Software Activation Configuration Guide, Cisco IOS Release 15M&T

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 1
Finding Feature Information 1
Information About the Cisco Software Licensing Process 2
Cisco Software Licensing Concepts 2
   Cisco Product License Registration Portal 2
   Product Authorization Key 2
   Unique Device Identifier 2
   Cisco Software License Validation 2
   Cisco License Manager 3
   Software End-User License Agreement 3
License Models for Images and Features 3
   Cisco IOS Universal Image-Based Licenses 3
   Feature-Based Licenses 4
License Types 5
   Permanent Licenses 5
   Temporary Licenses 5
      Built-in Licenses for Emergencies 5
      Evaluation Licenses 5
      Extension Licenses 6
   Uncounted or Counted Licenses 6
      Pay as You Grow Model 6
   Subscription Licenses 6
Software Activation Processes 6
   Manufacturing Preinstalled Licenses 7
   Automated Software Activation by Using Cisco License Manager 7
   License Software Activation by Using EXEC Commands 8
   License Software Activation by Using License Call Home 9
   License Transfer Between Devices 10
Contents

License Transfer Between Two Working Devices 10
RMA License Transfer Between a Failed and a Working Device 11
License Resend Request 12
Additional References 12
Feature Information for Cisco IOS Software Activation 13
Glossary 13

CHAPTER 2

Configuring the Cisco IOS Software Activation Feature 15
Finding Feature Information 15
Restrictions for Cisco IOS Software Activation 15
Information About the Cisco IOS Software Activation 16
License Activation MIB Support 16
How to Activate Software from a Cisco IOS Device 16
Installing and Upgrading Licenses by Using Software Activation Commands 16
Managing Licenses by Using Software Activation Commands 18
  Adding a Comment to a License File 18
  Saving All Licenses to a Specified Storage Area 19
  Saving License Credential Information Associated with a Device to a Specified Storage Area 20
Displeyed All Licenses in a Device 21
Displaying Detailed Information about Licensed Features 21
Displaying Licensed Feature Sets Available in an Image 22
Removing Licenses by Using Software Activation Commands 23
  Removing a License Entry from a Permanent License File 23
  Rehosting (Revoking and Transferring) a License 24
Troubleshooting License Operations by Using Software Activation Commands 25
Configuring Examples for Software Licensing 26
  Example: Installing and Upgrading Licenses 26
  Example: Adding a Comment to a License File 26
  Example: Saving All Licenses to a Specified Storage Area 27
  Example: Removing Licenses 27
  Example: Rehosting (Revoking and Transferring) a License 28
  Example: Generic Command Enhanced with Licensing Information 28
    reload 28
    show running-config 28
CHAPTER 3 Configuring Cisco License Call Home 33

Finding Feature Information 33
Prerequisites for Cisco License Call Home 33
Restrictions for Cisco License Call Home 34
Information About Cisco License Call Home 34
Cisco License Call Home Interface 34
How to Configure Cisco License Call Home 35
Installing Licenses or Upgrading Software by Using Cisco License Call Home 35
Rehosting a License by Using Cisco License Call Home 36
Requesting a License Resend by Using Cisco License Call Home 37
Configuration Examples for Cisco License Call Home 38
Example: Installing Licenses or Upgrading Software by Using Cisco License Call Home 38
Example: Rehosting a License by Using Cisco License Call Home 39
Example: Requesting a License Resend by Using Cisco License Call Home 40
Additional References 40
Feature Information for Cisco License Call Home 41

CHAPTER 4 Configuring Call Home 43

Finding Feature Information 43
Prerequisites for Call Home 43
Information About Call Home 44
Benefits of Using Call Home 44
Obtaining Smart Call Home Services 45
Anonymous Reporting 45
How to Configure Call Home 46
Configuring Smart Call Home (Single Command) 46
Configuring and Enabling Smart Call Home 47
Enabling and Disabling Call Home 48
Configuring Contact Information 49
Example 51
CHAPTER 5
Cisco Smart Licensing Client 91
Finding Feature Information 91
Prerequisites for Cisco Smart Licensing Client 91
Restrictions for Cisco Smart Licensing Client 92
Information About Cisco Smart Licensing Client 92
Cisco Smart Licensing - An Overview 92
Transitioning from CISL to Smart Licensing 92
Cisco One Suites 92
How to Activate Cisco Smart Licensing Client 93
Enable Smart Licensing 93
Smart License Disable 94
Device Registration 96
Troubleshooting for Cisco Smart Licensing Client 96
Configuration Examples for Cisco Smart Licensing Client 97
Example: Enabling Smart Licensing 97
Additional References for Cisco Smart Licensing Client 97
Feature Information for Cisco Smart Licensing Client 98
CHAPTER 6 Configuring Licensing Storage Expansion for Cisco 2800 and Cisco 3800 Series Routers

Finding Feature Information 101
Information About Licensing Storage Expansion 102
License Storage and Memory Allocation 102
When to Use Licensing Storage Expansion 102
Downgrading to an Image That Does Not Support Licensing Storage Expansion 103
How to Configure Licensing Storage Expansion 103
Expanding License Storage 103
What to Do Next 104
Compressing the Configuration Files in NVRAM 104
Configuration Examples for Licensing Storage Expansion 105
Example: Expanding License Storage 105
Example: Compressing the Configuration Files in NVRAM 105
Additional References 106
Feature Information for Licensing Storage Expansion 106
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, page 1
- Information About the Cisco Software Licensing Process, page 2
- Additional References, page 12
- Feature Information for Cisco IOS Software Activation, page 13
- Glossary, page 13

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](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](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*

<table>
<thead>
<tr>
<th>Universal image</th>
<th>Feature set license</th>
<th>Fixed feature images</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Advanced enterprise services license</td>
<td>Advanced enterprise services</td>
</tr>
<tr>
<td>Advanced enterprise services</td>
<td>+</td>
<td>Advanced IP services</td>
</tr>
<tr>
<td>Advanced IP services IP base</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Advanced IP services license</td>
<td>=</td>
<td>Advanced IP services</td>
</tr>
<tr>
<td>IP base</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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 system’s 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.


**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
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 license 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.

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.

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.


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 workflow for manual license fulfillment.

**Figure 4: License Upgrade Work Flow for Manual License Fulfillment**

The license upgrade process workflow 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 Software Activation by Using License Call Home**

You can interact with the Cisco Product License Registration portal by using the Cisco License Call Home interface included with the Cisco IOS Software Activation feature.

The License Call Home feature works as a client-server model. Each transaction requires a separate connection to the Cisco licensing infrastructure. The License Call Home feature is interactive: it prompts you to obtain required information, converts that information into a defined data structure, and then connects to the Cisco licensing back-end to interact with the Cisco licensing infrastructure. A License Call Home EXEC command initiates the request, and the Cisco licensing infrastructure provides the response.

Once you purchase a PAK, you use Cisco License Call Home commands to perform these tasks:

- Install or upgrade a license.
- Transfer a license.
- Request that a license be resent.
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 ticket 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

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS commands</td>
<td>Master Commands List, All Releases</td>
</tr>
<tr>
<td>Software activation commands</td>
<td>Software Activation Command Reference</td>
</tr>
<tr>
<td>Software activation configuration</td>
<td>“Configuring the Cisco IOS Software Activation Feature” module</td>
</tr>
</tbody>
</table>

MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>CISCO-LICENSE-MGMT-MIB</td>
<td>To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use the Cisco MIB Locator at this URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td><a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a></td>
</tr>
</tbody>
</table>
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 . An account on Cisco.com is not required.

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS Software Activation</td>
<td>12.4(15)XZ</td>
<td>The Cisco IOS Software Activation feature supports basic licensing processes.</td>
</tr>
<tr>
<td></td>
<td>12.4(20)T</td>
<td>This feature is platform-independent.</td>
</tr>
<tr>
<td></td>
<td>15.0(1)M</td>
<td>This feature module provides information about Cisco Software Activation:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• &quot;Configuring the Cisco IOS Software Activation Feature&quot; module</td>
</tr>
</tbody>
</table>

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, page 15
- Restrictions for Cisco IOS Software Activation, page 15
- Information About the Cisco IOS Software Activation, page 16
- How to Activate Software from a Cisco IOS Device, page 16
- Configuring Examples for Software Licensing, page 26
- Additional References, page 31
- Feature Information for Cisco IOS Software Activation, page 32

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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| 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 | Enables privileged EXEC mode.  
  - Enter your password if prompted. |
| Example: Device> enable | |
| Step 3 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. |
| Example: Device# show license udi | |
| 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. |
### 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]`

---

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device# license install tftp://infra-sun/&lt;user&gt;/license/5400/38a.lic</td>
<td>• Accept the end-user license agreement if prompted.</td>
</tr>
</tbody>
</table>

**Step 6**

configure terminal

**Example:**

Device# configure terminal

Enters the global configuration mode.

**Step 7**

license boot level {metroaggrservices}

**Example:**

Device(config)# license boot level metroaggrservices

Activates the metroaggrservices license on the device upon the next reload.

**Step 8**

write memory

**Example:**

Device# write memory

Saves the running configuration to NVRAM.

**Step 9**

reload

**Example:**

Device# reload

(Optional) Restarts the device to enable the new feature set.

**Note** A reload is not required when moving from an evaluation license to a permanent license of the same license level on ASR 903 routers.
## Detailed Steps

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><strong>Enter your password if prompted.</strong></td>
</tr>
<tr>
<td><code>Device&gt; enable</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td><code>license comment add feature-name comment [switch switch-num]</code></td>
<td>Adds or deletes information about a specific license.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><strong>(Only on Cisco Catalyst 3750-E switch platforms) If a switch number is specified, this command is executed on the specified switch.</strong></td>
</tr>
<tr>
<td><code>Device# license comment add gsmamrbCodecPack &quot;Use this permanent license&quot;</code></td>
<td><strong>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.</strong></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td><code>show license file [switch switch-num]</code></td>
<td>Displays comments added to a Cisco software license file.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><strong>If the device is a switch, this command obtains statistics from the specified switch.</strong></td>
</tr>
<tr>
<td><code>Device# show license file</code></td>
<td></td>
</tr>
</tbody>
</table>

### Saving All Licenses to a Specified Storage Area

#### Summary Steps

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

#### Detailed Steps

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><strong>Enter your password if prompted.</strong></td>
</tr>
<tr>
<td><code>Device&gt; enable</code></td>
<td></td>
</tr>
</tbody>
</table>
### 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**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device&gt; <code>enable</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td><code>license save credential file-sys://lic-location [switch switch-num]</code></td>
<td>Saves credential information associated with a device to a specified URL.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device# <code>license save credential flash:cred.lic</code></td>
<td></td>
</tr>
</tbody>
</table>
Displaying All Licenses in a Device

SUMMARY STEPS

1. enable
2. show license all

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>show license all</td>
<td>Displays information about all licenses in the device.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device# show license all</td>
<td></td>
</tr>
</tbody>
</table>

Displaying Detailed Information about Licensed Features

SUMMARY STEPS

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

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
</tbody>
</table>
### Displaying Licensed Feature Sets Available in an Image

**SUMMARY STEPS**

1. `enable`
2. `show license feature`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Device&gt; enable</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td><code>show license feature</code></td>
<td>Displays a list of licensed features available in an image.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Device# show license feature</code></td>
<td></td>
</tr>
</tbody>
</table>
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

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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Device&gt; enable</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td><code>license revoke revoke permission-file-url output-rehost-ticket-url</code></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Device# license revoke tftp://infra-sun/ramanp/pt.lic flash:rt.lic</code></td>
<td>An end-user license agreement is displayed for all grace-period licenses in the permission ticket.</td>
</tr>
<tr>
<td></td>
<td>You must read and accept the agreement. If you do not accept the agreement, the rehost operation stops.</td>
</tr>
</tbody>
</table>
# 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

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>show license file [switch switch-num]</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Device# show license file</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>show license statistics</td>
<td>Displays license statistics information. The display includes relevant statistics for error counts and is useful for troubleshooting licensing-related problems.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Device# show license statistics</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>show license status [switch switch-num]</td>
<td>Displays the status of licenses in the system. If the device is a switch, this command obtains status from the specified switch.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Device# show license status</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>debug license {all</td>
<td>core</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Device# debug license errors</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>no debug license {all</td>
<td>core</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Device# no debug license errors</td>
</tr>
</tbody>
</table>
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 NLL SLM CODE CL
    ND_LCK NLL *1YCHJRBMWKZAD2400 NLL NLL NLL 5_MINS <UDI><PID>AS54X
    M-AC-RPS/<PID><SN>JAE0948QXKD/<SN></UDI> ,Jx8qaVf:1XwaH9PaXjKvnmz
    7gWh:cxdf9nUxzY6o8fRuQbu,7wTUz237Cz6g9VjfrCk,0a2Pdo,Ow66ivxCRFL:x
```
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 fFlash:all_licenses.lic
```

Example: Removing Licenses

The following examples show 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
  Index: 1  Version: 1.0
  Feature: premium
  Period left: 1 hour 0 minute
  License Type: Evaluation
  License State: Active, Not in Use, EULA not accepted
  Evaluation total period: 1 hour 0 minute
  Evaluation period left: 1 hour 0 minute
  License Count: Non-Counted
  License Priority: None
  Store Index: 0
  Store Name: Evaluation License Storage
```
Example: Rehosting (Revoking and Transferring) a License

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

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

Example: Generic Command Enhanced with Licensing Information

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

```
reload
```

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

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

```
show running-config
```

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

```
Device# show running-config
Building configuration...
Current configuration : 4772 bytes
!
version 12.4
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service internal
!
hostname cs1-xfr-enhance-2951
!
...
license udi pid CISCO2951 sn FHH1211F037
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
```
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 no no no no
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 NLL SLM_CODE DEMO NLL N
IL N N L N L 5 MINS N L GT5VbrMaMd5ONY5U0cKtgvLTEjQ17P2o3g84HE8Tq
s0Ju3XphqN:2Am66pBNxXKXSvGs6+WLC>Qv8Z7qFJn/Xh1xoyieg63
YID++16gXeZv0PyO5YqY2E1nuB77Fgzc7/9HNE2aZQgq1xO3a+nsLU70x7x0xI
xY2a031yMuj+MFzq1hK0JVLpyEvq8H21M4UjVbhoN0gy1Wyj1aJ8AQ1KVBQfzhr
10yO1Vz8jGFpQ1x6t2+++/Vtc/q3SF/5Ko8XCY=<+</WLC>
Comment:
Hash: CLWUVZgY84MRT03J1yImZqwAQA=
------------------ 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 statistics ------------------
License Type Supported
permanent Expired license
extension Expired node locked license
evaluation Expired non node locked license
paid subscription Expired node locked subscription license
with valid end date
extension subscription Expired node locked subscription license
evaluation subscription Expired node locked subscription license
```

Software Activation Configuration Guide, Cisco IOS Release 15M&T
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

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

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco License Manager application</td>
<td>User Guide for Cisco License Manager</td>
</tr>
<tr>
<td>Software activation conceptual overview</td>
<td>“Cisco IOS Software Activation Conceptual Overview” module</td>
</tr>
<tr>
<td>Software activation commands</td>
<td>Software Activation Command Reference</td>
</tr>
<tr>
<td>Cisco IOS commands</td>
<td>Master Commands List, All Releases</td>
</tr>
<tr>
<td>Integrated Services Routers licensing</td>
<td>Software Activation on Cisco Integrated Services Routers</td>
</tr>
</tbody>
</table>

### MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>CISCO-LICENSE-MGMT-MIB</td>
<td>To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

### Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td><a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a></td>
</tr>
</tbody>
</table>
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 . An account on Cisco.com is not required.

Table 2: Feature Information for Cisco IOS Software Activation

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

The Cisco License Call Home feature provides a robust set of commands that communicate with the Cisco licensing infrastructure, makes connections and data transfers, and provides interactive prompts to help you install and maintain software licenses. This module describes the tasks and the commands used to activate software by using the Cisco License Call Home feature, license keys, and Cisco EXEC commands. When you activate software from a Cisco device, you can license software without the need for additional application software.

- Finding Feature Information, page 33
- Prerequisites for Cisco License Call Home, page 33
- Restrictions for Cisco License Call Home, page 34
- Information About Cisco License Call Home, page 34
- How to Configure Cisco License Call Home, page 35
- Configuration Examples for Cisco License Call Home, page 38
- Additional References, page 40
- Feature Information for Cisco License Call Home, page 41

Finding Feature Information

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

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

Prerequisites for Cisco License Call Home

- You must obtain the device certificate from the Cisco licensing infrastructure before starting.
You must have a CCO user login account.

Restrictions for Cisco License Call Home

- The device must have an Internet connection and use HTTPS to connect to the Cisco licensing infrastructure. To set up a secure HTTP connection, see the HTTP 1.1 Web Server and Client chapter in the *Cisco IOS Network Management Configuration Guide*.
- Only certain platforms support the Cisco License Call Home feature, and these devices must be running a Cisco IOS crypto K9 image. For information about platform support, see the "Feature Information for Cisco License Call Home" section.

Information About Cisco License Call Home

Cisco License Call Home Interface

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

- Install or upgrade a license.
- Transfer a license.
- Request that a license be resent.
The figure below shows how the Cisco License Call Home feature interfaces to the Cisco licensing back-end system. The architecture shown in the figure below allows the use of the License Call Home EXEC commands to communicate with the Cisco licensing infrastructure and to perform administrative license operations.

**Figure 7: Cisco License Call Home Interface**

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

**How to Configure Cisco License Call Home**

**Installing Licenses or Upgrading Software by Using Cisco License Call Home**

**SUMMARY STEPS**

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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> Obtain the PAK.</td>
<td>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.</td>
</tr>
<tr>
<td><strong>Step 2</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> show license call-home pak <em>pak-id</em></td>
<td>Displays the stock keeping unit (SKU) list and features available for the PAK provided.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device# show license call-home pak 3XPXR9E7D30</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> license call-home install <em>pak-id</em></td>
<td>Installs a license by using the Cisco License Call Home feature.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device# license call-home install pak 3XPXR9E7D30</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> show license feature</td>
<td>Displays the list of licensed features.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device# show license feature</td>
<td></td>
</tr>
</tbody>
</table>

**Rehosting a License by Using Cisco License Call Home**

**SUMMARY STEPS**

1. enable
2. license call-home revoke udi *target-udi* output-of-rehosted-license-url
3. show license detail
4. license install *stored-location-url*
### Detailed Steps

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> license call-home revoke udi target-udi output-of-rehosted-license-url</td>
<td>Revokes and transfers a license by using source and target UDIs. Sends the rehost ticket to the Cisco licensing infrastructure with the target unique device identifier (UDI), converts it to a license file, and stores it in the URL specified.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device# license call-home revoke udi AS54XM-AC-RPS:JAE0948QT6R flash:licensetargetudi.xml</td>
<td>• Select from multiple SKUs for rehosting when you are prompted, and supply information when required.</td>
</tr>
<tr>
<td><strong>Step 3</strong> show license detail</td>
<td>Verifies that the license has been transferred.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device# show license detail</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> license install stored-location-url</td>
<td>(Optional) Installs the revoked license.</td>
</tr>
<tr>
<td></td>
<td>• For details about installing and upgrading licenses, see the &quot;Configuring the Cisco IOS Software Activation Feature&quot; module.</td>
</tr>
</tbody>
</table>

## Requesting a License Resend by Using Cisco License Call Home

### Summary Steps

1. enable
2. license call-home resend dest-lic-location
3. license install stored-location-url

### Detailed Steps

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
</tbody>
</table>
Configuration Examples for Cisco License Call Home

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

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

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

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

Device# license call-home revoke udi AS54XM-AC-RPS:JAE0948QT6R flash:licensetargetudi.xml
CCO User name: User1
CCO password : ************

Retrieving the sku from swift .........................
1. SKU Name : Gatekeeper
   SKU Type : Product
   Description :
   Ordered Qty : 1
   Available Qty : 1
   Feature List :
   Feature name: gatekeeper Count: Uncounted
   Platform Supported : N/A
      5400
      5350
      2800
      3800

3. SKU Name : Gatekeeper
   SKU Type : Product
   Description :
   Ordered Qty : 1
   Available Qty : 1
   Feature List :
   Feature name: gatekeeper Count: Uncounted
   Platform Supported : N/A
      5400
      5350
      2800
      3800

4. SKU Name : GSMAMRNB
   SKU Type : Product
   Description : Transfer this feature set
   Ordered Qty : 1
   Available Qty : 1
   Feature List :
   Feature name: gsmamrb-codec-pac Count: Uncounted
   Platform Supported : 5400
      5350

5. All of the above

Please select the sku number you want to revoke : 4
Retrieving the permission ticket from swift .............
Installing permission ticket and retrieving rehost ticket........Done

Device# show license detail
Index: 1 Feature: gsmamrb-codec-pack Version: 1.0
License Type: Evaluation
License State: Active, Not in Use, EULA accepted
   Evaluation total period: 8 weeks 4 days
   Evaluation period left: 8 weeks 4 days
Lock type: Non Node locked
Vendor info
License Addition: Additive
Example: Requesting a License Resend by Using Cisco License Call Home

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

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

### Additional References

#### Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco License Manager application</td>
<td>User Guide for Cisco License Manager</td>
</tr>
<tr>
<td>Software activation conceptual overview</td>
<td>&quot;Cisco IOS Software Activation Conceptual Overview&quot; module</td>
</tr>
<tr>
<td>Software activation commands</td>
<td>Software Activation Command Reference</td>
</tr>
<tr>
<td>Cisco IOS commands</td>
<td>Master Commands List, All Releases</td>
</tr>
<tr>
<td>Integrated Services Routers licensing</td>
<td>Software Activation on Cisco Integrated Services Routers</td>
</tr>
</tbody>
</table>

#### Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td><a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a></td>
</tr>
</tbody>
</table>
Feature Information for Cisco License Call Home

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

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

Table 3: Feature Information for Cisco License Call Home

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco License Call Home</td>
<td>12.4(15)XZ</td>
<td>The Cisco License Call Home feature provides a robust set of commands that communicate with the Cisco licensing infrastructure, makes connections and data transfers, and provides interactive prompts to help you install and maintain software licenses.</td>
</tr>
<tr>
<td></td>
<td>12.4(20)T</td>
<td>In 12.4(15)XZ, this feature was introduced on the Cisco AS5300, AS5350, AS5350XM, AS5400, AS5400HPX, AS5400XM, 2800, 2851, 2821, 2811, 3800, 3825, and 3845 platforms.</td>
</tr>
<tr>
<td></td>
<td>15.1(1)SG</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco IOS XE Release 3.3SG</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>The following commands were introduced or modified by this feature: license call-home install, license call-home resend, license call-home revoke, license call-home url, show license call-home.</td>
</tr>
</tbody>
</table>
CHAPTER 4

Configuring Call Home

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

- Finding Feature Information, page 43
- Prerequisites for Call Home, page 43
- Information About Call Home, page 44
- How to Configure Call Home, page 46
- Additional References, page 87
- Feature Information for Call Home, page 89

Finding Feature Information

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

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

Prerequisites for Call Home

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

- Obtain e-mail, phone, and street address information for the Call Home contact to be configured so that the receiver can determine the origin of messages received.
• Identify the name or IPv4 address of a primary Simple Mail Transfer Protocol (SMTP) server and any backup servers, if using e-mail message delivery.

• Verify IP connectivity from the router to the e-mail server(s) or the destination HTTP server.

• If Cisco Smart Call Home is used, an active service contract covering the device is required to provide full SCH service.

Information About Call Home

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

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

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

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

Benefits of Using Call Home

The Call Home feature offers the following benefits:

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

• Multiple concurrent message destinations.

• Multiple message categories, including configuration, environmental conditions, inventory, syslog, and crash events

• Filtering of messages by severity and pattern matching.

• Scheduling of periodic message sending.
Obtaining Smart Call Home Services

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

Smart Call Home offers the following features:

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

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

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

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

Anonymous Reporting

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

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

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

For more information about what is sent in these messages, see the Alert Group Trigger Events and Commands section.
# How to Configure Call Home

## Configuring Smart Call Home (Single Command)

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

### SUMMARY STEPS

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

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Enables all Call Home basic configurations using a single command.</td>
</tr>
<tr>
<td>`call-home reporting {anonymous</td>
<td>contact-email-addr email-address} [http-proxy {ipv4-address</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config)# call-home reporting contact-email-addr <a href="mailto:email@company.com">email@company.com</a></td>
<td></td>
</tr>
</tbody>
</table>

#### Note
- HTTP proxy option allows you to make use of your own proxy server to buffer and secure internet connections from your devices.
- After successfully enabling Call Home either in anonymous or full registration mode using the `call-home reporting` command, an inventory message is sent out. If Call Home is enabled in anonymous mode, an anonymous inventory message is sent out. If Call Home is enabled in full registration mode, a Full Inventory message for full registration mode is sent. For more information about what is sent in these messages, see the "Alert Group Trigger Events and Commands" section.

For more information, see the "Alert Group Trigger Events and Commands" section.
Configuring and Enabling Smart Call Home

SUMMARY STEPS

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

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>configure terminal</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Enters call home configuration mode.</td>
</tr>
<tr>
<td>call-home</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config)# call-home</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Enters call home destination profile configuration mode for the CiscoTAC-1 destination profile.</td>
</tr>
<tr>
<td>profile CiscoTAC-1</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config-call-home)# profile CiscoTAC-1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>(Required only if using HTTPS) Configures the message transport method for http.</td>
</tr>
<tr>
<td>destination transport-method http</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(cfg-call-home-profile)# destination transport-method http</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td>Command or Action</td>
</tr>
<tr>
<td>--------</td>
<td>------------------</td>
</tr>
<tr>
<td></td>
<td>active</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Device(cfg-call-home-profile)# active</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 6</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>exit</td>
<td>Exits call home destination profile configuration mode and returns to call home configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(cfg-call-home-profile)# exit</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 7</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>contact-email-addr email-address</td>
<td>Assigns the customer’s e-mail address. Enter up to 200 characters in e-mail address format with no spaces.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(cfg-call-home)# contact-email-addr <a href="mailto:username@example.com">username@example.com</a></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 8</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>exit</td>
<td>Exits call home configuration mode and returns to global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(cfg-call-home)# exit</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 9</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>service call-home</td>
<td>Enables the Call Home feature.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)# service call-home</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 10</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>exit</td>
<td>Exits global configuration mode and returns to privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)# exit</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 11</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>copy running-config startup-config</td>
<td>Saves the configuration to NVRAM.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device# copy running-config startup-config</td>
<td></td>
</tr>
</tbody>
</table>

### 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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Enables the Call Home feature.</td>
</tr>
<tr>
<td>service call-home</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# service call-home</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Disables the Call Home feature.</td>
</tr>
<tr>
<td>no service call-home</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# no service call-home</td>
<td></td>
</tr>
</tbody>
</table>

### 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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Router&gt; configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Enters call home configuration mode.</td>
</tr>
<tr>
<td>call-home</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Router(config)# call-home</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Assigns the customer's e-mail address. Enter up to 200 characters in e-mail address format with no spaces.</td>
</tr>
<tr>
<td>contact-email-addr <code>email-address</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Router(cfg-call-home)# contact-email-addr username@example.com</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>(Optional) Assigns the customer's phone number.</td>
</tr>
<tr>
<td>phone-number <code>+phone-number</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>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 (&quot; &quot;).</td>
</tr>
<tr>
<td><code>Router(cfg-call-home)# phone-number +1-222-333-4444</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>(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 (&quot; &quot;).</td>
</tr>
<tr>
<td>street-address <code>street-address</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Router(cfg-call-home)# street-address &quot;1234 Any Street, Any city, Any state, 12345&quot;</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>(Optional) Identifies the customer ID. Enter up to 64 characters. If you include spaces, you must enclose your entry within double quotation marks (&quot; &quot;).</td>
</tr>
<tr>
<td>customer-id <code>text</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Router(cfg-call-home)# customer-id Customer1234</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>(Optional) Identifies the customer site ID. Enter up to 200 characters. If you include spaces, you must enclose your entry within double quotation marks (&quot; &quot;).</td>
</tr>
<tr>
<td>site-id <code>text</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Router(cfg-call-home)# site-id Site1 ManhattanNY</code></td>
<td></td>
</tr>
</tbody>
</table>
### Configuring Call Home

**Configuring a Destination Profile**

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

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

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

---

**Note**

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

---

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 8</strong> contract-id <strong>text</strong></td>
<td>(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 (“ ”).</td>
</tr>
</tbody>
</table>

---

**Example**

The following examples show the configuration of contact information:

```plaintext
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# call-home
Device(config-call-home)# contact-email-addr username@example.com
Device(config-call-home)# phone-number +1-222-333-4444
Device(config-call-home)# street-address "1234 Any Street, Any city, Any state, 12345"
Device(config-call-home)# customer-id Customer1234
Device(config-call-home)# site-id Site1ManhattanNY
Device(config-call-home)# contract-id Company1234
Device(config-call-home)# exit
```
You can configure the following attributes for a destination profile:

- **Profile name**—String that uniquely identifies each user-defined destination profile. The profile name is limited to 31 characters and is not case-sensitive. You cannot use `all` as a profile name.
- **Transport method**—The transport mechanism, either e-mail or HTTP (including HTTPS), for delivery of alerts.
  - For user-defined destination profiles, e-mail is the default, and you can enable one or both transport mechanisms. If you disable both methods, e-mail is enabled.
  - For the predefined Cisco TAC profile, you can enable either transport mechanism, but not both.
- **Destination address**—The actual address related to the transport method by which the alert should be sent.
  
  In Call Home version 3, you can change the destination of the CiscoTAC-1 profile.
- **Message formatting**—The message format used for sending the alert. The format options for a user-defined destination profile are long-text, short-text, or XML. The default is XML. For the predefined Cisco TAC profile, only XML is allowed. If you use the Cisco Smart Call Home service, the destination profile must use the XML message format.
- **Message size**—The maximum destination message size. The valid range is 50 to 3,145,728 bytes and the default is 3,145,728 bytes.
- **Reporting method**—You can choose which data to report for a profile. You can report Smart Call Home data or Smart Licensing data for a profile. Only one active profile is allowed to report Smart Licensing data at a time.
- **Anonymous reporting**—You can choose for your customer identity to remain anonymous, and no identifying information is sent.
- **Subscribing to interesting alert-groups**—You can choose to subscribe to alert-groups highlighting your interests.

This section includes the following tasks:

**Creating a New Destination Profile**

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

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

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> call-home</td>
<td>Enters call home configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config)# call-home</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> profile name</td>
<td>Enters call home destination profile configuration mode for the specified destination profile name. If the specified destination profile does not exist, it is created.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config-call-home)# profile profile1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> destination transport-method email</td>
<td>(Optional) Configures the message transport method for email. This is the default.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config-call-home-profile)# destination transport-method email</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> destination address email email-address</td>
<td>(Required) Configures the destination e-mail address to which Call Home messages are sent.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config-call-home-profile)# destination address email <a href="mailto:myaddress@example.com">myaddress@example.com</a></td>
<td></td>
</tr>
</tbody>
</table>
Configuring Call Home

### Configuring a Destination Profile

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 6</strong></td>
<td>destination preferred-msg-format long-text</td>
</tr>
<tr>
<td></td>
<td>short-text</td>
</tr>
<tr>
<td></td>
<td>xml</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(cfg-call-home-profile)# destination preferred-msg-format xml</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>destination message-size bytes</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(cfg-call-home-profile)# destination message-size 3145728</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>active</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(cfg-call-home-profile)# active</td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td>exit</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(cfg-call-home-profile)# exit</td>
</tr>
<tr>
<td><strong>Step 10</strong></td>
<td>end</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(cfg-call-home)# end</td>
</tr>
</tbody>
</table>

### Setting Profiles to Anonymous Mode

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

**SUMMARY STEPS**

1. configure terminal
2. call-home
3. copy profile source-profile target-profile
## DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>call-home</td>
<td>Enters call home configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config)# call-home</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>copy profile source-profile target-profile</td>
<td>Creates a new destination profile with the same configuration settings as the existing destination profile, where:</td>
</tr>
<tr>
<td></td>
<td>Example: Device(cfg-call-home)# copy profile profile1 profile2</td>
<td></td>
</tr>
</tbody>
</table>

### Subscribing to Alert Groups

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

- Configuration
- Environment
- Inventory
- Syslog
- Crash

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

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

#### Note

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

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

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

Message Severity Threshold

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

Note

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

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

Note

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

Table 4: Severity and Syslog Level Mapping

<table>
<thead>
<tr>
<th>Level</th>
<th>Keyword</th>
<th>Syslog Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9</td>
<td>catastrophic</td>
<td>N/A</td>
<td>Network-wide catastrophic failure.</td>
</tr>
<tr>
<td>8</td>
<td>disaster</td>
<td>N/A</td>
<td>Significant network impact.</td>
</tr>
<tr>
<td>7</td>
<td>fatal</td>
<td>Emergency (0)</td>
<td>System is unusable.</td>
</tr>
<tr>
<td>6</td>
<td>critical</td>
<td>Alert (1)</td>
<td>Critical conditions, immediate attention needed.</td>
</tr>
<tr>
<td>5</td>
<td>major</td>
<td>Critical (2)</td>
<td>Major conditions.</td>
</tr>
</tbody>
</table>
### Configuring Snapshot Command List

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

**SUMMARY STEPS**

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

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1**
| configure terminal | Enters global configuration mode. |
| Example:
| Device# configure terminal | |
| **Step 2**
| call-home | Enters Call Home configuration mode. |
| Example:
| Device(config)# call-home | |
| **Step 3**
| [no | default] alert-group-config snapshot | Enters snapshot configuration mode. The `no` or `default` command will remove all snapshot command. |
| Example:
| Device(cfg-call-home)# alert-group-config snapshot | |
### Configuring General email Options

#### Configuring the Mail Server

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

Consider the following guidelines when configuring the mail server:

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

To configure general email options, perform the following steps:

**SUMMARY STEPS**

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device# <code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td><code>call-home</code></td>
<td>Enters call home configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# <code>call-home</code></td>
<td></td>
</tr>
</tbody>
</table>
| Step 3 | `mail-server {ipv4-address | name} priority number` | Assigns an email server address and its relative priority among configured email servers. Provide either of these:  
• The email server’s IP address or  
• The email server’s fully qualified domain name (FQDN) of 64 characters or less.  
Assign a priority number between 1 (highest priority) and 100 (lowest priority). |
| Example: | Device(cfg-call-home)# `mail-server stmp.example.com priority 1` | |
| Step 4 | `sender from email-address` | (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. |
| Example: | Device(cfg-call-home)# `sender from username@example.com` | |
| Step 5 | `sender reply-to email-address` | (Optional) Assigns the e-mail address that will appear in the reply-to field in Call Home e-mail messages. |
| Example: | Device(cfg-call-home)# `sender reply-to username@example.com` | |
| Step 6 | `source-interface interface-name` | Assigns the source interface name to send call-home messages.  
`interface-name`—Source interface name. Maximum length is 64.  
**Note** For HTTP messages, use the `ip http client source-interface interface-name` command in global configuration mode to configure the source interface name. This allows all HTTP clients on the device to use the same source interface. |
| Example: | Device(cfg-call-home)# `source-interface loopback1` | |
| Step 7 | `source-ip-address ipv4/ipv6 address` | Assigns source IP address to send call-home messages. |
### Purpose

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(cfg-call-home)# <strong>ip-address</strong> 209.165.200.226</td>
<td>• <em>ipv4/ipv6 address</em>—Source IP (ipv4 or ipv6) address. Maximum length is 64.</td>
</tr>
</tbody>
</table>

### Step 8

<table>
<thead>
<tr>
<th>vrf vrf-name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
</tr>
<tr>
<td>Device(cfg-call-home)# <strong>vrf</strong> vpn1</td>
</tr>
</tbody>
</table>

(Optional) Specifies the VRF instance to send call-home email messages. If no vrf is specified, the global routing table is used.

**Note** For HTTP messages, if the source interface is associated with a VRF, use the **ip http client source-interface interface-name** command in global configuration mode to specify the VRF instance that will be used for all HTTP clients on the device.

---

**Example: General email Options**

The following example shows general email options:

Device# **configure terminal**

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

Device(config)# **call-home**

Device(cfg-call-home)# **mail-server smtp.example.com priority 1**

Device(cfg-call-home)# **mail-server 192.168.0.1 priority 2**

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

---

**Specifying HTTP Proxy Server**

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

**SUMMARY STEPS**

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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> call-home</td>
<td>Enters call home configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config)# call-home</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> http-proxy {ipv4-address</td>
<td>ipv6-address name} name</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config)# http-proxy 1.1.1.1 port 1</td>
<td></td>
</tr>
</tbody>
</table>

**Enabling AAA Authorization to Run IOS Commands for Call Home Messages**

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

**SUMMARY STEPS**

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

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> call-home</td>
<td>Enters call home configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config)# call-home</td>
<td></td>
</tr>
</tbody>
</table>
Configuring Syslog Throttling

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

**SUMMARY STEPS**

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

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> call-home</td>
<td>Enters call home configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config)# call-home</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> [no] syslog-throttling</td>
<td>Enables or disables Call Home syslog message throttling and avoids sending repetitive Call Home syslog messages. By default, syslog message throttling is enabled.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(cfg-call-home)# syslog-throttling</td>
<td></td>
</tr>
</tbody>
</table>
Configuring Call Home Data Privacy

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

**SUMMARY STEPS**

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

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device# <code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td><code>call-home</code></td>
<td>Enters call home configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config)# <code>call-home</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td>`data-privacy {level {normal</td>
<td>high}</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(cfg-call-home)# <code>data-privacy level high</code></td>
<td></td>
</tr>
</tbody>
</table>

**Note**

Enabling the data-privacy command can affect CPU utilization when scrubbing a large amount of data.

- `normal`—Scrubs all normal-level commands.
- `high`—Scrubs all normal-level commands plus the IP domain name and IP address commands.
- `hostname`—Scrubs all high-level commands plus the hostname command.

**Note**

Scrubbing the hostname from configuration messages can cause Smart Call Home processing failure on some platforms.

**Working With Destination Profiles**

This section describes some of the tasks that you can complete with destination profiles:
Activating and Deactivating a Destination Profile

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

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

**SUMMARY STEPS**

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

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>configure terminal</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Enters call home configuration mode.</td>
</tr>
<tr>
<td>call-home</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# call-home</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Enters call home destination profile configuration mode for the specified destination profile. If the specified destination profile does not exist, it is created.</td>
</tr>
<tr>
<td>profile name</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-call-home)# profile test</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Enables the destination profile. By default, a new profile is enabled when it is created.</td>
</tr>
<tr>
<td>active</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(cfg-call-home-profile)# active</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Disables the destination profile.</td>
</tr>
<tr>
<td>no active</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(cfg-call-home-profile)# no active</td>
<td></td>
</tr>
</tbody>
</table>
### Purpose
Command or Action | Purpose
---|---
**Step 6** | 
end | Exits call home destination profile configuration mode and returns to privileged EXEC mode.

---

**Renaming a Destination Profile**

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

**SUMMARY STEPS**

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

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
</tbody>
</table>
`configure terminal` | Enters global configuration mode.

*Example:*

Router# `configure terminal`

| **Step 2** | 
`call-home` | Enters call home configuration mode.

*Example:*

Router(config)# `call-home`

| **Step 3** | 
`rename profile source-profile target-profile` | 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.

*Example:*

Router(cfg-call-home)# `rename profile2 testprofile`

---

**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(config-call-home-profile)# destination transport-method http
Router(config-call-home-profile)# active
```

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

### Verifying the Call Home Profile Configuration

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

## Sending Call Home Communications Manually

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

### Sending a Call Home Test Message Manually

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

**SUMMARY STEPS**

1. `call-home test ["test-message"] profile name`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> <code>call-home test [&quot;test-message&quot;] profile name</code></td>
<td>Sends a test message to the specified destination profile. The user-defined test message text is optional, but must be enclosed in quotes (&quot; &quot;) if it contains spaces. If no user-defined message is configured, a default message is sent.</td>
</tr>
</tbody>
</table>

**Example:**

```
Router# call-home test profile profile1
```

### Sending Call Home Alert Group Messages Manually

You can use the `call-home send` command to manually send a specific alert group message.
Note the following guidelines when manually sending a Call Home alert group message:

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

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

**SUMMARY STEPS**

1. `call-home send alert-group configuration [profile name]`
2. `call-home send alert-group inventory [profile name]`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Sends a configuration alert group message to one destination profile if specified, or to all subscribed destination profiles.</td>
</tr>
<tr>
<td>call-home send alert-group configuration [profile name]</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>Device# call-home send alert-group configuration profile CiscoTAC-1</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Sends an inventory alert group message to one destination profile if specified, or to all subscribed destination profiles.</td>
</tr>
<tr>
<td>call-home send alert-group inventory [profile name]</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>Device# call-home send alert-group inventory</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
</tbody>
</table>
| `call-home request output-analysis "show-command"` | Sends the output of the specified show command for analysis. The show command must be contained in quotes ("").
| **Example:** `call-home request output-analysis "show diag" profile TG` | |
| **Step 2** | 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.
| `call-home request {config-sanity | bugs-list | command-reference | product-advisory}` | **Example:** `call-home request config-sanity profile TG` |
Example

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

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

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

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

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

• The specified IOS command or list of IOS commands can be any run command, including commands for all modules. The command must be contained in quotes (")

• If the email option is selected using the "email" keyword and an email address is specified, the command output is sent to that address. If neither the email nor the HTTP option is specified, the output is sent in long-text format with the specified service request number to the Cisco TAC (attach@cisco.com).

• If neither the "email" nor the "http" keyword is specified, the service request number is required for both long-text and XML message formats and is provided in the subject line of the email.

• If the HTTP option is specified, the CiscoTac-1 profile destination HTTP or HTTPS URL is used as the destination. The destination email address can be specified so that Smart Call Home can forward the message to the email address. The user must specify either the destination email address or an SR number but they can also specify both.

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

SUMMARY STEPS

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

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 call-home send {cli command</td>
<td>cli list} [email email msg-format {long-text</td>
</tr>
<tr>
<td>Example:Router# call-home send “show version; show running-config show inventory” <a href="mailto:emailsupport@example.com">emailsupport@example.com</a> msg-format xml</td>
<td>EXECUTES THE CLI OR CLI LIST AND SENDS OUTPUT VIA EMAIL OR HTTP.</td>
</tr>
<tr>
<td></td>
<td>• {cli command</td>
</tr>
<tr>
<td></td>
<td>RUN COMMAND, INCLUDING COMMANDS FOR ALL MODULES. THE COMMANDS MUST BE CONTAINED IN QUOTES (&quot;&quot;).</td>
</tr>
<tr>
<td></td>
<td>• email email msg-format {long-text</td>
</tr>
<tr>
<td></td>
<td>THE SPECIFIED EMAIL ADDRESS IN LONG-TEXT OR XML FORMAT WITH THE SERVICE</td>
</tr>
<tr>
<td></td>
<td>REQUEST NUMBER IN THE SUBJECT. THE EMAIL ADDRESS, THE SERVICE REQUEST NUMBER, OR BOTH MUST BE</td>
</tr>
<tr>
<td></td>
<td>SPECIFIED. THE SERVICE REQUEST NUMBER IS REQUIRED IF THE EMAIL ADDRESS IS NOT SPECIFIED (DEFAULT</td>
</tr>
</tbody>
</table>
### Configuring Call Home

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

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

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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>is <a href="mailto:attach@cisco.com">attach@cisco.com</a> for long-text format and <a href="mailto:callhome@cisco.com">callhome@cisco.com</a> for XML format).</td>
<td></td>
</tr>
<tr>
<td>• http {destination-email-address} — If the http option is selected, the command output will be sent to Smart Call Home backend server (URL specified in TAC profile) in XML format. destination-email-address can be specified so that the backend server can forward the message to the email address. The email address, the service request number, or both must be specified.</td>
<td></td>
</tr>
<tr>
<td>• tac-service-request SR# — Specifies the service request number. The service request number is required if the email address is not specified.</td>
<td></td>
</tr>
</tbody>
</table>

### Example

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

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

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

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

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

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

```
MIIDAJCCAmCAHR3Z/gfPqB63EH1n+6eJNMYwDQYJKoZIhvcNAQCEFBAwQgExCzAJ
BgNVBAYTAlVTMRcwFQYDVQQKEw5WZXJpU2lnbiwxMDQwHgYDVQQdEB5WZXJpU2lnbiw
SW5jLiItIEZvciBhZDQ0MSgtIEcyMTowOAYDVQQdEtZVZXJpU2lnbiwSW5jLiAtIEZv
cm90b3JhZ2VudCAtIEcyMTowOAYDVQQdEtZVZXJpU2lnbiwSW5jLiAtIEZvcm90b3JhZ
2VudCAtIEcyMTowOAYDVQQdEtZVZXJpU2lnbiwSW5jLiAtIEZvcm90b3JhZ2VudCAtIEcy
MTowOAYDVQQdEtZVZXJpU2lnbiwSW5jLiAtIEZvcm90b3JhZ2VudCAtIEcyMTowOAYDVQQd
EtZVZXJpU2lnbiwSW5jLiAtIEZvcm90b3JhZ2VudCAtIEcyMTowOAYDVQQdEtZVZXJpU2lnbiw
SW5jLiAtIEZvcm90b3JhZ2VudCAtIEcyMTowOAYDVQQdEtZVZXJpU2lnbiwSW5jLiAtIEZv
cm90b3JhZ2VudCAtIEcyMTowOAYDVQQdEtZVZXJpU2lnbiwSW5jLiAtIEZvcm90b3JhZ2Vud
CAtIEcyMTowOAYDVQQdEtZVZXJpU2lnbiwSW5jLiAtIEZvcm90b3JhZ2VudCAtIEcyMTowO
AYDVQQdEtZVZXJpU2lnbiwSW5jLiAtIEZvcm90b3JhZ2VudCAtIEcyMTowOAYDVQQdEtZVZX
JpU2lnbiwSW5jLiAtIEZvcm90b3JhZ2VudCAtIEcyMTowOAYDVQQdEtZVZXJpU2lnbiwSW5jL
iAtIEZvcm90b3JhZ2VudCAtIEcyMTowOAYDVQQdEtZVZXJpU2lnbiwSW5jLiAtIEZvcm90b3J
hZ2VudCAtIEcyMTowOAYDVQQdEtZVZXJpU2lnbiwSW5jLiAtIEZvcm90b3JhZ2VudCAtIEcy
MTowOAYDVQQdEtZVZXJpU2lnbiwSW5jLiAtIEZvcm90b3JhZ2VudCAtIEcyMTowOAYDVQQdEt
ZVZXJpU2lnbiwSW5jLiAtIEZvcm90b3JhZ2VudCAtIEcyMTowOAYDVQQdEtZVZXJpU2lnbiwSW
5jLiAtIEZvcm90b3JhZ2VudCAtIEcyMTowOAYDVQQdEtZVZXJpU2lnbiwSW5jLiAtIEZvcm90b
3JhZ2VudCAtIEcyMTowOAYDVQQdEtZVZXJpU2lnbiwSW5jLiAtIEZvcm90b3JhZ2VudCAtIEcy
MTowOAYDVQQdEtZVZXJpU2lnbiwSW5jLiAtIEZvcm90b3JhZ2VudCAtIEcyMTowOAYDVQQdEtZ
VZXJpU2lnbiwSW5jLiAtIEZvcm90b3JhZ2VudCAtIEcyMTowOAYDVQQdEtZVZXJpU2lnbiwSW5j
LiAtIEZvcm90b3JhZ2VudCAtIEcyMTowOAYDVQQdEtZVZXJpU2lnbiwSW5jLiAtIEZvcm90b3J
hZ2VudCAtIEcyMTowOAYDVQQdEtZVZXJpU2lnbiwSW5jLiAtIEZvcm90b3JhZ2VudCAtIEcyMTow
OAYDVQQdEtZVZXJpU2lnbiwSW5jLiAtIEZvcm90b3JhZ2VudCAtIEcyMTowOAYDVQQdEtZVZXJpU
2lnbiwSW5jLiAtIEZvcm90b3JhZ2VudCAtIEcyMTowOAYDVQQdEtZVZXJpU2lnbiwSW5jLiAtIEZ
vcm90b3JhZ2VudCAtIEcyMTowOAYDVQQdEtZVZXJpU2lnbiwSW5jLiAtIEZvcm90b3JhZ2VudCAt
IEcyMTowOAYDVQQdEtZVZXJpU2lnbiwSW5jLiAtIEZvcm90b3JhZ2VudCAtIEcyMTowOAYDVQ
```

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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> crypto pki trustpoint <em>name</em></td>
<td>Declares a CA trustpoint on your router and enters CA trustpoint configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# crypto pki trustpoint cisco</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> enrollment terminal</td>
<td>Specifies a manual cut-and-paste method of certificate enrollment.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(ca-trustpoint)# enrollment terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> exit</td>
<td>Exits CA trustpoint configuration mode and returns to global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(ca-trustpoint)# exit</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> crypto pki authenticate <em>name</em></td>
<td>Authenticates the named CA.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# crypto pki authenticate cisco</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>The CA name should match the <em>name</em> specified in the <code>crypto pki trustpoint</code> command.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>Specifies the security certificate text.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Enter the base 64 encoded CA certificate.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>End with a blank line or the word &quot;quit&quot; on a line by itself</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>&lt;Paste certificate text here&gt;</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> quit</td>
<td>Specifies the end of the security certificate text.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>quit</td>
<td></td>
</tr>
</tbody>
</table>
### Command or Action

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>yes</td>
<td>Confirms acceptance of the entered security certificate.</td>
</tr>
</tbody>
</table>
|      | **Example:** 
|      | % Do you accept this certificate? [yes/no]: yes |
| 9    | end              | Exits global configuration mode and returns to privileged EXEC mode. |
|      | **Example:** 
|      | Router# end |
| 10   | copy running-config startup-config | Saves the configuration to NVRAM. |
|      | **Example:** 
|      | Router# copy running-config startup-config |

**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(config-trustpoint)# enrollment terminal
Router(config-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
MTI1MDA6CmFscGE3ZjIyLmFqQmFQkgZjIyLmNyd29yZXJzaW9uLmNyb3NzLmN0

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
```

**Example:**

```
Router# configure terminal
Router(config)# crypto pki trustpoint cisco
Router(config-trustpoint)# enrollment terminal
Router(config-trustpoint)# exit
Router(config)# crypto pki authenticate cisco

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
```

**Example:**

```
Router# crypto pki trustpoint cisco
Router(config-trustpoint)# enrollment terminal
Router(config-trustpoint)# exit
Router(config)# crypto pki authenticate cisco

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
```

**Example:**

```
Router# crypto pki trustpoint cisco
Router(config-trustpoint)# enrollment terminal
Router(config-trustpoint)# exit
Router(config)# crypto pki authenticate cisco

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
```

**Example:**

```
Router# crypto pki trustpoint cisco
Router(config-trustpoint)# enrollment terminal
Router(config-trustpoint)# exit
Router(config)# crypto pki authenticate cisco

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
```
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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>call-home send alert-group inventory profile CiscoTAC-1</code></td>
<td>Sends an inventory alert group message to the CiscoTAC-1 destination profile.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Display the Call Home configuration in summary.</td>
</tr>
<tr>
<td>show call-home</td>
<td></td>
</tr>
<tr>
<td>Example: Device# show call-home</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Display the Call Home configuration in detail.</td>
</tr>
<tr>
<td>show call-home detail</td>
<td></td>
</tr>
<tr>
<td>Example: Device# show call-home detail</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Display the available alert groups and their status.</td>
</tr>
<tr>
<td>show call-home alert-group</td>
<td></td>
</tr>
<tr>
<td>Example: Device# show call-home alert-group</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Check and display the availability of the configured e-mail server(s).</td>
</tr>
<tr>
<td>show call-home mail-server status</td>
<td></td>
</tr>
<tr>
<td>Example: Device# show call-home mail-server status</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Display the configuration of the specified destination profile. Use the all keyword to display the configuration of all destination profiles.</td>
</tr>
<tr>
<td>show call-home profile {all</td>
<td>name}</td>
</tr>
<tr>
<td>Example: Device# show call-home profile all</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>Display the statistics of Call Home events.</td>
</tr>
<tr>
<td>show call-home statistics</td>
<td></td>
</tr>
<tr>
<td>Example: Device# show call-home statistics</td>
<td></td>
</tr>
</tbody>
</table>
Configuration Examples for Call Home

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

**Example: Call Home Information in Summary**

```plaintext
Device# show call-home
Current call home settings:
  call home feature : disable
  call home message's from address: username@example.com
  call home message's reply-to address: username@example.com
  vrf for call-home messages: Mgmt-intf
  contact person's email address: username@example.com
  contact person's phone number: +14085551234
  street address: 1234 Any Street Any city Any state 12345
  customer ID: customer@example.com
  contract ID: 123456789
  site ID: example.com
  Mail-server[1]: Address: smtp.example.com Priority: 1
  Mail-server[2]: Address: 192.168.0.1 Priority: 2
  Rate-limit: 20 message(s) per minute

Available alert groups:

<table>
<thead>
<tr>
<th>Keyword</th>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>configuration</td>
<td>Enable</td>
<td>configuration info</td>
</tr>
<tr>
<td>diagnostic</td>
<td>Enable</td>
<td>diagnostic info</td>
</tr>
<tr>
<td>environment</td>
<td>Enable</td>
<td>environmental info</td>
</tr>
<tr>
<td>inventory</td>
<td>Enable</td>
<td>inventory info</td>
</tr>
<tr>
<td>syslog</td>
<td>Enable</td>
<td>syslog info</td>
</tr>
</tbody>
</table>

Profiles:

- Profile Name: campus-noc
- Profile Name: CiscoTAC-1
```

**Example: Configured Call Home Information in Detail**

```plaintext
Device# show call-home detail
Current call home settings:
  call home feature: enable
  call home message's from address: router@example.com
  call home message's reply-to address: support@example.com
  vrf for call-home messages: Not yet set up
  contact person's email address: technical@example.com
  contact person's phone number: +1-408-555-1234
  street address: 1234 Picaboo Street, Any city, Any state, 12345
  customer ID: ExampleCorp
  contract ID: X123456789
  site ID: SantaClara
  source ip address: Not yet set up
  source interface: GigabitEthernet1
  Mail-server[1]: Address: 192.168.2.1 Priority: 1
  Mail-server[2]: Address: 223.255.254.254 Priority: 2
  http proxy: 192.168.1.1:80
  aaa-authorization: disable
  aaa-authorization username: callhome (default)
  data-privacy: normal
  syslog throttling: enable
  Rate-limit: 20 message(s) per minute
  Snapshot command[0]: show version
  Snapshot command[1]: show clock

Available alert groups:

<table>
<thead>
<tr>
<th>Keyword</th>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>configuration</td>
<td>Enable</td>
<td>configuration info</td>
</tr>
<tr>
<td>crash</td>
<td>Enable</td>
<td>crash and traceback info</td>
</tr>
<tr>
<td>inventory</td>
<td>Enable</td>
<td>inventory info</td>
</tr>
<tr>
<td>syslog</td>
<td>Enable</td>
<td>syslog info</td>
</tr>
</tbody>
</table>

Profiles:

- Profile Name: campus-noc
  Profile status: ACTIVE
```
Configuring Call Home

Preferred Message Format: xml
Message Size Limit: 3145728 Bytes
Transport Method: email
Email address(es): noc@example.com
HTTP address(es): Not yet set up
Alert-group Severity
------------------------ ------------
configuration normal
  crash normal
  inventory normal
Syslog-Pattern Severity
------------------------ ------------
  .!*CALL_LOOP.* debug

Profile Name: CiscoTAC-1
Profile status: INACTIVE
Profile mode: Full Reporting
Preferred Message Format: xml
Message Size Limit: 3145728 Bytes
Transport Method: email
Email address(es): callhome@cisco.com
HTTP address(es): https://tools.cisco.com/its/service/odc/services/DDCEService
Periodic configuration info message is scheduled every 14 day of the month at 11:12
Periodic inventory info message is scheduled every 14 day of the month at 10:57
Alert-group Severity
------------------------ ------------
crash normal
Syslog-Pattern Severity
------------------------ ------------
  .!*CALL_LOOP.* debug

Example: Available Call Home Alert Groups

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

Example: Email Server Status Information

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

Examples: Information for All Destination Profiles

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

Periodic configuration info message is scheduled every 14 day of the month at 11:12
Periodic inventory info message is scheduled every 14 day of the month at 10:57
Alert-group Severity
------------------------------- ------------
crash normal
Syslog-Pattern Severity
------------------------------- ------------
.*CALL_LOOP.* debug

Example: Information for a User-Defined Destination Profile

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

Example: Call Home Statistics

Device# show call-home statistics
Message Types Total Email HTTP
------------------------------- -------------------- -------------------- ------------------
Total Success 3 3 3 3
Config 3 3 0 0
Diagnostic 0 0 0 0
Environment 0 0 0 0
Inventory 2 2 0 0
SysLog 0 0 0 0
Test 0 0 0 0
Request 0 0 0 0
Send-CLI 0 0 0 0
Total In-Queue 0 0 0 0
Config 0 0 0 0
Diagnostic 0 0 0 0
Environment 0 0 0 0
Inventory 0 0 0 0
SysLog 0 0 0 0
Test 0 0 0 0
Request 0 0 0 0
Send-CLI 0 0 0 0
Total Failed 0 0 0 0
Config 0 0 0 0
Diagnostic 0 0 0 0
Environment 0 0 0 0
Inventory 0 0 0 0
SysLog 0 0 0 0
Test 0 0 0 0
Request 0 0 0 0
Send-CLI 0 0 0 0
Total RateLimit -dropped 0 0 0 0
Config 0 0 0 0
Diagnostic 0 0 0 0
Environment 0 0 0 0
Inventory 0 0 0 0

Software Activation Configuration Guide, Cisco IOS Release 15M&T
Default Settings

Lists of default Call Home settings.

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

Alert Group Trigger Events and Commands

Call Home trigger events are grouped into alert groups, with each alert group assigned CLI commands to execute when an event occurs. The CLI command output is included in the transmitted message. Table 5: Call Home Alert Groups, Events, and Actions, on page 80 lists the trigger events included in each alert group, including the severity level of each event and the executed CLI commands for the alert group.
Table 5: Call Home Alert Groups, Events, and Actions

<table>
<thead>
<tr>
<th>Alert Group</th>
<th>Call Home Trigger Event</th>
<th>Syslog Event</th>
<th>Severity</th>
<th>Description and CLI Commands Executed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Crash</td>
<td>SYSTEM_CRASH</td>
<td>—</td>
<td>—</td>
<td>Events related to system crash.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Commands executed:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>show version</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>show logging</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>show region</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>show stack</td>
</tr>
<tr>
<td>—</td>
<td>TRACEBACK</td>
<td>—</td>
<td>—</td>
<td>Detects software traceback events.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Commands executed:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>show version</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>show logging</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>show region</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>show stack</td>
</tr>
<tr>
<td>Configuration</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>User-generated request for configuration. (Sent to TAC.)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>CLI commands executed:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>show platform</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>show inventory</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>show running-config</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>show all</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>show startup-config</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>show version</td>
</tr>
<tr>
<td>Environmental</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>Events related to power, fan, and environment sensing elements, such as temperature alarms. (Sent to TAC.)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>CLI commands executed:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>show platform</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>show environment</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>show inventory</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>show logging</td>
</tr>
</tbody>
</table>
### Inventory

Inventorystatus should be provided whenever a unit is cold-booted, or when FRUs are inserted or removed. This is considered a noncritical event, and the information is used for status and entitlement. (Sent to TAC.)

CLI commands executed:
- `show diag all eeprom detail | include MAC`
- `show license all`
- `show platform show platform hardware qfp active infrastructure chipset 0 capabilities show platform software vnic-if interface-mapping show version`

---

### Syslog

Event logged to syslog.

CLI commands executed:
- `show logging`

---

#### Message Contents

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

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

This section also includes the following subsections that provide sample messages:
**Table 6: Format for a Short Text Message**

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

**Table 7: Common Fields for All Long Text and XML Messages**

<table>
<thead>
<tr>
<th>Data Item (Plain Text and XML)</th>
<th>Description (Plain Text and XML)</th>
<th>MML Tag (XML Only)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time stamp</td>
<td>Date and time stamp of event in ISO time notation: YYYY-MM-DD HH:MM:SS GMT+HH:MM.</td>
<td>CallHome/Event/Time</td>
</tr>
<tr>
<td>Message name</td>
<td>Name of message. Specific event names are listed in the Alert Group Trigger Events and Commands section.</td>
<td>For short text message only</td>
</tr>
<tr>
<td>Message type</td>
<td>Specifically &quot;Call Home&quot;.</td>
<td>CallHome/Event/Type</td>
</tr>
<tr>
<td>Message subtype</td>
<td>Specific type of message: full, delta, test</td>
<td>CallHome/Event/SubType</td>
</tr>
<tr>
<td>Message group</td>
<td>Specifically &quot;reactive&quot;. Optional, because default is &quot;reactive&quot;.</td>
<td>Not applicable. For long-text message only</td>
</tr>
<tr>
<td>Severity level</td>
<td>Severity level of message.</td>
<td>Body/Block/Severity</td>
</tr>
<tr>
<td>Source ID</td>
<td>Product type for routing through the workflow engine. This is typically the product family name.</td>
<td>For long-text message only</td>
</tr>
<tr>
<td>Data Item (Plain Text and XML)</td>
<td>Description (Plain Text and XML)</td>
<td>MML Tag (XML Only)</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>----------------------------------</td>
<td>-------------------</td>
</tr>
</tbody>
</table>
| **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@serial 1`.  
  - `type` is the product model number from backplane IDPROM.  
  - `@` is a separator character.  
  - `Sid` is `C`, identifying the serial ID as a chassis serial number.  
  - `serial` is the number identified by the `Sid` field.  
  Example: `ASR1006@C@FOX105101DH` | CallHome/CustomerData/ContractData/DeviceId |
| **Customer ID**               | Optional user-configurable field used for contract information or other ID by any support service. | CallHome/CustomerData/ContractData/CustomerId |
| **Contract ID**               | Optional user-configurable field used for contract information or other ID by any support service. | CallHome/CustomerData/ContractData/ContractId |
| **Site ID**                   | Optional user-configurable field used for site IDs supplied by Cisco Systems or other data meaningful to alternate support services. | CallHome/CustomerData/ContractData/SiteId |
| **Server ID**                 | If the message is generated from the fabric switch, this is the unique device identifier (UDI) of the switch.  
The format is `type@Sid@serial 1`.  
  - `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 |
## Configuring Call Home

<table>
<thead>
<tr>
<th>Data Item (Plain Text and XML)</th>
<th>Description (Plain Text and XML)</th>
<th>MML Tag (XML Only)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contact name</td>
<td>Name of person to contact for issues associated with the node experiencing the event.</td>
<td>CallHome/CustomerData/SystemInfo/Contact</td>
</tr>
<tr>
<td>Contact e-mail</td>
<td>E-mail address of person identified as contact for this unit.</td>
<td>CallHome/CustomerData/SystemInfo/ContactEmail</td>
</tr>
<tr>
<td>Contact phone number</td>
<td>Phone number of the person identified as the contact for this unit.</td>
<td>CallHome/CustomerData/SystemInfo/ContactPhoneNumber</td>
</tr>
<tr>
<td>Street address</td>
<td>Optional field containing street address for RMA part shipments associated with this unit.</td>
<td>CallHome/CustomerData/SystemInfo/StreetAddress</td>
</tr>
<tr>
<td>Model name</td>
<td>Model name of the router. This is the &quot;specific model as part of a product family name.</td>
<td>CallHome/Device/Cisco_Chassis/Model</td>
</tr>
<tr>
<td>Serial number</td>
<td>Chassis serial number of the unit.</td>
<td>CallHome/Device/Cisco_Chassis/SerialNumber</td>
</tr>
<tr>
<td>Chassis part number</td>
<td>Top assembly number of the chassis.</td>
<td>CallHome/Device/Cisco_Chassis/AdditionalInformation/AD@name=&quot;PartNumber&quot;</td>
</tr>
<tr>
<td>System object ID</td>
<td>System Object ID that uniquely identifies the system.</td>
<td>CallHome/Device/Cisco_Chassis/AdditionalInformation/AD@name=&quot;sysObjectID&quot;</td>
</tr>
<tr>
<td>System description</td>
<td>System description for the managed element.</td>
<td>CallHome/Device/Cisco_Chassis/AdditionalInformation/AD@name=&quot;sysDescr&quot;</td>
</tr>
<tr>
<td>Fields specific to a particular alert group message are inserted here.</td>
<td>The following fields may be repeated if multiple CLI commands are executed for this alert group.</td>
<td></td>
</tr>
</tbody>
</table>

- **Command output name**: The exact name of the issued CLI command. [/*ml/Attachments/AttachmentName]
- **Attachment type**: Attachment type. Usually “inline”. [/*ml/Attachments/AttachmentType]
- **MIME type**: Normally “text” or “plain” or encoding type. [/*ml/Attachments/Attachment/Data@encoding]
- **Command output text**: Output of command automatically executed. [/*ml/Attachments/AttachmentData]
### Table 8: Inserted Fields for a Reactive or Proactive Event Message

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

### Table 9: Inserted Fields for an Inventory Event Message

<table>
<thead>
<tr>
<th>Data Item (Plain Text and XML)</th>
<th>Description (Plain Text and XML)</th>
<th>MML Tag (XML Only)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chassis hardware version</td>
<td>Hardware version of chassis.</td>
<td>CallHome/Device/Cisco_Chassis/HardwareVersion</td>
</tr>
<tr>
<td>Supervisor module software version</td>
<td>Top-level software version.</td>
<td>CallHome/Device/Cisco_Chassis/AdditionalInformation/AD@name=&quot;SoftwareVersion&quot;</td>
</tr>
<tr>
<td>FRU name</td>
<td>Name of the affected FRU generating the event message.</td>
<td>CallHome/Device/Cisco_Chassis/Cisco_Card/Model</td>
</tr>
<tr>
<td>FRU s/n</td>
<td>Serial number of FRU.</td>
<td>CallHome/Device/Cisco_Chassis/Cisco_Card/SerialNumber</td>
</tr>
<tr>
<td>FRU part number</td>
<td>Part number of FRU.</td>
<td>CallHome/Device/Cisco_Chassis/Cisco_Card/PartNumber</td>
</tr>
</tbody>
</table>
### Sample Syslog Alert Notification in XML Format

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

```xml
<?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: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:MessageId>M8:9S1NMSF22DW:51AEAC68</aml-session:MessageId>
    </aml-session:Session>
  </soap-env:Header>
  <soap-env:Body>
      <aml-block:Header>
        <aml-block:Type>http://www.cisco.com/2005/05/callhome/syslog</aml-block:Type>
        <aml-block:CreationDate>2013-06-05 03:11:36 GMT+00:00</aml-block:CreationDate>
        <aml-block:Builder>
          <aml-block:Name>CSR1000v</aml-block:Name>
          <aml-block:Version>2.0</aml-block:Version>
        </aml-block:Builder>
        <aml-block:BlockGroup>
          <aml-block:GroupId>G9:9S1NMSF22DW:51AEAC68</aml-block:GroupId>
          <aml-block:Number>0</aml-block:Number>
          <aml-block:IsLast>true</aml-block:IsLast>
          <aml-block:IsPrimary>true</aml-block:IsPrimary>
          <aml-block:WaitForPrimary>false</aml-block:WaitForPrimary>
        </aml-block:BlockGroup>
        <aml-block:Severity>2</aml-block:Severity>
      </aml-block:Header>
      <aml-block:Content>
        <ch:CallHome xmlns:ch="http://www.cisco.com/2005/05/callhome" version="1.0">
          <ch:EventTime>2013-06-05 03:11:36 GMT+00:00</ch:EventTime>
          <ch:MessageDescription>*Jun 5 03:11:36.041: %CLEAR-5-COUNTERS: Clear counter on all interfaces by console*</ch:MessageDescription>
          <ch:SubType>syslog</ch:SubType>
          <ch:Brand>Cisco Systems</ch:Brand>
          <ch:Series>CSR1000v Cloud Services Router</ch:Series>
          <ch:Email>weijuhua@cisco.com</ch:Email>
          <ch:ContractData>
            <ch:ContractId>CSR1000V8C9S1NMSF22DW</ch:ContractId>
          </ch:ContractData>
        </ch:CallHome>
      </aml-block:Content>
    </aml-block:Block>
  </soap-env:Body>
</soap-env:Envelope>
```
Additional References

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

Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE commands</td>
<td>Cisco IOS Master Commands List, All Releases</td>
</tr>
<tr>
<td>Explains how the Smart Call Home service offers web-based access to important information on select Cisco devices and offers higher network availability, and increased operational efficiency by providing real-time alerts.</td>
<td>Smart Call Home User Guide</td>
</tr>
</tbody>
</table>
### Related Topic

<table>
<thead>
<tr>
<th>Title</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Smart Call Home site page on Cisco.com for access to all related product information.</td>
<td>Cisco Smart Call Home site</td>
</tr>
<tr>
<td>Public Key Infrastructure (PKI) and Certificate Authority configuration in Cisco IOS XE software</td>
<td>Cisco IOS XE Security Configuration Guide: Secure Connectivity</td>
</tr>
</tbody>
</table>

### Standards

<table>
<thead>
<tr>
<th>Standard</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.</td>
<td>—</td>
</tr>
</tbody>
</table>

### MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>CISCO-CALLHOME-MIB</td>
<td>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: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

### RFCs

<table>
<thead>
<tr>
<th>RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.</td>
<td>—</td>
</tr>
</tbody>
</table>
Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td><a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a></td>
</tr>
</tbody>
</table>

Feature Information for Call Home

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

Note

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

Table 10: Feature Information for Call Home

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Call Home</td>
<td>Cisco IOS XE Release 3.13S</td>
<td>The Call Home feature provides e-mail-based and web-based notification of critical system events. A versatile range of message formats are available for optimal compatibility with pager services, standard e-mail, or XML-based automated parsing applications. The following commands were introduced or modified:</td>
</tr>
</tbody>
</table>
Cisco Smart Licensing Client

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

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

- Finding Feature Information, page 91
- Prerequisites for Cisco Smart Licensing Client, page 91
- Restrictions for Cisco Smart Licensing Client, page 92
- Information About Cisco Smart Licensing Client, page 92
- How to Activate Cisco Smart Licensing Client, page 93
- Troubleshooting for Cisco Smart Licensing Client, page 96
- Configuration Examples for Cisco Smart Licensing Client, page 97
- Additional References for Cisco Smart Licensing Client, page 97
- Feature Information for Cisco Smart Licensing Client, page 98

Finding Feature Information

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

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

Prerequisites for Cisco Smart Licensing Client

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

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

Note: Cisco Smart Licensing Client is not supported on Cisco's Integrated Services Routers Generation 2 (ISR G2) platform.

Information About Cisco Smart Licensing Client

Cisco Smart Licensing - An Overview

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

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

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

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

Transitioning from CISL to Smart Licensing

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

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

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

Cisco One Suites

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

Enable Smart Licensing

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

SUMMARY STEPS

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

DETAILED STEPS

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Step 2</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>license smart enable</td>
<td>Activates Smart Licensing on the device.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device# license smart enable</td>
<td>Note When you enable Smart Licensing, the Cisco Software License (CSL) and all licensing calls pass through the Smart Agent. For the 'no' case, if Smart Licensing is already registered, the Smart Agent performs the &quot;license smart deregister&quot; operation that deactivates Smart Licensing. Reload the device to activate the CSL on the device.</td>
</tr>
</tbody>
</table>
### Smart License Disable

**SUMMARY STEPS**

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

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Device&gt; enable</code></td>
<td></td>
</tr>
</tbody>
</table>

- Enter your password if prompted.
<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>no license smart enable</td>
<td>Deactivates Smart Licensing on the device.</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config)# no license smart enable</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> When you disable Smart Licensing, the Cisco Software License (CSL) and all licensing calls pass through the Smart Agent. For the 'no' case, if Smart Licensing is already registered, the Smart Agent performs the &quot;license smart deregister&quot; operation that deactivates Smart Licensing. Reload the device to activate the CSL on the device.</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>license accept end user agreement</td>
<td>Uses the <code>license accept end user agreement</code> command to configure a one-time acceptance of the EULA for all Cisco IOS software packages and features.</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config)# license accept end user agreement</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> After the <code>license accept end user agreement</code> command is issued and the EULA accepted, the EULA is automatically applied to all Cisco IOS software licenses.</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>exit</td>
<td>Exits the global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config)# exit</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>write memory</td>
<td>Saves the running configuration to NVRAM.</td>
</tr>
<tr>
<td></td>
<td>Example: Device# write memory</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>reload</td>
<td>(Optional) Restarts the device to enable the new feature set.</td>
</tr>
<tr>
<td></td>
<td>Example: Device# reload</td>
<td><strong>Note</strong> Reload the device if you have not reloaded the device after configuring the Cisco One Suites.</td>
</tr>
<tr>
<td>8</td>
<td>show license all</td>
<td>(Optional) Displays summary information about all licenses.</td>
</tr>
<tr>
<td></td>
<td>Example: Device# show license all</td>
<td></td>
</tr>
</tbody>
</table>
Device Registration

SUMMARY STEPS

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

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Device&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> license smart register idtoken idtoken [force]</td>
<td>Registers the device with the back-end server. Token id can be obtained from your virtual a/c in the Smart Licensing server.</td>
</tr>
<tr>
<td>Example:</td>
<td>• force: To forcefully register your device irrespective of either the device is registered or not.</td>
</tr>
<tr>
<td>Device# license smart register idtoken 123</td>
<td>Note The device supplies the token ID to the Cisco server, which sends back a &quot;Device Certificate&quot; that is valid for 365 days.</td>
</tr>
<tr>
<td><strong>Step 3</strong> license smart deregister</td>
<td>Deregisters the device from the backend server.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device# license smart deregister</td>
</tr>
<tr>
<td><strong>Step 4</strong> license smart renew [ID</td>
<td>auth]</td>
</tr>
<tr>
<td>Example:</td>
<td>Device# license smart renew ID</td>
</tr>
</tbody>
</table>

Troubleshooting for Cisco Smart Licensing Client

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

• show version
• show running-config
• show license tech support
• show license entitlement
• show license feature
• show license certificate
• debug smart_lic error
• debug smart_lic trace

Configuration Examples for Cisco Smart Licensing Client

Example: Enabling Smart Licensing

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

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

Additional References for Cisco Smart Licensing Client

Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS commands</td>
<td>Cisco IOS Master Commands List, All Releases</td>
</tr>
<tr>
<td>Cisco License Manager Application</td>
<td>User Guide for Cisco License Manager</td>
</tr>
<tr>
<td>Software Activation Conceptual Overview</td>
<td>“Cisco IOS Software Activation Conceptual Overview” module</td>
</tr>
<tr>
<td>Software Activation Commands</td>
<td>Software Activation Command Reference</td>
</tr>
<tr>
<td>Integrated Services Routers Licensing</td>
<td>Software Activation on Cisco Integrated Services Routers</td>
</tr>
</tbody>
</table>
Standards and RFCs

MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>CISCO-LICENSE-MGMT-MIB</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td><a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a></td>
</tr>
</tbody>
</table>

Feature Information for Cisco Smart Licensing Client

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature. Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to . An account on Cisco.com is not required.
The Smart Licensing feature is a standardized licensing platform that simplifies the Cisco software experience and helps you understand how Cisco software is used across your network. Smart Licensing is the next generation licensing platform for all Cisco software products.

This feature is platform-independent.

The following commands were introduced or modified by this feature: `license smart enable`, `show license all`
CHAPTER 6

Configuring Licensing Storage Expansion for Cisco 2800 and Cisco 3800 Series Routers

At present, the Cisco 2800 and Cisco 3800 series platforms are running out of licensing storage to support current and potential Cisco Software Licensing projects on Cisco 2800 and Cisco 3800 series platforms, Cisco software licenses are stored in a section of NVRAM. The Licensing Storage Expansion feature reconfigures the NVRAM to provide additional license storage when the default license storage allocation is used up.

- Finding Feature Information, page 101
- Information About Licensing Storage Expansion, page 102
- How to Configure Licensing Storage Expansion, page 103
- Configuration Examples for Licensing Storage Expansion, page 105
- Additional References, page 106
- Feature Information for Licensing Storage Expansion, page 106

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 Licensing Storage Expansion

License Storage and Memory Allocation

Software licenses for Cisco 2800 and Cisco 3800 series routers are stored in NVRAM. The Cisco 2800 series routers have 16 KB of NVRAM allocated for license storage, and the Cisco 3800 series routers have 32 KB allocated. With the introduction of more licensed Cisco software products, the amount of space allocated for license storage will not be adequate. The License Storage Expansion feature reconfigures NVRAM to provide 64 KB of space for license storage in both the Cisco 2800 and Cisco 3800 series routers.

NVRAM stores two types of files that are not licenses: configuration files (startup-config and user-specific configuration files), and block files (non-configuration files that you can store in NVRAM). The reconfiguration of NVRAM reduces the amount of space available for configuration and block files. In Cisco 2800 series routers, this space is reduced from 240 KB to 192 KB. In Cisco 3800 series routers, this space is reduced from 480 KB to 448 KB.

The table below gives the NVRAM allocations for license and configuration storage before and after license storage expansion.

<table>
<thead>
<tr>
<th>Router Series</th>
<th>Default License Storage</th>
<th>Default Configuration Storage</th>
<th>Expanded License Storage</th>
<th>Resized Configuration Storage</th>
</tr>
</thead>
<tbody>
<tr>
<td>2800</td>
<td>16 KB</td>
<td>240 KB</td>
<td>64 KB</td>
<td>192 KB</td>
</tr>
<tr>
<td>3800</td>
<td>32 KB</td>
<td>480 KB</td>
<td>64 KB</td>
<td>448 KB</td>
</tr>
</tbody>
</table>

If the configuration files in NVRAM are larger than the allocation for resized storage, you receive a message telling you to compress the files. To compress the files, use the `service compress-config` command described in Compressing the Configuration Files in NVRAM, on page 104.

When the License Storage Expansion feature is run, configuration files are retained in the resized NVRAM. Block files are also retained, if possible. However, it might be necessary to store block files outside NVRAM, in other memory. If the configuration files are too big for the resized NVRAM, they will be compressed and rewritten into NVRAM. Block files will not be compressed.

When NVRAM is successfully resized, a message is sent to the console to indicate that you must reboot the router for the change to take effect.

When to Use Licensing Storage Expansion

When you try to install a license, but there is not enough room for it in license storage, you receive an error message `License store is full`. The following example illustrates this condition:

```
Device# license install flash:gk7.lic
Installing licenses from "flash:gk7.lic"
Installing...Feature gatekeeper...Failed
```
When you receive this error message, you must expand the license storage.

**Downgrading to an Image That Does Not Support Licensing Storage Expansion**

If you downgrade to a Cisco IOS image that does not support the `license expand nvram` command, all licenses stored in NVRAM are lost. This happens even if the image stores licenses in NVRAM. We recommend that you to save all your licenses before downgrading.

**How to Configure Licensing Storage Expansion**

**Expanding License Storage**

**Before You Begin**

Back up your Cisco software configuration before performing this procedure.

If NVRAM holds block files (files used for things other than configuration), some of these files will be lost when NVRAM is reconfigured when there is insufficient space for them in resized storage. To avoid the loss of block files, you must back them up by manually removing them and storing them elsewhere. Block files are not compressed.

**SUMMARY STEPS**

1. enable
2. license expand nvram

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode. Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> license expand nvram</td>
<td>Initiates reconfiguration of NVRAM to expand license storage to 64 KB. As a result, the memory allocated for configuration files is reduced.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device# license expand nvram</td>
<td></td>
</tr>
</tbody>
</table>
What to Do Next

If NVRAM does not have sufficient space to expand license storage, continue with Compressing the Configuration Files in NVRAM, on page 104.

If License Storage Expansion is successful, reboot the device so that the change can take effect.

Compressing the Configuration Files in NVRAM

SUMMARY STEPS

1. configure terminal
2. service compress-config
3. end
4. copy system:running-config nvram:startup-config

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>service compress-config</td>
<td>Activates compression of configuration files whenever the configuration is saved to startup configuration in NVRAM.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config)# service compress-config</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td>end</td>
<td>Exits global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config)# end</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td></td>
</tr>
<tr>
<td>copy system:running-config nvram:startup-config</td>
<td>Saves the running configuration to the startup configuration in NVRAM.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device# copy system:running-config nvram:startup-config</td>
<td></td>
</tr>
<tr>
<td>• The running configuration is compressed during the copy operation because service compress-config (Step 2) is activated.</td>
<td></td>
</tr>
</tbody>
</table>
Configuration Examples for Licensing Storage Expansion

Example: Expanding License Storage

The following example shows how to expand the allocation for license storage in NVRAM.

```
Device> enable
Password:
Device# license expand nvram
Caution: IOS configuration space will be re-partitioned in NVRAM.
You must back up your IOS configuration before running this command.
Do you wish to continue NVRAM re-partition? [confirm]
Device# y
```

When you enter `y`, NVRAM is checked to make sure that it has enough space for your files and the expanded licensing storage. If there is enough space for your files in the resized NVRAM, this message is sent to the console:

```
License storage expanded successfully.
IOS must be restarted for changes to take effect.
```

If there is not enough space for your configuration files, this message is sent to the console:

```
Error: startup-config is too large. Compress the config with “service compress-config”
followed by “copy system:running-config nvram:startup-config” and rerun “licence expand
nvram”.
```

If, after compression, the startup configuration file is still too large for the resized NVRAM, this message is sent:

```
Error: cannot expand the license storage. Insufficient NVRAM to store compressed
configuration.
```

If expansion cannot take place because the block files are too large, this message is sent to the console:

```
Error: cannot expand the license storage. Existing block files are too large. Back up
existing block files, delete them from nvram and reissue “license expand nvram”.
If the license expand nvram command is issued on an already expanded NVRAM, this message is sent to
the console:
Error: license storage already expanded to maximum size.
```

Example: Compressing the Configuration Files in NVRAM

The following example shows how to compress configuration files for a Cisco 2800 series router that are larger than 192 KB.

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# service compress-config
Device(config)# end
Device#
%SYS-5-CONFIG_I: Configured from console by console
Device# copy system:running-config nvram:startup-config
Building configuration...
Compressing configuration from 201179 bytes to 152674 bytes
[OK]
```
Additional References

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Software activation concepts and configuration</td>
<td>“Cisco IOS Software Activation Conceptual Overview” module</td>
</tr>
<tr>
<td></td>
<td>“Configuring the Cisco IOS Software Activation Feature” module</td>
</tr>
<tr>
<td>Software activation commands</td>
<td>Software Activation Command Reference</td>
</tr>
<tr>
<td>Cisco IOS commands</td>
<td>Master Commands List, All Releases</td>
</tr>
</tbody>
</table>

Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td><a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a></td>
</tr>
</tbody>
</table>

Feature Information for Licensing Storage Expansion

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 . An account on Cisco.com is not required.
Table 13: Feature Information for Licensing Storage Expansion

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Licensing Storage Expansion</td>
<td>12.4(20)T, 15.0(1)M</td>
<td>Reconfigures NVRAM in Cisco 2800 and Cisco 3800 series routers to expand storage for software licenses to 64 KB. The following command was introduced: license expand nvram</td>
</tr>
</tbody>
</table>
INDEX

C

call home destination profiles 76
  displaying 76

D

device IDs 81
  call home format 81

E

e-mail notifications 89
  Call Home 89

I

IDs 81
  serial IDsserial IDs 81
    description 81

S

server IDs 81
  description 81
source IDs 81
  call home event format 81