Priority: 1 [Not Available]
    Mail-server[2]: Address: 192.168.0.1 Priority: 2 [Not Available]
```

Information About All Destination Profiles (Predefined and User-Defined)

```
Router# show call-home profile all
Profile Name: campus-noc
    Profile status: ACTIVE
    Preferred Message Format: long-text
    Message Size Limit: 3145728 Bytes
    Transport Method: email
    Email address(es): username@example.com
    HTTP  address(es): Not yet set up
    Alert-group               Severity
    ------------------------  ------------
    inventory                 normal
    Syslog-Pattern            Severity
    ------------------------  ------------
    N/A                       N/A
Profile Name: CiscoTAC-1
    Profile status: INACTIVE
    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 23 day of the month at 12:13
    Periodic inventory info message is scheduled every 23 day of the month at 11:58
    Alert-group               Severity
```

```
    ------------------------  ------------
    diagnostic                minor
    environment               minor
    inventory                 normal
    Syslog-Pattern            Severity
    ------------------------  ------------
    .*                        major
Router#
```

Information About a User-Defined Destination Profile

```
Router# show call-home profile campus-noc
Profile Name: campus-noc
    Profile status: ACTIVE
    Preferred Message Format: long-text
    Message Size Limit: 3145728 Bytes
    Transport Method: email
    Email address(es): username@example.com
    HTTP  address(es): Not yet set up
    Alert-group               Severity
    ------------------------  ------------
    inventory                 normal
    Syslog-Pattern            Severity
    ------------------------  ------------
    N/A                       N/A
```

Call Home Statistics

```
Router# show call-home statistics
Message Types    Total                Email                HTTP
-------------   -------------------- -------------------- ------------------
Total Success   6                    6                    0
    Config      4                    4                    0
    Diagnostic  0                    0                    0
    Environment 0                    0                    0
    Inventory   2                    2                    0
    SysLog      0                    0                    0
    Test        0                    0                    0
    Request     0                    0                    0
    Send-CLI    0                    0                    0
Total In-Queue  0                    0                    0
    Config      0                    0                    0
    Diagnostic  0                    0                    0
    Environment 0                    0                    0
    Inventory   0                    0                    0
    SysLog      0                    0                    0
    Test        0                    0                    0
    Request     0                    0                    0
    Send-CLI    0                    0                    0
Total Failed    0                    0                    0
    Config      0                    0                    0
    Diagnostic  0                    0                    0
    Environment 0                    0                    0
    Inventory   0                    0                    0
    SysLog      0                    0                    0
    Test        0                    0                    0
    Request     0                    0                    0
    Send-CLI    0                    0                    0
Total Ratelimit
      -dropped  0                    0                    0
    Config      0                    0                    0
    Diagnostic  0                    0                    0
    Environment 0                    0                    0
    Inventory   0                    0                    0
    SysLog      0                    0                    0
    Test        0                    0                    0
    Request     0                    0                    0
    Send-CLI    0                    0                    0
Last call-home message sent time: 2010-01-11 18:32:32 GMT+00:00
```

Default Settings

Lists of default Call Home settings.

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

Alert Group Trigger Events and Commands

Call Home trigger events are grouped into alert groups, with each alert group assigned CLI commands to execute when an event occurs. The CLI command output is included in the transmitted message. Table 4: Call Home Alert Groups, Events, and Actions , on page 72 lists the trigger events included in each alert group, including the severity level of each event and the executed CLI commands for the alert group.

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

Alert Group	Call Home Trigger Event	Syslog Event	Severity	Description and CLI Commands Executed
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**
Crash	Reload System crash and device reload		7	Crash dump reporting allows crash information to be collected and send to Cisco backend when a system is reloaded due to reload. **Note** Kernal crash can't be processed. CLI commands executed: **show version show logging show region show inventory show stack**
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**
—	—	%ENVIRONMENTAL-1-ALERT	1	Any sensor in fp/cc/rp has exceeded a certain threshold and resulted in this environmental alert.
—	ENVM	%ENVIRONMENTAL-1-SENSORFAIL	1	Any sensor in fp/cc/rp has failed and resulted in this environmental alert.

Alert Group	Call Home Trigger Event	Syslog Event	Severity	Description and CLI Commands Executed
—	—	%ENVMON-ENVIRONMENTAL-4-SENSOROK	1	Any sensor in fp/cc/rp has recovered and resulted in this environmental alert.
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 platform show inventory oid show version show diag all eeprom detail**
Syslog	—	—	—	Event logged to syslog. CLI commands executed: **show inventory show logging**
—	SYSLOG	LOG_EMERG	0	System is unusable.
—	SYSLOG	LOG_ALERT	1	Action must be taken immediately.
—	SYSLOG	LOG_CRIT	2	Critical conditions.
—	SYSLOG	LOG_ERR	3	Error conditions.
—	SYSLOG	LOG_WARNING	4	Warning conditions.
—	SYSLOG	LOG_NOTICE	5	Normal but signification condition.
—	SYSLOG	LOG_INFO	6	Informational.
—	SYSLOG	LOG_DEBUG	7	Debug-level messages.

Alert Group	Call Home Trigger Event	Syslog Event	Severity	Description and CLI Commands Executed
Test	—	TEST	—	User-generated test message. (Sent to TAC.) CLI commands executed: **show platform show inventory show version**

Message Contents

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

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

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

Table 5: Format for a Short Text Message

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

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

Data Item (Plain Text and XML)	Description (Plain Text and XML)	MML Tag (XML Only)
Time stamp	Date and time stamp of event in ISO time notation: *YYYY-MM-DD HH:MM:SS GMT+HH:MM.*	CallHome/EventTime

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

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

Data Item (Plain Text and XML)	Description (Plain Text and XML)	MML Tag (XML Only)	
System description	System description for the managed element.	CallHome/Device/Cisco_Chassis/AdditionalInformation/AD@name="sysDescr"	
Fields specific to a particular alert group message are inserted here.	The following fields may be repeated if multiple CLI commands are executed for this alert group.		
	Command output name	The exact name of the issued CLI command.	/aml/Attachments/Attachment/Name
	Attachment type	Attachment type. Usually "inline".	/aml/Attachments/Attachment@type
	MIME type	Normally "text" or "plain" or encoding type.	/aml/Attachments/Attachment/Data@encoding
	Command output text	Output of command automatically executed.	/mml/attachments/attachment/data

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

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

Data Item (Plain Text and XML)	Description (Plain Text and XML)	MML Tag (XML Only)
FRU software version	Software version(s) running on affected FRU.	CallHome/Device/Cisco_Chassis/ Cisco_Card/SoftwareIdentity/ VersionString

Table 8: Inserted Fields for an Inventory Event Message

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

The following example shows a Syslog alert notification in long text format:

```
TimeStamp : 2014-07-09 09:17 GMT+00:00
Message Name : syslog
Message Type : Call Home
Message Group : reactive
Severity Level : 4
Source ID : ASR920
Device ID : ASR-920@C@CAT1740U01D
Customer ID :
Contract ID :
Site ID :
Server ID : ASR-920@C@CAT1740U01D
```

```
Event Description : *Jul  9 09:17:03.055: %LINK-3-UPDOWN: Interface GigabitEthernet0/0/11,
 changed state to up System Name : Router Contact Email : vmalshet@cisco.com Contact Phone
 :
Street Address :
Affected Chassis : ASR-920
Affected Chassis Serial Number : CAT1740U01D Affected Chassis Part No : 68-3992-01 Affected
 Chassis Hardware Version : 1.0 Supervisor Software Version : 15.5(20140708:133902) Command
 Output Name : show logging Attachment Type : command output MIME Type : text/plain Command
 Output Text : 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, 183 messages logged, xml disabled,
                     filtering disabled
    Monitor logging: level debugging, 0 messages logged, xml disabled,
                     filtering disabled
    Buffer logging:  level debugging, 48 messages logged, xml disabled,
                    filtering disabled
    Exception Logging: size (4096 bytes)
    Count and timestamp logging messages: disabled
    Persistent logging: disabled
    Trap logging: level informational, 114 message lines logged
        Logging Source-Interface:       VRF Name:

Log Buffer (1000000 bytes):

*Jul  9 08:25:11.492: %SYS-5-LOG_CONFIG_CHANGE: Buffer logging: level debugging, xml disabled,
 filtering disabled, size (1000000) *Jul  9 08:25:17.639: %SYS-5-CONFIG_I: Configured from
 console by console *Jul  9 08:27:13.757: DEBUG - Found job name 9, to be triggered in 1049
 secs, changing to 1 seconds *Jul  9 08:27:13.757: DEBUG - *Jul  9 08:27:14.758: DEBUG -
Invoking callback 0x3B9887B0 for job 9 *Jul  9 08:27:14.758: DEBUG - *Jul  9 08:27:14.957:
 %SSH-5-DISABLED: SSH 1.99 has been disabled *Jul  9 08:27:21.719: %SSH-5-ENABLED: SSH 1.99
 has been enabled *Jul  9 08:27:21.910: %PKI-4-NOCONFIGAUTOSAVE: Configuration was modified.
  Issue "write memory" to save new IOS PKI configuration *Jul  9 08:27:21.910: DEBUG - Found
 job name 9, to be triggered in 1 secs, changing to 1189 seconds *Jul  9 08:27:21.910: DEBUG
 - *Jul  9 08:30:36.996: DEBUG - Found job name 9, to be triggered in 1189 secs, changing
to 1 seconds *Jul  9 08:30:36.997: DEBUG - *Jul  9 08:30:37.995: DEBUG - Invoking callback
 0x3B9887B0 for job 9 *Jul  9 08:30:37.996: DEBUG - *Jul  9 08:30:38.198: %SSH-5-DISABLED:
 SSH 1.99 has been disabled *Jul  9 08:30:41.734: %SSH-5-ENABLED: SSH 1.99 has been enabled
 *Jul  9 08:30:41.935: %PKI-4-NOCONFIGAUTOSAVE: Configuration was modified.  Issue "write
memory" to save new IOS PKI configuration *Jul  9 08:30:41.935: DEBUG - Found job name 9,
to be triggered in 1 secs, changing to 928 seconds *Jul  9 08:30:41.935: DEBUG - *Jul  9
08:46:09.936: DEBUG - Invoking callback 0x3B9887B0 for job 9 *Jul  9 08:46:09.936: DEBUG -
 *Jul  9 08:46:10.136: %SSH-5-DISABLED: SSH 1.99 has been disabled *Jul  9 08:46:14.301:
%SSH-5-ENABLED: SSH 1.99 has been enabled *Jul  9 08:46:14.483: %PKI-4-NOCONFIGAUTOSAVE:
Configuration was modified.  Issue "write memory" to save new IOS PKI configuration *Jul
9 08:46:14.483: DEBUG - Found job name 9, to be triggered in 928 secs, changing to 1033
seconds *Jul  9 08:46:14.483: DEBUG - *Jul  9 09:03:27.484: DEBUG - Invoking callback
0x3B9887B0 for job 9 *Jul  9 09:03:27.484: DEBUG - *Jul  9 09:03:27.688: %SSH-5-DISABLED:
SSH 1.99 has been disabled *Jul  9 09:03:33.000: %SSH-5-ENABLED: SSH 1.99 has been enabled
 *Jul  9 09:03:33.190: %PKI-4-NOCONFIGAUTOSAVE: Configuration was modified.  Issue "write
memory" to save new IOS PKI configuration *Jul  9 09:03:33.191: DEBUG - Found job name 9,
to be triggered in 1033 secs, changing to 1144 seconds *Jul  9 09:03:33.191: DEBUG - *Jul
 9 09:07:03.174: DEBUG - Invoking callback 0x3B988508 for job 12 *Jul  9 09:07:03.174: DEBUG
 - *Jul  9 09:07:03.174: %SMART_LIC-3-EVAL_EXPIRED_WARNING: Evaluation period expired on
Jan  1 00:00:00 1970 UTC where Jan  1 00:00:00 1970 UTC is the UTC date that it expired.
*Jul  9 09:07:03.174: DEBUG - Found job name 12, to be triggered in 3600 secs, changing to
 3600 seconds *Jul  9 09:07:03.174: DEBUG - *Jul  9 09:10:32.325: SMART-LICENSE-TRACE:
call_home_smart_license_status_get[446], Get smart license status 1 *Jul  9 09:11:14.883:
%SYS-5-CONFIG_I: Configured from console by console *Jul  9 09:12:23.087: %SYS-5-CONFIG_I:
 Configured from console by console *Jul  9 09:12:58.243: %SYS-5-CONFIG_I: Configured from
 console by console *Jul  9 09:13:29.983: %LINK-5-CHANGED: Interface GigabitEthernet0/0/11,
 changed state to administratively down *Jul  9 09:13:30.682: %LINEPROTO-5-UPDOWN: Line
protocol on Interface GigabitEthernet0/0/11, changed state to down *Jul  9 09:13:43.831:
%SYS-5-CONFIG_I: Configured from console by console *Jul  9 09:16:42.319: %SYS-5-CONFIG_I:
 Configured from console by console *Jul  9 09:16:58.459: %LINK-3-UPDOWN: Interface
GigabitEthernet0/0/11, changed state to down Router# Command Output Name : show inventory
Attachment Type : command output MIME Type : text/plain Command Output Text : show inventory
NAME: "Chassis", DESCR: "Cisco ASR920 Series - 12GE and 2-10GE - AC model"
```

```
PID: ASR-920           , VID: V01, SN: CAT1740U01D

NAME: "IM subslot 0/0", DESCR: "12-port Gig & 2-port Ten Gig Dual Ethernet Interface Module"
PID: 12xGE-2x10GE-FIXED, VID: V00, SN: N/A

NAME: "subslot 0/0 transceiver 1", DESCR: "GE SX"
PID: GLC-SX-MMD          , VID: A   , SN: FNS17481N4J

NAME: "subslot 0/0 transceiver 2", DESCR: "GE SX"
PID: FTLF8519P2BCL-CS  , VID: 0000, SN: FNS11270EAW

NAME: "subslot 0/0 transceiver 3", DESCR: "GE ZX"
PID: GLC-ZX-SMD          , VID: M1  , SN: OPL14450280

NAME: "subslot 0/0 transceiver 4", DESCR: "GE SX"
PID: GLC-SX-MMD          , VID: A   , SN: FNS17220A5R

NAME: "subslot 0/0 transceiver 5", DESCR: "GE SX"
PID: QFBR-5766LP       , VID:     , SN: AGS09498EPL

NAME: "subslot 0/0 transceiver 6", DESCR: "GE SX"
PID: GLC-SX-MMD          , VID: A   , SN: FNS17472EX1

NAME: "subslot 0/0 transceiver 7", DESCR: "GE SX"
PID: GLC-SX-MMD          , VID: A   , SN: FNS17372HFX

NAME: "subslot 0/0 transceiver 9", DESCR: "GE SX"
PID: GLC-SX-MMD          , VID: A   , SN: FNS17481M3M

NAME: "subslot 0/0 transceiver 13", DESCR: "SFP+ 10GBASE-SR"
PID: SFP-10G-SR          , VID: G4.1, SN: AVD1744A0UW

NAME: "module R0", DESCR: "ASR 920 Route Switch Processor , Base Scale, 64Gbps "
PID: ASR-920-12CZ-A    , VID: V00, SN: CAT1740U01D
```

Sample Syslog Alert Notification in XML Format

The following example shows a 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>M2:CAT1740U01D:53BD07BB</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>2014-07-09 09:13:31 GMT+00:00</aml-block:CreationDate>
<aml-block:Builder>
<aml-block:Name>ASR920</aml-block:Name>
<aml-block:Version>2.0</aml-block:Version>
</aml-block:Builder>
<aml-block:BlockGroup>
<aml-block:GroupId>G3:CAT1740U01D:53BD07BB</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>2014-07-09 09:13:29 GMT+00:00</ch:EventTime> <ch:MessageDescription>*Jul  9
09:13:29.983: %LINK-5-CHANGED: Interface GigabitEthernet0/0/11, changed state to
administratively down</ch:MessageDescription> <ch:Event> <ch:Type>syslog</ch:Type>
<ch:SubType></ch:SubType> <ch:Brand>Cisco Systems</ch:Brand>
<ch:Series>ASR920 Series Router</ch:Series> </ch:Event> <ch:CustomerData> <ch:UserData>
<ch:Email>vmalshet@cisco.com</ch:Email>
</ch:UserData>
<ch:ContractData>
<ch:CustomerId></ch:CustomerId>
<ch:SiteId></ch:SiteId>
<ch:ContractId></ch:ContractId>
<ch:DeviceId>ASR-920@C@CAT1740U01D</ch:DeviceId>
</ch:ContractData>
<ch:SystemInfo>
<ch:Name>Router</ch:Name>
<ch:Contact></ch:Contact>
<ch:ContactEmail>vmalshet@cisco.com</ch:ContactEmail>
<ch:ContactPhoneNumber></ch:ContactPhoneNumber>
<ch:StreetAddress></ch:StreetAddress>
</ch:SystemInfo>
<ch:CCOID></ch:CCOID>
</ch:CustomerData>
<ch:Device>
<rme:Chassis xmlns:rme="http://www.cisco.com/rme/4.0">
<rme:Model>ASR-920</rme:Model>
<rme:HardwareVersion>1.0</rme:HardwareVersion>
<rme:SerialNumber>CAT1740U01D</rme:SerialNumber>
<rme:AdditionalInformation>
<rme:AD name="PartNumber" value="68-3992-01" /> <rme:AD name="SoftwareVersion"
value="15.5(20140708:133902)" /> <rme:AD name="SystemObjectId" value="1.3.6.1.4.1.9.1.2062"
 /> <rme:AD name="SystemDescription" value="Cisco IOS Software, ASR920 Software
(PPC_LINUX_IOSD-UNIVERSALK9_NPE-M), Experimental Version 15.5(20140708:133902)
[mcp_dev-mrameshj-july4 114] Copyright (c) 1986-2014 by Cisco Systems, Inc.
Compiled Tue 08-Jul-14 23:52 by mrameshj" /> <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, 178 messages logged, xml disabled,
                     filtering disabled
    Monitor logging: level debugging, 0 messages logged, xml disabled,
                     filtering disabled
    Buffer logging:  level debugging, 43 messages logged, xml disabled,
                    filtering disabled
    Exception Logging: size (4096 bytes)
    Count and timestamp logging messages: disabled
    Persistent logging: disabled
    Trap logging: level informational, 109 message lines logged
        Logging Source-Interface:       VRF Name:

Log Buffer (1000000 bytes):

*Jul  9 08:25:11.492: %SYS-5-LOG_CONFIG_CHANGE: Buffer logging: level debugging, xml disabled,
 filtering disabled, size (1000000) *Jul  9 08:25:17.639: %SYS-5-CONFIG_I: Configured from
 console by console *Jul  9 08:27:13.757: DEBUG - Found job name 9, to be triggered in 1049
 secs, changing to 1 seconds *Jul  9 08:27:13.757: DEBUG - *Jul  9 08:27:14.758: DEBUG -
Invoking callback 0x3B9887B0 for job 9 *Jul  9 08:27:14.758: DEBUG - *Jul  9 08:27:14.957:
 %SSH-5-DISABLED: SSH 1.99 has been disabled *Jul  9 08:27:21.719: %SSH-5-ENABLED: SSH 1.99
 has been enabled *Jul  9 08:27:21.910: %PKI-4-NOCONFIGAUTOSAVE: Configuration was modified.
  Issue "write memory" to save new IOS PKI configuration *Jul  9 08:27:21.910: DEBUG - Found
 job name 9, to be triggered in 1 secs, changing to 1189 seconds *Jul  9 08:27:21.910: DEBUG
 - *Jul  9 08:30:36.996: DEBUG - Found job name 9, to be triggered in 1189 secs, changing
to 1 seconds *Jul  9 08:30:36.997: DEBUG - *Jul  9 08:30:37.995: DEBUG - Invoking callback
```

```
 0x3B9887B0 for job 9 *Jul  9 08:30:37.996: DEBUG - *Jul  9 08:30:38.198: %SSH-5-DISABLED:
 SSH 1.99 has been disabled *Jul  9 08:30:41.734: %SSH-5-ENABLED: SSH 1.99 has been enabled
 *Jul  9 08:30:41.935: %PKI-4-NOCONFIGAUTOSAVE: Configuration was modified.  Issue "write
memory" to save new IOS PKI configuration *Jul  9 08:30:41.935: DEBUG - Found job name 9,
to be triggered in 1 secs, changing to 928 seconds *Jul  9 08:30:41.935: DEBUG - *Jul  9
08:46:09.936: DEBUG - Invoking callback 0x3B9887B0 for job 9 *Jul  9 08:46:09.936: DEBUG -
 *Jul  9 08:46:10.136: %SSH-5-DISABLED: SSH 1.99 has been disabled *Jul  9 08:46:14.301:
%SSH-5-ENABLED: SSH 1.99 has been enabled *Jul  9 08:46:14.483: %PKI-4-NOCONFIGAUTOSAVE:
Configuration was modified.  Issue "write memory" to save new IOS PKI configuration *Jul
9 08:46:14.483: DEBUG - Found job name 9, to be triggered in 928 secs, changing to 1033
seconds *Jul  9 08:46:14.483: DEBUG - *Jul  9 09:03:27.484: DEBUG - Invoking callback
0x3B9887B0 for job 9 *Jul  9 09:03:27.484: DEBUG - *Jul  9 09:03:27.688: %SSH-5-DISABLED:
SSH 1.99 has been disabled *Jul  9 09:03:33.000: %SSH-5-ENABLED: SSH 1.99 has been enabled
 *Jul  9 09:03:33.190: %PKI-4-NOCONFIGAUTOSAVE: Configuration was modified.  Issue "write
memory" to save new IOS PKI configuration *Jul  9 09:03:33.191: DEBUG - Found job name 9,
to be triggered in 1033 secs, changing to 1144 seconds *Jul  9 09:03:33.191: DEBUG - *Jul
 9 09:07:03.174: DEBUG - Invoking callback 0x3B988508 for job 12 *Jul  9 09:07:03.174: DEBUG
 - *Jul  9 09:07:03.174: %SMART_LIC-3-EVAL_EXPIRED_WARNING: Evaluation period expired on
Jan  1 00:00:00 1970 UTC where Jan  1 00:00:00 1970 UTC is the UTC date that it expired.
*Jul  9 09:07:03.174: DEBUG - Found job name 12, to be triggered in 3600 secs, changing to
 3600 seconds *Jul  9 09:07:03.174: DEBUG - *Jul  9 09:10:32.325: SMART-LICENSE-TRACE:
call_home_smart_license_status_get[446], Get smart license status 1 *Jul  9 09:11:14.883:
%SYS-5-CONFIG_I: Configured from console by console *Jul  9 09:12:23.087: %SYS-5-CONFIG_I:
 Configured from console by console *Jul  9 09:12:58.243: %SYS-5-CONFIG_I: Configured from
 console by console Router#]]></aml-block:Data> </aml-block:Attachment> <aml-block:Attachment
 type="inline"> <aml-block:Name>show inventory</aml-block:Name> <aml-block:Data
encoding="plain"> <![CDATA[show inventory
NAME: "Chassis", DESCR: "Cisco ASR920 Series - 12GE and 2-10GE - AC model"
PID: ASR-920           , VID: V01, SN: CAT1740U01D

NAME: "IM subslot 0/0", DESCR: "12-port Gig & 2-port Ten Gig Dual Ethernet Interface Module"
PID: 12xGE-2x10GE-FIXED, VID: V00, SN: N/A

NAME: "subslot 0/0 transceiver 1", DESCR: "GE SX"
PID: GLC-SX-MMD          , VID: A   , SN: FNS17481N4J

NAME: "subslot 0/0 transceiver 2", DESCR: "GE SX"
PID: FTLF8519P2BCL-CS  , VID: 0000, SN: FNS11270EAW

NAME: "subslot 0/0 transceiver 3", DESCR: "GE ZX"
PID: GLC-ZX-SMD          , VID: M1  , SN: OPL14450280

NAME: "subslot 0/0 transceiver 4", DESCR: "GE SX"
PID: GLC-SX-MMD          , VID: A   , SN: FNS17220A5R

NAME: "subslot 0/0 transceiver 5", DESCR: "GE SX"
PID: QFBR-5766LP       , VID:     , SN: AGS09498EPL

NAME: "subslot 0/0 transceiver 6", DESCR: "GE SX"
PID: GLC-SX-MMD          , VID: A   , SN: FNS17472EX1

NAME: "subslot 0/0 transceiver 7", DESCR: "GE SX"
PID: GLC-SX-MMD          , VID: A   , SN: FNS17372HFX

NAME: "subslot 0/0 transceiver 9", DESCR: "GE SX"
PID: GLC-SX-MMD          , VID: A   , SN: FNS17481M3M

NAME: "subslot 0/0 transceiver 13", DESCR: "SFP+ 10GBASE-SR"
PID: SFP-10G-SR          , VID: G4.1, SN: AVD1744A0UW

NAME: "module R0", DESCR: "ASR 920 Route Switch Processor , Base Scale, 64Gbps "
PID: ASR-920-12CZ-A    , VID: V00, SN: CAT1740U01D


Router#]]></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 proactive diagnostics and real-time alerts.	Smart Call Home User Guide
Smart Call Home site page on Cisco.com for access to all related product information.	Cisco Smart Call Home site
Public Key Infrastructure (PKI) and Certificate Authority configuration in Cisco IOS XE software	Cisco IOS XE Security Configuration Guide: Secure Connectivity

Standards

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

MIBs

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

RFCs

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

Technical Assistance

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

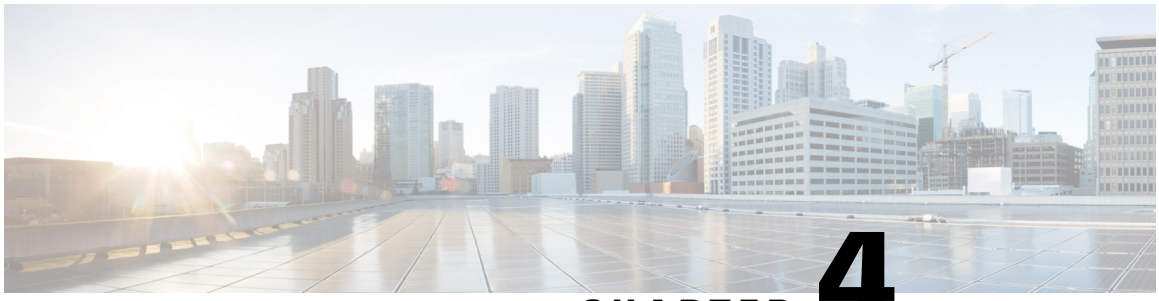
Feature Information for Call Home

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 9: Feature Information for Call Home

Feature Name	Releases	Feature Information
Call Home	Cisco IOS XE Release 3.13.0S	This feature was introduced on the Cisco ASR 920 Series Aggregation Services Router (ASR-920-12CZ-A, ASR-920-12CZ-D, ASR-920-4SZ-A, ASR-920-4SZ-D).



CHAPTER 4

What Is Smart Licensing ?

Smart Licensing is a system that consists of a license manager on a Cisco IOS XE device that manages licenses for various software and hardware features. The license manager parses and authenticates a license before accepting it. The software features on the router use the license manager APIs to check out and release licenses. Licenses are stored in persistent storage on the router.

Information About Smart Licensing

Smart Licensing is a cloud-based, software license management solution that enables you to automate time-consuming, manual licensing tasks. The solution allows you to easily track the status of your license and software usage trends.

Smart Licensing helps simplify three core functions:

- **Purchasing:** The software that you have installed in your network can automatically self-register themselves, without Product Activation Keys (PAKs).

- **Management:** You can automatically track activations against your license entitlements. Additionally, there is no need to install the license file on every node. You can create license pools (logical grouping of licenses) to reflect your organization structure. Smart Licensing offers you Cisco Smart Software Manager, a centralized portal that enables you to manage all your Cisco software licenses from one centralized website.
- **Reporting:** Through the portal, Smart Licensing offers an integrated view of the licenses you have purchased and what has been actually deployed in your network. You can use this data to make better purchase decisions, based on your consumption.

Restrictions:

- If the interface is configured using **ip http client source-interface interface**command with IPv6 address, it establishes a session with remote server with IPv6 connectivity.
- If the interface is configured using **ip http client source-interface interface** command with IPv4 address, it establishes a session with remote server with IPv4 connectivity.
- If the interface is configured using **ip http client source-interface interface**command with IPv6 address and IPv4 address, it establishes a session with remote server with IPv6 connectivity.
- If **ip http client source-interface interface** command is not configured, the interface establishes a session with remote server with IPv6 address.

Smart Versus Traditional Licensing

Traditional (node locked) licencing	Smart (dynamic) licencing
You must procure the license and manually install it on the device.	Your device initiates a call home and requests the licenses it needs.
Node-locked licences - license is associated with a specific device.	Pooled licences - licences are company account-specific, and can be used with any compatible device in your company. You can activate or deactivate different types of licenses on the device without actually installing a license file on the device.
No common install base location to view licenses purchased or software usage trends	Licenses are stored securely on Cisco servers accessible 24x7x365.
No easy means to transfer licenses from one device to another.	Licenses can be moved between product instances without a license transfer. This greatly simplifies the reassignment of a software license as part of the Return Material Authorization (RMA) process.
Limited visibility into all software licenses being used in the network. Licenses are tracked only on per node basis.	Complete view of all Smart Software Licenses used in the network using a consolidated usage report of software licenses and devices in one easy-to-use portal.

Create a Cisco Smart Account

Cisco Smart Account is an account where all products enabled for Smart Licensing are deposited. Cisco Smart Account allows you to manage and activate your licenses to devices, monitor license use, and track Cisco license purchases. Through transparent access, you have a real-time view into your Smart Licensing products. IT administrators can manage licenses and account users within your organization's Smart Account through the Smart Software Manager.

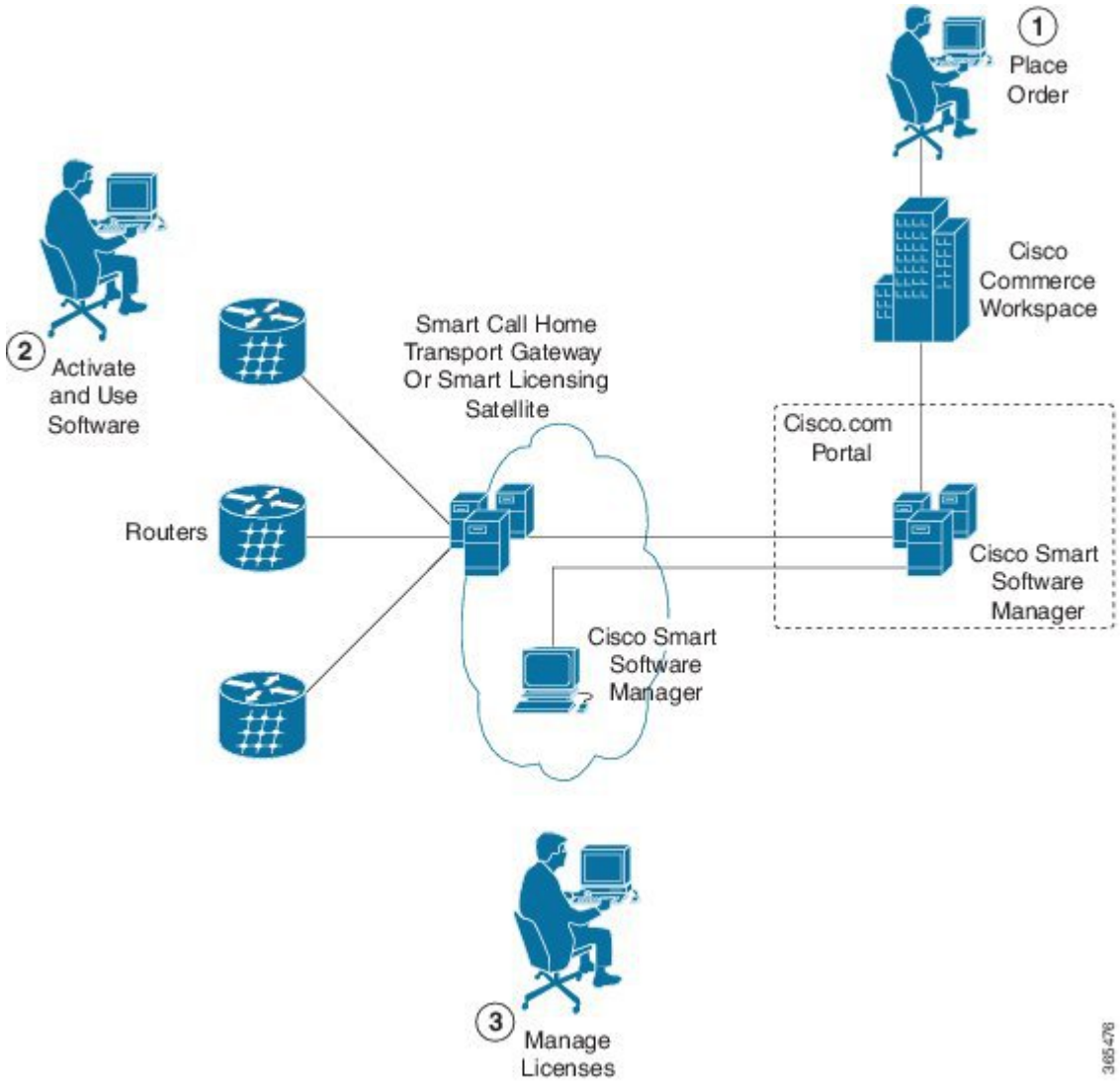
You can create your Cisco Smart Account at this webpage: https://webapps.cisco.com/software/company/smartaccounts/home#accountcreation-account/request.

For information on how to create a Cisco Smart Account, see: http://www.cisco.com/c/en/us/products/collateral/software/one-software/solution-overview-c22-733273.html.

Smart Licensing Working

Smart Licensing involves the three steps shown in the illustration below, that depicts the working model of the Smart Licensing.

Figure 7: Smart Licensing - Example



- **Setting up Smart Licensing:** You can place the order for Smart Licensing, to manage licenses on Cisco.com portal. You agree to the terms and conditions governing the use and access of Smart Licensing in the Smart Software Manager portal.
- **Enabling and Use Smart Licensing:** Enable Smart Licensing, *on page 91* describes the steps you must follow to enable Smart Licensing. *Smart Licencing Workflow* provides an illustration.
  After you enable Smart Licensing, you can use either of the following options to communicate:

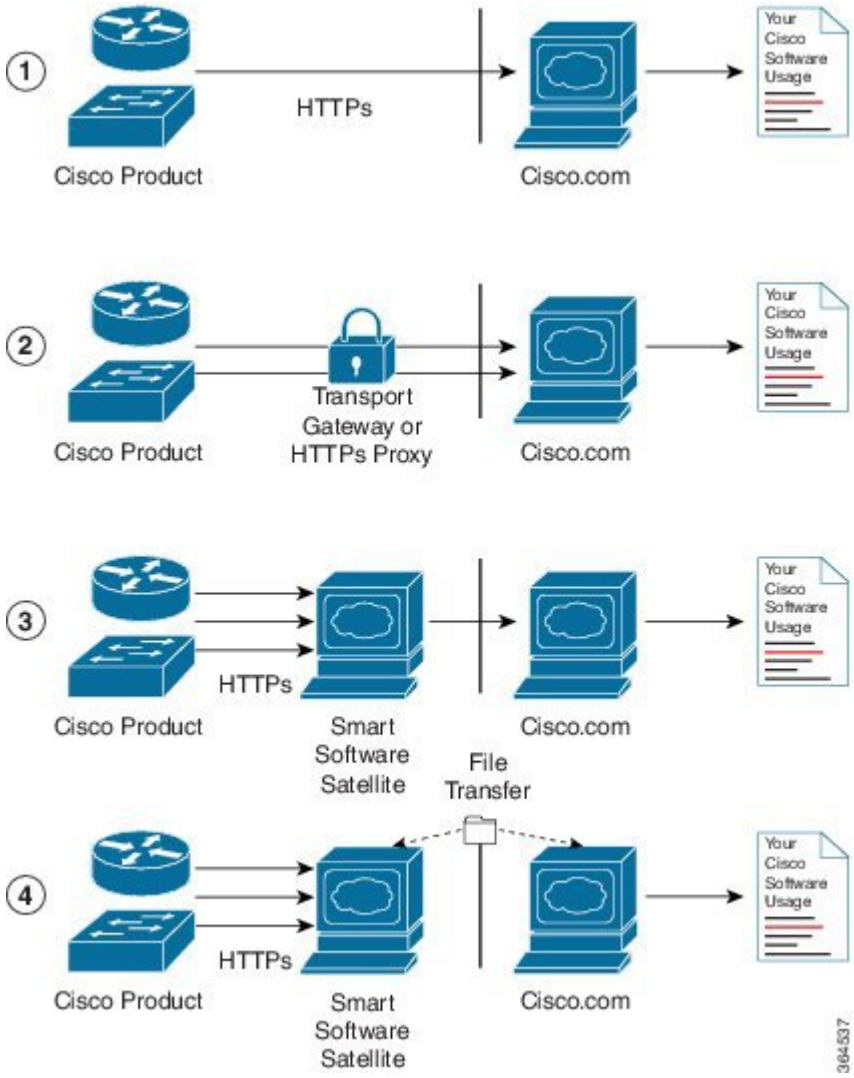
- **Smart Call Home:** The Smart Call Home feature is automatically configured after the Smart Licensing is enabled. Smart Call Home is used by Smart Licensing as a medium for communication with the Cisco license service. Call Home feature allows Cisco products to periodically call-home and perform an audit and reconciliation of your software usage information. This information helps Cisco efficiently track your install base, keep them up and running, and more effectively pursue service and support contract renewals, without much intervention from your end.
- **Smart Licensing Satellite:** The Smart licensing satellite option provides an on-premises collector that can be used to consolidate and manage Smart license usage, as well facilitate communications back to Cisco License Service at http://www.cisco.com.

- **Manage and Report Licenses:** You can manage and view reports about your overall software usage in the Smart Software Manager portal.

Deployment Options for Smart Licensing

The following illustration shows the various options available for deploying Smart Licensing:

Figure 8: Smart Licensing Deployment Options



1 **Direct cloud access:** In direct cloud access deployment method, Cisco products send usage information directly over the internet to Cisco.com (Cisco license service); no additional components are needed for deployment.

2 **Direct cloud access through an HTTPs proxy:** In direct cloud access through an HTTPs proxy deployment method, Cisco products send usage information over the internet through a proxy server - either a Smart Call Home Transport Gateway or off-the-shelf Proxy (such as Apache) to Cisco License Service.

3 **Mediated access through an on-premises collector-connected:** In mediated access through an on-premises collector-connected deployment method, Cisco products send usage information to a locally-connected

collector, which acts as a local license authority. Periodically, the information is exchanged to keep the databases in synchronization.

4 **Mediated access through an on-premises collector-disconnected:** In the mediated access through an on-premises collector-disconnected deployment method, Cisco products send usage information to a local disconnected collector, which acts as a local license authority. Exchange of human-readable information is performed occasionally (maybe once a month) to keep the databases in synchronization.

Options **1** and **2** provide an easy deployment option, and options **3** and **4** provide a secure environment deployment option. Smart Software Satellite provides support for options **3** and **4**.

Enable Smart Licensing

On successful registration, the device will receive an identity certificate. This certificate is saved on your device and automatically used for all future communications with Cisco. Every 30 days, Smart Licensing will automatically renew the registration information with Cisco. If registration fails, an error will be logged. Additionally, license usage data is collected and a report is sent to you every month. If required, you can configure your Smart Call Home settings such that sensitive information (like hostname, username and password) are filtered out from the usage report.

Note Once Smart Licensing mode is enabled, all CLIs related to the traditional licensing mode are disabled.

Before You Begin

You must have purchased the product for which you are adding the license. When you purchase the product, you are provided with a user name and password to the Cisco Smart Software Manager portal, from where you can generate the product instance registration tokens.

SUMMARY STEPS

1. Login to Cisco Smart Software Manager at https://tools.cisco.com/rhodui/index.
2. **license smart enable**
3. **license boot level** { *advancedmetroipaccess* | *metroaccess* | *metroipaccess* }
4. **license feature** { *atm* | *gnss* | *ipsec* | *port* | *ptp* | *upoe* }
5. **license smart register idtoken** *token_ID*

DETAILED STEPS

	Command or Action	Purpose
Step 1	Login to Cisco Smart Software Manager at https://tools.cisco.com/rhodui/index.	Get a token from the Cisco portal using the link. You must log in to the portal using a Cisco provided username and password. Once you have generated the token, select **Copy** hyperlink to copy the token or download the token to a text file. The token is used to register and activate a device, and assign the device to a virtual account. **Note** This token is valid for 30 days.

	Command or Action	Purpose
Step 2	**license smart enable** **Example:** `Device(config)#license smart enable`	Enables basic Smart Licensing. Use the **no** form of this command to disable Smart Licensing and revert to the traditional or strict mode of licensing. **Note** If you revert smart licencing to CSL, router need to be rebooted.
Step 3	**license boot level** { *advancedmetroipaccess* | *metroaccess* | *metroipaccess* } **Example:** `Device(config)#license boot level advancedmetroipaccess`	Enables technological license, these licenses need router reboot after configuring.
Step 4	**license feature** { *atm* | *gnss* | *ipsec* | *port* | *ptp* | *upoe* } **Example:** `Device(config)#license feature atm`	Enables different feature level licences available. **Note** Feature level license supported depends on the ASR 920 variant. For more information see, http://www.cisco.com/c/en/us/td/docs/routers/asr920/configuration/guide/csa/b_port_licensing_asr920.html

Step 5	**license smart register idtoken** *token_ID*
	
	Example:
	`Device# license smart register idtoken NmE1Yzg0OWMtYmJ4`
	
	`license smart register: Registration process is`
	`in progress.Please check the syslog for the`
	
	`registration status and result`
		Enables to register your device.

What to Do Next

You can use the Cisco Smart Software Manager to:

- Create virtual accounts
- Assign a registered device to a virtual account
- View licenses in a virtual account
- Manage product instance registration tokens
- Transfer a license
- View, transfer or remove product instances in a virtual account

Verify Smart Licensing Configuration

After enabling Smart Licensing, you can use the **show** commands to verify the default Smart Licensing configuration. If any issue is detected, take corrective action before making further configurations.

SUMMARY STEPS

1. **show license status**
2. **show license all**
3. exit
4. **show license tech support**
5. **show license usage**
6. **show license summary**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**show license status**
	
	Example:
	`Device#show license status`
		Displays the compliance status of Smart Licensing. Following are the possible status:
		• **Enabled**: Indicates that Smart Licensing is enabled.
		• **Waiting**: Indicates the initial state after your device has made a license entitlement request. The device establishes communication with Cisco and successfully registers itself with the Cisco license manager.
		• **Authorized**: Indicates that your device is able to communicate with the Cisco license manager, and is authorised to initiate requests for license entitlements.
		• **Out-Of-Compliance**: Indicates that one or more of your licenses are out-of-compliance. You must buy additional licenses.
		• **Eval Period**: Indicates that Smart Licencing is consuming the evaluation period. You must register the device with the Cisco Licensing manager, else your license expires.
		• **Grace Period**: Indicates that connectivity to the Cisco license manager is lost. You must try restore connectivity to renew the authorization period.
		• **Disabled**: Indicates that Smart Licensing is disabled.
		• **Invalid**: Indicates that Cisco does not recognize the entitlement tag as it is not in the database.
		
		Example:
		`Smart Licensing is ENABLED`
		
		`Registration:`
		`  Status: REGISTERED`
		`  Smart Account: BU Production Test`
		`  Virtual Account:Device`
		`  Export-Controlled Functionality: Allowed`
		`  Initial Registration: SUCCEEDED on Dec 17 02:31:11 2015 UTC`
		`  Last Renewal Attempt: None`
		`  Next Renewal Attempt: Jun 14 02:31:10 2016 UTC`
		`  Registration Expires: Dec 16 02:25:58 2016 UTC`
		
		`License Authorization:`
		`  Status: AUTHORIZED on Feb 01 05:08:29 2016 UTC`
		`  Last Communication Attempt: FAILED on Feb 01 05:08:29 2016 UTC`

	Command or Action	Purpose
		Failure reason: Fail to send out Call Home HTTP message. Next Communication Attempt: Feb 02 04:09:56 2016 UTC Communication Deadline: Mar 16 03:00:33 2016 UTC
Step 2	**show license all** **Example:** `Device#show license all`	Displays all entitlements in use. It can also be used to check if Smart Licensing is enabled. Additionally, it shows associated licensing certificates, compliance status, UDI, and other details.
Step 3	exit	

Step 4	**show license tech support**	Displays the output of the license commands. Example:
		`Smart Licensing Status`
		`=====================`
		
		`Smart Licensing is ENABLED`
		
		`Registration:`
		`Status: REGISTERED`
		`Smart Account: BU Production Test`
		`Virtual Account:Device`
		`Export-Controlled Functionality: Allowed`
		`Initial Registration: SUCCEEDED on Dec 17 02:31:11 2015 UTC`
		`Last Renewal Attempt: None`
		`Next Renewal Attempt: Jun 14 02:31:11 2016 UTC`
		`Registration Expires: Dec 16 02:25:59 2016 UTC`
		
		`License Authorization:`
		`Status: AUTHORIZED on Feb 01 05:08:29 2016 UTC`
		`Last Communication Attempt: FAILED on Feb 01 05:08:29 2016 UTC`
		`Failure reason: Fail to send out Call Home HTTP message.`
		`Next Communication Attempt: Feb 02 04:09:57 2016 UTC`
		`Communication Deadline: Mar 16 03:00:34 2016 UTC`
		
		`Evaluation Period:`
		`Evaluation Mode: Not In Use`
		`Evaluation Period Remaining: 89 days, 23 hours, 20 minutes, 20 seconds`

Step 5	**show license usage**	Displays the license usage information. Example:
		`Device#show license usage`
		`License Authorization:`
		`Status: AUTHORIZED on Feb 01 05:08:29 2016 UTC`
		
		`Device METRO IP ACCESS (metroipaccess):`
		`Description: Device METRO IP ACCESS`
		`Count: 1`
		`Version: 1.0`
		`Status: AUTHORIZED`
		
		`Device 1588 (1588):`
		`Description: Device 1588`
		`Count: 1`
		`Version: 1.0`

	Command or Action	Purpose
		Status: AUTHORIZED Device ATM (atm): Description: Device ATM Count: 1 Version: 1.0 Status: AUTHORIZED Device UPOE (upoe): Description: Device UPOE Count: 1 Version: 1.0 Status: AUTHORIZED Device GNSS (gnss): Description: Device GNSS Count: 1 Version: 1.0 Status: AUTHORIZED Device 6-1GE PORT LICENSE (1GEupgradelicense): Description: Device 6-1GE PORT LICENSE Count: 2 Version: 1.0 Status: AUTHORIZED Device 2-10G PORT LICENSE (10GEupgradelicense): Description: Device 2-10G PORT LICENSE Count: 2 Version: 1.0 Status: AUTHORIZED
Step 6	**show license summary**	Displays the summary of all active licenses. Example: Smart Licensing is ENABLED Registration: Status: REGISTERED Smart Account: BU Production Test Virtual Account: Device Export-Controlled Functionality: Allowed Last Renewal Attempt: None Next Renewal Attempt: Jun 14 02:31:11 2016 UTC License Authorization: Status: AUTHORIZED Last Communication Attempt: FAILED Next Communication Attempt: Feb 02 04:09:57 2016 UTC License Usage: License Entitlement tag Count Status --- Device METRO IP ACCESS (metroipaccess) 1 AUTHORIZED

	Command or Action	Purpose
		Device 1588 (1588) 1 AUTHORIZED Device ATM (atm) 1 AUTHORIZED Device UPOE (upoe) 1 AUTHORIZED Device GNSS (gnss) 1 AUTHORIZED Device 6-1GE PORT L... (1GEupgradelicense) 2 AUTHORIZED Device 2-10G PORT L... (10GEupgradelicense) 2 AUTHORIZED

Renew Smart Licensing Registration

In general, your registration is automatically renewed every 30 days. Use this option to make an on-demand manual update of your registration. Thus, instead of waiting 30 days for the next registration renewal cycle, you can issue this command to instantly find out the status of your license.

Before You Begin

You must ensure that the following conditions are met to renew your smart license:

- Smart licensing is enabled.
- The device is registered.

SUMMARY STEPS

1. **license smart renew** {**auth** | **id**}

DETAILED STEPS

	Command or Action	Purpose

Step 1	**license smart renew** {**auth**	**id**}
		
		Example:
		`Device# license smart renew auth`
		`Tue Apr 22 09:12:37.086 PST`
		
		`license smart renew auth: Authorization process is in progress.`
		`Please check the syslog for the authorization status and result.`
			Renew your ID or authorization with Cisco smart licensing. If ID certification renewal fails, then the product instance goes to an unidentified state and starts consuming the evaluation period.
			Note Authorization periods are renewed by the Smart Licensing system every 30 days. As long as the license is in an 'Authorized' or 'Out-of-compliance' (OOC), the authorization period is renewed. Grace period starts when an authorization period expires. During the grace period or when the grace period is in the 'Expired' state, the system continues to try renew the authorization period. If a retry is successful, a new authorization period starts.

De-register Smart Licensing

When your device is taken off the inventory, shipped elsewhere for redeployment or returned to Cisco for replacement using the return merchandise authorization (RMA) process, you can use the de-register option to cancel the registration on your device. Use the following steps to cancel device registration:

SUMMARY STEPS

1. **license smart deregister**

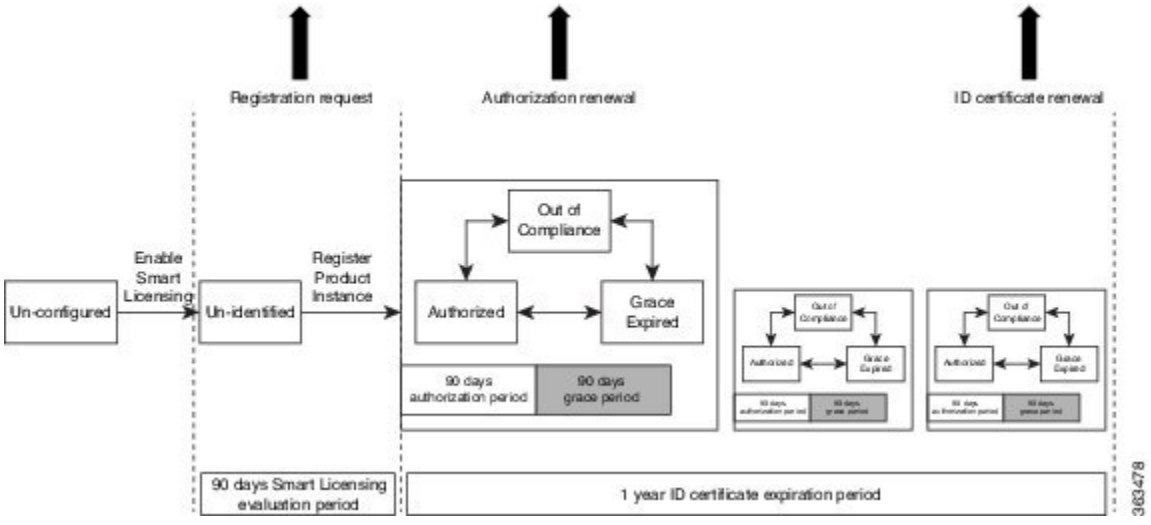
DETAILED STEPS

	Command or Action	Purpose

Step 1	**license smart deregister**
	
	Example:
	`Device# license smart deregister`
	
	`license smart deregister: Success`
	
	`License command "license smart deregister " completed successfully.`
		Cancels the device registration, and sends it into a 30-day evaluation mode. All Smart Licensing entitlements and certificates on the platform are removed.
		Note Though the product instance has been de-registered from the Cisco license cloud service, Smart Licencing is still enabled.

Smart Licensing Workflow

The Smart Licensing workflow is depicted in this flowchart.



Cisco Smart Software Manager Overview

Cisco Smart Software Manager enables you to manage all of your Cisco Smart software licenses from one centralized website. With Cisco Smart Software Manager, you organize and view your licenses in groups called virtual accounts (collections of licenses and product instances). Use the Cisco Smart Software Manager to do the following tasks:

- Create, manage or view virtual accounts.
- Create and manage Product Instance Registration Tokens.
- Transfer licenses between virtual accounts or view licenses.
- Transfer, remove or view product instances.
- Run reports against your virtual accounts.
- Modify your email notification settings.
- View overall account information.

The Cisco Smart Software Manager **Help** describes the procedures for carrying out these tasks. You can access the Cisco Smart Software Manager on https://webapps.cisco.com/software/csws/ws/platform/home, by clicking **Licensing**, and then selecting **Smart Software Manager**; and then login using the username and password provided by Cisco.

Note Use Chrome 32.0, Firefox 25.0 or Safari 6.0.5 web browsers to access the Cisco Smart Software Manager. Also, ensure that Javascript 1.5 or a later version is enabled in your browser.

Licenses, Product Instances, and Registration Tokens

Licenses

Licenses are required for all Cisco products. All Cisco product licenses are one of two types which vary depending on the product:

- Perpetual licenses—Licenses that do not expire.
- Term licenses—Licenses that automatically expire after a set amount of time: one year, three years, or whatever term was purchased.

In addition, there are demo licenses that expire after at most 60 days. As implied by the name, demo licenses are not intended for production use.

All product licenses reside in a virtual account.

Product Instances

A product instance is an individual device with a unique device identifier (UDI) that is registered using a product instance registration token (or registration token). You can register any number of instances of a product with a single registration token. Each product instance can have one or more licenses residing in the same virtual account. Product instances must periodically connect to the Cisco Smart Software Manager servers during a specific renewal period. If a product instance fails to connect, it is marked as having a license

shortage, but continues to use the license. If you remove the product instance, its licenses are released and made available within the virtual account.

Product Instance Registration Tokens

A product requires a registration token until you have registered the product. Registration tokens are stored in the Product Instance Registration Token Table associated with your enterprise account. Once the product is registered the registration token is no longer necessary and can be revoked and removed from the table without effect. Registration tokens can be valid from 1 to 365 days.

Virtual Accounts

Smart Licencing allows you to create multiple license pools or virtual accounts within the Smart Software Manager portal. Using the **Virtual Accounts** option you can aggregate licenses into discrete bundles associated with a cost center so that one section of an organization cannot use the licenses of another section of the organization. For example, if you segregate your company into different geographic regions, you can create a virtual account for each region to hold the licenses and product instances for that region.

All new licenses and product instances are placed in the default virtual account in the Smart Software Manager, unless you specify a different one during the order process. Once in the default account, you may choose to transfer them to any other account as desired, provided you have the required access permissions.

Use the Smart Software Manager portal at https://tools.cisco.com/rhodui/index to create license pools or transfer licenses.

Compliance reporting

On a periodic basis, as described by the terms of the Smart Licensing contract, reports are automatically sent to you containing inventory and license compliance data. These reports will take one of three forms:

- **Periodic Record:** This record is generated on a periodic (configurable) basis with relevant inventory data saved at a given point of time. This report is saved within the Cisco cloud for archival.
- **Manual Record:** You can manually generate this record with relevant inventory data saved at any given point of time. This report will be saved within the Cisco cloud for archival.
- **Compliance Warning Report:** This report is automatically or manually generated when a license compliance event occurs. This report does not contain a full inventory data, but only any shortfalls in entitlements for a given software license.

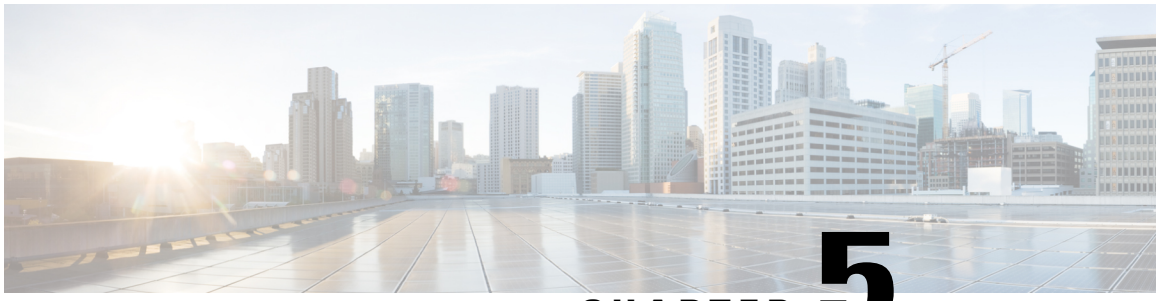
  You can view these reports from the Smart Software Manager portal at https://tools.cisco.com/rhodui/index.

Traditional Licensing Consideration in Smart Licensing

Traditional licensing, and the associated commands, currently co-exist with Smart Licensing. By default, the software image is loaded with the traditional, strictly-enforced mode of licensing. You may want to retain the traditional licensing model in the following scenarios:

- when there are multiple users, and you do not know the actual end user of your software.

- when the software is deployed in a location with limited access to the license and inventory management solution.
- when the user has opted not to establish a Smart Call Home relationship with Cisco.
- when a Smart Call Home relationship cannot be maintained with the user owing to logistics and a fallback is required.



CHAPTER 5

Flexi License

Flexi license allows you to select the port of your choice . When you buy a chassis few ports are enabled for free of charge (6, 12, 4 - depending upon the chassis). With this license in place, you can choose the ports of your choice to activate additional 6, 12, or 4 ports on the chassis.

By deactivating the enabled port, you can activate other ports of your choice.

Note Flexi Licensing is applicable for both, 1G and 10G ports.

Note This license upgrade will not disturb the existing port state.

This document describes about flexi license on Cisco ASR 920 Series Routers beginning with Cisco IOS XE 3.18.0S

Prerequisites for Flexi Licensing

Before activating this license, you must obtain and install the license. For information on obtaining and installing licenses, see Configuring the Cisco IOS Software Activation Feature.

Flexi license restrictions for dual rate ports

- If 10G license is installed for a dual rate port and SFP is inserted in that port, the interface will come up in 1G mode.
- If 10G license is installed for a dual rate port and SFP+ is inserted in that port, the interface will come up in 10G mode.

- If 10G license is **not** installed for particular port and SFP is inserted, the interface will come up in 1G mode.
- If there is a 10G license and SFP+ is inserted in the chassis(for the ports Te0/0/12-Te0/0/15), Te0/0/12–Te0/0/15 will come up in 10G mode.
- If sufficient 10G licenses or Bulk Licenses are not available for a port and an SFP+ is inserted, the 10G mode is not enabled. The interface will be in 'link down state' and the following system warning message will be generated. `Warning: SFP+ inserted at port X tengig license not in use`

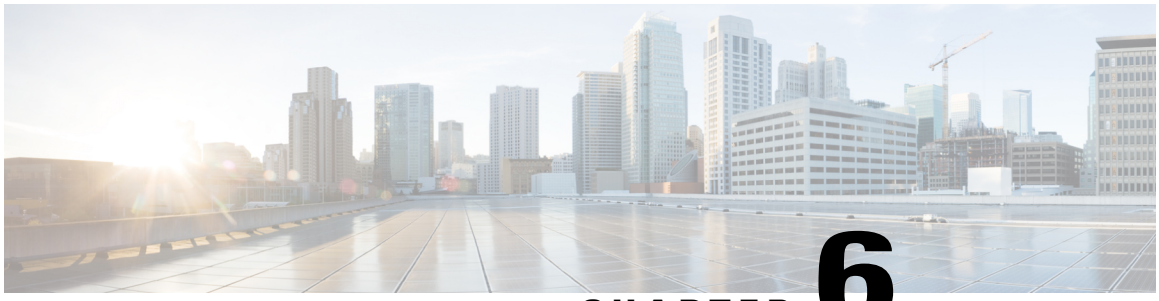
Information about Flexi Licensing

With this license, you can now choose the ports of your choice to activate 6, 12, or 4 ports on the chassis.

Below table displays the details of the licensed and non licensed ports on different models of ASR 920 series.

Cisco ASR 920 Series models	1G ports	10G ports
ASR-920-4SZ-A ASR-920-4SZ-D	All 6 ports will operate in 1G mode by default and no license is required to activate these ports.	4 SFP + will operate in 10G mode depending on the license count. License count 1: Any 2 SFP+ will operate in 10G mode. License count 2: All 4 SFP+ (ports 2-5) will operate in 10G mode.
ASR-920-12CZ-A ASR-920-12CZ-D	Any 6 ports and remaining 6 port s will be enabled after purchasing license. (By default Gi0/0/12 & Gi0/0/13 will operate as 1G mode if 10 G license is not in use)	2 SFP+ will operate in 10G mode.
ASR-920-10SZ-PD	Any 6 ports. (By default Gi0/0/10 & Gi0/0/11 will operate as 1G mode if 10 G license is not in use) and the remaining 6 ports can be activated in 1G mode.	2 SFP+ will operate in 10 G mode.
ASR-920-24SZ-IM	Any 12 ports from 0-15 and the remaining ports will be enabled in 1G mode.	SFP+ Ports (24 - 27) will be enabled based on license count available: License count 1: Any two ports will be enabled. License count 2: All ports will be enabled.

Cisco ASR 920 Series models	1G ports	10G ports
ASR-920-24TZ-M	Any 12 ports and the remaining ports will be enabled in 1G mode.	SFP+ Ports (24 - 27) will be enabled based on license count available: License count 1: Any two ports will be enabled License count 2: All ports will be enabled
ASR-920-24SZ-M	Any 12 ports and the remaining ports will be enabled in 1G mode.	SFP+ Ports (24 - 27) will be enabled based on license count available: License count 1: Any two ports will be enabled. License count 2: All ports will be enabled.
ASR-920-12SZ-IM	Any of the four ports from 0-15 will be enabled as 1G port.Ports will be enabled depending on license count available: License count 1: 6 ports out of 12 remainig in 1G mode will be enabled. License count 2: All the ports will be enabled in 1G mode.	SFP+ Ports any two will be enabled based on license count available: License count 1: Any two ports will be enabled. License count 2: Remaining 2-10G will be enabled.



CHAPTER 6

Licensing 1G and 10G ports on Cisco ASR 920 Series Router

The Cisco Software License Activation feature is a set of processes and components to activate Cisco IOS-XE software feature sets by obtaining and validating fee-based Cisco software licenses.

For information on software license activation and concepts, see the Cisco IOS Software Activation Conceptual Overview.

Refer the following link for the License Registration Portal:https://slexui.cloudapps.cisco.com/SWIFT/LicensingUI/Quickstart

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 Port Upgrade Licensing and Bulk Port Licensing

Before activating the Port Upgrade and Bulk Port license, you must obtain and install the license. For information on obtaining and installing licenses, see Configuring the Cisco IOS Software Activation Feature.

Restrictions for Port Upgrade Licensing and Bulk Port Licensing

Note Port Upgrade Licensing is applicable for both, 1G and 10G ports.

- If 10G license is installed and activated for a dual rate port and an SFP is inserted in that port, the interface will come up in 1G mode.
- If 10G license is installed and activated for a dual rate port and an SFP+ is inserted in that port, the interface will come up in 10G mode.
- If 10G license is **not** installed for particular port and SFP is inserted, the interface will come up in 1G mode.
- On the Cisco ASR-920-12SZ-IM router, if there is no license and a 1G SFP is inserted in the chassis, ports Gi0/0/12–Gi0/0/15 will be administratively down.

  If there is a license and a 1G SFP is inserted in the chassis, ports Gi0/0/12–Gi0/0/15 will come up in 10G mode only.
- If sufficient 10G licenses or Bulk Licenses are not available or not activated for a port and an SFP+ is inserted, the 10G mode is not enabled. The interface will be in 'link down state' and the following system warning message will be generated. `Warning: SFP+ inserted at port X tengig license not in use`
- If an activated 10G license is uninstalled or deactivated for a particular port with SFP+, the interface is initialized to 1G mode and 10G interfaces will be in administratively down state.

Information about Port Upgrade and Bulk Port Licensing

Bulk licenses have the highest priority in all Cisco ASR 920 router models, followed by the 12x1G licenses (applicable only on the Cisco ASR-920-24SZ-*xx* models), and then the 1G licenses.

When a 6x1G license is enabled, activating the 12x1G releases the 6x1G license. However, if the 12x1G license is activated, enabling 6x1G license causes no change, that is, the 6x1G license is rejected.

Similarly, when any type of license is in use and a bulk license is activated, all licenses are released and only the bulk license is activated. On the other hand, if a bulk license is in use, all other license configurations are rejected.

Port Upgrade License

Port upgrade license is available in pay-as-you-grow model. Few ports in the router are enabled by default. However, you must purchase the licenses to enable other ports.

- 1 GigabitEthernet Upgrade License (**L-ASR920-1G-6**)—1G ports are bundled as a group of six ports. You must purchase one license bundle to enable six 1G ports.
- 10 GigabitEthernet Upgrade License (**L-ASR920-10G-2**)—10G ports are bundled as a group of two ports. You must purchase one license bundle to enable two 10G ports.

The Cisco ASR 920 Series routers support dual rate 10G ports. Initially all the 10G ports operate in 1G mode. You must purchase 10G Upgrade license to operate in 10G mode.

Table 10: Cisco ASR 920 Series models licensed and non-licensed ports

Cisco ASR 920 Series models	1G ports	10G ports
ASR-920-12CZ-A ASR-920-12CZ-D	There are 12*1G ports. The 12*1G ports are grouped as (4 SFP + 8 AMS port) The first six ports (4 SFP + 2 AMS Port) are non-licensed ports that are enabled by default. The last 6 ports (6 AMS Ports) are licensed ports. • Ports enabled by default: **Gi0/0/0 - Gi0/0/5** • Licensed ports: **Gi0/0/6 - Gi0/0/11**	There are 2*10G ports that operate in 1G mode by default. To operate in 10G mode, you have to activate 10 Gigabit Ethernet Upgrade license with single bundle. • Ports enabled by default: **Te0/0/12 - Te0/0/13** (operating in 1G mode) • Licensed ports: **Te0/0/12 - Te0/0/13** (license needed for 10G mode)
ASR-920-4SZ-A ASR-920-4SZ-D	The two ports operate in 1G mode by default and no license is required to activate these ports. • Ports enabled by default: **Gi0/0/0 - Gi0/0/1** • Licensed ports: **None**	There are 4*10G ports that operate in 1G mode by default. To operate in 10G mode, you have to activate 10 GigabitEthernet Upgrade license with single bundle or two bundles. When you install and activate with the single bundle (bundle count 1), then the first two ports are enabled in 10G mode (Interfaces Te0/0/2 and Te0/0/3 only). If you install the second bundle (bundle count 2), all the 10G ports (Te0/0/2 - Te0/0/5) are enabled in 10G mode. • Ports enabled by default: **Te0/0/2 - Te0/0/5** (operating in 1G mode) • Licensed ports: **Te0/0/2 - Te0/0/5** (license needed for 10G mode available in bundles of 2 ports)

Cisco ASR 920 Series models	1G ports	10G ports
ASR-920-10SZ-PD	There are 10*1G ports. These 10*1G ports are grouped as: • Two copper ports • Eight SFP ports The first four ports (Gi0/0/0 -Gi0/0/3) are non-licensed ports, that is, these ports are enabled by default. The last six ports (Gi0/0/4 - Gi0/0/9) are licensed ports, that is, you need a license to enable them.	There are 2*10G ports that operate in 1G mode by default. For the ports to operate in 10G mode, you must to activate the 10 Gigabit Ethernet Upgrade License with a single bundle. • Ports enabled by default—Te0/0/10 – Te0/0/11 (operate in 1G mode) • Licensed ports—Te0/0/10 – Te0/0/11 (license needed to operate in 10G mode)
ASR-920-24SZ-IM ASR-920-24SZ-M ASR-920-24TZ-M	There are 24*1G ports. The first 12 ports (Gi0/0/0 – Gi 0/0/11) are active by default and no license is required for these ports. The last 12 ports (Gi 0/0/12 – Gi 0/0/23) are licensed ports, that is, you need a license to enable them. You can use a 12*1G bundle license to activate all the licensed 1G ports at once. **Note** In case of the ASR-920-24SZ-IM model, if the pluggable IM (8*1G Copper) is activated, ports 16-23 are disabled and removed from the interface list. Even when all the license bundles are activated before the IM activation, once IM is activated, the ports16-23 will be disabled. License will remain activated for these ports; however, you must explicitly deactivate/release the port license by executing the **(no) license feature port onegig *bundle_count*** command. In case of the ASR-920-24SZ-IM model, when activating the 8T1/E1 IM, ports Gi 0/0/20 – Gi 0/0/23 are disabled and the interfaces are removed from the list.	There are 4*10G ports and they are disabled by default. Since dual rate ports are not supported, these ports cannot be used in 1G mode. To activate the 10G ports, upgrade license with single or two bundles is required. When you install and activate a single bundle (bundle count=1), the first two TenGigabitEthernet ports are enabled —Te0/0/24 – Te0/0/25. If you install the second bundle (bundle count=2), all 10G ports (Te0/0/23 – Te0/0/27) are activated.

Cisco ASR 920 Series models	1G ports	10G ports
ASR-920-12SZ-IM	There are 12*1G ports(Gi0/0/0 - Gi0/0/11). Ports 12–15 are dual rate ports. These ports work in 1G mode by default. • Ports enabled by default: **Tei0/0/12 - Te0/0/15** • Licensed ports: **Gi0/0/0 - Gi0/0/11**	There are 4*10G ports (Te0/0/12 - Te0/0/15) that operate in 1G mode by default. To operate in 10G mode, you must activate 10 Gigabit Ethernet Upgrade license with bundle count 2, or bulk license. • Ports enabled by default: **Te0/0/12 - Te0/0/15** (operates in 1G mode) • Licensed ports: **Te0/0/12 - Te0/0/15** (10G/Bulk license and SFP+ needed to operate in 10G mode)

Table 11: Cisco ASR 920 Series models ports behavior

Cisco ASR 920 Series models	1G ports	10G ports
ASR-920-12CZ-A ASR-920-12CZ-D	Without license: You will have all the non-licensed ports Gi0/0/0 - Gi0/0/5. The licensed ports Gi0/0/6 - Gi0/0/11 are "admin-down", that is the licensed ports are in Shutdown state. You cannot activate the interface using the **no shutdown** command on the licensed ports unless you have the valid 1 GigabitEthernet Upgrade license installed and activated. With License: After you install and activate the license, then the licensed ports Gi0/0/6 - Gi0/0/11 come out of "admin-down" state, and will be **Up** or **Down** state based on the connection.	Without License: The licensed ports Te0/0/12 - Te0/0/13 operate in 1G mode. With License: After you install and activate the license, the licensed ports Te0/0/12-Te0/0/13 operate in 1G or 10G mode.
ASR-920-4SZ-A ASR-920-4SZ-D	Without License: The ports Gi0/0/0 - Gi0/0/1 operate in 1G mode.	Without License: The licensed ports Te0/0/2-Te0/0/5 operate in 1G mode. With License: If you install and activate the license with single bundle (bundle count 1), then the ports Te0/0/2 - Te0/0/3 will be activated in 10G mode and the remaining ports will be in 1G mode. If you install and activate the license with second bundle (bundle count 2), then all the licensed ports Te0/0/2 - Te0/0/5 will operate in 1G or 10G mode.

Cisco ASR 920 Series models	1G ports	10G ports
ASR-920-10SZ-PD	Without license: The ports Gi0/0/0 – Gi0/0/3 are non-licensed. The licensed ports Gi0/0/4 - Gi0/0/9 are in "admin-down" state, that is, licensed ports are in shutdown state. You cannot activate the interface using the **no shutdown** command on the licensed ports unless you have a valid 1 Gigabit Ethernet upgrade license installed and activated. With License: After you install and activate the license, the licensed ports Gi0/0/4 – Gi0/0/9 are no longer in "admin-down" state. These ports are in **UP** or **DOWN** state based on the connection.	Without License: The ports Te0/0/10 – Te0/0/11 operate in 1G mode. With License: After you install and activate the license, the ports Te0/0/10 – Te0/0/11 operate in 1G or 10G mode.
ASR-920-24SZ-IM ASR-920-24SZ-M , ASR-920-24TZ-M	Without License: The ports Gi0/0/0 – Gi0/0/11 are non-licensed. The licensed ports Gi0/0/12 – Gi0/0/23 are in "admin-down" state, that is, the ports are in shutdown state. You cannot activate the interface using the **no shutdown** command. With License: After you install and activate the license with single bundle of six 1G ports, the ports Gi0/0/12 – Gi0/0/17 are activated. If you install the license with second bundle of six 1G ports, all ports Gi0/0/12 – Gi0/0/23 are activated. L-ASR920-1G-6 license is not supported on the router. Only L-ASR920-1G-12 license is supported.	Without license: With no 10G licensed installed, the ports Te0/0/24 – Te0/0/27 cannot be used. They remain in "admin-down" state and cannot be activated using the **no shutdown** command. With license: After you install and activate the license with single bundle count, ports Te0/0/24 – Te0/0/25 are activated. The remaining ports will be in "admin-down" state. When you install the second bundle license (bundle count=2), all TenGig ports (Te0/0/24 – Te0/0/27) are activated. L-ASR920-1G-6 license is not supported on the router. Only L-ASR920-1G-12 license is supported.

Cisco ASR 920 Series models	1G ports	10G ports
ASR-920-12SZ-IM	Without license: The licensed ports Gi0/0/0 - Gi0/0/11 are "admin-down", that is, licensed ports are in Shutdown state. You cannot activate the interface using the **no shutdown** command on the licensed ports unless you have the valid 1 GigabitEthernet Upgrade license/Bulk license installed and activated. With License: After you install and activate the license, then the licensed ports Gi0/0/0 - Gi0/0/11 come out of "admin-down" state, and will be **Up** or **Down** state based on the connection.	Without License: The licensed ports Te0/0/12 - Te0/0/15 operate in 1G mode. With License: After you install and activate the 10G license with single bundle count, ports Te0/0/12 – Te0/0/13 are activated and will work in 1G or 10 G mode based on SFP type. The remaining ports will operate in 1G mode if you have a valid 1G license. When you install the second bundle license (bundle count=2), all TenGiabotEthernet ports (Te0/0/12 – Te0/0/15) are activated and work in 1G or 10G mode based on the SFP type.

Bulk Port License

Bulk port licensing allows you to enable all the ports with a single license. When Bulk port license is activated, even while the 1 GigabitEthernet or 10 GigabitEthernet Upgrade Licenses are in use, there is no impact on the corresponding interfaces. The existing 1 GigabitEthernet or 10 GigabitEthernet Upgrade Licenses are released.

- Bulk port license for enabling all licensed ports on ASR-920-12CZ models
  - **ASR920-12G-2-10G—**Enables six 1G combo ports and upgrades two 10G SFP+ ports to operate in 10G mode.
- Bulk port license for enabling all licensed ports on ASR-920-4SZ models
  - **ASR920-2G-4-10G—**Enables all four SFP+ ports to operate in 10G mode.
- Bulk port license for enabling all licensed ports on ASR-920-10SZ-PD models
  - **ASR920-10G-2-10G—**Enables six 1G ports and upgrades the two 10G SFP+ ports to operate in 10Gmode.
- Bulk port license for enabling all licensed ports on ASR-920-24SZ-IM, ASR-920-24SZ-M, and ASR-920-24TZ-M models
  - **ASR920-24G-4-10G—**Enables all SFP (12-23) and SFP+ (24-27) ports

Note In case of the ASR-920-24SZ-IM model, if the pluggable IM (8x1G Copper) is activated, ports 16-23 are disabled and removed from the interface list.

- Bulk port license for enabling all licensed ports on ASR-920-12SZ-IM models

- **ASR920-12G-4-10G—**Enables twelve 1G ports and upgrades four 10G SFP+ ports to operate in 10G mode.

Note If there is no license and a 1G SFP is inserted in the chassis ports Gi0/0/12–Gi0/0/15 will be administratively down

If there is a license and 1G SFP is inserted in the chassis, ports Gi0/0/12–Gi0/0/15 will work in 10G mode only.

Configuring Ports Using Port Upgrade License on Cisco ASR 920 Series Router

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **license feature port** {**onegig** | **6xonegig** | **tengig**} *bundle_count* | **12xonegig**

DETAILED STEPS

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

Step 3	**license feature port** {**onegig** | **6xonegig** | **tengig**} *bundle_count* | **12xonegig**
	
	Example:
	`Router(config)# license feature port 6xonegig 2`
	`ASR-920-24SZ(config)# license feature port 12xonegig`
		Note For all Cisco ASR 920 router models except Cisco ASR-920-24SZ-*xx*, use **license feature port** {**onegig** | **tengig**} *bundle_count* command.
		For the Cisco ASR-920-24SZ-*xx*, use **license feature port** {**6xonegig** *bundle_count* | **tengig** *bundle_count* | **12xonengig**} command.
		Activates the Port Upgrade license and enables the associated ports.
		• **onegig—**Specifies 1G port.
		• **12xonegig—**Specifies 1G port for all twelve ports.
		Note This option is applicable only to the Cisco ASR-920-24SZ-*xx* models.
		• **tengig—**Specifies 10G port.
		• *bundle_count***—**Specifies the bundle count 1 or 2.

	Command or Action	Purpose
		Note The *bundle_count* option is not applicable when used with **12xonegig**. **Note** In case of Cisco ASR-920-24SZ-*xx* models, when for onegig upgrade license and bundle count 1 is specified, the lower ports (12-17) are enabled. If bundle count 2 is specified, all ports (12-23) are enabled. **Note** In case of ASR-920-24SZ-*xx* models, when for tengig upgrade license and bundle count 1 is specified, the lower ports (24-25) are enabled. If bundle count 2 is specified, all ports (24-27) are enabled. To deactivate the license and disable the associated ports, use the **no license feature port** command. • Use bundle count 1 to disable the ports Te0/0/4 and Te0/0/5. • Use bundle count 2 to directly disable all the four 10G ports. For ASR-920-12SZ-IM, to disable ports Gi0/0/0 to Gi0/0/11: • For 1G ports: bundle count 2 will disable/enable all ports (Gi0/0/0–Gi0/0/11) • For 10G ports: • bundle count=1, disables Gi0/0/12–Gi0/0/13 • bundle count =2, disables Gi0/0/12–Gi0/0/15

Configuring Ports Using Bulk Port License on Cisco ASR 920 Series Router

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **license feature port bulk**

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**license feature port bulk** **Example:** `Router(config)# license feature port bulk`	Activates the Bulk Port license and enables all the associated ports. To deactivate the license and disable all the associated ports, use the **no license feature port bulk** command.

Verifying Port Upgrade and Bulk Port Licensing

Verifying the installed license

This example shows only license installed but not activated.

```
Router# show license all

License Store: Primary License Storage
StoreIndex: 0   Feature: 1GEupgradelicense                Version: 1.0
        License Type: Permanent
        License State: Active, Not in Use
        License Count: 1/0/0  (Active/In-use/Violation)
        License Priority: Medium
```

Activating the 1GigabitEthernet Port Upgrade License

```
Router(config)# license feature port onegig 1

*Apr  2 11:03:58.894 IST:  1G Upgrade License with bundle count 1 for ports 6 to 11 Enabled
```

Note For all Cisco ASR 920 router models, use **license feature port** {**onegig** | **tengig**} *bundle_count* command.

For the Cisco ASR-920-24SZ-*xx*, you can also use the **license feature port** {**6xonegig** *bundle_count* | **12xonengig**} command.

Activating the 10GigabitEthernet Port Upgrade License for ASR-920-12CZ-A/ ASR-920-12CZ-D model

```
Router(config)# license feature port tengig 1
Router# show interface description

Interface                      Status         Protocol Description
Gi0/0/0                        up             up
Gi0/0/1                        up             up
Gi0/0/2                        up             up
Gi0/0/3                        up             up
Gi0/0/4                        up             up
Gi0/0/5                        down           down
Gi0/0/6                        up             up
Gi0/0/7                        up             up
Gi0/0/8                        up             up
```

```
Gi0/0/9                        up             up
Gi0/0/10                       up             up
Gi0/0/11                       up             up
Te0/0/12                       up             up
Te0/0/13                       up             up
Gi0                            up             up
```

Activating the 10GigabitEthernet Port Upgrade License for ASR-920-4SZ-A/ ASR-920-4SZ-D model with bundle count 1

```
Router(config)# license feature port tengig 1
Router# show interface description

Gi0/0/0                        up             up
Gi0/0/1                        up             up
Te0/0/2                        up             up
Te0/0/3                        up             up
Te0/0/4                        down           down
Te0/0/5                        down           down
Gi0                            up             up
```

Activating the 10GigabitEthernet Port Upgrade License for ASR-920-4SZ-A/ ASR-920-4SZ-D model with bundle count 2

```
Router(config)# license feature port tengig 2
Router# show interface description

Interface                      Status         Protocol Description
Gi0/0/0                        up             up
Gi0/0/1                        up             up
Te0/0/2                        up             up
Te0/0/3                        up             up
Te0/0/4                        up             up
Te0/0/5                        up             up
Gi0                            up             up
```

Verifying the Port Upgrade Licenses Installed and Activated (bundle count 2)

```
Router# show license all

License Store: Primary License Storage
StoreIndex: 0   Feature: 1GEupgradelicense                Version: 1.0
        License Type: Permanent
        License State: Active, In Use
        License Count: 1/2/0  (Active/In-use/Violation)
        License Priority: Medium

StoreIndex: 2   Feature: 10GEupgradelicense               Version: 1.0
        License Type: Permanent
        License State: Active, In Use
        License Count: 1/2/0  (Active/In-use/Violation)
        License Priority: Medium
License Store: Built-In License Storage
```

Deactivating the 1GigabitEthernet Port Upgrade License

```
Router(config)# no license feature port onegig 1
Router# show interface description

Interface                      Status         Protocol Description
Gi0/0/0                        up             up
Gi0/0/1                        up             up
Gi0/0/2                        up             up
Gi0/0/3                        up             up
Gi0/0/4                        up             up
Gi0/0/5                        down           down
```

```
Gi0/0/6                        admin down     down
Gi0/0/7                        admin down     down
Gi0/0/8                        admin down     down
Gi0/0/9                        admin down     down
Gi0/0/10                       admin down     down
Gi0/0/11                       admin down     down
Te0/0/12                       up             up
Te0/0/13                       up             up
Gi0                            up             up
```

Uninstalling the 1GigabitEthernet Port Upgrade License

```
Router# license clear 1GEupgradelicense

Feature: 1GEupgradelicense
    1   License Type: Permanent
        License State: Active, Not in Use
        License Addition: Exclusive
        License Count: 3
        Comment:
        Store Index: 0
        Store Name: Primary License Storage
Are you sure you want to clear? (yes/[no]): yes
Router#
*Apr  2 11:00:16.097 IST: %LICENSE-6-REMOVE: Feature 1GEupgradelicense 1.0 was removed from
 this device.
UDI=ASR-920:CAT1748U1B6; StoreIndex=0:Primary License Storage
```

Deactivating the 10GigabitEthernet Port Upgrade License on ASR-920-12CZ-A/ ASR-920-12CZ-D model

```
Router(config)# no license feature port tengig 1
Router# show interface description

Interface                      Status         Protocol Description
Gi0/0/0                        up             up
Gi0/0/1                        up             up
Gi0/0/2                        up             up
Gi0/0/3                        up             up
Gi0/0/4                        up             up
Gi0/0/5                        down           down
Gi0/0/6                        up             up
Gi0/0/7                        up             up
Gi0/0/8                        up             up
Gi0/0/9                        up             up
Gi0/0/10                       up             up
Gi0/0/11                       up             up
Te0/0/12                       down           down
Te0/0/13                       down           down
Gi0                            up             up
```

Uninstalling the 10GigabitEthernet Port Upgrade License on ASR-920-12CZ-A/ ASR-920-12CZ-D model

```
Router# license clear 10GEupgradelicense

Feature: 10GEupgradelicense
    1   License Type: Permanent
        License State: Active, Not in Use
        License Addition: Exclusive
        License Count: 1
        Comment:
        Store Index: 0
        Store Name: Primary License Storage


Are you sure you want to clear? (yes/[no]): yes
Router#
```

```
*Apr  2 11:00:16.097 IST: %LICENSE-6-REMOVE: Feature 10GEupgradelicense 1.0 was removed
from this device.
UDI=ASR-920:CAT1748U1B6; StoreIndex=0:Primary License Storage
```

Deactivating the 10GigabitEthernet Port Upgrade License on ASR-920-4SZ-A/ ASR-920-4SZ-D model with bundle count 1

```
Router(config)# no license feature port tengig 1
Router# show interface description

Interface                      Status         Protocol Description
Gi0/0/0                        up             up
Gi0/0/1                        up             up
Te0/0/2                        up             up
Te0/0/3                        up             up
Te0/0/4                        down           down
Te0/0/5                        down           down
Gi0                            up             up
```

Deactivating the 10GigabitEthernet Port Upgrade License on ASR-920-4SZ-A/ ASR-920-4SZ-D model with bundle count 2

```
Router(config)# no license feature port tengig 2
Router# show interface description

Interface                      Status         Protocol Description
Gi0/0/0                        up             up
Gi0/0/1                        up             up
Te0/0/2                        down           down
Te0/0/3                        down           down
Te0/0/4                        down           down
Te0/0/5                        down           down
Gi0                            up             up
```

Uninstalling the 10GigabitEthernet Port Upgrade License on ASR-920-4SZ-A/ ASR-920-4SZ-D model

```
Router# license clear 10GEupgradelicense

Feature: 10GEupgradelicense
    1   License Type: Permanent
        License State: Active, Not in Use
        License Addition: Exclusive
        License Count: 1
        Comment:
        Store Index: 0
        Store Name: Primary License Storage


Are you sure you want to clear? (yes/[no]): yes
Router#
*Apr  2 11:00:16.097 IST: %LICENSE-6-REMOVE: Feature 10GEupgradelicense 1.0 was removed
from this device.
UDI=ASR-920:CAT36821784; StoreIndex=0:Primary License Storage
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mcl/allreleasemcl/all-book.html

Standards and RFCs

Standard/RFC	Title
No specific Standards and RFCs are supported by the features in this document.	—

MIBs

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

Technical Assistance

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

Feature Information for Port Upgrade and Bulk Port Licensing

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 12: Feature Information for Port Upgrade and Bulk Port Licensing

Feature Name	Releases	Feature Information
Port Upgrade and Bulk Port Licensing	Cisco IOS XE Release 3.13.0S	This feature was introduced on the Cisco ASR 920 Series Aggregation Services Router (ASR-920-12CZ-A, ASR-920-12CZ-D, ASR-920-4SZ-A, ASR-920-4SZ-D).
Port Upgrade and Bulk Port Licensing	Cisco IOS XE Release 3.14.0S	This feature was introduced on the Cisco ASR 920 Series Aggregation Services Router (ASR-920-10SZ-PD, ASR-920-24SZ-IM, ASR-920-24SZ-M, and ASR-920-24TZ-M).