# Cisco Unified SRST Feature Overview

This chapter describes Cisco Unified Survivable Remote Site Telephony (Cisco Unified SRST) and what it does. It also includes information about support for Cisco Unified IP Phones and Platforms, specifications, features, prerequisites, restrictions and where to find additional reference documents.



## SRST Overview

Cisco Unified SRST provides Cisco Unified CM with fallback support for Cisco Unified IP phones that are attached to a Cisco router on your local network. Cisco Unified SRST enables routers to provide call-handling support for Cisco Unified IP phones when they lose connection to remote primary, secondary, or tertiary Cisco Unified CM installations or when the WAN connection is down.

Cisco Unified CM supports Cisco Unified IP phones at remote sites attached to Cisco multiservice routers across the WAN. Before Cisco Unified SRST, when the WAN connection between a router and the Cisco Unified CM failed or when connectivity with Cisco Unified CM was lost for some reason, Cisco Unified IP phones on the network became unusable for the duration of the failure. Cisco Unified SRST overcomes this problem and ensures that the Cisco Unified IP phones offer continuous (although minimal) service by providing call-handling support for Cisco Unified IP phones directly from the Cisco Unified SRST router. The system automatically detects a failure and uses Simple Network Auto Provisioning (SNAP) technology to autoconfigure the branch office router to provide call processing for Cisco Unified IP phones that are registered with the router. When the WAN link or connection to the primary Cisco Unified CM is restored, call handling reverts to the primary Cisco Unified CM.

When Cisco Unified IP phones lose contact with primary, secondary, and tertiary Cisco Unified CM, they must establish a connection to a local Cisco Unified SRST router to sustain the call-processing capability necessary to place and receive calls. The Cisco Unified IP phone retains the IP address of the local Cisco Unified SRST router as a default router in the Network Configuration area of the Settings menu. The Settings menu supports a maximum of five default router entries; however, Cisco Unified CM accommodates a maximum of three entries. When a secondary Cisco Unified CM is not available on the network, the local

Cisco Unified SRST Router's IP address is retained as the standby connection for Cisco Unified CM during normal operation.

**Note** Cisco Unified CM fallback mode telephone service is available only to those Cisco Unified IP phones that are supported by a Cisco Unified SRST router. Other Cisco Unified IP phones on the network remain out of service until they re-establish a connection with their primary, secondary, or tertiary Cisco Unified CM.

### How Fallback Occurs

Typically, it takes three times the keepalive period for a phone to discover that its connection to Cisco Unified CM has failed. The default keepalive period is 30 seconds. If the phone has an active standby connection established with a Cisco Unified SRST router, the fallback process takes 10 to 20 seconds after connection with Cisco Unified CM is lost. An active standby connection to a Cisco Unified SRST router exists only if the phone has the location of a single Cisco Unified CM in its Unified Communications Manager list. Otherwise, the phone activates a standby connection to its secondary Cisco Unified CM.

If a Cisco Unified IP phone has multiple Cisco Unified CM in its Cisco Unified CM list, it progresses through its list of secondary and tertiary Cisco Unified CM before attempting to connect with its local Cisco Unified SRST router. Therefore, the time that passes before the Cisco Unified IP phone eventually establishes a connection with the Cisco Unified SRST router increases with each attempt to contact to a Cisco Unified CM. If each attempt to connect to a Cisco Unified CM takes about 1 minute, the Cisco Unified IP phone in question could remain offline for 3 minutes or more following a WAN link failure.

**Note**

- The time it takes for a Cisco Unified IP Phone to fall back to the SRST router can vary depending on the phone type. Phones such as the Cisco 7902, Cisco 7905, and Cisco 7912 can take approximately 2.5 minutes to fall back to the SRST mode.
- During a WAN connection failure, when Cisco Unified SRST is enabled, Cisco Unified IP phones display a message informing you that they are operating in Cisco Unified CM fallback mode. For example, the Cisco Unified IP Phone 7960G and Cisco Unified IP Phone 7940G display a "CM Fallback Service Operating" message, and the Cisco Unified IP Phone 7910 displays a "CM Fallback Service" message when operating in Cisco Unified CM fallback mode. When the Cisco Unified CM is restored, the message goes away and full Cisco Unified IP phone functionality is restored.

### Resumption of Primary Call Control

While in Cisco Unified CM fallback mode, Cisco Unified IP phones periodically attempt to re-establish a connection with Cisco Unified CM at the central office. Generally, the default time that Cisco Unified IP phones wait before attempting to re-establish a connection to a remote Cisco Unified CM is 120 seconds. The time can be changed in Cisco Unified CM by editing the Connection Monitor Duration parameter. See the "Configure SRST" chapter of the *System Configuration Guide for Cisco Unified Communications Manager*. A manual reboot can immediately reconnect Cisco Unified IP phones to Cisco Unified CM.

When a connection is re-established with Cisco Unified CM, Cisco Unified IP phones automatically cancel their registration with the Cisco Unified SRST Router. However, if a WAN link is unstable, Cisco Unified IP phones can bounce between Cisco Unified CM and Cisco Unified SRST. A Cisco Unified IP phone cannot re-establish a connection with the primary Cisco Unified CM at the central office if it is currently engaged in an active call.

### Supported Call Combinations

Cisco Unified SRST supports the following call combinations:

- SIP phone to SIP phone
- SIP phone to SCCP phone
- SIP phone to PSTN/router voice-port
- SIP phone to WAN VoIP using SIP
- SCCP phone to SIP phone
- SCCP phone to SCCP phone
- SCCP phone to PSTN/router voice-port
- SCCP phone to WAN VoIP using SIP or H.323

The following figure shows a remote site that connects to primary call control over a WAN IP connection. In this example, the WAN is down, making primary call control impossible to reach via IP networks. The SRST router acts as a fallback server, providing backup call control for IP Phones at the remote site, which can still use the PSTN for external calls, and for calls to phones that still register to the primary site.

***Figure 1: Branch Office Cisco Unifed IP Phones Connected to a Remote Central Cisco Unified Communications Manage Operating in SRST Mode***

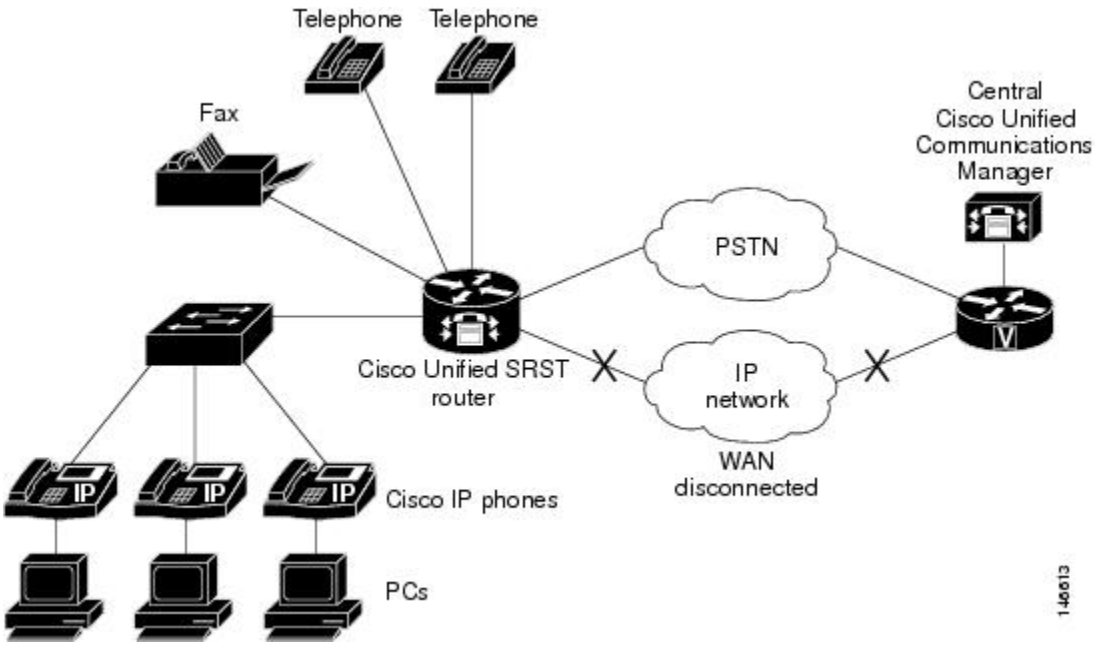


Figure 1: Branch Office Cisco Unified IP Phones Connected to a Remote Central Cisco Unified Communications Manage Operating in SRST Mode

# SRST Operating Modes

SRST can be deployed in any of the following operating modes.

- Unified SRST mode (the default operating mode)
- Enhanced SRST mode
- Webex Survivability Gateway mode

Note that you cannot run SRST in more than one of these modes at the same time. However, the basic feature set of Unified SRST support is included with both Enhanced SRST mode or Webex Survivability Gateway mode. As a result, if you enable either of these modes, your router also supports Unified SRST features.

# Unified SRST Mode

By default, SRST is running in Unified SRST mode, unless one of the other modes has been enabled. Unified SRST supports basic call failover service for SIP or SCCP endpoints. Support is for audio-only calls with base features such as Call Transfer, Conference and Music on Hold.

No specific configuration is required to enabled Unified SRST mode. Once calling services are enabled on the router, Unified SRST is configured by default. If you have one of the other operating modes enabled (Enhanced SRST or Webex Survivability Gateway mode), you can revert to Unified SRST mode by running the **default mode** command while in voice register global configuration mode.

**Note** If you enable either Enhanced SRST mode or Webex Survivability Gateway mode, your router supports the same features as Unified SRST even though the router is not running in Unified SRST mode.

# Enhanced SRST Mode

Enhanced SRST mode can be enabled by running the **mode esrst** command while in voice register global configuration mode or in telephony-service configuration mode.

Enhanced SRST mode provides the same support as Unified SRST mode, but adds advanced calling features such as:

- Video calls (local calling only)
- Shared Line
- BLF
- B-ACD
- cBarge
- Privacy on Hold
- Voice hunt group support is enhanced to include:
  - Shared Lines
  - Mixed Shared Lines (SIP and SCCP)
  - Hunt Statistics Collection
  - Mixed Deployment (SIP and SCCP)

For more information, including configuration info, see the Enhanced SRST chapter.

# Webex Survivability Gateway Mode

Webex Survivability Gateway mode provides Site Survivability for Webex Calling endpoints. If you're depoying Webex Calling, configure this mode on a gateway in the local network. This operating mode is enabled by running the **mode Webex-sgw** command while in voice register global configuration mode.

To configure Webex Survivability Gateway mode on a gateway, see the Webex article Site Survivability for Webex Calling.

### Survivability Gateway Colocation with Unified SRST

As of Cisco IOS XE 17.9.3 and Cisco IOS XE Dublin 17.11.1a onwards, you can colocate a Survivability Gateway configuration and a Unified SRST mode configuration on the same gateway. This feature lets your gateway support survivability for Webex Calling endpoints and on-premises endpoints that register to Unified Communications Manager.

To configure colocation, the gateway must be in Webex Survivability Gateway mode. Do the following:

- Complete the procedures in the preceding Webex article link to configure Webex Survivability Gateway mode on a gateway.
- Complete the procedures in the subsequent chapters of this document to configure the same gateway with Unified SRST survivability for on-premises endpoints.

### Call routing considerations for colocation

Consider the following when configuring call routing for colocation scenarios:

- The Survivability Gateway routes internal calls automatically provided that both endpoints in the call are registered to the Survivability Gateway. Internal calls are automatically routed between any registered clients (SRST or Webex Calling).
- It's possible to have a situation where the connection to one call control system goes down while the connection to the other call control system remains up. As a result, one set of endpoints registers to the Survivability Gateway while another set of endpoints at the same site registers to primary call control. In this case, you may need to route calls between the two sets of endpoints to a SIP trunk or PSTN circuit.
- External calls and E911 calls can be routed to a SIP trunk or PSTN circuit.

# Secure SRST

Secure SRST refers to security features that can be enabled for any of the SRST operating modes: Unified SRST mode, Enhanced SRST mode, or Webex Survivability Gateway mode. Secure SRST provides security features such as TLS 1.2 signaling and SRTP media using secure encryption ciphers. For SIP registrations, you can enable SIP OAuth authentication or apply a security policy that blocks nonsecure registrations, adding more security to your deployment.

**Note** TLS version 1.3 security feature is not supported for Webex Survivability Gateway operating mode.

Starting from Cisco Unified SRST 14.4 Release (Cisco IOS XE 17.14.1a), SRST security feature is enhanced to support TLS version 1.3 in addition to TLS versions 1.0, 1.1 and 1.2 and associated ciphers. It is recommended that TLS version 1.2 or 1.3 is used wherever possible to ensure security or compliance. The following functionalities are supported with secure SRST:

- The TLS exclusivity functionality enables only the configured version of TLS (1.0 or 1.1 or 1.2 or 1.3).
- In the default form, all the TLS versions 1.3, 1.2, and 1.1 are supported. However, to configure TLS v1.0, you must explicitly specify the TLS version.
- In sip-ua configuration mode, SIP SRST supports minimum TLS version functionality. You can configure the minimum TLS version only with TLS v1.2, which supports both TLS v1.2 and v1.3 cipher negotiations.

Secure SRST resolves a situation that can occur for secure Cisco IP phones during network failure situations. Secure Cisco IP phones that are located at remote sites and that are attached to gateway routers can communicate securely with Unified Communications Manager using the WAN. However, if the network connection breaks, either because of a WAN link failure, or because of a Unified Communications Manager server failure, all communication through the remote phones becomes nonsecure by default. Secure SRST overcomes this situation by providing security features that are active while the endpoints are registered to the SRST router.

Secure SRST provides authentication, integrity, and media encryption.

- Authentication provides assurance to one party that another party is whom it claims to be.
- Integrity provides assurance that the given data has not been altered between the entities.
- Encryption implies confidentiality, that is, that no one can read the data except the intended recipient.

These security features allow privacy for SRST voice calls and protect against voice security violations and identity theft.

For more information on how to configure security for SRST, see Configure Secure SRST for SCCP and SIP.

# SRST for SIP Networks

This guide describes Cisco Unified SRST functionality for SIP networks. Cisco Unified SIP SRST provides backup to an external SIP call control (IP-PBX) by providing basic registrar and redirect server or back-to-back user agent (B2BUA) services. These services are used by a SIP IP phone in the event of a WAN connection outage when the SIP phone is unable to communicate with its primary SIP proxy.

Cisco Unified SIP SRST can support SIP phones with standard RFC 3261 feature support locally and across SIP WAN networks. With Cisco Unified SIP SRST, SIP phones can place calls across SIP networks in the same way as SCCP phones.

SIP proxy, registrar, and B2BUA servers are key components of a SIP VoIP network. These servers are usually located in the core of a VoIP network. If SIP phones located at remote sites at the edge of the VoIP network lose connectivity to the network core (because of a WAN outage), they may be unable to make or receive calls. Cisco Unified SIP SRST functionality on a SIP PSTN gateway provides service reliability for SIP-based IP phones in the event of a WAN outage. Cisco Unified SIP SRST enables the SIP IP phones to continue to make and receive calls to and from the PSTN and also to make and receive calls to and from other SIP IP phones.

To see a branch office Cisco Unifed IP Phones connected to a remote central Cisco Unified CM Operating in SRST mode, see Figure Branch Office Cisco Unifed IP Phones Connected to a Remote Central Cisco Unified Communications Manage Operating in SRST Mode.

# Prerequisites for Configuring Cisco Unified SIP SRST

Before configuring Cisco Unified SIP SRST, you must do the following:

An SRST feature license is required to enable the Cisco Unified SIP SRST feature. Contact your account representative if you have further questions. For more information about Licensing on Unified SRST, refer to Licensing section in Cisco Unified SIP SRST on Cisco 4000 Series Integrated Services Router chapter.

# Restrictions for Configuring Cisco Unified SIP SRST

The following table provides a history of restrictions from Cisco SIP SRST Version 3.0 to the present version of Cisco Unified SIP SRST.

| Cisco Unified SRST Version | Cisco IOS Release | Restrictions |
|---|---|---|
| Version 8.0 | 15.1(1)T | SIP phones may be configured on the Cisco Unified CM with an Authenticated device security mode. The Cisco Unified CM ensures integrity and authentication for the phone using a TLS connection with NULL-SHA cipher for signaling. If such an Authenticated SIP phone fails over to the Cisco Unified SRST device, and if the Cisco Unified CM and SRST device are configured to support secure SIP SRST, it will register using TCP instead of TLS/TCP, thus disabling the Authenticated mode until the phone fails back to the Cisco Unified CM. |

| Cisco Unified SRST Version | Cisco IOS Release | Restrictions |
|---|---|---|
| Version 4.1 | 12.4.(15)T | |

| Cisco Unified SRST Version | Cisco IOS Release | Restrictions |
|---|---|---|
| | | • Cisco Unified SRST does not support BLF speed-dial notification, call forward all synchronization, dial plans, directory services, or music-on-hold (MOH).<br>• Prior to SIP phone load 8.0, SIP phones maintained dual registration with both Cisco Unified Communications Manager and Cisco Unified SRST simultaneously. In SIP phone load 8.0 and later versions, SIP phones use keepalive to maintain a connection with Cisco Unified SRST during active registration with Cisco Unified Communications Manager. Every two minutes, a SIP phone sends a keepalive message to Cisco Unified SRST. Cisco Unified SRST responds to this keepalive with a 404 message. This process repeats until fallback to Cisco Unified SRST occurs. After fallback, SIP phones send a keepalive message every two minutes to Cisco Unified Communications Manager while the phones are registered with Cisco Unified SRST. Cisco Unified SRST continues to support dual registration for SIP phone loads older than 8.0.<br>• Enhanced 911 Services for Cisco Unified SRST does not interface with the Cisco Emergency Responder.<br>• The information about the most recent phone that called 911 is not preserved after a reboot of Cisco Unified SRST.<br>• Cisco Emergency Responder does not have access to any updates made to the emergency call history table when remote IP Phones are in Cisco Unified SRST fallback mode. Therefore, if the PSAP calls back after the Cisco Unified IP Phones register back to Cisco Unified Communications Manager, Cisco Emergency Responder will not have any history of those calls. As a result, those calls will not get routed to the original 911 caller. Instead, the calls are routed to the default destination that is configured on Cisco Emergency Responder for the corresponding ELIN.<br>• For Cisco Unified Wireless 7920 and 7921 IP Phones, a caller's location can only be determined by the static information configured by the system administrator. For more information, see Precautions for Mobile Phones in Configuring Enhanced 911 Services.<br>• The extension numbers of 911 callers can be translated to only two emergency location identification numbers (ELINs) for each emergency response location (ERL).<br>• Using ELINs for multiple purposes can result in unexpected interactions with existing Cisco Unified SRST features. These multiple uses of an ELIN can include configuring an ELIN for use as an actual phone number (ephone-dn, voice register dn, or FXS destination-pattern), a Call Pickup number, or an alias rerouting number. For more information, see Multiple Usages of an ELIN in Configuring Enhanced 911 Services.<br>• There are a number of other ways that your configuration of Enhanced 911 Services can interact with existing Cisco Unified SRST features and cause |

| Cisco Unified SRST Version | Cisco IOS Release | Restrictions |
|---|---|---|
| | | unexpected behavior. For a complete description of interactions between Enhanced 911 Services and existing Cisco Unified SRST features, see the Interactions with Existing Cisco Unified CME Features in Configuring Enhanced 911 Services. |

| Cisco Unified SRST Version | Cisco IOS Release | Restrictions |
|---|---|---|
| Version 4.0<br>Version 3.4<br>Version 3.2<br>Version 3.1<br>Version 3.0 | 12.4(4)XC<br>12.4(4)T<br>12.3(11)T<br>12.3(7)T<br>12.2(15)ZJ<br>12.3(4)T | Not Supported<br>• MOH is not supported for a call hold invoked from a SIP phone. A caller hears only silence when placed on hold by a SIP phone.<br>• As of Cisco IOS Release 12.4(4)T, bridged call appearance, find-me, incoming call screening, paging, SIP presence, call park, call pickup, and SIP location are not supported.<br>• SIP-NAT is not supported.<br>• Cisco Unity Express is not supported.<br>• Transcoding is not supported.<br><br>Phone Features<br>• For call waiting to work on the Cisco ATA and Cisco IP Phone 7912 and Cisco Unified IP Phone 7905G with a 1.0(2) build, the incoming call leg should be configured with the G.711 codec.<br><br>**Note** Cisco Unified IP Phone 7905G, Cisco Unified IP Phone 7912G, and Cisco Analog Telephone Adaptor (ATA) 186 are not capable of dual registration; thus they are not supported and have limited functionality with Cisco Unified SIP SRST.<br><br>General<br>• Call detail records (CDRs) are only supported by standard IOS RADIUS support; CDRs are not supported otherwise.<br>• All calls must use the same codec, either G.729r8 or G.711.<br>• Calls that have been transferred cannot be transferred a second time.<br>• URL dialing is not supported. Only number dialing is supported.<br>• The SIP registrar functionality provided by Cisco Unified SIP SRST provides no security or authentication services.<br>• SIP IP phones that do not support dual concurrent registration with both their primary and their backup SIP proxy or registrar may be unable to receive incoming calls from the Cisco Unified SIP SRST gateway during a WAN outage. These phones may take a significant amount of time to discover that their primary SIP proxy or registrar is unreachable before they initiate a fallback registration to their backup proxy or registrar (the SIP SRST gateway).<br>• SIP-phone-to-SIP-trunk support requires Refer and 302/300 Redirection to be supported by the SIP trunk (Version 3.0). |

# SRST for SCCP Devices

Cisco Unified SRST provides Cisco Unified CM with fallback support for SCCP-based Cisco IP phones that are attached to a Cisco router on your local network. You can deploy SRST for SCCP phones in either of the following modes:

- Unified SRST mode
- Enhanced SRST mode

## Prerequisites for Configuring Cisco Unified SCCP SRST

Before configuring Cisco Unified SRST, you must do the following:

- An SRST feature license is required to enable the Cisco Unified SCCP SRST feature. Contact your account representative if you have further questions. For more information about Licensing on Unified SRST, refer Licensing.
- You have an account on Cisco.com to download software.

  To obtain an account on Cisco.com, go to http://www.cisco.com and click**Register** at the top of the screen.

## Restrictions for Configuring Cisco Unified SCCP SRST

The following table provides a history of restrictions from Cisco SCCP SRST Version 1.0 to the present version of Cisco Unified SCCP SRST.

| Cisco Unified SRST Version | Cisco IOS Release | Restrictions |
|---|---|---|
| Version 4.1 | 12.4.(15)T | • Enhanced 911 Services for Cisco Unified SRST does not interface with the Cisco Emergency Responder.<br>• The information about the most recent phone that called 911 is not preserved after a reboot of Cisco Unified SRST.<br>• Cisco Emergency Responder does not have access to any updates made to the emergency call history table when remote IP phones are in Cisco Unified SRST fallback mode. Therefore, if the PSAP calls back after the Cisco Unified IP phones register back to Cisco Unified Communications Manager, Cisco Emergency Responder will not have any history of those calls. As a result, those calls will not get routed to the original 911 caller. Instead, the calls are routed to the default destination that is configured on Cisco Emergency Responder for the corresponding ELIN.<br>• For Cisco Unified Wireless IP Phone 7920 and 7921, a caller's location can only be determined by the static information configured by the system administrator. For more information, see the Precautions for Mobile Phones in Configuring Enhanced 911 Services.<br>• The extension numbers of 911 callers can be translated to only two emergency location identification numbers (ELINs) for each emergency response location (ERL).<br>• Using ELINs for multiple purposes can result in unexpected interactions with existing Cisco Unified SRST features. These multiple uses of an ELIN can include configuring an ELIN for use as an actual phone number (ephone-dn, voice register dn, or FXS destination-pattern), a Call Pickup number, or an alias rerouting number. For more information, see the Multiple Usages of an ELIN in Configuring Enhanced 911 Services .<br>• There are a number of other ways that your configuration of Enhanced 911 Services can interact with existing Cisco Unified SRST features and cause unexpected behavior. For a complete description of interactions between Enhanced 911 Services and existing Cisco Unified SRST features, see the Interactions with Existing Cisco Unified CME Features in Configuring Enhanced 911 Services. |

| Cisco Unified SRST Version | Cisco IOS Release | Restrictions |
|---|---|---|
| Version 4.0<br>Version 3.4<br>Version 3.2<br>Version 3.1<br>Version 3.0<br>Version 2.1<br>Version 2.02<br>Version 2.01<br>Version 2.0 | 12.4(4)XC<br>12.4(4)T<br>12.3(11)T<br>12.3(7)T<br>12.2(15)ZJ<br>12.3(4)T<br>12.2(15)T<br>12.2(13)T<br>12.2(11)T<br>12.2(8)T1<br>12.2(8)T<br>12.2(2)XT | • All of the restrictions in Cisco SRST Version 1.0.<br>• Caller-id display on supported Cisco Unified IP phones: SIP phones in fallback mode displays the name and number of the caller. SCCP phones in fallback mode display only the caller-id number assigned to the line; the caller-ID name configuration for SCCP phones is not preserved during SRST fallback.<br><br>Call transfer is supported only on the following:<br>• VoIP H.323, VoFR, and VoATM between Cisco gateways running Cisco IOS Release 12.2(11)T and using the H.323 nonstandard information element<br>• FXO and FXS loop-start (analog)<br>• FXO and FXS ground-start (analog)<br>• Ear and mouth (E&M) (analog) and DID (analog)<br>• T1 channel-associated signaling (CAS) with FXO and FXS ground-start signaling<br>• T1 CAS with E&M signaling<br>• All PRI and BRI switch types<br><br>The following Cisco Unified IP Phone function keys are dimmed because they are not supported during SRST operation:<br>• MeetMe<br>• GPickUp (group pickup)<br>• Park<br>• Confrn (conference)<br>• Although the Cisco IAD2420 series integrated access devices (IADs) support the Cisco Unified SRST feature, this feature is not recommended as a solution for enterprise branch offices. |

| Cisco Unified SRST Version | Cisco IOS Release | Restrictions |
|---|---|---|
| Version 1.0 | 12.2(2)XB<br>12.2(2)XG<br>12.1(5)YD | • Does not support first generation Cisco Unified IP phones, such as Cisco IP Phone 30 VIP and Cisco IP Phone 12 SP+.<br>• Does not support other Cisco Unified Communications Manager applications or services: Cisco IP SoftPhone, Cisco One: Voice and Unified Messaging Application, or Cisco IP Contact Center.<br>• Does not support Centralized Automatic Message Accounting (CAMA) trunks on the Cisco 3660 routers.<br>**Note** If you are in one of the states in the United States of America where there is a regulatory requirement for CAMA trunks to interface to 911 emergency services, and you would like to connect more than 48 Cisco Unified IP phones to the Cisco 3660 multiservice routers in your network, contact your local Cisco account team for help in understanding and meeting the CAMA regulatory requirements. |

**Note** Voice VRF is not supported for SCCP SRST on Cisco Integrated Services Router Generation 2 (ISR G2).

# Supported Devices, Platform and Components

### Supported Devices, Router Platforms and Memory Specifications

Refer to *Unified SRST/E-SRST Supported Firmware, Platforms, Memory, and Voice Products* for information on:

- Supported Cisco IP Phones
- Supported router platforms
- Maximum number of IP phones, directory numbers or virtual voice ports per router
- Memory specifications per router

For support information for your release, see Compatibility Information for Unified SRST/E-SRST 14.3 Supported Firmware, Platforms, Memory, and Voice Products.

### Supported Cisco IOS Releases

For a list of Cisco IOS releases that support SRST, see Cisco Unified CME and Cisco IOS Software Version Compatibility Matrix.

**Note** Platform support for particular Cisco IOS software releases is dependent on the availability of the software images for those platforms. Software images for some platforms may be deferred, delayed, or changed without prior notice. For updated information about platform support and availability of software images for each Cisco IOS software release, see the online release notes or, if supported, Cisco Feature Navigator.

### Cisco Feature Navigator

Cisco IOS software is packaged in feature sets that are supported on specific platforms. To get updated information regarding platform support for this feature, access Cisco Feature Navigator. Cisco Feature Navigator dynamically updates the list of supported platforms as new platform support is added for the feature.

### Cisco Unified Communications Manager

For compatibility information for Cisco Unified Communications Manager, see Compatibility Matrix for Cisco Unified Communications Manager.

### Language Support

For information on supported languages and locale files, see Cisco Unified Communications Manager Express Localization Matrix.

### Interface Support with Cisco Unified Communications Manager Express and SRST

Cisco Unified Communications Manager Express and Cisco Unified SRST routers have multiple interfaces and is used for signaling and data packet transfers. The two types of interfaces available on a Cisco router include the physical interface and the virtual interface. The types of physical interfaces available on a router depend on its interface processors or port adapters. Virtual interfaces are software-based interfaces that you create in the memory of the networking device using Cisco IOS commands. To configure a virtual interface for connectivity, use the Loopback Interface for Cisco Unified Communications Manager Express and Cisco Unified SRST.

Cisco Unified Communications Manager Express and Cisco Unified SRST supports the following interfaces:

- Gigabit Ethernet Interface (IEEE 802.3z) (**interface gigabitethernet**)
- Loopback Interface (interface loopback)
- Fast Ethernet Interface (interface fastethernet)

### Signal Support

Cisco Unified SRST supports FXS, FXO, T1, E1, and E1 R2 signals.

### Switch Support

Cisco SRST 3.2 and later versions support all PRI and BRI switches including the following:

- basic-1tr6
- basic-5ess
- basic-dms100

- basic-net3
- basic-ni
- basic-ntt NTT switch type for Japan
- basic-ts013
- primary-4ess Lucent 4ESS switch type for the United States
- primary-5ess Lucent 5ESS switch type for the United States
- primary-dms100 Northern Telecom DMS-100 switch type for the United States
- primary-net5 NET5 switch type for the United Kingdom, Europe, Asia, and Australia
- primary-ni National ISDN switch type for the United States
- primary-ntt NTT switch type for Japan
- primary-qsig QSIG switch type
- primary-ts014 TS014 switch type for Australia (obsolete)

# Where to Go Next

The next chapters of this book describe how to configure Cisco Unified SIP SRST. As shown in the following table, each chapter takes you through tasks in the order in which they need to be performed. The first task for configuring Cisco Unified SRST is to ensure that the basic software and hardware in your system are configured correctly for Cisco Unified SRST.

| Task | Where Task Is Described |
|---|---|
| **7**. Setting up a Cisco Unified SRST system to communicate with your network | Setting Up the Network |
| **8**. Configuring Version 4.1 features | Cisco Unified SIP SRST 4.1 |
| **9**. Setting up the basic Cisco Unified SRST phone configuration using SCCP | Setting Up Cisco Unified IP Phones using SCCP |
| **10**. Providing a backup to an external SIP call control (IP-PBX) by supplying basic registrar services | Setting Up Cisco Unified IP Phones using SIP |
| **11**. Configuring incoming and outgoing calls | Configuring Call Handling |
| **12**. Configuring optional security for SRST | Configuring Secure SRST for SCCP and SIP |
| **13**. Setting up voicemail | Integrating Voicemail with Cisco Unified SRST |
| **14**. Setting up video parameters | Setting Video Parameters |
| **15**. Monitoring and maintaining Cisco Unified Survivable Remote Site Telephony (SRST) | Monitoring and Maintaining Cisco Unified SRST |

# Related Documents and References

### Related Documents

| Related Topic | Documents |
|---|---|
| Cisco IOS voice product configuration | • Cisco IOS Voice Configuration Library<br>• Cisco IOS Voice Command Reference<br>• Cisco IOS Debug Command Reference<br>• Cisco IOS Tcl IVR and VoiceXML Application Guide<br>• Cisco IOS Survivable Remote Site Telephony Version 3.2 System Administrator Guide |
| Configuring SRST and MGCP Fallback | • Configuring MGCP Gateway Support for Cisco Unified Communications Manager<br>• MGCP Gateway Fallback Transition to Default H.323 Session Application<br>• Configuring SRS Telephony and MGCP Fallback |
| Cisco Unified Communications Manager user documentation | • Cisco Unified Communications Manager<br>• Cisco Unified Communications Manager Security Guide<br>• Cisco Unified Communications Operating System Administration Guide |
| Cisco Unified IP Phones | • Cisco 7900 Series Unified IP Phones End-User Guides<br>• Cisco IP Phone Authentication and Encryption for Cisco Communications Manager<br>• Cisco Unified IP Phone 7970 Series Administration Guide for Cisco Unified CallManager, Release 5.0 (for models 7970G and 7971G-GE) (SCCP), "Understanding Security Features for Cisco IP Phones" section. |
| Cisco Unified SRST commands and specifications | • Cisco Unified SRST and Cisco Unified SIP SRST Command Reference (All Versions)<br>• Cisco Unified SRST 8.0 Supported Firmware, Platforms, Memory, and Voice Products<br>• Cisco Unified SRST 4.3 Supported Firmware, Platforms, Memory, and Voice Products |

| Related Topic | Documents |
|---|---|
| Cisco Security Documentation | • Media and Signaling Authentication and Encryption Feature for Cisco IOS MGCP Gateways<br>• Cisco IOS Certificate Server<br>• Manual Certificate Enrollment (TFTP and Cut-and-Paste)<br>• Certification Authority Interoperability Commands<br>• Certificate Enrollment Enhancements |
| Cisco SIP SRST V3.4: Cisco IOS SIP Survivable Remote Site Telephony Feature Roadmap | • Cisco IOS SIP SRST Feature Roadmap |
| Cisco SIP functionality | • Cisco IOS SIP Configuration Guide |
| Cisco SRST command reference | • Cisco IOS Survivable Remote Site Telephony Version 3.2 Command Reference |
| Command reference information for voice and telephony commands | • Cisco IOS Voice Command Reference<br>• Cisco IOS Debug Command Reference |
| DHCP | • Cisco IOS DHCP Server |
| Media Inactive Call Detection | • Media Inactive Call Detection |
| Phone documentation for Cisco Unified SRST | • Cisco Unified IP Phones 7900 Series<br>• Survivable Remote Site Telephony |
| Standard Glossary | • Cisco IOS Voice Configuration Library Glossary |
| Standard Preface | • Cisco IOS Voice Configuration Library Preface |

### Standards

| Standard | Title |
|---|---|
| ITU X. 509 Version 3 | Public-Key and Attribute Certificate Frameworks |

### MIBs

| MIB | MIBs Link |
|---|---|
| No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature. | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br>http://www.cisco.com/go/mibs |

### RFCs

| RFC | Title |
|---|---|
| RFC2246 | The Transport Layer Security (TLS) Protocol Version 1.0 |
| RFC 2543 | SIP: Session Initiation Protocol |
| RFC 3261 | SIP: Session Initiation Protocol |
| RFC3711 | The Secure Real-Time Transport Protocol (SRTP) |

### Technical Assistance

| Description | Link |
|---|---|
| The Cisco Technical Support & Documentation website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content. | http://www.cisco.com/techsupport |

### Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.