



## **Cisco VG450 Voice Gateway Software Configuration Guide**

**First Published:** 2018-10-30

**Last Modified:** 2022-04-22

### **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

**Full Cisco Trademarks with Software License ?**

---

**CHAPTER 1**

**Preface 1**

- Preface 2
- Audience and Scope 3
- Feature Compatibility 4
- Document Conventions 5
- Communications, Services, and Additional Information 7
- Documentation Feedback 8
- Troubleshooting 9

---

**CHAPTER 2**

**Understanding Interface Numbering and Cisco IOS Software Basics 11**

- Understanding Interface Numbering and Cisco IOS Software Basics 12
  - Identifying Cisco VG450 12
    - Cisco VG450 Port Numbering Conventions 12
  - Understanding Cisco IOS Software Basics 12
    - Getting Help 13
    - Command Modes 13
    - Undoing a Command or Feature 14
    - Saving Configuration Changes 14
  - Upgrading to a New Cisco IOS Release 14
  - Where to Go Next 14

---

**CHAPTER 3**

**Installing the Software Using Install Commands 17**

- Installing the Software Using install Commands 18

Restrictions for Installing the Software Using install Commands	19
Information About Installing the Software Using install Commands	20
Install Mode Process Flow	20
Booting the Platform in Install Mode	24
One-Step Installation or Converting from Bundle Mode to Install Mode	25
Three-Step Installation	26
Upgrading in Install Mode	28
Downgrading in Install Mode	28
Terminating a Software Installation	28
Configuration Examples for Installing the Software Using install Commands	29
Troubleshooting Software Installation Using install Commands	37

**CHAPTER 4****Configuring with the Command-Line Interface 39**

Configuring with the Command-Line Interface	40
Configuring the Host Name and Password	40
Summary Steps	40
Detailed Steps	40
Verifying the Host Name and Password	41
Configuring a Gigabit Ethernet Interfaces	42
TLS 1.2 support on SCCP Gateways	44
Saving Configuration Changes	48
Enabling UC License	49
Configuring the Voice Port	50

**CHAPTER 5****Configuring Voice Ports 53**

Voice Ports	54
Prerequisite	54
Configuring the Voice Port	54
Cisco IOS Bulk Configuration	55
Configuring FXS Ports for Supplementary Services	57
Configuring the Device Control Session Application for SIP	59
Configuring the Outbound Voip Dial-peer	60
Configuring Pots Dial-peer	61
Configuring Voice-card and SIP	61

Enabling Device Control Session Application Line features	62
Configuring Feature Access Code	62
Autoconfiguration	63
Verifying the Device Control Session Application Configuration	64
Autoconfiguration for SCCP	66
Prerequisites	66
STCApp Autoconfiguration	66
Configuring STCAPP Autoconfiguration	67
STCApp Autoconfiguration Examples	68

---

**CHAPTER 6 Support for Security-Enhanced Linux 71**

Overview	72
Prerequisites for SELinux	73
Restrictions for SELinux	74
Information About SELinux	75
Supported Platforms	75
Configuring SELinux	76
Configuring SELinux (EXEC Mode)	76
Configuring SELinux (CONFIG Mode)	76
Examples for SELinux	76
SysLog Message Reference	77
Verifying SELinux Enablement	79
Troubleshooting SELinux	80

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2019-2022 Cisco Systems, Inc. All rights reserved.





# Preface

---

- [Preface, on page 2](#)
- [Audience and Scope, on page 3](#)
- [Feature Compatibility, on page 4](#)
- [Document Conventions, on page 5](#)
- [Communications, Services, and Additional Information, on page 7](#)
- [Documentation Feedback, on page 8](#)
- [Troubleshooting, on page 9](#)

# Preface

This preface describes the audience, organization, and conventions of this document. It also provides information on how to obtain other documentation.

This preface includes the following sections:



# Audience and Scope

This document is designed for the person who is responsible for configuring your Cisco Enterprise router. This document is intended primarily for the following audiences:

- Customers with technical networking background and experience.
- System administrators familiar with the fundamentals of router-based internetworking but who might not be familiar with Cisco IOS software.
- System administrators who are responsible for installing and configuring internetworking equipment, and who are familiar with Cisco IOS software.

# Feature Compatibility

For more information about the Cisco IOS XE software, including features available on your device as described in the configuration guides, see the respective router documentation set.

To verify support for specific features, use the [Cisco Feature Navigator](#) tool. This tool enables you to determine the Cisco IOS XE software images that support a specific software release, feature set, or a platform.

# Document Conventions

This documentation uses the following conventions:

Convention	Description
<b>^</b> or <b>Ctrl</b>	The <b>^</b> and <b>Ctrl</b> symbols represent the Control key. For example, the key combination <b>^D</b> or <b>Ctrl-D</b> means hold down the <b>Control</b> key while you press the <b>D</b> key. Keys are indicated in capital letters but are not case sensitive.
<i>string</i>	A string is a nonquoted set of characters shown in italics. For example, when setting an SNMP community string to public, do not use quotation marks around the string or the string will include the quotation marks.

The command syntax descriptions use the following conventions:

Convention	Description
<b>bold</b>	Bold text indicates commands and keywords that you enter exactly as shown.
<i>italics</i>	Italic text indicates arguments for which you supply values.
[x]	Square brackets enclose an optional element (keyword or argument).
	A vertical line indicates a choice within an optional or required set of keywords or arguments.
[x   y]	Square brackets enclosing keywords or arguments separated by a vertical line indicate an optional choice.
{x   y}	Braces enclosing keywords or arguments separated by a vertical line indicate a required choice.

Nested sets of square brackets or braces indicate optional or required choices within optional or required elements. For example, see the following table.

Convention	Description
[x {y   z}]	Braces and a vertical line within square brackets indicate a required choice within an optional element.

Examples use the following conventions:

Convention	Description
screen	Examples of information displayed on the screen are set in Courier font.
<b>bold screen</b>	Examples of text that you must enter are set in Courier bold font.
<>	Angle brackets enclose text that is not printed to the screen, such as passwords.
!	An exclamation point at the beginning of a line indicates a comment line. Exclamation points are also displayed by the Cisco IOS XE software for certain processes.
[ ]	Square brackets enclose default responses to system prompts.



**Caution** Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.



**Note** Means *reader take note*. Notes contain helpful suggestions or references to materials that may not be contained in this manual.

# Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at [Cisco Profile Manager](#).
- To get the business impact you're looking for with the technologies that matter, visit [Cisco Services](#).
- To submit a service request, visit [Cisco Support](#).
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit [Cisco Marketplace](#).
- To obtain general networking, training, and certification titles, visit [Cisco Press](#).
- To find warranty information for a specific product or product family, access [Cisco Warranty Finder](#).

## Cisco Bug Search Tool

[Cisco Bug Search Tool](#) (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.

# Documentation Feedback

To provide feedback about Cisco technical documentation, use the feedback form available in the right pane of every online document.

# Troubleshooting

For the most up-to-date, detailed troubleshooting information, see the Cisco TAC website at <https://www.cisco.com/en/US/support/index.html>.

Go to **Products by Category** and choose your product from the list, or enter the name of your product. Look under **Troubleshoot and Alerts** to find information for the issue that you are experiencing.







# Understanding Interface Numbering and Cisco IOS Software Basics

---

- [Understanding Interface Numbering and Cisco IOS Software Basics](#), on page 12

# Understanding Interface Numbering and Cisco IOS Software Basics

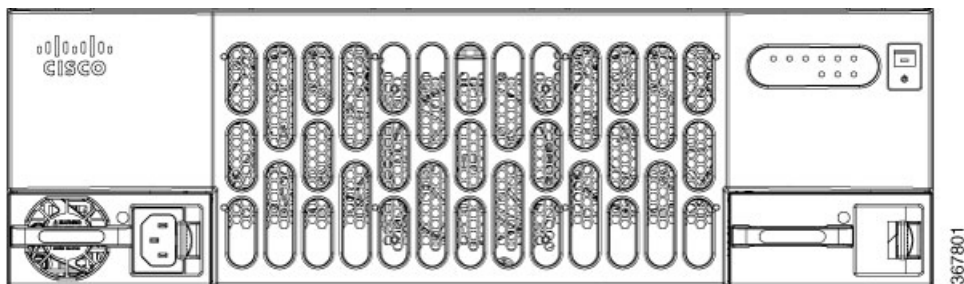
This chapter provides an overview of interface numbering in the Cisco VG450 Voice Gateways (VG). It also describes how to use the Cisco IOS software commands.

This chapter presents the following major topics:

## Identifying Cisco VG450

The following figure shows the front panels of the Cisco VG450 Voice Gateway Chassis:

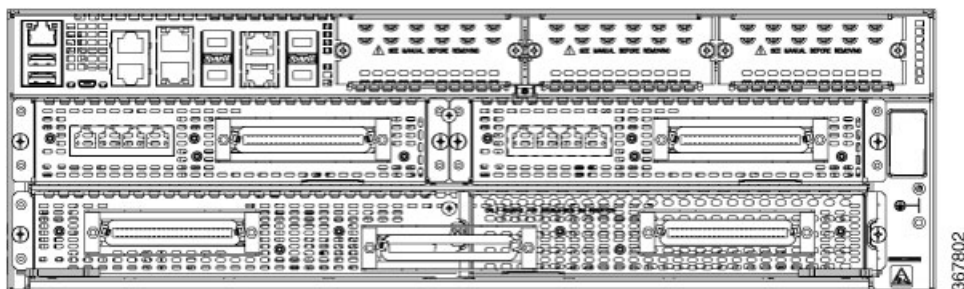
*Figure 1: Front panel of the Cisco VG450 Voice Gateway*



## Cisco VG450 Port Numbering Conventions

The following figure shows the Cisco VG450 back panel:

*Figure 2: Back panel of the VG450 Voice Gateway*



## Understanding Cisco IOS Software Basics

This section describes what you need to know about the Cisco IOS software before you configure the router using the CLI. This chapter includes the following:

Understanding these concepts will save time as you begin to use the commands. If you have never used Cisco IOS software or need a refresher, take a few minutes to read this chapter before you proceed to the next chapter.

If you are already familiar with Cisco IOS software, proceed to the [“Configuring the Host Name and Password” section on page 2-1](#)

## Getting Help

Use the question mark (?) and arrow keys to help you enter commands:

- For a list of available commands, enter a question mark:

```
Router> ?
```

- To complete a command, enter a few known characters followed by a question mark (with no space):

```
Router> s?
```

- For a list of command variables, enter the command followed by a space and a question mark:

```
Router> show ?
```

- To redisplay a command you previously entered, press the Up Arrow key. You can continue to press the Up Arrow key for more commands.

## Command Modes

The Cisco IOS user interface is divided into different modes. Each command mode permits you to configure different components on your router. The commands available at any given time depend on which mode you are currently in. Entering a question mark (?) at the prompt displays a list of commands available for each command mode. The following table lists the most common command modes.

**Table 1: Common Command Modes**

Command Mode	Access Method	Router Prompt Displayed	Exit Method
User EXEC	Log in.	Router>	Use the <b>logout</b> command.
Privileged EXEC	From user EXEC mode, enter the <b>enable</b> command.	Router#	To exit to user EXEC mode, use the <b>disable</b> , <b>exit</b> , or <b>logout</b> command.
Global configuration	From the privileged EXEC mode, enter the <b>configure terminal</b> command.	Router (config)#	To exit to privileged EXEC mode, use the <b>exit</b> or <b>end</b> command, or press <b>Ctrl-Z</b> .
Interface configuration	From the global configuration mode, enter the GigabitEthernet interface command such as, <b>gigabitethernet0/0</b> .	Router (config-if)#	To exit to global configuration mode, use the <b>exit</b> command. To exit directly to privileged EXEC mode, press <b>Ctrl-Z</b> .



### Timesaver

Each command mode restricts you to a subset of commands. If you are having trouble entering a command, check the prompt, and enter the question mark (?) for a list of available commands. You might be in the wrong command mode or be using the wrong syntax.

In the following example, notice how the prompt changes after each command, to indicate a new command mode for Cisco VG450:

```
Router> enable
Password: <enable password>
Router# configure terminal
Router(config)# interface gigabitEthernet 0/0/0
Router#
%SYS-5-CONFIG_I: Configured from console by console
```

The last message is normal and does not indicate an error. Press **Return** to get the Router# prompt.




---

**Note** Press **Ctrl-Z** in any mode to immediately return to enable mode ( Router# ), instead of entering **exit**, which returns you to the previous mode.

---

## Undoing a Command or Feature

If you want to undo a command you entered or disable a feature, enter the keyword **no** before most commands; for example, **no ip routing**.

## Saving Configuration Changes

You need to enter the **copy running-config startup-config** command to save your configuration changes to nonvolatile random-access memory (NVRAM), so the changes are not lost if there is a system reload or power outage. For example:

```
Router# copy running-config startup-config
Building configuration...
```

It might take a minute or two to save the configuration to NVRAM. After the configuration has been saved, the following appears:

```
[OK]
Router#
```

## Upgrading to a New Cisco IOS Release

To install or upgrade to a new Cisco IOS release, see *How to Update/Upgrade Cisco IOS Software*.

## Where to Go Next

Now that you have learned some Cisco IOS software basics, you can begin to configure the router using the CLI.

Remember that:

- You can use the question mark (?) and arrow keys to help you enter commands.
- Each command mode restricts you to a set of commands. If you have difficulty entering a command, check the prompt and then enter the question mark (?) for a list of available commands. You might be in the wrong command mode or be using the wrong syntax.
- To disable a feature, generally enter the keyword **no** before the command; for example, **no ip routing**.

- You need to save your configuration changes to NVRAM so the changes are not lost if there is a system reload or power outage.

Proceed to [Chapter 2, “Configuring the Host Name and Password,”](#) to begin configuring the router.





## Installing the Software Using Install Commands

---

- [Installing the Software Using install Commands, on page 18](#)
- [Restrictions for Installing the Software Using install Commands, on page 19](#)
- [Information About Installing the Software Using install Commands, on page 20](#)
- [Configuration Examples for Installing the Software Using install Commands, on page 29](#)
- [Troubleshooting Software Installation Using install Commands, on page 37](#)

## Installing the Software Using install Commands

From Cisco IOS XE Cupertino 17.9.1a, Cisco Voice Gateways VG400, VG420, and VG450 are shipped in install mode by default. From Cisco IOS XE 17.12.1a, Cisco Voice Gateway VG410 is also shipped in the install mode. You can boot the platform, and upgrade or downgrade to Cisco IOS XE software versions using a set of **install** commands that are detailed in the following sections.



## Restrictions for Installing the Software Using install Commands

- ISSU is not covered in this feature.
- Install mode requires a reboot of the system.

# Information About Installing the Software Using install Commands

From Cisco IOS XE Cupertino 17.9.1a release, for devices shipped in install mode, a set of **install** commands can be used for starting, upgrading and downgrading of platforms in install mode. This update is applicable to the Cisco Voice Gateway 400 Series.

The following table describes the differences between Bundle mode and Install mode:

**Table 2: Bundle Mode vs Install Mode**

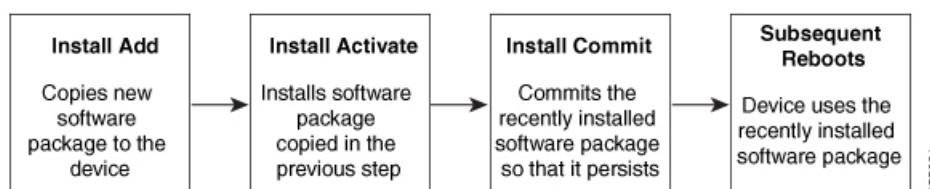
Bundle Mode	Install Mode
This mode provides a consolidated boot process, using local (hard disk, flash) or remote (TFTP) .bin image.	This mode uses the local (bootflash) packages.conf file for the boot process.
This mode uses a single .bin file.	.bin file is replaced with expanded .pkg files in this mode.
CLI: <code>#boot system file &lt;filename&gt;</code>	CLI: <code>#install add file bootflash: [activate commit]</code>
To upgrade in this mode, point the boot system to the new image.	To upgrade in this mode, use the <b>install</b> commands.

## Install Mode Process Flow

The install mode process flow comprises three commands to perform installation and upgrade of software on platforms—**install add**, **install activate**, and **install commit**.

The following flow chart explains the install process with **install** commands:

Process with Install Commit



The **install add** command copies the software package from a local or remote location to the platform. The location can be FTP, HTTP, HTTPS, or TFTP. The command extracts individual components of the .package file into subpackages and packages.conf files. It also validates the file to ensure that the image file is specific to the platform on which it is being installed.

The **install activate** command performs the required validations and provisions the packages previously added using the **install add** command. It also triggers a system reload.

The **install commit** command confirms the packages previously activated using the **install activate** command, and makes the updates persistent over reloads.



**Note** Installing an update replaces any previously installed software image. At any time, only one image can be installed in a device.

The following set of install commands is available:

**Table 3: List of install Commands**

Command	Syntax	Purpose
<b>install add</b>	<b>install add file</b> <i>location:filename.bin</i>	<p>Copies the contents of the image and the package to the software repository. File location may be local or remote. This command does the following:</p> <ul style="list-style-type: none"> <li>• Validates the file-checksum, platform compatibility checks, and so on.</li> <li>• Extracts individual components of the package into subpackages and packages.conf</li> <li>• Copies the image into the local inventory and makes it available for the next steps.</li> </ul>
<b>install activate</b>	<b>install activate</b>	<p>Activates the package added using the <b>install add</b> command.</p> <ul style="list-style-type: none"> <li>• Use the <b>show install summary</b> command to see which image is inactive. This image will get activated.</li> <li>• System reloads on executing this command. Confirm if you want to proceed with the activation. Use this command with the <b>prompt-level none</b> keyword to automatically ignore any confirmation prompts.</li> </ul>

Command	Syntax	Purpose
<b>(install activate) auto abort-timer</b>	<b>install activate auto-abort timer</b> <30-1200>	<p>The <b>auto-abort timer</b> starts automatically, with a default value of 120 minutes. If the <b>install commit</b> command is not executed within the time provided, the activation process is terminated, and the system returns to the last-committed state.</p> <ul style="list-style-type: none"> <li>• You can change the time value while executing the <b>install activate</b> command.</li> <li>• The <b>install commit</b> command stops the timer, and continues the installation process.</li> <li>• The <b>install activate auto-abort timer stop</b> command stops the timer without committing the package.</li> <li>• Use this command with the <b>prompt-level none</b> keyword to automatically ignore any confirmation prompts.</li> <li>• This command is valid only in the three-step install variant.</li> </ul>
<b>install commit</b>	<b>install commit</b>	<p>Commits the package activated using the <b>install activate</b> command, and makes it persistent over reloads.</p> <ul style="list-style-type: none"> <li>• Use the <b>show install summary</b> command to see which image is uncommitted. This image will get committed.</li> </ul>

Command	Syntax	Purpose
<b>install abort</b>	<b>install abort</b>	<p>Terminates the installation and returns the system to the last-committed state.</p> <ul style="list-style-type: none"> <li>• This command is applicable only when the package is in activated status (uncommitted state).</li> <li>• If you have already committed the image using the <b>install commit</b> command, use the <b>install rollback to</b> command to return to the preferred version.</li> </ul>
<b>install remove</b>	<b>install remove {file &lt;filename&gt;   inactive}</b>	<p>Deletes inactive packages from the platform repository. Use this command to free up space.</p> <ul style="list-style-type: none"> <li>• <b>file</b>: Removes specified files.</li> <li>• <b>inactive</b>: Removes all the inactive files.</li> </ul>
<b>install rollback to</b>	<b>install rollback to {base   label   committed   id}</b>	<p>Rolls back the software set to a saved installation point or to the last-committed installation point. The following are the characteristics of this command:</p> <ul style="list-style-type: none"> <li>• Requires reload.</li> <li>• Is applicable only when the package is in committed state.</li> <li>• Use this command with the <b>prompt-level none</b> keyword to automatically ignore any confirmation prompts.</li> </ul> <p><b>Note</b> If you are performing install rollback to a previous image, the previous image must be installed in install mode.</p>

The following show commands are also available:

Table 4: List of show Commands

Command	Syntax	Purpose
<b>show install log</b>	<b>show install log</b>	Provides the history and details of all install operations that have been performed since the platform was booted.
<b>show install package</b>	<b>show install package</b> <filename>	Provides details about the .pkg/.bin file that is specified.
<b>show install summary</b>	<b>show install summary</b>	Provides an overview of the image versions and their corresponding install states.
<b>show install active</b>	<b>show install active</b>	Provides information about the active packages.
<b>show install inactive</b>	<b>show install inactive</b>	Provides information about the inactive packages, if any.
<b>show install committed</b>	<b>show install committed</b>	Provides information about the committed packages.
<b>show install uncommitted</b>	<b>show install uncommitted</b>	Provides information about uncommitted packages, if any.
<b>show install rollback</b>	<b>show install rollback</b> {point-id   label}	Displays the package associated with a saved installation point.
<b>show version</b>	<b>show version</b> [rp-slot] [installed   user-interface]   provisioned   running]	Displays information about the current package, along with hardware and platform information.

## Booting the Platform in Install Mode

You can install, activate, and commit a software package using a single command (one-step install) or multiple separate commands (three-step install).

If the platform is working in bundle mode, the one-step install procedure must be used to initially convert the platform from bundle mode to install mode. Subsequent installs and upgrades on the platform can be done with either one-step or three-step variants.

# One-Step Installation or Converting from Bundle Mode to Install Mode



## Note

- All the CLI actions (for example, add, activate, and so on) are executed.
- The configuration save prompt will appear if an unsaved configuration is detected.
- The reload prompt will appear after the second step in this workflow. Use the **prompt-level none** keyword to automatically ignore the confirmation prompts.
- If the prompt-level is set to None, and there is an unsaved configuration, the install fails. You must save the configuration before reissuing the command.

Use the one-step install procedure described below to convert a platform running in bundle boot mode to install mode. After the command is executed, the platform reboots in install boot mode.

Later, the one-step install procedure can also be used to upgrade the platform.

This procedure uses the **install add file activate commit** command in privileged EXEC mode to install a software package, and to upgrade the platform to a new version.

## SUMMARY STEPS

1. **enable**
2. **install add file location: *filename* [activate commit]**
3. **exit**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b> <b>Example:</b> Device>enable	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	<b>install add file location: <i>filename</i> [activate commit]</b> <b>Example:</b> See the following examples: <ul style="list-style-type: none"> <li>• <b>VG400:</b> <pre>Device#install add file bootflash:vg400-universalk9-ED-V179-THROTTLE-LATEST-20220428_010838-V1790-23.SSA.bin activate commit</pre> </li> <li>• <b>VG410:</b> <pre>Device# install add file bootflash:vg4x0-universalk9.17.12.01a.SPA.bin activate commit</pre> </li> </ul>	Copies the software install package from a local or remote location (through FTP, HTTP, HTTPS, or TFTP) to the platform and extracts the individual components of the .package file into subpackages and packages.conf files. It also performs a validation and compatibility check for the platform and image versions, activates the package, and commits the package to make it persistent across reloads.  The platform reloads after this command is run.
Step 3	<b>exit</b> <b>Example:</b>	Exits privileged EXEC mode and returns to user EXEC mode.

	Command or Action	Purpose
	Device# exit	

## Three-Step Installation



- Note**
- All the CLI actions (for example, add, activate, and so on) are executed.
  - The configuration save prompt will appear if an unsaved configuration is detected.
  - The reload prompt will appear after the install activate step in this workflow. Use the **prompt-level none** keyword to automatically ignore the confirmation prompts.

The three-step installation procedure can be used only after the platform is in install mode. This option provides more flexibility and control to the customer during installation.

This procedure uses individual **install add**, **install activate**, and **install commit** commands for installing a software package, and to upgrade the platform to a new version.

### SUMMARY STEPS

1. **enable**
2. **install add file location: *filename***
3. **show install summary**
4. **install activate [auto-abort-timer <time>]**
5. **install abort**
6. **install commit**
7. **install rollback to committed**
8. **install remove {file filesystem: *filename* | inactive}**
9. **show install summary**
10. **exit**

### DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b> Device>enable	Enables privileged EXEC mode. Enter your password, if prompted.
<b>Step 2</b>	<b>install add file location: <i>filename</i></b> <b>Example:</b> See the following examples: <ul style="list-style-type: none"> <li>• <b>VG400:</b>                Device#install add file                bootflash:vg400-universal-9.ED_V179_THROTTLE_LATEST_2020428_010838_V17_9_0_23.SSA.bin             </li> </ul>	Copies the software install package from a remote location (through FTP, HTTP, HTTPS, or TFTP) to the platform, and extracts the individual components of the .package file into subpackages and packages.conf files.



	Command or Action	Purpose
	<ul style="list-style-type: none"> <li>• <b>VG410:</b></li> </ul> <pre>Device#install add file bootflash:vg410-rivesalk9-BD_V72_THRMTF_LATEST_2023028_04130_V7_12_1_1.SPA.bin</pre>	
<b>Step 3</b>	<b>show install summary</b> <b>Example:</b> <pre>Device#show install summary</pre>	(Optional) Provides an overview of the image versions and their corresponding install state.
<b>Step 4</b>	<b>install activate [auto-abort-timer &lt;time&gt;]</b> <b>Example:</b> <pre>Device# install activate auto-abort-timer 120</pre>	Activates the previously added package and reloads the platform. <ul style="list-style-type: none"> <li>• When doing a full software install, do not provide a package filename.</li> <li>• In the three-step variant, <b>auto-abort-timer</b> starts automatically with the <b>install activate</b> command; the default for the timer is 120 minutes. If the <b>install commit</b> command is not run before the timer expires, the install process is automatically terminated. The platform reloads and boots up with the last committed version.</li> </ul>
<b>Step 5</b>	<b>install abort</b> <b>Example:</b> <pre>Device#install abort</pre>	(Optional) Terminates the software install activation and returns the platform to the last committed version. <ul style="list-style-type: none"> <li>• Use this command only when the image is in activated state and not when the image is in committed state.</li> </ul>
<b>Step 6</b>	<b>install commit</b> <b>Example:</b> <pre>Device#install commit</pre>	Commits the new package installation and makes the changes persistent over reloads.
<b>Step 7</b>	<b>install rollback to committed</b> <b>Example:</b> <pre>Device#install rollback to committed</pre>	(Optional) Rolls back the platform to the last committed state.
<b>Step 8</b>	<b>install remove {file filesystem: filename   inactive}</b> <b>Example:</b> <pre>Device#install remove inactive</pre>	(Optional) Deletes the software installation files. <ul style="list-style-type: none"> <li>• <b>file:</b> Deletes a specific file.</li> <li>• <b>inactive:</b> Deletes all the unused and inactive installation files.</li> </ul>
<b>Step 9</b>	<b>show install summary</b> <b>Example:</b> <pre>Device#show install summary</pre>	(Optional) Displays information about the current state of the system. The output of this command varies according to the <b>install</b> commands run prior to this command.

	Command or Action	Purpose
Step 10	<b>exit</b> <b>Example:</b> Device#exit	Exits privileged EXEC mode and returns to the user EXEC mode.

## Upgrading in Install Mode

Use either the one-step installation or the three-step installation to upgrade the platform in install mode.

## Downgrading in Install Mode

Use the **install rollback** command to downgrade the platform to a previous version by pointing it to the appropriate image, provided the image you are downgrading to was installed in install mode.

The **install rollback** command reloads the platform and boots it with the previous image.



**Note** The **install rollback** command succeeds only if you have not removed the previous file using the **install remove inactive** command.

Alternatively, you can downgrade by installing the older image using the **install** commands.

## Terminating a Software Installation

You can terminate the activation of a software package in the following ways:

- When the platform reloads after activating a new image, the auto-abort-timer is triggered (in the three-step install variant). If the timer expires before issuing the **install commit** command, the installation process is terminated, and the platform reloads and boots with the last committed version of the software image.

Alternatively, use the **install auto-abort-timer stop** command to stop this timer, without using the **install commit** command. The new image remains uncommitted in this process.

- Using the **install abort** command returns the platform to the version that was running before installing the new software. Use this command before issuing the **install commit** command.

# Configuration Examples for Installing the Software Using Install Commands

The following is an example of the one-step installation or converting from bundle mode to install mode:

```
install-vg400# install add file
bootflash:vg400-universalk9.BLD_V179_THROTTLE_LATEST_20220428_010838_V17_9_0_23.SSA.bin
activate commit

*May 11 23:45:54.588: %INSTALL-5-INSTALL_START_INFO: R0/0: install_mgr: Started install
add_activate_commit
bootflash:vg400-universalk9.BLD_V179_THROTTLE_LATEST_20220428_010838_V17_9_0_23.SSA.bininstall_add_activate_commit:
  START Wed May 11 23:45:54 UTC 2022
install_add: Adding IMG
--- Starting initial file syncing ---
Copying
bootflash:vg400-universalk9.BLD_V179_THROTTLE_LATEST_20220428_010838_V17_9_0_23.SSA.bin
from R0 to R0
Info: Finished copying to the selected
Finished initial file syncing

--- Starting Add ---
Performing Add on all members
  [1] Finished Add package(s) on R0
Checking status of Add on [R0]
Add: Passed on [R0]
Finished Add

Image added. Version: 17.09.01.0.5

install_activate: Activating IMG
Following packages shall be activated:
/bootflash/vg400-firmware_sm_dsp_sp2700.BLD_V179_THROTTLE_LATEST_20220428_010838_V17_9_0_23.SSA.pkg
/bootflash/vg400-mono-universalk9.BLD_V179_THROTTLE_LATEST_20220428_010838_V17_9_0_23.SSA.pkg
/bootflash/vg400-rpboot.BLD_V179_THROTTLE_LATEST_20220428_010838_V17_9_0_23.SSA.pkg

This operation may require a reload of the system. Do you want to proceed? [y/n]y

--- Starting Activate ---
Performing Activate on all members
  [1] Activate package(s) on R0

*May 11 23:47:07.393: %INSTALL-5-INSTALL_AUTO_ABORT_TIMER_PROGRESS: R0/0: rollback_timer:
Install auto abort timer will expire in 7200 seconds [1] Finished Activate on R0
Checking status of Activate on [R0]
Activate: Passed on [R0]
Finished Activate

--- Starting Commit ---
Performing Commit on all members
  [1] Commit package(s) on R0
  [1] Finished Commit on R0
Checking status of Commit on [R0]
Commit: Passed on [R0]
Finished Commit operation

SUCCESS: install_add_activate_commit Wed May 11 23:47:53 UTC 2022
```

```

install-vg400#
*May 11 23:47:53.019: %INSTALL-5-INSTALL_COMPLETED_INFO: R0/0: install_mgr: Completed install
  add_activate_commitMay 11 23:4350: %PMAN-5-EXITACTION: R0/0: pvp: Process manager is
  exiting: reload action requested

Initializing Hardware ...

:
Press RETURN to get started!

```

The following is an example of the three-step installation:

```

install-vg400# install add
bootflash:vg400-universalk9_npe.BLD_POLARIS_DEV_LATEST_20220427_001035_V17_9_0_6.SSA.bin

*May 12 00:11:54.785: %INSTALL-5-INSTALL_START_INFO: R0/0: install_mgr: Started install add

bootflash:vg400-universalk9_npe.BLD_POLARIS_DEV_LATEST_20220427_001035_V17_9_0_6.SSA.bininstall_add:
  START Thu May 12 00:11:54 UTC 2022
install_add: Adding IMG
--- Starting initial file syncing ---
Copying
bootflash:vg400-universalk9_npe.BLD_POLARIS_DEV_LATEST_20220427_001035_V17_9_0_6.SSA.bin
from R0 to R0
Info: Finished copying to the selected
Finished initial file syncing

--- Starting Add ---
Performing Add on all members
  [1] Finished Add package(s) on R0
Checking status of Add on [R0]
Add: Passed on [R0]
Finished Add

Image added. Version: 17.09.01.0.158205

SUCCESS: install_add
/bootflash/vg400-universalk9_npe.BLD_POLARIS_DEV_LATEST_20220427_001035_V17_9_0_6.SSA.bin
Thu May 12 00:12:26 UTC 2022

install-vg400#
*May 12 00:12:26.874: %INSTALL-5-INSTALL_COMPLETED_INFO: R0/0: install_mgr: Completed install
  add bootflash:/vg400-universalk9_npe.BLD_POLARIS_DEV_LATEST_20220427_001035_V17_9_0_6.SSA.bin
install-vg400#

install-vg400# install activate

*May 12 00:14:37.594: %INSTALL-5-INSTALL_START_INFO: R0/0: install_mgr: Started install
  activate NONEinstall_activate: START Thu May 12 00:14:37 UTC 2022
install_activate: Activating IMG
Following packages shall be activated:
/bootflash/vg400-firmware_sm_dsp_sp2700.BLD_POLARIS_DEV_LATEST_20220427_001035_V17_9_0_6.SSA.pkg
/bootflash/vg400-mono-universalk9_npe.BLD_POLARIS_DEV_LATEST_20220427_001035_V17_9_0_6.SSA.pkg
/bootflash/vg400-rpboot.BLD_POLARIS_DEV_LATEST_20220427_001035_V17_9_0_6.SSA.pkg

This operation may require a reload of the system. Do you want to proceed? [y/n]y

--- Starting Activate ---
Performing Activate on all members

*May 12 00:18:06.168: %INSTALL-5-INSTALL_AUTO_ABORT_TIMER_PROGRESS: R0/0: rollback_timer:

```

```

Install auto abort timer will expire in 7200 seconds [1] Activate package(s) on R0
[1] Finished Activate on R0
Checking status of Activate on [R0]
Activate: Passed on [R0]
Finished Activate

SUCCESS: install_activate Thu May 12 00:18:27 UTC 2022

install-vg400#
*May 12 00:18:27.511: %INSTALL-5-INSTALL_COMPLETED_INFO: R0/0: install_mgr: Completed install
activateMay 12 00:18:36.881: %PMAN-5-EXITACTION: R0/0: pvp: Process manager is exiting:
reload action requested

Initializing Hardware ...
:
:

Press RETURN to get started!

install-vg400>

install-vg400# install commit

*May 12 01:20:23.889: %INSTALL-5-INSTALL_START_INFO: R0/0: install_mgr: Started install
commitinstall_commit: START Thu May 12 01:20:23 UTC 2022
--- Starting Commit ---
Performing Commit on all members
[1] Commit packages(s) on R0
[1] Finished Commit packages(s) on R0
Checking status of Commit on [R0]
Commit: Passed on [R0]
Finished Commit operation

SUCCESS: install_commit Thu May 12 01:20:31 UTC 2022

install-vg400#
*May 12 01:20:31.351: %INSTALL-5-INSTALL_COMPLETED_INFO: R0/0: install_mgr: Completed install
commit

```

The following is an example of downgrading in install mode:

```

install-vg400# install add file bootflash:vg400-universalk9.17.08.01a.SPA.bin activate
commit

*May 12 02:13:24.633: %INSTALL-5-INSTALL_START_INFO: R0/0: install_mgr: Started install
add_activate_commit bootflash:vg400-universalk9.17.08.01a.SPA.bininstall_add_activate_commit:
START Thu May 12 02:13:24 UTC 2022
install_add: Adding IMG
--- Starting initial file syncing ---
Copying bootflash:vg400-universalk9.17.08.01a.SPA.bin from R0 to R0
Info: Finished copying to the selected
Finished initial file syncing

--- Starting Add ---
Performing Add on all members
[1] Finished Add package(s) on R0
Checking status of Add on [R0]
Add: Passed on [R0]

```

```

Finished Add

Image added. Version: 17.08.01.0.1526

install_activate: Activating IMG
Following packages shall be activated:
/bootflash/vg400-firmware_sm_dsp_sp2700.17.08.01a.SPA.pkg
/bootflash/vg400-mono-universalk9.17.08.01a.SPA.pkg
/bootflash/vg400-rpboot.17.08.01a.SPA.pkg

This operation may require a reload of the system. Do you want to proceed? [y/n]y

--- Starting Activate ---
Performing Activate on all members
  [1] Activate package(s) on  R0

*May 12 02:17:10.699: %INSTALL-5-INSTALL_AUTO_ABORT_TIMER_PROGRESS: R0/0: rollback_timer:
Install auto abort timer will expire in 7200 seconds [1] Finished Activate on  R0
Checking status of Activate on [R0]
Activate: Passed on [R0]
Finished Activate

--- Starting Commit ---
Performing Commit on all members
  [1] Commit package(s) on  R0
  [1] Finished Commit on  R0
Checking status of Commit on [R0]
Commit: Passed on [R0]
Finished Commit operation

SUCCESS: install_add_activate_commit Thu May 12 02:17:55 UTC 2022

install-vg400#
*May 12 02:17:55.312: %INSTALL-5-INSTALL_COMPLETED_INFO: R0/0: install_mgr: Completed install
add_activate_commitMay 12 02:18:08.796: %PMAN-5-EXITACTION: R0/0: pvp: Process manager is
exiting: reload action requested

Initializing Hardware ...
:
:
Press RETURN to get started!

install-vg400# show version
Cisco IOS XE Software, Version 17.08.01a
Cisco IOS Software [Cupertino], ISR Software (X86_64_LINUX_IOSD-UNIVERSALK9-M), Version
17.8.1a, RELEASE SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2022 by Cisco Systems, Inc.
Compiled Wed 20-Apr-22 13:16 by mcpre

Cisco IOS-XE software, Copyright (c) 2005-2022 by cisco Systems, Inc.
All rights reserved. Certain components of Cisco IOS-XE software are
licensed under the GNU General Public License ("GPL") Version 2.0. The
software code licensed under GPL Version 2.0 is free software that comes
with ABSOLUTELY NO WARRANTY. You can redistribute and/or modify such
GPL code under the terms of GPL Version 2.0. For more details, see the
documentation or "License Notice" file accompanying the IOS-XE software,
or the applicable URL provided on the flyer accompanying the IOS-XE
software.

```

ROM: 16.12(2r)

```
install-vg400 uptime is 1 minute
Uptime for this control processor is 4 minutes
System returned to ROM by Install
System image file is "bootflash:packages.conf"
Last reload reason: Install
```

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at: <http://www.cisco.com/wwl/export/crypto/tool/stqrg.html>

If you require further assistance please contact us by sending email to [export@cisco.com](mailto:export@cisco.com).

Suite License Information for Module:'esg'

```
-----
Suite                Suite Current      Type                Suite Next reboot
-----
```

Technology Package License Information:

```
-----
Technology           Technology-package   Technology-package
                    Current             Type                Next reboot
-----
```

uck9	uck9	Smart License	uck9
securityk9	None	Smart License	None
ibase	ibasek9	Smart License	ibasek9

The current throughput level is 35000 kbps

Smart Licensing Status: Smart Licensing Using Policy

```
cisco VG400-8FXS (1RU) processor with 1654554K/3071K bytes of memory.
Processor board ID FGL2517L2XS
Router operating mode: Autonomous
2 Gigabit Ethernet interfaces
8 Voice FXS interfaces
32768K bytes of non-volatile configuration memory.
4194304K bytes of physical memory.
6598655K bytes of flash memory at bootflash:.
```

Configuration register is 0x2102

install-vg400#

The following is an example of terminating a software installation:

```
install-vg400# install abort
install_abort: START Tue May 03 18:31:20 UTC 2022

This operation may require a reload of the system. Do you want to proceed? [y/n]y

--- Starting Abort ---
Performing Abort on all members
 [1] Abort packages(s) on R0
Checking status of Abort on [R0]
Abort: Passed on [R0]
Finished Abort operation

SUCCESS: install_abort Tue May 03 18:32:43 UTC 2022
install-vg400#May  3 18:32:48.735: %PMAN-5-EXITACTION: R0/0: pvp: Process manager is exiting:
 reload action requested

Initializing Hardware ...
:
:
  Press RETURN to get started!

install-vg400>
```

The following are sample outputs for show commands:

#### show install log

```
install-vg400# show install log
[0|install_op_boot]: START Thu May 12 06:22:15 Universal 2022
[0|install_op_boot]: END SUCCESS  Thu May 12 06:22:17 Universal 2022
```

#### show install summary

```
install-vg400# show install summary
[ R0 ] Installed Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
             C - Activated & Committed, D - Deactivated & Uncommitted

-----
Type  St   Filename/Version
-----
IMG   C    17.09.01.0.5
-----

Auto abort timer: inactive
-----
```

#### show install package filesystem: filename

```
install-vg400# show install package
bootflash:vg400-universalk9.BLD_POLARIS_DEV_LATEST_20220427_001035_V17_9_0_6.SSA.bin
  Package: vg400-universalk9.BLD_POLARIS_DEV_LATEST_20220427_001035_V17_9_0_6.SSA.bin
  Size: 648938943
  Timestamp:
  Canonical path:
  /bootflash/vg400-universalk9.BLD_POLARIS_DEV_LATEST_20220427_001035_V17_9_0_6.SSA.bin

  Raw disk-file SHA1sum:
    80700b261910c44785f46cac327b3aa81ed42edb
  Header size:      1152 bytes
  Package type:     30000
  Package flags:    0
  Header version:   3
```



## Internal package information:

```
Name: rp_super
BuildTime: 2022-04-26_20.04
ReleaseDate: 2022-04-27_02.02
BootArchitecture: i686
RouteProcessor: goldbeach
Platform: VG400
User: mcpre
PackageName: universalk9
Build: BLD_POLARIS_DEV_LATEST_20220427_001035_V17_9_0_6
CardTypes:
```

Package is bootable from media and tftp.

Package contents:

```
Package: vg400-mono-universalk9.BLD_POLARIS_DEV_LATEST_20220427_001035_V17_9_0_6.SSA.pkg
Size: 606901316
Timestamp:
```

## Raw disk-file SHA1sum:

```
53642fa806fa46a262aa247118272e49b48f14c0
Header size: 1092 bytes
Package type: 30000
Package flags: 0
Header version: 3
```

## Internal package information:

```
Name: mono
BuildTime: 2022-04-26_20.04
ReleaseDate: 2022-04-27_02.02
BootArchitecture: i686
RouteProcessor: goldbeach
Platform: VG400
User: mcpre
PackageName: mono-universalk9
Build: BLD_POLARIS_DEV_LATEST_20220427_001035_V17_9_0_6
CardTypes:
```

Package is bootable from media and tftp.

Package contents:

```
Package:
vg400-firmware_sm_dsp_sp2700.BLD_POLARIS_DEV_LATEST_20220427_001035_V17_9_0_6.SSA.pkg
Size: 2094140
Timestamp:
```

## Raw disk-file SHA1sum:

```
3cc7413e84187ee831a8b92fde7516ccff8f68b2
Header size: 1084 bytes
Package type: 40000
Package flags: 0
Header version: 3
```

## Internal package information:

```
Name: firmware_sm_dsp_sp2700
BuildTime: 2022-04-26_20.04
ReleaseDate: 2022-04-27_02.02
BootArchitecture: none
RouteProcessor: goldbeach
Platform: VG400
User: mcpre
PackageName: firmware_sm_dsp_sp2700
Build: BLD_POLARIS_DEV_LATEST_20220427_001035_V17_9_0_6
```

CardTypes:

Package is not bootable.

### show install active

```
install-vg400# show install active
[ R0 ] Active Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
           C - Activated & Committed, D - Deactivated & Uncommitted
```

```
-----
Type  St   Filename/Version
-----
IMG   C    17.09.01.0.5
-----
```

```
Auto abort timer: inactive
-----
```

### show install inactive

```
install-vg400# show install inactive
[ R0 ] Inactive Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
           C - Activated & Committed, D - Deactivated & Uncommitted
```

```
-----
Type  St   Filename/Version
-----
```

```
No Inactive Packages
```

### show install committed

```
install-vg400# show install committed
[ R0 ] Committed Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
           C - Activated & Committed, D - Deactivated & Uncommitted
```

```
-----
Type  St   Filename/Version
-----
IMG   C    17.09.01.0.5
-----
```

```
Auto abort timer: inactive
-----
```

### show install uncommitted

```
install-vg400# show install uncommitted
[ R0 ] Uncommitted Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
           C - Activated & Committed, D - Deactivated & Uncommitted
```

```
-----
Type  St   Filename/Version
-----
```

```
No Uncommitted Packages
```

# Troubleshooting Software Installation Using Install Commands

**Problem** Troubleshooting the software installation

**Solution** Use the following show commands to view installation summary, logs, and software versions.

- **show install summary**
- **show install log**
- **show version**
- **show version running**

**Problem** Other installation issues

**Solution** Use the following commands to resolve installation issue:

- **dir** *<install directory>*
- **more location:***packages.conf*
- **show tech-support install:** this command automatically runs the **show** commands that display information specific to installation.
- **request platform software trace archive target bootflash** *<location>*: this command archives all the trace logs relevant to all the processes running on the system since the last reload, and saves this information in the specified location.





## Configuring with the Command-Line Interface

---

- [Configuring with the Command-Line Interface, on page 40](#)

# Configuring with the Command-Line Interface

This chapter describes how to use the Cisco IOS software CLI to configure basic Cisco VG450 Analog functionality. Follow the procedures in this chapter to configure the Cisco VG450, or if you want to change the configuration after you have run the setup command facility.

This chapter does not describe every configuration possible—only a small portion of the most commonly used configuration procedures. For advanced configuration topics, refer to the respective technology configuration guides.

This chapter presents the following major topics:

## Configuring the Host Name and Password

One of the first configuration tasks you might want to do is to configure the host name and set an encrypted password. Configuring a host name allows you to distinguish a router from another. Setting an encrypted password allows you to prevent unauthorized configuration changes.

### Summary Steps

1. **enable**
2. **configure terminal**
3. **hostname 450**
4. **enable secret guessme**
5. **line con 0**
6. **exec-timeout 0 0**
7. **exit**

### Detailed Steps

#### SUMMARY STEPS

1. Router> enable
2. Router# configure terminal
3. Router(config)# hostname 450
4. Router(config)# enable secret guessme
5. Router(config)# line con 0Router(config-line)# exec-timeout 0 0
6. Router(config-line)# exit

#### DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	Router> enable  <b>Example:</b>  Password: password  <b>Example:</b>	Enables privileged EXEC mode.  • Enter your password if prompted.

	Command or Action	Purpose
	Router#	
<b>Step 2</b>	Router# configure terminal  <b>Example:</b>  Enter configuration commands, one per line. End with CNTL/Z.  <b>Example:</b>  Router(config)#	Enters global configuration mode.
<b>Step 3</b>	Router(config)# hostname 450  <b>Example:</b>	Changes the name of Cisco VG450 to a meaningful name. Substitutes the host name to Router .
<b>Step 4</b>	Router(config)# enable secret guessme	Enters an enable secret password. This password provides access to privileged EXEC mode. When you enter enable at the user EXEC prompt ( Router> ), you must enter the enable secret password to gain access to configuration mode. Substitute your enable secret password for guessme .
<b>Step 5</b>	Router(config)# line con 0 Router(config-line)# exec-timeout 0 0	Enters line configuration mode to configure the console port.  • Prevents the Cisco VG450, EXEC mode from timing out if you do not enter any information on the console screen for an extended period.
<b>Step 6</b>	Router(config-line)# exit	Exits from config-line mode and enters into the global configuration mode.

## Verifying the Host Name and Password

To verify that you configured the correct host name and password, perform the following steps:

### SUMMARY STEPS

1. Enter the **show config** command:
2. Exit global configuration mode and attempt to re-enter it using the new enable password:

### DETAILED STEPS

**Step 1** Enter the **show config** command:

**Example:**

```
Router# show config
Using 2745 out of 262136 bytes
```

```

!
version XX.X
.
.
!
hostname 450
!
enable secret 5 $1$60L4$X2JY0woDc0.kqallo0/w8/
.
.
.

```

Check the host name and encrypted password displayed near the top of the command output.

**Step 2** Exit global configuration mode and attempt to re-enter it using the new enable password:

**Example:**

```

Router# exit
.
.
.
Router con0 is now available
Press RETURN
to get started.
Router> enable
Password: guessme
Router#

```

If you are having trouble, ensure the following:

- Caps Lock is off.
- You entered the correct passwords. Passwords are case sensitive.

## Configuring a Gigabit Ethernet Interfaces

To configure a Gigabit Ethernet interface, use the configuration software provided with your Cisco VG450 or network module, if any. Otherwise, for high power and flexibility, use configuration mode (manual configuration).



**Note** Before you begin, disconnect all the WAN cables from Cisco VG450 to prevent it from running the AutoInstall process. Cisco VG450 attempt to run AutoInstall whenever you power them on if there is a WAN connection on both ends, and Cisco VG450 do not have a valid configuration file stored in NVRAM (for instance, when you add a new interface). It can take several minutes for Cisco VG450 to determine that AutoInstall is not connected to a remote TCP/IP host.

This section describes a basic configuration, including enabling the interface and specifying IP routing. Depending on your own requirements and the protocols you plan to route, you might also have to enter other configuration commands.

Before you begin configuring the interfaces, perform the following tasks:

- Connect a console to Cisco VG450.



- Power on Cisco VG450.

## SUMMARY STEPS

1. Router> enable
2. Router# configure terminal
3. Router# ip routing
4. Router(config)# interface gigabitEthernet 0/0/0
5. Router(config-if)# ip address 172.16.74.3 255.255.255.0
6. Router(config-if)# exit
7. Router(config-if)# Ctrl-z

## DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	Router> enable <b>Example:</b> Password: password <b>Example:</b> Router#	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	Router# configure terminal <b>Example:</b> Enter configuration commands, one per line. End with CNTL/Z. <b>Example:</b> Router(config)#	Enters global configuration mode.
<b>Step 3</b>	Router# ip routing <b>Example:</b> Router# ip? <b>Example:</b> ip ipc iphc-profile ipv6	Enables routing protocols as required for your global configuration. This example uses IP routing.
<b>Step 4</b>	Router(config)# interface gigabitEthernet 0/0/0 <b>Example:</b> Router(config-if)#	Enters interface configuration mode. You have entered interface configuration mode when the prompt changes to Router(config-if)#.
<b>Step 5</b>	Router(config-if)# ip address 172.16.74.3 255.255.255.0	Assigns an IP address and subnet mask to the interface.
<b>Step 6</b>	Router(config-if)# exit	Exits back to global configuration mode.

	Command or Action	Purpose
		Repeat Step 4 through Step 6 if your Cisco VG450 has more than one interface that you need to configure.
<b>Step 7</b>	Router(config-if)# Ctrl-z  <b>Example:</b>  Router#	Returns to enable mode when you finish configuring interfaces.

## TLS 1.2 support on SCCP Gateways

The TLS 1.2 support on SCCP Gateways feature details the configuration of TLS 1.2 on SCCP protocol for digital signal processor (DSP) farm including Unicast conference bridge

(CFB), Media Termination Point (MTP), and SCCP telephony control (STC) application (STCAPP).

DSP on gateways can be used as media resources for transrating or transcoding. Each media resource uses Secure Skinny Client Control Protocol (SCCP) to communicate with Cisco Unified Communications Manager. Currently SSL 3.1, which is equivalent to TLS1.0, is used for sending secure signals. This feature enhances the support to TLS 1.2. From Cisco IOS XE Cupertino 17.7.1a, TLS 1.2 is enhanced to support the Next-Generation Encryption (NGE) cipher suites.



**Note** Cisco Unified Communications Manager (CUCM) Version 14SU2 has been enhanced to support Secured SCCP gateways with the Subject Name field (CN Name) with or without colons, for example, AA:22:BB:44:55 or AA22BB4455.

CUCM checks the CN field of the incoming certificate from the SCCP Gateway and verifies it against the DeviceName configured in CUCM for this gateway. DeviceName contains MAC address of the gateway. CUCM converts the MAC address in the DeviceName to MAC address with colons (for example: AA:22:BB:44:55) and validates with the CN name in the Gateway's certificate. Therefore, CUCM mandates Gateway to use MAC address with colons for the CN field in the certificate, that is, subject name.

Due to new guidelines from Defense Information Systems Agency (DISA), it is a requirement not to use colons for the subject name field CN. For example, AA22BB4455.

### SCCP TLS connection

CiscoSSL is based on OpenSSL. SCCP uses CiscoSSL to secure the communication signals.

If a resource is configured in the secure mode, the SCCP application initiates a process to complete Transport Layer Security (TLS) handshaking. During the handshake, the server sends information to CiscoSSL about the TLS version and cipher suites supported. Previously, only SSL3.1 was supported for SCCP secure signalling. SSL3.1 is equivalent to TLS 1.0. The TLS 1.2 Support feature introduces TLS1.2 support to SCCP secure signalling.

After TLS handshaking is complete, SCCP is notified and SCCP kills the process.

If the handshaking is completed successfully, a REGISTER message is sent to Cisco Unified Communications Manager through the secure tunnel. If handshaking fails and a retry is needed, a new process is initiated.



---

**Note** For SCCP-based signalling, only TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA cipher suite is supported.

---

### Cipher Suites

For SCCP-based signaling, TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA cipher suite is supported.

From Cisco IOS XE Cupertino 17.7.1a, the following NGE cipher suites are also supported:

- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-RSA-AES256-GCM-SHA384

These cipher suites enable secure voice signaling for both STCAPP analog phone and SCCP DSPFarm conferencing service. The cipher suite selection is negotiated between GW and CUCM.

The following prerequisites are applicable for using NGE cipher suites:

- Configure TLS 1.2. For more information, see *Configuring TLS*.
- Use the CUCM Release 14.1 SU1 or later, and Voice Gateways or platforms that support TLS 1.2.
- From CUCM Web UI, navigate to Cipher Management and set the CIPHER switch as NGE. For more information, [Cipher Management](#).

For more information about verifying these cipher suites, see *Verifying TLS version and Cipher Suites*.

For the SRTP encrypted media, you can use higher-grade cipher suites: AEAD-AES-128-GCM or AEAD-AES-256-GCM. These cipher suites selection is automatically negotiated between GW and CUCM for both secure analog voice and hardware conference bridge voice media. Authenticated Encryption with Associated Data (AEAD) ciphers simultaneously provide confidentiality, integrity, and authenticity, without built-in SHA algorithms to validate message integrity.

### Supported Platforms

The TLS 1.2 support on SCCP Gateways feature is supported on the following platforms:

- Cisco VG400, VG420, and VG450 Analog Voice Gateways

### Configuring TLS version for STC application

Perform the following task to configure a TLS version for the STC application:

```
enable
configure terminal
stcapp security tls-version v1.2
exit
```



---

**Note** The stcapp security tls command sets the TLS version to v.1.0, v1.1, or v1.2 only. If not configured explicitly, TLS v1.0 is selected by default.

---

### Configuring TLS version in Secure Mode for DSP Farm Profile

Perform the following task to configure the TLS version in secure mode for DSP farm profile:

```
enable
configure terminal
dspfarm profile 7 conference security
    tls-version v1.2
exit
```



**Note** Note: The `tls` command can be configured only in security mode.

### Verifying TLS version and Cipher Suites

Perform the following task to verify the TLS version and cipher suite:

```
# show dspfarm profile 100
Dspfarm Profile Configuration

Profile ID = 100, Service = CONFERENCING, Resource ID = 2
Profile Service Mode : secure
Trustpoint : Overlord_DSPFarm_GW
TLS Version : v1.2
TLS Cipher : ECDHE-RSA-AES256-GCM-SHA384
Profile Admin State : UP
Profile Operation State : ACTIVE
Application : SCCP Status : ASSOCIATED
Resource Provider : FLEX_DSPRM Status : UP
Total Number of Resources Configured : 10
Total Number of Resources Available : 10
Total Number of Resources Out of Service : 0
Total Number of Resources Active : 0
Maximum conference participants : 8
Codec Configuration: num_of_codecs:6
Codec : g711ulaw, Maximum Packetization Period : 30 , Transcoder: Not Required
Codec : g711alaw, Maximum Packetization Period : 30 , Transcoder: Not Required
Codec : g729ar8, Maximum Packetization Period : 60 , Transcoder: Not Required
Codec : g729abr8, Maximum Packetization Period : 60 , Transcoder: Not Required
Codec : g729r8, Maximum Packetization Period : 60 , Transcoder: Not Required
Codec : g729br8, Maximum Packetization Period : 60 , Transcoder: Not Required
```

### Verifying STCAPP Application TLS version

Perform the following tasks to verify TLS version of the STCAPP application:

```
Device# show call application voice stcapp
App Status: Active
CCM Status: UP
CCM Group: 120
Registration Mode: CCM
Total Devices: 0
Total Calls in Progress: 0
Total Call Legs in Use: 0
ROH Timeout: 45
TLS Version: v1.2

# show stcapp dev voice 0/1/0
Port Identifier: 0/1/0
Device Type: ALG
Device Id: 585
```

```

Device Name:          ANB3176C85F0080
Device Security Mode : Encrypted
  TLS version         : TLS version 1.2
  TLS cipher          : ECDHE-RSA-AES256-GCM-SHA384
Modem Capability:    None
Device State:        IS
Diagnostic:           None
Directory Number:    80010
Dial Peer(s):        100
Dialtone after remote onhook feature: activated
Busytone after remote onhook feature: not activated
Last Event:          STCAPP_CC_EV_CALL_MODIFY_DONE
Line State:          ACTIVE
Line Mode:           CALL_CONF
Hook State:          OFFHOOK
mwi:                 DISABLE
vmwi:                OFF
mwi config:          Both
Privacy:             Not configured
HG Status:           Unknown
PLAR:                DISABLE
Callback State:      DISABLED
CWT Repetition Interval: 0 second(s) (no repetition)
Number of CCBs:      1
Global call info:
  Total CCB count     = 3
  Total call leg count = 6

```

```

Call State for Connection 2 (ACTIVE): TsConnected
Connected Call Info:

```

```

  Call Reference: 33535871
  Call ID (DSP): 187
  Local IP Addr: 172.19.155.8
  Local IP Port: 8234
  Remote IP Addr: 172.19.155.61
  Remote IP Port: 8154
  Calling Number: 80010
  Called Number:
  Codec:          g711ulaw
  SRTP:           on
  RX Cipher:      AEAD_AES_256_GCM
  TX Cipher:      AEAD_AES_256_GCM

```

Perform the following task to verify the sRTP cipher suite for the DSPfarm connection.

```
# show sccp connection detail
```

```

bridge-info(bid, cid) - Normal bridge information(Bridge id, Calleg id)
mmbridge-info(bid, cid) - Mixed mode bridge information(Bridge id, Calleg id)

sess_id  conn_id  call-id  codec  pkt-period  dtmf_method  type  dscp
bridge-info(bid, cid)  mmbridge-info(bid, cid)  srtplib  cryptosuite  call_ref  spid  conn_id_tx

16778224  -  125  N/A  N/A  rfc2833_pt thru  confmsp  All RTPSPI
  Callegs  All MM-MSP Callegs  N/A  N/A

16778224  16777232  126  g711u  20  rfc2833_pt thru  s- rtpspi  (101,125)
  N/A  30751576  16777219  -  AEAD_AES_256_GCM  184

16778224  16777231  124  g711u  20  rfc2833_pt thru  s- rtpspi  (100,125)
  N/A  30751576  16777219  -  AEAD_AES_256_GCM  184

```

Total number of active session(s) 1, connection(s) 2, and callegs 3

### Verifying Call Information

To display call information for TDM and IVR calls stored in the Forwarding Plane Interface (FPI), use the **showvoipfpi calls** command. You can select a call ID and verify the cipher suite using the command **show voip fpi calls confID call\_id\_number**. In this example, cipher suite 6 is AES\_256\_GCM.

```
#show voip fpi calls
Number of Calls : 2
-----
      confID correlator      AcallID      BcallID      state      event
-----
          1           1          87          88      ALLOCATED  DETAIL_STAT_RSP
          21          21          89          90      ALLOCATED  DETAIL_STAT_RSP

#show voip fpi calls confID 1
-----
VoIP-FPI call entry details:
-----
Call Type      :          TDM_IP      confID      :          1
correlator     :          1          call_state   :      ALLOCATED
last_event     :  DETAIL_STAT_RSP  alloc_start_time :      1796860810
modify_start_time:          0      delete_start_time:          0
Media Type(SideA):          SRTP      cipher suite  :          6
-----
FPI State Machine Stats:
-----
create_req_call_entry_inserted      :          1
.....
```

**Table 5: Feature Information for TLS 1.2 support on SCCP Gateways**

Feature Name	Releases	Feature Information
Support for NGE Cipher Suites	Cisco IOS XE Cupertino 17.7.1a	This feature supports NGE cipher suites for secure voice signaling and secure media. These cipher suites are applicable for both STCAPP analog phone and SCCP DSPFarm conferencing service.

## Saving Configuration Changes

To prevent the loss of the Cisco VG450 configuration, save it to NVRAM.

### SUMMARY STEPS

1. Router> enable
2. Router# copy running-config startup-config
3. Router(config-if)# Ctrl-z

## DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	Router> enable <b>Example:</b> Password: password <b>Example:</b> Router#	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	Router# copy running-config startup-config	Saves the configuration changes to NVRAM so that they are not lost during resets, power cycles, or power outages.
<b>Step 3</b>	Router(config-if)# Ctrl-z <b>Example:</b> Router# <b>Example:</b> %SYS-5-CONFIG_I: Configured from console by console	Returns to user EXEC mode.

## Enabling UC License

To enable the UC license in the Cisco VG450, perform the following steps:

## Summary Steps

1. enable
2. configure terminal
3. license accept end user agreement
4. license boot level uck9
5. exit
6. save
7. reload

## Detailed Steps

## SUMMARY STEPS

1. enable
2. configure terminal
3. license accept end user agreement
4. license boot level uck9
5. exit
6. write
7. reload

## DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b>  Router>enable	Enables privileged EXEC mode.  • Enter your password if prompted.
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b>  Router# configure terminal	Enters global configuration mode.
<b>Step 3</b>	<b>license accept end user agreement</b> <b>Example:</b>  Router(config)# license accept end user agreement	Configures a one-time acceptance of the UC license.  • Accepts UC license by typing YES.
<b>Step 4</b>	<b>license boot level uck9</b> <b>Example:</b>  Router(config)# license boot level uck9	Enables the Unified Communication License Level license.
<b>Step 5</b>	<b>exit</b> <b>Example:</b>  Router(config)# exit	Returns to privileged EXEC mode.
<b>Step 6</b>	<b>write</b> <b>Example:</b>  Router# write	Saves the configuration.
<b>Step 7</b>	<b>reload</b> <b>Example:</b>  Router# reload	Reloads the router.

## Configuring the Voice Port

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice-port** *slot/bay/port*
4. **description** *string*
5. **no shutdown**



## DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b> <pre>Router&gt; enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b> <pre>Router# configure terminal</pre>	Enters global configuration mode.
<b>Step 3</b>	<b>voice-port <i>slot/bay/port</i></b> <b>Example:</b> <pre>Router(config)# voice-port 1/0/8</pre>	Enters voice-port configuration mode.
<b>Step 4</b>	<b>description <i>string</i></b> <b>Example:</b> <pre>Router(config-voiceport)# description Voice Port One</pre>	Attaches a text string to the configuration that describes the connection for this voice port. This description appears in various displays and is useful for tracking the purpose or use of the voice port. The string argument is a character string from 1 to 255 characters in length. By default, there is no text string (describing the voice port) attached to the configuration.
<b>Step 5</b>	<b>no shutdown</b> <b>Example:</b> <pre>Router(config-voiceport)# no shutdown</pre>	Activates the voice port. If a voice port is not being used, shut down the voice port by using shutdown command.

## What to do next





## Configuring Voice Ports

---

- [Voice Ports](#), on page 54
- [Configuring FXS Ports for Supplementary Services](#) , on page 57
- [Configuring the Device Control Session Application for SIP](#), on page 59
- [Autoconfiguration for SCCP](#), on page 66

# Voice Ports

This chapter explains how to configure voice ports using the commands specific for Cisco VG450 Analog Voice Gateways and associated service modules.

This chapter contains the following topics:

## Prerequisite

Before you configure voice ports on Cisco VG450 you must establish a working IP network.

## Configuring the Voice Port

This section discuss the changes and modifications on the following commands:

For configuration examples, see *Cisco VG450 Configuration Examples*.

### loop-length

The loop-length CLI is created to configure the analog FXS voice port. It has the following format:

```
voice-port x/y/z  
[no] loop-length [long | short]
```

The loop-length CLI has the following characteristics:

- For Cisco VG450 platform, the default is short loop-length. This command is not applicable to analog FXS on motherboard slot.
- This command is applicable to all 48 FXS voice ports on SM-D-48FXS-E and the first 4 (0-3) FXS voice ports on SM-D-72FX like Cisco VG450 platform.
- The default FXS is short loop-length and long loop-length FXS needs to be configured and can be applied on motherboard NIM slots.
- The first sixteen voice ports 0/0/0-15 can be configured as long loop (OPX-lite).
- FXS voice ports on VIC 1 (0/1/0 - 0/1/23) will not support long loop. By default, they are short-loop FXS.
- Shutdown and no shutdown are required on the voice port after loop-length is configured for it to take effect.
- Because up to 2 ren is supported on long-loop (OPX-lite) FXS, when loop-length long is configured on the FXS voice port, if its existing ren configuration is greater than 2, it will be changed automatically to 2, a message "The existing ren configuration is changed to 2" is displayed on the console.
- When loop-length short is configured on the FXS voice port, if the voice port has ring dc-offset configured, the ring dc-offset configuration will be removed. A message "The existing ring dc-offset configuration is removed" is displayed on the console.

**ren**

The existing `ren` CLI under FXS voice port will accept value 1-2 for FXS voice port with loop-length long configured. For short loop-length analog FXS voice port, `ren` CLI will accept value 1-5.

**ren dc-offset**

The existing `ring dc-offset` CLI is configurable on the long loop-length FXS voice port.

**cm-current-enhance**

The existing `cm-current-enhance` CLI is configurable on the long loop-length FXS voice port.

**vmwi**

The existing `vmwi [fsk | dc-voltage]` is configurable on all on-board FXS voice ports.

## Cisco IOS Bulk Configuration

An optional bulk-configuration mechanism for voice-port and voice dial peer is available to save on time.

**group**

The `group` option is added to dial-peer CLI for dial peer bulk configuration. It has the following formats:

```
dial-peer group <tag> pots
```

```
dial-peer group <tag> pots all stcapp
```

The second command from the above list will create dial peers on all analog voice ports as `stcapp` ports by expanding it to the following three commands:

```
dial-peer group <tag> pots
service stcapp
port all
```

The `group` command is specific for `stcapp`-controlled analog ports. Therefore, only a subset of dial peer commands are supported, which are as follows:

1. `port`
2. `description`
3. `service`
4. `shutdown`
5. `preference`

The `port` subcommand specifies what ports to configure for a specific `group` command. It has the following formats:

```
port <voice port#> [ans | called | dest] <E164 address> [desc <description>]
port <voice port#> [desc <description>]
port <voice port#>
port <start voice port#>-<end port#> [ans | called | dest] <E164 address> <interval>
[desc <description>]
port <start voice port#>-<end port#> [ans | called | dest] <E164 address> [desc
<description>]
```

```
port <start voice port#>-<end port#> [desc <description>]
port <start voice port#>-<end port#>
port all [ans | called | dest] <E164 address> <interval> [desc <description>]
port all [ans | called | dest] <E164 address> [desc <description>]
port all [desc <description>]
port all
```

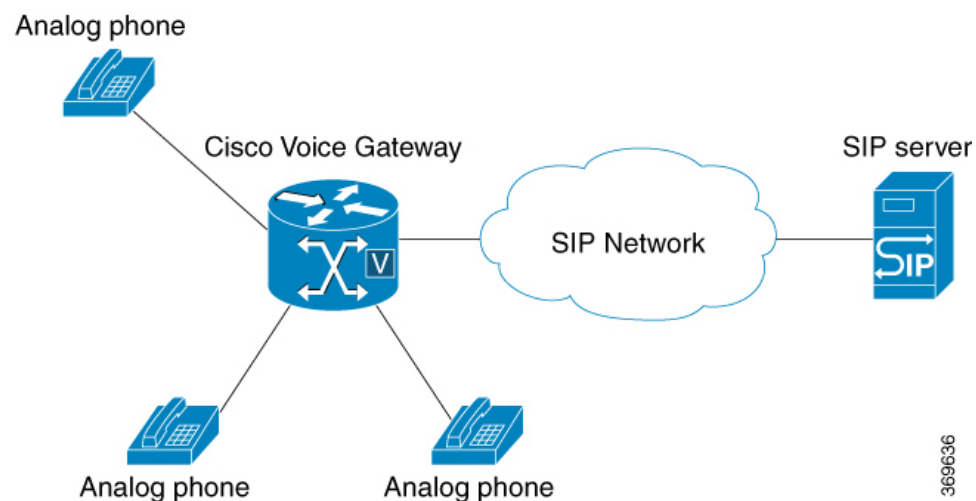
- The voice port# is composed of slot#/subunit#/port# or slot#/port#.
- The ans is the abbreviation for answer-address, which has the same meaning as the subcommand under dial-peer voice <tag> pots.
- The called is the abbreviation for incoming called-number, which has the same meaning as the subcommand under dial-peer voice <tag> pots.
- The dest is the abbreviation for description, which has the same meaning as the subcommand under dial-peer voice <tag> pots.
- The <interval> denotes the interval value of the E164 number for each adjacent port. The default is zero and the allowable value is from 1 to 100, inclusively.
- Multiple port commands are allowed and can be removed one by one with exact port specification or all at once using no port all.
- No overlay port commands are allowed. As a result, no other port commands are allowed if port all is configured.

# Configuring FXS Ports for Supplementary Services

To handle supplementary services for Foreign Exchange Station (FXS) ports, the event handler handles the hookflash or onhook events. Additionally the event handler also sends events to call control and triggers the supplementary service on SIP SPI. However, currently, FXS ports do not register to Cisco Unified Communications Manager (CUCM) as SIP endpoints. To ensure the FXS port are registered as a SIP endpoint:

- Each configured FXS ports need to register to CUCM. CUCM creates the database for proper call routing based on the registered endpoint.
- SIP stack adds or modifies SIP headers content to a proper interface with CUCM and enables new features such as directed call retrieval, call pick-up, and so on.

**Figure 3: Supplementary Services for FXS ports**



The FXS Ports for Supplementary Services feature is supported on Cisco VG450 Voice Gateway and Cisco 4461 ISR. The FXS ports for Supplementary Services supports CUCM version 12.5.1 SU1 or later.

## Call Transfer

The call transfer status includes the following concepts:

- Hookflash—A hookflash is a brief interruption in the loop as the system places the active call on hold.
- On hook—This option completes the call transfer.

The following table describes the call transfer action.

**Table 6: Supported Call Transfer Action**

State	Action	Result	Response on FXS line
Active call	Controller hookflash	Held call	Second dial tone

State	Action	Result	Response on FXS line
Held call and outgoing dialed, alerting, and active call	Controller on hook	Held call and active call transferred	Transfer

### Three-Way Conference

A three-way conference call allows three people to participate in a single phone session. The following table describes the three-way conference action.

**Table 7: Supported Three-Way Conference Action**

State	Action	Result
Active Call	First party hookflash	Held call
First party held and second party active	Active call hookflash	First and second calls are bridged
Three-way conference	Controller on hook	Both call legs torn down
Three-way conference	First called party on hook	Call between controller and first called party terminated. Call between controller and second called party remains active.
Three-way conference	Second called party on hook	Call between controller and second called party terminated, call between controller and first called party remains
Three-way conference	Controller hookflash	Call between controller and second called party terminated, call between controller and first called party remains



# Configuring the Device Control Session Application for SIP

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **application global service default dsapp**
4. **param dial-peer *number***
5. **param callWaiting *string***
6. **param callConference *string***
7. **param callTransfer *string***

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b> <b>Example:</b> <pre>Router&gt; enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b> <b>Example:</b> <pre>Router# configure terminal</pre>	Enters global configuration mode.
Step 3	<b>application global service default dsapp</b> <b>Example:</b> <pre>router(config)#application router(config-app)#global router(app-global)#service default dsapp</pre>	<p><b>(Optional)</b> Enables the new hookflash functionality globally. Device Control Session Application (DSAPP) drives these hookflash features and it must be configured for new bookflash functionality for an application framework module in IOS. DSAPP can be configured globally or on a dial-peer basis.</p> <p><b>Note</b> This is a global configuration command. After you configure this command, all the calls are impacted. Even a FXO call will be controlled by DSAPP application which can lead to a failure. If the gateway is controlled by a DSAPP application, it is not recommended to make DSAPP as the default call controller.</p>
Step 4	<b>param dial-peer <i>number</i></b> <b>Example:</b>	If multiple dial-peer matches are made for the destination-pattern, <b>dial-peer 100</b> command is used.

	Command or Action	Purpose
	<pre>router(config)#application router(config-app)#service dsapp router(app-global)#param dial-peer 100</pre>	<p><b>Note</b> When you configure DSAPP on a dial-peer basis, specify a VOIP dial-peer for any outbound call. If all outbound calls that use the hookflash functionality are on the same server, it is recommended to use the <b>param dial-peer</b> command.</p> <p>When multiple matches are possible on hookflash, enable <b>peer parameters callXXXX TRUE</b> for DSAPP to interpret hookflash to SIP supplementary service messages.</p>
<b>Step 5</b>	<p><b>param callWaiting</b> <i>string</i></p> <p><b>Example:</b></p> <pre>router(config)#application router(config-app)#service dsapp router(app-global)#param dial-peer 100 router(app-global)#param callWaiting TRUE</pre>	Enables call waiting feature.
<b>Step 6</b>	<p><b>param callConference</b> <i>string</i></p> <p><b>Example:</b></p> <pre>router(config)#application router(config-app)#service dsapp router(app-global)#param dial-peer 100 router(app-global)#param callWaiting TRUE router(app-global)#param callConference TRUE</pre>	Enables call conference feature.
<b>Step 7</b>	<p><b>param callTransfer</b> <i>string</i></p> <p><b>Example:</b></p> <pre>router(config)#application router(config-app)#service dsapp router(app-global)#param dial-peer 100 router(app-global)#param callWaiting TRUE router(app-global)#param callConference TRUE router(app-global)#param callTransfer TRUE</pre>	Enables call transfer feature.

## Configuring the Outbound Voip Dial-peer

Outbound dial-peer is configured like regular voip dial-peer for SIP. In addition to the parameters required, the following configurations are required:

- **service dsapp**—specifies that the dial-peer is controlled by DSAPP application.
- **session transport tcp**—specifies only TCP signaling is supported.
- **voice-class sip extension gw-ana**— this parameter is used to interop with CUCM
- **voice-class sip bind control source-interface GigabitEthernetx/y/z**—indicates this interface's mac address as the base mac.
- **dual tone multifrequency (DTMF)**—Specify how a Session Initiation Protocol (SIP) gateway relays dual tone multifrequency (DTMF) tones between telephony interfaces and an IP network. It supports SIP-Notify, SIP-KPML and RTP-NTE. It can be configured with any of these options.

```
dial-peer voice 714281111 voip
  service dsapp
  destination-pattern .+
  session protocol sipv2
  session target ipv4:172.16.0.
  incoming called-number 7141116...
  voice-class sip bind control source-interface GigabitEthernet0/0/0
  codec g711ulaw
```

Note- G711 is the only codec supported for conference calls. It is recommended to add this command.

```
Example for dtmf relay
dtmf-relay method1 [...[method6]]
```

```
dtmf-relay sip-noftity
dtmf-relay sip-kpml
dtmf-relay rtp-nte
```

## Configuring Pots Dial-peer

You can configure the pots dial-peer like a regular pots dial-peer for FXS. In addition to the parameters required, you have to configure the following command under **pots dial-peer** to interpret HF correctly and interop with CUCM:

- **service dsapp**—specifyies this dial-peer to be controlled by DSAPP application.
- **voice-class sip extension gw-ana**– this parameter is used to interop with CUCM.

```
dial-peer voice 19993000 pots
  service dsapp
  destination-pattern 2124506300
  voice-class sip extension gw-ana
  port 3/0/0
```

## Configuring Voice-card and SIP

When you configure the voice-card, all the traffic should go through the CUCM and the hairpin calls are not supported. You have to configure **no local-bypass** command for the voice-card that have FXS SIP endpoints.

For FXS SIP endpoints to register, configure the **registrar IP address** under the sip-ua mode and use the TCP as the transport type. UDP protocol is not supported.

```
!
voice-card 3/0
  no local-bypass
  no watchdog
!
!
sip-ua
```

```

registrar ipv4:172.16.0.0 expires 3600 tcp
protocol mode dual-stack
!

```

## Enabling Device Control Session Application Line features

To register to CUCM as a SIP endpoint, and to distinguish line feature from trunk, you should configure the **dsapp line** command.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dsapp line**

### DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b> Router# configure terminal	Enters global configuration mode.
<b>Step 3</b>	<b>dsapp line</b> <b>Example:</b> router(config)# router(config)#dsapp line router(config)#	Specifies the format of each call feature.  <b>Note</b> If you do not configure the <b>dsapp line</b> command, the gateway will act like a SIP trunk and the analog phones may not register as SIP endpoints. Also, you cannot configure the FAC. Ensure to configure the <b>dsapp line</b> command to enable the FXS for SIP supplementary services.

## Configuring Feature Access Code

The **dsapp line feature access-code** command invokes the feature to translate the Feature Access Code (FAC) to the format that the CUCM understands. If you do not configure this command, the whole FAC digits are sent to the CUCM and may not invoke features. You can also change the default FAC in the sub-mode.

Analog phones do not have soft keys. The required supplementary service features are invoked through FAC. By default, prefix of the FAC is ‘\*\*’ and it can also be changed using the CLI command.

```

router(config)#dsapp line feature access-code
router(config-dsapline-fac)#prefix *#
router(config-dsapline-fac)#cancel-call-waiting **4
router(config-dsapline-fac)#exit
router# show dsapp line feature codes
  dsapp line feature access-code
    prefix *#
    call forward all *#1
    call forward cancel *#2
    pickup local *#5
    pickup group *#7
    pickup direct *#6
    cancel-call-waiting **4
    last-redial *#3

```

If the **dsapp line feature access-code** is not configured, the voice gateway does not translate the FAC to the format that the CUCM understands. The whole FAC digits is sent to the CUCM.

After the FAC is disabled and re-enabled, all the FAC and prefix are rolled back to the default values.

```

router(config)#no dsapp line feature access-code

  Feature access-code disabled

router(config)#do show dsapp line feature codes

  dsapline feature access-code disabled

router(config)#dsapp line feature access-code
router(config-dsapline-fac)#do show dsapp line feature codes

  dsapp line feature access-code
    prefix **
    call forward all **1
    call forward cancel **2
    pickup local **5
    pickup group **7
    pickup direct **6
    cancel-call-waiting **9
    last-redial **3

router(config-dsapline-fac)#do show run | b dsapp line

dsapp line
!

dsapp line feature access-code
!

```

## Autoconfiguration

To enable the autoconfiguration, use the **ccm-manager sipana auto-config local** command. To get the XML configuration file, use the **ccm-manager config server** command to download the configuration file from the CUCM TFTP server.

```

!
ccm-manager sipana auto-config local GigabitEthernetx/y/z
!
ccm-manager config server x.x.x.x

```



**Note** For DSAPP autoconfiguration, add only the dial-peer. After the auto-config is enabled, only the dial-peers are added for each endpoint configured on CUCM.

## Verifying the Device Control Session Application Configuration

Use the following commands to verify the the DSAPP configuration:

- **show dsapp line device summary**
- **show dsapp line feature codes**
- **show ccm-manager config-download**

The **show dsapp line device summary** command shows whether the FXS ports are successfully registered to the CUCM as SIP endpoints.

```
router#show dsapp line device summary
Total Devices:          3
Port      Device      Registration  Dev   Directory  Last Number
Identifier Name      State        Type   Number     Dialed
-----
3/0/0     ANDD309DD761600 REGISTERED   ALG    2124506300 Not Avail
3/0/1     ANDD309DD761601 REGISTERED   ALG    2124506301 Not Avail
3/0/2     ANDD309DD761602 UNREGISTERED ALG    2124506302 Not Avail
router#
```

The **show dsapp line feature codes** command shows whether FAC is enabled and feature codes

```
router#show dsapp line feature codes
```

```
dsapp line feature access-code
prefix **
call forward all **1
call forward cancel **2
pickup local **5
pickup group **7
pickup direct **6
cancel-call-waiting **9
last-redial **3
```

```
router#
```

The **show ccm-manager config-download** command provides download status and history of the auto-configuration.

```
Art_Utah_73#show ccm-manager config-download
```

```
SIP Line Side Analog auto-configuration status
=====
Registered with Call Manager: Yes
Local interface: GigabitEthernet0/0/0 (2c5a.0fc8.8b70)
Current version-id: 1541004382-f60b9ac2-ce5b-439e-92e5-02b62e26d15c
Current config applied at: 16:47:40 UTC Oct 31 2018
Gateway downloads succeeded: 2
Gateway download attempts: 2
Last gateway download attempt: 16:47:40 UTC Oct 31 2018
Last successful gateway download: 16:47:40 UTC Oct 31 2018
Current TFTP server: 172.19.156.84
Gateway resets: 1
```

```
Managed endpoints: 3
Endpoint downloads succeeded: 6
Endpoint download attempts: 6
Last endpoint download attempt: 16:47:40 UTC Oct 31 2018
Last successful endpoint download: 16:47:40 UTC Oct 31 2018
Endpoint resets: 0
Endpoint restarts: 0
```

```
Configuration Error History:
```

## Autoconfiguration for SCCP

To enable autoconfiguration on CUCM controlled SCCP endpoints (STCAPP endpoints), you have to configure both CUCM and voice gateway. STCAPP gateway supports configuration downloaded from CUCM. In this scenario, you have to first configure the CUCM and then push the configurations to voice gateway so that the voice gateway can generate the associated configurations.

There are two ways to reset/reconfigure:

- Voice gateway can initiate the process and download the configuration XML file to voice gateway.

Or

- CUCM can trigger the download by sending RESET message to gateway.
  - Voice gateway starts downloading the configurations XML file.
  - In the later sections, this is referred as CUCM push configuration to voice gateway.

## Prerequisites

For autoconfiguration, voice gateway requires the following basic configuration:

- Download the autoconfiguration file from CUCM and set the configuration server to CUCM.
 

```
ccm-manager config server x.x.x.x - This is the CUCM IP address.
```
- To download the XML file, must use the *ccm-manager sccp local FastEthernet0/0* interface.
- SCCP msut specify the ethernet interface *sccp local FastEthernet0/0*

Domain Name Server (DNS) requires the following basic configuration:

- DNS IP address must be present.
 

```
ip name-server x.x.x.x - This is the DNS server IP address.
```
- If the network does not have a DNS, then configure CUCM IP address.

```
ccm x.x.x.x identifier <ccm_id> version 7.0
sccp ccm group <group_id>
associate ccm <ccm_id> priority <priority>
sccp To enable the auto-config
"ccm-manager sccp
```

- To enable STCAPP, configure the **stcapp ccm group**.

```
Stcapp ccm-group <group_id>
```

- Enable the STCAPP.

```
Stcapp
```

## STCApp Autoconfiguration

To enable autoconfiguration:



### Before you begin

- 
- Step 1** When you execute the **ccm-manager sccp** command for the first time, the autoconfiguration initiates a configuration file download request to the configuration server.
- Step 2** After the configuration file is downloaded, the XML file will be parsed to determine the following CUCM details: CUCM name, Ports configured in CUCM, and each port's network locale (translated into voice-port as *cptone*)
- Step 3** Once the CUCM name is identified, autoconfiguration will use the DNS to resolve the IP of the server. In case, if the DNS is not available, the CUCM IP address must be manually configured.
- Step 4** When CUCM adds a port in the configuration, you can go to the device (gateway) and click **ApplyConfig** which will push the configuration XML file to gateway.
- a) After the configuration XML file is pushed to the gateway, the gateway will apply the newly added port to its running configuration.
- Step 5** For the modified ports, CUCM will send a reset request to restart the port.
- Step 6** For the deleted ports, CUCM will push the new XML file to voice gateway.
- a) Voice gateway will parse it and remove the dial-peers of the deleted ports.
- Note** When you click **ApplyConfig**, there will be a service interruption for a short period of time.
- 

## Configuring STCAPP Autoconfiguration

To enable auto-configuration:

### Before you begin

Ensure that the prerequisites are configured. For more information on the prerequisites, see the [STCApp Autoconfiguration](#) section.

- 
- Step 1** After the configuration file is downloaded, voice gateway parses it. The voice gateway creates the corresponding CLIs/dial-peer running configurations.
- a) The voice port *cptone* is updated according to the network locale.
- Step 2** The voice gateway starts the SCCP and STCAPP. This ensures that the voice gateway is up and running.
- Step 3** Users can save this running configuration.
- Step 4** For voice port configuration, the initial timeout and the inter-digit timeout is set to 60 seconds. This value is set by the voice gateway and it is not downloaded from CUCM.
- Step 5** After the voice gateway is up and running, CUCM modifies the following:
- a) If a port or multiple ports are added on the CUCM, then the CUCM accesses the gateway level, and clicks **ApplyConfig**. This triggers the CUCM to push the XML file to voice gateway. The voice gateway parses it and adds the newly created ports on CUCM (including the dial-peer CLIs) .
- b) If a port is modified on the CUCM, the voice gateway will receive a message *StationReset to RESET* that port. User needs to go to the gateway level and click **ApplyConfig** to push the configuration to voice gateway. The voice gateway will update the *cptone* according to CUCM's network locale configuration
- c) If a port or multiple ports are deleted on the CUCM and if a user clicks **ApplyConfig** at the gateway level, a XML file will be pushed to voice gateway.

- Step 6** To remove a port at both CUCM and voice gateway follow these steps:
- Go to the gateway, and see if all the ports are configured.
  - Go to the port that needs to be deleted.
  - At the port level, click **Delete** and confirm to delete the port.
  - Go back to gateway level and click **Save**.
  - At the gateway level, click **ApplyConfig**.
  - After the ports are removed, an XML file is pushed to voice gateway.
  - The voice gateway will first delete all the dial-peers that are configured.
  - The voice gateway will read them all back according to the new XML file.

## STCApp Autoconfiguration Examples

This section provides the sample configuration for the STCApp autoconfiguration.

### Example: Prerequisites Configuration

This example shows the prerequisites configuration which is required if there is no DNS in the network.

```

ccm-manager config server 1.5.29.100
ccm-manager sccp local FastEthernet0/0
ccm-manager sccp
!
!
sccp local FastEthernet0/0
sccp ccm 1.5.29.100 identifier 10 version 7.0

sccp ccm group 1
  associate ccm 10 priority 1

```

### Example: STCAPP Auto-config

This example shows the console messages of the STCAPP autoconfiguration.

```

Art_224_30(config)#ccm-manager sccp
Art_224_30(config)#
Loading SKIGW0C86385E3D.cnf.xml from 1.5.29.100 (via FastEthernet0/0): !
[OK - 6559 bytes]

Translating "CUCM-10-5"

sccp ccm CUCM-10-5 identifier 1 version 4.1
      ^
% Invalid input detected at '^' marker.

Selected CCM identifier is not configured in global SCCP configuration mode;
Please configure it in global SCCP config mode and then retry.
SCCP operational state bring up is successful.
Loading AN0C86385E3D400.cnf.xml from 1.5.29.100 (via FastEthernet0/0): !
[OK - 5414 bytes]

Loading AN0C86385E3D401.cnf.xml from 1.5.29.100 (via FastEthernet0/0): !
[OK - 5414 bytes]

Loading AN0C86385E3D402.cnf.xml from 1.5.29.100 (via FastEthernet0/0): !
[OK - 5414 bytes]

```

```
*Mar  1 00:01:57.291: %SYS-5-CONFIG_I: Configured from console by console
.....
*Mar  1 00:01:57.723: %SYS-5-CONFIG_I: Configured from console by console
```

### Example: Adding Dial Peers

This example shows the added dial peers.

```
sccp local FastEthernet0/0
sccp ccm 1.5.29.100 identifier 10 version 7.0
sccp
!
sccp ccm group 1
  associate ccm 10 priority 1
!
dial-peer cor custom
!
!
dial-peer voice 999200 pots
  service stcapp
  port 2/0
!
dial-peer voice 999201 pots
  service stcapp
  port 2/1
!
dial-peer voice 999202 pots
  service stcapp
  port 2/2
```

### Example: Adding a Port

This example shows the added port. When a port is added on CUCM, the CUCM clicks **ApplyConfig** at the gateway level. The new port dial-peer is added.

```
Loading SKIGW0C86385E3D.cnf.xml from 1.5.29.100 (via FastEthernet0/0): !
[OK - 6559 bytes]

stcapp shutdown initiated... waiting for calls to clear.
stcapp shutdown complete.
Loading AN0C86385E3D400.cnf.xml from 1.5.29.100 (via FastEthernet0/0): !
[OK - 5414 bytes]

Loading AN0C86385E3D401.cnf.xml from 1.5.29.100 (via FastEthernet0/0): !
[OK - 5414 bytes]

Loading AN0C86385E3D402.cnf.xml from 1.5.29.100 (via FastEthernet0/0): !
[OK - 5414 bytes]

*Mar  1 00:20:40.999: %SYS-5-CONFIG_I: Configured from console by console
.....
*Mar  1 00:20:41.427: %SYS-5-CONFIG_I: Configured from console by console

Running Config:

dial-peer voice 999200 pots
  service stcapp
```

### Example: Modifying a Port

This example shows the modified port. When a port's setting is modified, user needs to go to gateway level and click **ApplyConfig**. The voice will parse the configuration and run the cptone configuration on the voice-port.

```

Loading SKIGW0C86385E3D.cnf.xml from 1.5.29.100 (via FastEthernet0/0): !
[OK - 6532 bytes]

stcapp shutdown initiated... waiting for calls to clear.
stcapp shutdown complete.
Loading ANOC86385E3D400.cnf.xml from 1.5.29.100 (via FastEthernet0/0): !
[OK - 5387 bytes]

Loading ANOC86385E3D401.cnf.xml from 1.5.29.100 (via FastEthernet0/0): !
[OK - 5414 bytes]

Loading ANOC86385E3D402.cnf.xml from 1.5.29.100 (via FastEthernet0/0): !
[OK - 5414 bytes]

*Mar  1 01:24:08.207: %SYS-5-CONFIG_I: Configured from console by console
.....
*Mar  1 01:24:08.627: %SYS-5-CONFIG_I: Configured from console by console
Art_224_30#

Running config:

voice-port 2/0
.....
  cptone JP
  timeouts initial 60
  timeouts interdigit 60
  timeouts ringing infinity
  caller-id enable

```

### Example: Deleting a Port

This example shows the deleted port. When a port is deleted on CUCM, and CUCM clicks **Apply Config** at the gateway level. The dial-peer associated with that port on the gateway will be removed.

Before port deletion on CUCM:

```

dial-peer voice 999200 pots
  service stcapp
  port 2/0
!
dial-peer voice 999201 pots
  service stcapp
  port 2/1
!
dial-peer voice 999202 pots
  service stcapp
  port 2/2

```

After port 2/0 deleted on CUCM:

```

!
dial-peer voice 999201 pots
  service stcapp
  port 2/1
!
dial-peer voice 999202 pots
  service stcapp
  port 2/2

```



## Support for Security-Enhanced Linux

---

- [Overview, on page 72](#)
- [Prerequisites for SELinux, on page 73](#)
- [Restrictions for SELinux, on page 74](#)
- [Information About SELinux, on page 75](#)
- [Configuring SELinux, on page 76](#)
- [Verifying SELinux Enablement, on page 79](#)
- [Troubleshooting SELinux, on page 80](#)

# Overview

Security-Enhanced Linux (SELinux) is a solution composed of Linux kernel security module and system utilities to incorporate a strong, flexible Mandatory Access Control (MAC) architecture into Cisco IOS-XE platforms.

SELinux provides an enhanced mechanism to enforce the separation of information, based on confidentiality and integrity requirements, which addresses threats of tampering and bypassing of application security mechanisms and enables the confinement of damage that malicious or flawed applications can cause.

# Prerequisites for SELinux

There are no specific prerequisites for this feature.

## Restrictions for SELinux

There are no specific restrictions for this feature.



# Information About SELinux

SELinux enforces mandatory access control policies that confine user programs and system services to the minimum privilege required to perform their assigned functionality. This reduces or eliminates the ability of these programs and daemons to cause harm when compromised (for example, through buffer overflows or misconfigurations). This is a practical implementation of principle of least privilege by enforcing MAC on Cisco IOS-XE platforms. This confinement mechanism works independently of the traditional Linux access control mechanisms. SELinux provides the capability to define policies to control the access from an application process to any resource object, thereby allowing for the clear definition and confinement of process behavior.

SELinux can operate either in **Permissive mode** or **Enforcing mode** when enabled on a system.

- In Permissive mode, SELinux does not enforce the policy, and only generates system logs for any denials caused by violation of the resource access policy. The operation is not denied, but only logged for resource access policy violation.
- In Enforcing mode, the SELinux policy is enabled and enforced. It denies resource access based on the access policy rules, and generates system logs.

From Cisco IOS XE 17.13.1a, SELinux is enabled in Enforcing mode by default on supported Cisco IOS XE platforms. In the Enforcing mode, any system resource access that does not have the necessary allow policy is treated as a violation, and the operation is denied. The violating operation fails when a denial occurs, and system logs are generated. In Enforcing mode, the solution works in access-violation prevention mode.

## Supported Platforms

From Cisco IOS XE 17.13.1a, SELinux is enabled on the following platforms:

- Cisco 1000 Series Aggregation Services Routers
- Cisco 1000 Series Integrated Services Routers
- Cisco 4000 Series Integrated Services Routers
- Cisco Catalyst 8000v Edge Software
- Cisco Catalyst 8200 Series Edge Platforms
- Cisco Catalyst 8300 Series Edge Platforms
- Cisco Catalyst 8500 and 8500L Series Edge Platforms
- Cisco VG Series Gateways: VG400, VG410, VG420, and VG450
- Cisco 1100 Terminal Services Gateway

## Configuring SELinux

There are no additional requirements or configuration steps needed to enable or use the SELinux feature in Enforcing mode.

The following commands are introduced as part of the SELinux feature:

```
set platform software selinux {default | enforcing | permissive}
platform security selinux {enforcing | permissive}
show platform software selinux
```




---

**Note** These new commands are implemented as **service internal** commands.

---

## Configuring SELinux (EXEC Mode)

Use the **set platform software selinux** command to configure SELinux in EXEC mode.

The following example shows SELinux configuration in EXEC mode:

```
Device# set platform software selinux ?

default  Set SELinux mode to default
enforcing Set SELinux mode to enforcing
permissive Set SELinux mode to permissive
```

## Configuring SELinux (CONFIG Mode)

Use the **platform security selinux** command to configure SELinux in configuration mode.

The following example shows SELinux configuration in CONFIG mode:

```
Device(config)# platform security selinux

enforcing Set SELinux policy to Enforcing mode
permissive Set SELinux policy to Permissive mode

Device(config)# platform security selinux permissive

Device(config)#
*Oct 20 21:52:45.155: %IOSXE-1-PLATFORM: R0/0:
SELINUX_MODE_PROG: Platform Selinux confinement mode downgraded to permissive!

Device(config)#
```

## Examples for SELinux

The following example shows the output for changing the mode from Enforcing to Permissive:

```
**Oct 20 21:44:03.609: %IOSXE-1-PLATFORM: R0/0:
SELINUX_MODE_PROG: Platform Selinux confinement mode downgraded to permissive!"
```

The following example shows the output for changing the mode from Permissive to Enforcing:

```

**Oct 20 21:44:34.160: %IOSXE-1-PLATFORM: R0/0:
SELINUX_MODE_PROG: Platform Selinux confinement mode upgraded to enforcing!"

```



**Note** If the SELinux mode is changed, this change is considered a system security event, and a system log message is generated.

## SysLog Message Reference

Facility-Severity-Mnemonic	%SELINUX-1-VIOLATION
Severity-Meaning	Alert Level Log
Message	N/A
Message Explanation	Resource access was made by the process for which a resource access policy does not exist. The operation was flagged, and resource access was denied. A system log was generated with information that process resource access has been denied.
Component	SELINUX
Recommended Action	<p>Contact Cisco TAC with the following relevant information as attachments:</p> <ul style="list-style-type: none"> <li>• The exact message as it appears on the console or in the system</li> <li>• Output of the <b>show tech-support</b> command (text file)</li> <li>• Archive of Btrace files from the box using the following command: <b>request platform software trace archive target &lt;URL&gt;</b></li> <li>• Output of the <b>show platform software selinux</b> command</li> </ul>

The following examples demonstrate sample syslog messages:

### Example 1:

```

*Nov 14 00:09:04.943: %SELINUX-1-VIOLATION: R0/0: audispd: type=AVC
msg=audit(1699927057.934:129): avc: denied { getattr } for pid=5899 comm="ls"
path="/root/test" dev="rootfs" ino=25839
scontext=system_u:system_r:polaris_iosd_t:s0
tcontext=system_u:object_r:admin_home_t:s0 tclass=file permissive=0

```

### Example 2:

```

*Nov 14 00:09:04.947: %SELINUX-1-VIOLATION: R0/0: audispd: t type=AVC
msg=audit(1699927198.486:130): avc: denied { write } for pid=6012 comm="echo"
path="/root/test" dev="rootfs" ino=25839

```

```
scontext=system_u:system_r:polaris_iosd_t:s0  
tcontext=system_u:object_r:admin_home_t:s0 tclass=file permissive= 0
```

## Verifying SELinux Enablement

Use the **show platform software selinux** command to view the SELinux configuration mode:

```
Device# show platform software selinux
=====
IOS-XE SELINUX STATUS
=====
SElinux Status :    Enabled
Current Mode   :    Enforcing
Config file Mode :  Enforcing
```

# Troubleshooting SELinux

If there is an instance of an SELinux violation on your device or network, please reach out to Cisco TAC with the following details:

- The message exactly as it appears on the console or in the system log. For example:

```
device#request platform software trace archive target  
flash:selinux_btrace_logs
```

- Output of the **show tech-support** command (text file)
- Archive of Btrace files from the box using the following command:  
**request platform software trace archive target <URL>**
- Output of the **show platform software selinux** command