Cisco Unified SIP SRST on Cisco 4000 Series Integrated Services Router

This chapter describes the support for Unified SIP SRST on the Cisco 4000 Series Integrated Services platform.

Note
Unified SRST 12.6 on Cisco IOS XE Gibraltar 16.11.1a Release is not a recommended release version for call flows that include Multicast Music On Hold.

Contents

- Overview, page 34
- Platform and Memory Support, page 34
- Cisco IOS Software Releases that Support Unified SRST, page 34
- Feature Support, page 36
- Unified IP Phone Support, page 37
- Cisco Unified Communications Manager Compatibility, page 38
- Supported PSTN Trunk Connectivity, page 38
- Language Support, page 39
- Switch Support, page 39
- Interface Support for Unified SRST, page 39
- Simple Network Management Protocol (SNMP) Support for Unified SRST, page 40
- Licensing, page 40
- Configure SIP Registrar Functionality for SIP Phones on Unified SRST, page 44
- Unified SRST, Unified E-SRST, and Unified Secure SRST Password Policy, page 57
- Toll Fraud Prevention for SIP Line Side on Unified SRST, page 60
- IPv6 Support for Unified SRST SIP IP Phones, page 67
- Configure Unified SRST on Cisco 4000 Series Integrated Services Platform, page 73
- Configure Voice Hunt Groups on Unified SRST, page 77
- Configure Feature Support on Unified SIP SRST, page 80
Overview

This chapter describes Unified SRST functionality on Cisco 4000 Series Integrated Services Routers for SIP phones. Unified SIP SRST provides backup to Unified Communications Manager when the IP connectivity to Unified Communications Manager is down.

Cisco Unified SIP SRST supports the following during a WAN outage:

- Basic Registration of SIP phones.
- Basic call support on SIP phones.
- Basic supplementary services such as Call Transfer, MOH, and Conference
- SIP phone to SIP phone
- SIP phone to PSTN / router voice-port
- SIP phone to Skinny Client Control Protocol (SCCP) phone
- SIP phone to WAN VoIP using SIP

Platform and Memory Support

From Unified SRST Release 10.0 (Cisco IOS Release 15.3(3)M), Unified SIP SRST is supported on the Cisco 4000 Series Integrated Services platform. As part of the Cisco IOS Release 15.3(3)M Release, support was introduced on the Cisco 4451-X Integrated Services Router. From Unified SRST Release 10.5 (Cisco IOS Release 15.4(3)M, 15.4(3)S), SIP SRST is supported on all Cisco 4000 Series Integrated Services Routers.

The following Cisco 4000 Series Integrated Services Router platforms are supported:

- Cisco ISR 4321 Integrated Services Routers
- Cisco ISR 4331 Integrated Services Routers
- Cisco ISR 4351 Integrated Services Routers
- Cisco ISR 4431 Integrated Services Routers
- Cisco ISR 4451 Integrated Services Routers

For more information on Platform and Memory Support, see Compatibility Information.

Cisco IOS Software Releases that Support Unified SRST

For information on the Unified SRST Release and the corresponding IOS Software, see Unified CME, Unified SRST, and Cisco IOS Software Version Compatibility Matrix for related compatibility information.
Install Cisco IOS Software

To verify that the recommended software is installed on the Cisco router and if necessary, download and install a Cisco IOS Voice or higher image, perform the following steps.

**Before You Begin**
- The Cisco router is installed including sufficient memory, all Cisco voice services hardware, and other optional hardware.

### SUMMARY STEPS

1. Identify which Cisco IOS software release is installed on router.
2. Determine whether the Cisco IOS release supports the recommended Unified SRST.
3. Download and extract the recommended Cisco IOS IP Voice or higher image to flash memory
4. Use the `reload` command to reload the Unified SRST router with the new software.

### DETAILED STEPS

**Step 1** Identify which Cisco IOS software release is installed on router. Log in to the router and use the `show version` EXEC command.

**Example:**
```
Router> show version
Cisco Internetwork Operating System Software
IOS (tm) 12.3 T Software (C2600-I-MZ), Version 12.3(11)T, RELEASE SOFTWARE
```

**Step 2** Compare the Cisco IOS release installed on the Cisco router to the information in the *Cisco Unified CME, Unified SRST, and Cisco IOS Software Version Compatibility Matrix* to determine whether the Cisco IOS release supports the recommended Unified SRST.

**Step 3** If necessary, download and extract the recommended Cisco IOS IP Voice or higher image to flash memory in the router.


**Step 4** To reload the Unified SRST router with the new software after replacing or upgrading the Cisco IOS release, use the `reload` privileged EXEC command.

**Example:**
```
Router# reload

System configuration has been modified. Save [yes/no]: y
Building configuration...
OK
Proceed with reload? Confirm.
11w2d: %Sys-5-RELOAD: Reload requested by console. Reload reason: reload command.
```
System bootstrap, System Version 12.2(8r)T, RELEASE SOFTWARE (fc1)
...
Press RETURN to get started.
...
Router>

Feature Support

The following features are known to be supported for Unified SIP SRST on Cisco 4000 Series Integrated Services Platform:

- Auto-answer (If enabled on Unified Communications Manager)
- Alert/Semi-Consult/Attended/Consult Transfer
- Ad-hoc Software Conference
- Hold or Resume
- Headset Answer
- Caller ID Display
- Call Forward to Voice Hunt Group
- Call Transfer to a Voice Hunt Group
- Voicemail
- Message Waiting Indicator (MWI)
- Do Not Disturb (DND)
- DTMF
- Feature Button or Programmable Line Key (PLK) - If enabled on Unified Communications Manager
- Key Expansion Module (KEM - Supported only on the 8851/8851NR/8861 phones)
- Bulk Registration Support
- Enabling or Disabling KPML
- Alias Feature
- Call Forward (All, Busy, No Answer, Mailbox)
- Call Forward All Softkey on Phone
- Unicast MOH
- Audio codecs (G.722, G.711, G.729, iLBC)
- Translation Profile
- Conference Blocking
- Transfer Blocking
- COR
- Voice Class Codec
- SNMP/MIB (Supported only to get mode and number of registered phones)
• Speed Dial (If enabled on Unified Communications Manager)
• Call Waiting (If enabled on Unified Communications Manager)
• Forced Authorization Code
• Redial
• Speakerphone (Dialing, Answering)
• System Message
• After Hours
• SSH to Phone
• Span to PC (except Cisco IP Phone 8831)
• Web Access to Phone
• Voice Hunt Group (Support for Parallel, Sequential, Peer, and Longest-Idle hunt groups). Basic features such as Call, Hold or Resume are only supported.)

Restrictions of Unified SRST on Cisco 4000 Series Integrated Services Routers

• Multicast MOH for SIP is not supported on the Cisco 4000 Series Integrated Services Routers.
• Transcoding is not supported on the Unified SRST.
• Multi-VRF is supported only on the Cisco Integrated Services Routers Generation 2 (ISR G2). Voice VRF is not supported for SCCP SRST on Cisco Integrated Services Router Generation 2 (ISR G2).
• Shared lines and Mixed shared lines are not supported on the Unified SRST (supported on the Unified E-SRST).
• Privacy (on hold) is not supported on the Unified SRST (supported on the Unified E-SRST).
• SNMP/MIB support is restricted to fetching information on mode and number of registered phones.
• Unified SRST supports only the basic voice hunt group features. To configure advanced voice hunt group features, you must deploy the Cisco Unified Enhanced Survivable Remote Site Telephony.
• Video Calling is not supported on Unified SIP SRST.

Unified IP Phone Support

Unified SIP SRST on Cisco 4000 Series Integrated Services Platform is supported on the following phone series:
• Cisco IP Phone 7800 Series
• Cisco IP Phone 8800 Series

For IPv6 Support on Unified SRST, all the legacy IP Phones and Voice Gateways must be converted or reconfigured to IPv4-Only SIP signaling from SCCP signaling, if applicable.
Cisco Unified Communications Manager Compatibility

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

Installing Cisco Unified Communications Manager

When installing Cisco Unified Communications Manager, consider the following:

- See the installation instructions for your version in the Cisco Unified Communications Manager Install and Upgrade Guides.
- Integrate Cisco Unified SRST with Cisco Unified Communications Manager. Integration is performed from Cisco Unified Communications Manager. See the Integrating Cisco Unified SIP SRST with Cisco Unified Communications Manager section.

Integrating Cisco Unified SIP SRST with Cisco Unified Communications Manager

The procedure for integrating Unified SRST with Cisco Unified Communications Manager is as follows:

For Cisco Communications Manager integration with Unified SIP SRST, you must create an SRST reference and apply it to a device pool. An SRST reference is the IP address of the Cisco Unified SRST Router.

**Step 1** Create an SRST reference.

a. From any page in Cisco Unified Communications Manager, click System and SRST.

b. On the Find and List SRST References page, click Add a New SRST Reference.

c. On the SRST Reference Configuration page, enter a name in the SRST Reference Name field and the IP address of the Cisco SRST router in the IP Address field.

d. Click Insert.

**Step 2** Apply the SRST reference or the default gateway to one or more device pools.

a. From any page in Cisco Unified Communications Manager, click System and Device Pool.

b. On the Device Pool Configuration page, click the required device pool icon.

c. On the Device Pool Configuration page, choose an SRST reference or “Use Default Gateway” from the SRST Reference field’s menu.

Supported PSTN Trunk Connectivity

Unified SRST is supported on SIP trunks. Also, Unified SIP SRST supports the following trunk types:

- FXO/FXS
- Basic Rate ISDN
- Primary Rate ISDN (T1 or E1)
Language Support

For information on language support, see *Localization Matrix*.

Switch Support

Unified SRST supports 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)

Interface Support for Unified SRST

Unified SRST routers have multiple interfaces that are 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 type of physical interfaces available on a router depends 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, you can use the Loopback Interface for Unified SRST.

The following interfaces are supported on Unified SRST:

- Gigabit Ethernet Interface (IEEE 802.3z) (*interface gigabitethernet*)
- Loopback Interface (*interface loopback*)
- Fast Ethernet Interface (*interface fastethernet*)
Simple Network Management Protocol (SNMP) Support for Unified SRST

Unified SRST supports Simple Network Management Protocol (SNMP) Management Information Base (MIBs) for monitoring the product status. Unified SRST Release 12.6 and later versions is SNMP Version 3 (SNMPv3) compliant. The following is the main SNMP MIB supported by Unified SRST:

- CISCO-SRST-MIB

For information on configuration of SNMP version 3 on Unified SRST router, see SNMP Configuration Guide.

Licensing

Cisco Unified SRST Permanent License

When you purchase a Cisco Unified SRST permanent license, the permanent license is installed on the device when the product is shipped to you. A permanent license never expires and you will gain access to that particular feature set for the lifetime of the device across all IOS release. If you purchase a permanent license for Cisco Unified SRST, you do not have to go through the Evaluation Right to Use and Right To Use (RTU) licensing processes for using the features. If you want to purchase a CME-SRST license for your existing device, you have to go through the RTU licensing process for using the features. There is no change in the existing process for purchasing the license.

The Cisco Unified SRST permanent license is available in the form of an XML cme-locked3 file. You must get the XML file and load it in the flash memory of the device. To install the permanent license from the command prompt, use the `license install flash0:cme-locked3` command. The `cme-locked3` is the XML file of the license.

Cisco Smart License

From Release 12.1 onwards, Unified SRST supports Smart Licensing, apart from the existing CSL licensing model. Smart Licensing is supported only on Cisco 4000 Series Integrated Services Router. Depending on the technology package available on the router, licenses such as UCK9 and Security are supported using Smart Licensing.

Smart Software Licensing is Cisco's new licensing model that gives you visibility into license ownership and consumption. Smart licenses is managed by a cloud-based deployment model, namely Cisco Smart Software Manager (CSSM), or an on-prem software, Smart Software Manager satellite. Unified SRST supports both CSSM and satellite. Your access to the customer Smart Account residing on CSSM is authenticated using valid Cisco credentials. With the Smart Licensing support for Unified SRST, your device can register with CSSM or Cisco Smart Software Manager satellite. You can access your Licenses at the Cisco Software Central.
Unified SRST must register with CSSM or Cisco Smart Software Manager satellite to report license consumption. You can register Unified SRST to a Virtual Account within a Smart Account by generating a token ID from it, and pasting it to the underlying platform, Cisco 4000 Series Integrated Services Router. Once the token is generated, it can be used to register many other product instances in your network.

On the Unified SRST router, you need to ensure that the call home feature is not disabled. Also, Smart Licensing must be enabled at the router using the CLI command `license smart enable`. Use the no form of the command to disable Smart Licensing.

For more information on configuring Smart Licensing in your router, see Cisco 4000 Series ISRs Software Configuration Guide. For more information on configuring Call Home for your devices, see Configure Call Home, page 42. Once Smart Licensing is enabled, the router enters a 90-day evaluation period that persists until it registers to CSSM or the Cisco Smart Software Manager satellite.

You can register the router to CSSM or Cisco Smart Software Manager satellite with the token ID. To register the device (Unified SRST router) with CSSM or Cisco Smart Software Manager satellite, use the CLI command `license smart register idtoken`. For information on registering the device with CSSM, see Device Registration, Software Activation Configuration Guide, Cisco IOS Release 15M&T.

Upon successful registration, Unified SRST is in Registered status. As part of the registration process, the router sends an authorization request, indicating the number of phone endpoints defined by the `max-pool`, for SIP SRST, and `max-ephone`, for SCCP SRST. Based on the licenses in the Smart Account, CSSM or Cisco Smart Software Manager satellite responds with one of the defined statuses such as Authorized (using less than or equal to the number of licenses provisioned in CSSM or Cisco Smart Software Manager satellite) or Out-of-Compliance (using more than it has licenses for).

The license limit on Unified SRST is restricted by the maximum platform limit defined for the Unified SRST router (a cumulative sum of phones configured under `max-pool` and `max-ephone`). Hence, the license usage count cannot exceed the platform limit set for the Unified SRST router even when the cumulative sum of phones configured under `max-pool` and `max-ephone` exceeds the defined platform limit. For more details on the platform limit defined for Unified SRST, see Cisco Unified SRST/E-SRST 12.1 Supported Firmware, Platforms, Memory, and Voice Products.

CSSM or Smart Software Manager satellite reports license consumption submitted by the platform in its User Interface (UI), and subtracts it from the available licenses in the Virtual Account within the Smart Account. Unified SRST supports only one license entitlement to validate phones configured on Unified SRST.

**SRST_EP** —This license type supports all phones configured on Unified SRST.

---

**Note**

The SRST_EP license count reflects the total phone count of both the ephones and pools that are configured in the Unified SRST irrespective of whether the phones are registered or not.

Unified SRST sends an authorization request when a license consumption changes or every 30 days to let CSSM or Cisco Smart Software Manager satellite know it’s still available and communicating. The ID certificate issued to identify Unified SRST at time of registration is valid for one year, and is automatically renewed every six months.

---

**Note**

If the router does not communicate with CSSM or Cisco Smart Software Manager satellite for 90 days, the license authorization expires. When the license authorization expires, the devices registered on Unified SRST change status to Out of Compliance.
The license count is evaluated for the number of phones configured across the routers. The CSSM Licenses page reflects the total license count usage. The total number of licenses available for a type of license (Quantity), number of licenses currently used (In Use), and the number of unused or over-used licenses (Surplus or Shortage). If you do not have enough Cisco Smart licenses, you are in Out-of-Compliance state.

For example, consider a smart account in CSSM with 50 SRST_EP licenses. If you have a registered Unified SRST with 20 phones configured, the CSSM licenses page reflects Quantity as 50, In Use as 20, and Surplus as 30. For more information on Smart Software Manager, see Cisco Smart Software Manager User Guide.

For more information on switching between CSL and Cisco Smart License, see Licensing Modes, page 43.

The license entitlement for Unified SRST smart license is displayed on the router as follows:

```
Router# show license summary
Smart Licensing is ENABLED

Registration:
  Status: REGISTERED
  Smart Account: ABC
  Virtual Account: XYZ
  Export-Controlled Functionality: Not Allowed
  Last Renewal Attempt: None
  Next Renewal Attempt: Jun 07 12:08:10 2017 UTC

License Authorization:
  Status: AUTHORIZED
  Last Communication Attempt: SUCCESS
  Next Communication Attempt: Apr 13 07:11:48 2017 UTC

License Usage:

<table>
<thead>
<tr>
<th>License</th>
<th>Entitlement tag</th>
<th>Count</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>regid.2014-12.com.ci...</td>
<td>{ISR_4351_UnifiedCommun..}</td>
<td>1</td>
<td>AUTHORIZED</td>
</tr>
<tr>
<td>regid.2016-10.com.ci...</td>
<td>{SRST_EP}</td>
<td>4</td>
<td>AUTHORIZED</td>
</tr>
</tbody>
</table>
```

### Configure Call Home

To configure the call home destination address and proxy server details for the HTTP proxy request, perform the following steps.

**Prerequisites**

- Cisco Smart Software Licensing is enabled.

**SUMMARY STEPS**

1. `configure terminal`
2. `call-home destination address http url`
3. `call-home http-proxy proxy_address port port number`
4. `end`
DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enters configuration mode.</td>
</tr>
<tr>
<td>Example: Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2 call-home destination address http url</td>
<td>Defines the destination URL to which Call Home messages, including licensing requests are sent. The destination URL can be the URL for Transport Gateway or CSSM satellite. The URL to the Cisco Smart Licensing production server is set by default.</td>
</tr>
<tr>
<td>Example: Router(config)# call-home destination address http <a href="http://10.22.183.117:8080/ddce/services/DDCEService">http://10.22.183.117:8080/ddce/services/DDCEService</a></td>
<td></td>
</tr>
<tr>
<td>Step 3 call-home http-proxy proxy_address port port number</td>
<td>Specifies the proxy server for the HTTP request.</td>
</tr>
<tr>
<td>Example: Router(config)# call-home http-proxy 7.7.7.7 port 3218</td>
<td></td>
</tr>
<tr>
<td>Step 4 end</td>
<td>Exits to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Router(config)# end</td>
<td></td>
</tr>
</tbody>
</table>

Licensing Modes

From Unified SRST 12.1 onwards, both CSL and Smart Licensing modes are supported. That is, you can continue with CSL by not enabling Smart Licensing. Alternatively, they can enable Smart Licensing and decide later to go back to CSL by disabling Smart Licensing with the no license smart enable command. When you switch to CSL from the Smart Licensing mode, you must ensure that the End User License Agreement (EULA) is signed. CSL is not supported unless the EULA is signed. Use the CLI command license accept end user agreement in global configuration mode to configure EULA.

To verify the status of the license issued to phones registered on Unified SRST, you can use the show license command.

Router#show license ?
all Show license all information
status Show license status information
summary Show license summary
tech Show license tech support information
udi Show license udi information
usage Show license usage information
Restrictions

- For the Unified SRST license, the UCK9 technology package must be available if the Collaboration Professional Suite package is not installed.

To purchase a license, go to http://www.cisco.com/cgi-bin/tablebuild.pl/ip-key. To activate cme-srst feature license, see the Activating CME-SRST Feature License document.

Configure SIP Registrar Functionality for SIP Phones on Unified SRST

Session Initiation Protocol (SIP) registrar functionality in Cisco IOS software is an essential part of Cisco Unified SIP Survivable Remote Site Telephony (SRST). According to RFC 3261, a SIP registrar is a server that accepts Register requests.

Unified SIP SRST provides backup to Cisco Unified Communications Manager. The registrar functionality is configured on the Unified SRST gateway so as to assist fallback of endpoints to Unified SRST from Unified Communications Manager.

These services are used by a SIP IP phone if there is a WAN connection outage, and the SIP phone is unable to communicate with its primary SIP call control (IP-PBX). The Unified SIP SRST device also provides PSTN gateway access for placing and receiving PSTN calls.

SUMMARY STEPS

1. enable
2. configure terminal
3. voice service voip
4. allow-connections sip to sip
5. sip
6. registrar server [expires [max sec] [min sec]]
7. end

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Configure Back up Registrar Service to SIP Phones

Backup registrar service to SIP IP phones can be provided by configuring a voice register pool on SIP gateways. The voice register pool configuration provides registration permission control and can be used to configure some dial-peer attributes that are applied to the dynamically created VoIP dial peers when SIP phone registrations match the pool. The following call types are supported:

- SIP IP phone to or from:
  - Local PSTN
  - Local analog FXS phones

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 3</strong></td>
<td>voice service voip</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config)# voice service voip</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>allow-connections sip to sip</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-voi-srv)# allow-connections sip to sip</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>sip</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-voi-srv)# sip</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>registrar server [expires [max sec] [min sec]]</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(conf-serv-sip)# registrar server expires max 600 min 60</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>end</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(conf-serv-sip)# end</td>
</tr>
</tbody>
</table>

#### Note
Ensure that the registration expiration timeout is set to a value smaller than the TCP connection aging timeout to avoid disconnection from the TCP.

- **expires** (Optional) Sets the active time for an incoming registration.
- **max sec** (Optional) Maximum expiration time for a registration, in seconds. The range is from 600 to 86400. The default is 3600.
- **min sec** (Optional) Minimum expiration time for a registration, in seconds. The range is from 60 to 3600. The default is 60.
Configure SIP Registrar Functionality for SIP Phones on Unified SRST

- Local SIP IP phone

The commands in the configuration provide registration permission control and set up a basic voice register pool. The pool gives users control over which registrations are accepted by a Cisco Unified SIP SRST device and which can be rejected. Registrations that match this pool create VoIP SIP dial peers with the dial-peer attributes set to these configurations. Although only the `id` command is mandatory, this configuration example shows basic functionality.

Prerequisites

- The SIP registrar must be configured before a voice register pool is set up.

Restrictions

- The `id` command identifies the individual SIP IP phone or sets of SIP IP phones that are to be configured. Thus, the `id` command configured in Step 5 is required and must be configured before any other voice register pool commands. For Unified SRST, it is recommended to configure `id ip/network/device-id-name` and avoid using `id mac`.

Note: It is recommended that `id mac` command is not configured for Unified SRST, as the phones falling back from Unified Communications Manager to Unified SRST do not mostly fall back on the same network.

Note: The command `proxy` described in Step 7 is an optional configuration.

Note: To monitor SIP proxies, the `call fallback active` command must be configured, as described in Step 3.

SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `call fallback active`
4. `voice register pool tag`
5. `id [{network address mask | ip address mask | mac address}] [device-id-name devicename]`
6. `preference preference-order`
7. `proxy ip-address [preference value] [monitor probe {icmp-ping | rtr} [alternate-ip-address]]` (Optional)
8. `voice-class codec tag`
9. `end`
### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>enable &lt;br&gt;<strong>Example:</strong> &lt;br&gt;Router&gt; enable</td>
</tr>
<tr>
<td></td>
<td>Enables privileged EXEC mode. &lt;br&gt;• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>configure terminal &lt;br&gt;<strong>Example:</strong> &lt;br&gt;Router# configure terminal</td>
</tr>
<tr>
<td></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>call fallback active &lt;br&gt;<strong>Example:</strong> &lt;br&gt;Router(config)# call fallback active</td>
</tr>
<tr>
<td></td>
<td>(Optional) Enables a call request to fall back to alternate dial peers if there is network congestion. &lt;br&gt;• This command is used if you want to monitor the proxy dial peer and fallback to the next preferred dial peer. For full information on the <strong>call fallback active</strong> command, see PSTN Fallback Feature.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>voice register pool tag &lt;br&gt;<strong>Example:</strong> &lt;br&gt;Router(config)# voice register pool 12</td>
</tr>
<tr>
<td></td>
<td>Enters voice register pool configuration mode for SIP phones. &lt;br&gt;• Use this command to control which registrations are accepted or rejected by a Cisco Unified SIP SRST device.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>id [{network address mask mask</td>
</tr>
<tr>
<td></td>
<td>Explicitly identifies a locally available individual or set of SIP IP phones. The keywords and arguments are defined as follows: &lt;br&gt;• <strong>network address mask mask</strong>: The <strong>network address mask mask</strong> keyword/argument combination is used to accept SIP Register messages for the indicated phone numbers from any IP phone within the indicated IP subnet. &lt;br&gt;• <strong>ip address mask mask</strong>: The <strong>ip address mask mask</strong> keyword/argument combination is used to identify an individual phone. &lt;br&gt;• <strong>mac address</strong>: MAC address of a particular Cisco Unified IP Phone. &lt;br&gt;• <strong>device-id-name devicename</strong>: Defines the device name to be used to download the phone’s configuration file.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>preference preference-order &lt;br&gt;<strong>Example:</strong> &lt;br&gt;Router(config-register-pool)# preference 2</td>
</tr>
<tr>
<td></td>
<td>Sets the preference order for the VoIP dial peers to be created. Range is from 0 to 10. Default is 0, which is the highest preference. &lt;br&gt;• The preference must be greater (lower priority) than the preference configured with the <strong>preference</strong> keyword in the <strong>proxy</strong> command.</td>
</tr>
</tbody>
</table>
## Configure SIP Registrar Functionality for SIP Phones on Unified SRST

**Configure Backup Registrar Service to SIP Phones (Using Optional Commands)**

The prior configurations set up a basic voice register pool. The configuration in this procedure adds optional attributes to increase functionality. As part of this configuration, you can support:

- Translation Profile—Applies the translation profile to a specific directory number or to all directory numbers on a SIP phone.
- Alias—Allows Cisco Unified SIP IP Phones to handle inbound PSTN calls to phone numbers that are unavailable when the main SIP call control (IP-PBX) is not available.

### Command or Action

<table>
<thead>
<tr>
<th>Step</th>
<th>Command/Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Step 7 | proxy ip-address [preference value] [monitor probe {icmp-ping | rtr} [alternate-ip-address]] | (Optional) Autogenerates additional VoIP dial peers to reach the main SIP proxy whenever a Cisco Unified SIP IP Phone registers with a Cisco Unified SIP SRST gateway. The keywords and arguments are defined as follows:  
- *ip-address*: IP address of the SIP proxy.  
- *preference value*: (Optional) Defines the preference of the proxy dial peers that are created. The preference must be less (higher priority) than the preference configured with the preference command. Range is from 0 to 10. The highest preference is 0. There is no default.  
- *monitor probe*: (Optional) Enables monitoring of proxy dial peers.  
- *icmp-ping*: Enables monitoring of proxy dial peers using ICMP ping.  
- *rtr*: Enables monitoring of proxy dial peers using RTR probes.  
- *alternate-ip-address*: (Optional) Enables monitoring of alternate IP addresses other than the proxy address. For example, to monitor a gateway front end to a SIP proxy.  

#### Example:

```
Router(config-register-pool)# proxy 10.2.161.187 preference 1
```

<table>
<thead>
<tr>
<th>Step 8</th>
<th>voice-class codec tag</th>
<th>Sets the voice class codec parameters. The <em>tag</em> argument is a codec group number between 1 and 10000.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>Router(config-register-pool)# voice-class codec 15</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 9</th>
<th>end</th>
<th>Returns to privileged EXEC mode.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>Router(config-register-pool)# end</td>
<td></td>
</tr>
</tbody>
</table>
• Class of restriction (COR)—COR specifies which incoming dial peers can use which outgoing dial peers to make a call. Each dial peer can be provisioned with an incoming and outgoing COR list.

Prerequisites

• Before configuring the 'alias' command, translation rules must be set using the translation-profile outgoing (voice register pool) command.

SUMMARY STEPS

1. enable
2. configure terminal
3. voice register pool tag
4. translation-profile outgoing profile-tag
5. alias tag pattern to target [preference value]
6. cor {incoming | outgoing} cor-list-name {cor-list-number starting-number [- ending-number] | default}
7. incoming called-number [number]
8. number tag number-pattern [preference value] [huntstop]
9. dtmf-relay [cisco-rtp] [rtp-nte] [sip-notify]
10. end

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1**
| enable
| Enables privileged EXEC mode.
| • Enter your password if prompted. |
| **Example:**
| Router> enable |
| **Step 2**
| configure terminal
| Enters global configuration mode. |
| **Example:**
| Router# configure terminal |
| **Step 3**
| voice register pool tag
| Enters voice register pool configuration mode.
| • Use this command to control which registrations are accepted or rejected by a Cisco Unified SIP SRST device. |
| **Example:**
| Router(config)# voice register pool 12 |
### Step 4: Configure SIP Registrar Functionality for SIP Phones on Unified SRST

**Command or Action**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>translation-profile outgoing profile-tag</td>
<td>Use this command to apply the translation profile to a specific directory number or to all directory numbers on a SIP phone.</td>
</tr>
</tbody>
</table>

**Example:**

```
Router(config-register-pool)#
voice translation-rule 1
rule 1 /1000/ /1006/
!
voice translation-profile 1
translate called 1
!
voice register pool xxx
translation-profile outgoing 1
```

### Step 5: Configure SIP Registrar Functionality for SIP Phones on Unified SRST

**Command or Action**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>alias tag pattern to target [preference value]</td>
<td>Allows Cisco Unified SIP IP Phones to handle inbound PSTN calls to phone numbers that are unavailable when the main proxy is not available. The keywords and arguments are defined as follows:</td>
</tr>
</tbody>
</table>

**Example:**

```
Router(config-register-pool)# alias 1 94... to 91011 preference 8
```

**• tag:** Number from 1 to 5 and the distinguishing factor when there are multiple alias commands.

**• pattern:** The prefix number; matches the incoming phone number and may include wildcards.

**• to:** Connects the tag number pattern to the alternate number.

**• target:** The target number; an alternate phone number to route incoming calls to match the number pattern.

**• preference value:** (Optional) Assigns a dial-peer preference value to the alias. The value argument is the value of the associated dial peer, and the range is from 1 to 10. There is no default.
**Configure SIP Registrar Functionality for SIP Phones on Unified SRST**

### Step 6

Configure a class of restriction (COR) on the VoIP dial peers associated with directory numbers. COR specifies which incoming dial peers can use which outgoing dial peers to make a call. Each dial peer can be provisioned with an incoming and outgoing COR list. The keywords and arguments are defined as follows:

- **incoming**: COR list to be used by incoming dial peers.
- **outgoing**: COR list to be used by outgoing dial peers.
- **cor-list-name**: COR list name.
- **cor-list-number**: COR list identifier. The maximum number of COR lists that can be created is four, comprised of incoming or outgoing dial peers.
- **starting-number**: Start of a directory number range, if an ending number is included. Can also be a standalone number.
- **(Optional) Indicator that a full range is configured.**
- **ending-number**: (Optional) End of a directory number range.
- **default**: Instructs the router to use an existing default COR list.

**Example:**

```
Router(config-register-pool)# cor incoming call91 1 91011
```

### Step 7

Applies incoming called parameters to dynamically created dial peers. The `number` argument is optional and indicates a sequence of digits that represent a phone number prefix.

**Example:**

```
Router(config-register-pool)# incoming called-number 308
```

### Step 8

Indicates the E.164 phone numbers that the registrar permits to handle the Register message from the Cisco Unified SIP IP Phone. The keywords and arguments are defined as follows:

- **tag**: Number from 1 to 10 and the distinguishing factor when there are multiple `number` commands.
- **number-pattern**: Phone numbers (including wildcards and patterns) that are permitted by the registrar to handle the Register message from the SIP IP phone.
- **preference value**: (Optional) Defines the number list preference order.
- **huntstop**: (Optional) Stops hunting if the dial peer is busy.

**Example:**

```
Router(config-register-pool)# number 1 50.. preference 2
```
### Verify SIP Registrar Configuration

To help you troubleshoot a SIP registrar and voice register pool, perform the following steps.

**SUMMARY STEPS**

1. debug voice register errors
2. debug voice register events
3. show sip-ua status registrar

### Command or Action

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Step 9 | `dtmf-relay [cisco-rtp] [rtp-nte] [sip-notify]` | Specifies how a SIP gateway relays dual tone multifrequency (DTMF) tones between telephony interfaces and an IP network. The keywords are defined as follows:  
  - **cisco-rtp**: (Optional) Forwards DTMF tones by using Real-Time Transport Protocol (RTP) with a Cisco proprietary payload type.  
  - **rtp-nte**: (Optional) Forwards DTMF tones by using RTP with the Named Telephone Event (NTE) payload type.  
  - **sip-notify**: (Optional) Forwards DTMF tones using SIP NOTIFY messages. |
| Example: | `Router(config-register-pool)# dtmf-relay rtp-nte` | |
| Step 10 | `end` | Returns to privileged EXEC mode. |
| Example: | `Router(config-register-pool)# end` | |
## DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> debug voice register errors</td>
<td>Use this command to debug errors that happen during registration. If there are no voice register pools configured for a particular registration request, the message “Contact doesn’t match any pools” is displayed.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router# debug voice register errors</td>
<td></td>
</tr>
<tr>
<td><em>Apr 22 11:52:54.523 PDT: VOICE_REG_POOL: Contact doesn't match any pools</em></td>
<td></td>
</tr>
<tr>
<td><em>Apr 22 11:52:54.539 PDT: VOICE_REG_POOL: Register request for (33015) from (10.2.152.39)</em></td>
<td></td>
</tr>
<tr>
<td><em>Apr 22 11:52:54.539 PDT: VOICE_REG_POOL: Contact doesn't match any pools.</em></td>
<td></td>
</tr>
<tr>
<td><em>Apr 22 11:52:54.559 PDT: VOICE_REG_POOL: Register request for (33017) from (10.2.152.39)</em></td>
<td></td>
</tr>
<tr>
<td><em>Apr 22 11:53:04.559 PDT: VOICE_REG_POOL: Maximum registration threshold for pool(3) hit</em></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> debug voice register events</td>
<td>Using the <strong>debug voice register events</strong> command should suffice to display registration activity. Registration activity includes matching of pools, registration creation, and automatic creation of dial peers. For more details and error conditions, you can use the <strong>debug voice register errors</strong> command. The phone number 91011 registered successfully, and <strong>type 1</strong> is reported, which means there is a pre-existing VoIP dial peer.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router# debug voice register events</td>
<td></td>
</tr>
<tr>
<td>Apr 22 10:50:21.731 PDT: VOICE_REG_POOL: Contact matches pool 1</td>
<td></td>
</tr>
<tr>
<td>Apr 22 10:50:21.731 PDT: VOICE_REG_POOL: key(91011) contact(192.168.0.2) add to contact table</td>
<td></td>
</tr>
<tr>
<td>Apr 22 10:50:21.731 PDT: VOICE_REG_POOL: key(91011) exists in contact table</td>
<td></td>
</tr>
<tr>
<td>Apr 22 10:50:21.731 PDT: VOICE_REG_POOL: contact(192.168.0.2) exists in contact table, ref updated</td>
<td></td>
</tr>
<tr>
<td>Apr 22 10:50:21.731 PDT: VOICE_REG_POOL: Created dial-peer entry of type 1</td>
<td></td>
</tr>
<tr>
<td>Apr 22 10:50:21.731 PDT: VOICE_REG_POOL: Registration successful for 91011, registration id is 257</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> show sip-ua status registrar</td>
<td>Use this command to display all the SIP endpoints currently registered with the contact address.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router# show sip-ua status registrar</td>
<td></td>
</tr>
<tr>
<td>Line</td>
<td>destination</td>
</tr>
<tr>
<td>=======</td>
<td>=============</td>
</tr>
<tr>
<td>91021</td>
<td>192.168.0.3</td>
</tr>
<tr>
<td>91011</td>
<td>192.168.0.2</td>
</tr>
<tr>
<td>95021</td>
<td>10.2.161.50</td>
</tr>
<tr>
<td>95012</td>
<td>10.2.161.50</td>
</tr>
<tr>
<td>95011</td>
<td>10.2.161.50</td>
</tr>
<tr>
<td>95500</td>
<td>10.2.161.50</td>
</tr>
<tr>
<td>94011</td>
<td>10.2.161.40</td>
</tr>
<tr>
<td>94500</td>
<td>10.2.161.40</td>
</tr>
</tbody>
</table>
Verify Proxy Dial-Peer Configuration

To use the `icmp-ping` keyword with the `proxy` command to assist in troubleshooting proxy dial peers, perform the following steps.

**SUMMARY STEPS**

1. `configure terminal`
2. `voice register pool tag`
3. `proxy ip-address [preference value] [monitor probe {icmp-ping | rtr} [alternate-ip-address]]`
4. `end`
5. `show voice register dial-peers`
6. `show dial-peer voice`
### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Use this command to enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> voice register pool tag</td>
<td>Use this command to enter voice register pool configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config)# voice register pool 1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> proxy ip-address [preference value] [monitor probe {icmp-ping</td>
<td>rtr}] [alternate-ip-address]</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-register-pool)# proxy 10.2.161.187 preference 1 monitor probe icmp-ping</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-register-pool)# end</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> show voice register dial-peers</td>
<td>Use this command to verify dial-peer configurations, and notice that icmp-ping monitoring is set.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router# show voice register dial-peers dial-peer voice 40035 voip preference 5 destination-pattern 91011 session target ipv4:192.168.0.2 session protocol sipv2 voice-class codec 1 dial-peer voice 40036 voip preference 1 destination-pattern 91011 session target ipv4:10.2.161.187 session protocol sipv2 voice-class codec 1 monitor probe icmp-ping 10.2.161.187</td>
<td></td>
</tr>
</tbody>
</table>
## Configure SIP Registrar Functionality for SIP Phones on Unified SRST

### Step 6

**show dial-peer voice**

**Example:**

```plaintext
Router# show dial-peer voice
VoiceOverIpPeer40036
peer type = voice, information type = voice,
description = '',
tag = 40036, destination-pattern = '91011',
answer-address = '', preference=1,
CLID Restriction = None
CLID Network Number = ''
CLID Second Number sent
source carrier-id = '', target carrier-id = '',
source trunk-group-label = '', target
trunk-group-label = '',
numbering Type = 'unknown'
group = 40036, Admin state is up, Operation state is
up,
ingoing called-number = '', connections/maximum = 0/unlimited,
Default output for incoming called-number command
DTMF Relay = disabled,
modem transport = system,
huntstop = disabled,
in bound application associated: 'DEFAULT'
out bound application associated: ''
dnis-map =
permission :both
incoming COR list:maximum capability
Default output for cor command
outgoing COR list:minimum requirement
Default output for cor command
Translation profile (Incoming):
Translation profile (Outgoing):
ingoing call blocking:
translation-profile = '',
disconnect-cause = 'no-service'
advertise 0x40 capacity_update_timer 25 addrFamily 4
oldAddrFamily 4
type = voip, session-target = 'ipv4:10.2.161.187',
technology prefix:
settle-call = disabled
ip media DSCP = ef, ip signaling DSCP = af31,
ip video rsvp-none DSCP = af41, ip video rsvp-pass
DSCP = af41
ip video rsvp-fail DSCP = af41,
UDP checksum = disabled,
session-protocol = sipv2, session-transport = system,
req-qos = best-effort, acc-qos = best-effort,
req-qos video = best-effort, acc-qos video = best-effort,
req-qos audio def bandwidth = 64, req-qos audio max
bandwidth = 0,
req-qos video def bandwidth = 384, req-qos video max
bandwidth = 0,
```

**Command or Action**

Use the `show dial-peer voice` command on dial peer 40036, and notice the monitor probe status.

**Note**

Also highlighted is the output of the `cor` and `incoming called-number` commands.
Unified SRST, Unified E-SRST, and Unified Secure SRST Password Policy

From Unified SRST 12.6 Release (Cisco IOS XE Gibraltar 16.11.1a) onwards, all configurations on Unified SRST, Unified E-SRST, and Unified Secure SRST must meet the password policy.

General Password Policy Guidelines:
- Passwords must have a minimum of 6 alphanumeric characters, and a maximum of 15 alphanumeric characters.
- Passwords must not contain symbols or special characters.
- Passwords must contain at least one numeral, one uppercase alphabet, and one lowercase alphabet.

If the password is not configured as per the policy, the Unified SRST router displays an error message:

```
Error: The password you have entered is incorrect.
Your password must contain:
```
Unified SRST, Unified E-SRST, and Unified Secure SRST Password Policy

1. A minimum of 6 and a maximum of 15 alphanumeric characters, excluding symbols and special characters.
2. A minimum of one numeral, one uppercase alphabet, and one lowercase alphabet.

The Unified CME password policy is applicable for Unified SRST configurations on Cisco IOS XE 16.11.1a and later. Unified SRST password policy is not applicable in the following scenarios:

- Upgrade from an older IOS version to Cisco IOS XE 16.11.1a
- Downgrade from Cisco IOS XE 16.11.1a to an older version

Guidelines for Password Configuration and Encryption

Configure the passwords relevant to Unified SRST, Unified E-SRST, and Unified Secure SRST using the CLI commands as follows:

- `call-manager-fallback` configuration mode
  - `xml user username password [0|6] password privilege-level`

**Note**
The 0 in the parameter `[0|6]` mentioned in the CLI command represents plain, unencrypted text and 6 represents level 6 password encryption.

- Apart from the parameter configurations ([0|6]) at the command level, configure the Unified SRST router to support encryption.
- Configure the CLI command `encrypt password` under `call-manager-fallback` configuration mode to support type 6 encryption on the Unified SRST router.
- Also, it is mandatory to configure `key config-key password-encrypt [Master key]` and `password encryption aes` to support encryption on the Unified SRST router.
- If the key used to encrypt the password is replaced with a new key (replace key or re-key), then the password is re-encrypted with the new key.
- You must adhere to SRST Password Policy for both type 0 and type 6 parameters that you configure on Unified SRST.
- Configure `no encrypt password` for type 0 password on the Unified SRST router. A type 0 password is displayed as unencrypted plain text.
- If you are performing a downgrade from Unified SRST 12.6 to an earlier version, then you must execute the CLI command `no encrypt password`. If the CLI command `no encrypt password` is configured, the password is presented as plain text.

**Example**
The following is a sample configuration on Unified SRST router to support password encryption:

```
Router(config)#key config-key password-encrypt <cisco123>
Router(config)#password encryption aes
Router(config)#call-manager-fallback
Router(config-cm-fallback)encrypt password
```

Deprecation of CLI commands

From Unified SRST Release 12.6 onwards, the following CLI commands that are configured under `call-manager-fallback` configuration mode are deprecated to enhance product security:
- log password password-string
- xmltest
- xschema schema-url
- xmThread number

## Removal of Passwords and Keys from Logs

From Unified SRST Release 12.6 onwards, passwords and sRTP keys are not printed to logs to enhance security of Unified SRST. The information about keys is available only in the show commands from Unified SRST 12.6 release onwards. The CLI command `show ephone offhook` for SCCP and `show sip-ua calls` for SIP are enhanced to display the keys that are in use per media stream, along with the sRTP Ciphers.

The following is a sample output for the show command, `show sip-ua calls`. The lines that are added to the show command output as part of the Unified SRST 12.6 enhancement are the local crypto key and the remote crypto key:

```plaintext
SIP UAC CALL INFO
Number of SIP User Agent Client(UAC) calls: 0
SIP UAS CALL INFO
Call 1
SIP Call ID : 007278df-12e00376-6ed02377-6ffbac908.55.0.195
State of the call : STATE_ACTIVE (7)
Sipstate of the call : SUBSTATE_NONE (0)
Calling Number : 1001
Called Number : 6901%23
Called URI : sip:6901%23@8.39.25.11;user=phone
Bit Flags : 0x10C0401C 0x10000100 0x4
CC Call ID : 196
Local UUID : 61488a9100105000a000007278df12e0
Remote UUID : c4b7f9475629538096ef61699b96746f
Source IP Address (Sig ) : 8.39.25.11
Destn SIP Req Addr:Port : [8.55.0.195]:52704
Destn SIP Resp Addr:Port: [8.55.0.195]:52704
Destination Name : 8.55.0.195
Number of Media Streams : 1
Number of Active Streams: 1
RTF Fork Object : 0x0
Media Mode : flow-through
Media Stream 1
State of the stream : STREAM_ACTIVE
Stream Call ID : 196
Stream Type : voice+dtmf (1)
Stream Media Addr Type : 1
Negotiated Codec : g711ulaw (160 bytes)
Codec Payload Type : 0
Negotiated Dtmf-relay : rtp-nte
Dtmf-relay Payload Type : 101
QoS ID : -1
Local QoS Strength : BestEffort
Negotiated QoS Strength : BestEffort
Negotiated QoS Direction : None
Local QoS Status : None
Media Source IP Addr:Port: [8.39.25.11]:8080
Media Dest IP Addr:Port : [8.55.0.195]:23022
Local Crypto Suite : AEAD_AES_256_GCM
Remote Crypto Suite : AEAD_AES_256_GCM
AEAD_AES_256_GCM
AEAD_AES_128_GCM
```
Toll Fraud Prevention for SIP Line Side on Unified SRST

Unified SRST Release 12.6 enhances the existing Toll Fraud Prevention feature by enforcing security on the SIP line side of Unified SRST. The feature enhancement secures the Unified SRST system against potential toll fraud exploitation by unauthorized users from the SIP line side.

Some of the key features of Toll Fraud Prevention on Unified SRST for secure calls over SIP lines are:

- Authenticates all the SIP line messages that are triggered from the endpoints to Unified SRST.
- If the IP address of the endpoint is not part of the IP address trusted list, the call is rejected by Unified SRST.
- Unified SRST authenticates both IPv4 an IPv6 addresses as part of the toll fraud prevention mechanism.

Prerequisites for Configuring Toll Fraud Prevention for SIP Line Side

- Unified SRST 12.6 or a later version.
- Cisco IOS XE Gibraltar Release 16.11.1a or later.

Note

Unified SRST 8.1 to 12.5 Releases restricts toll fraud prevention only to securing calls over the SIP trunk. For more information about Toll Fraud Prevention over a SIP trunk, see Configuring a Trusted IP Address List for Toll-Fraud Prevention.
Configuration Recommendations for Toll Fraud Prevention on Unified SRST

Unified SRST 12.6 enforces security and toll fraud prevention for SIP line side on Unified SRST. The `ip address trusted authentication` configuration blocks unauthorized calls from the line side. Hence, the toll fraud prevention feature secures Unified SRST 12.6 and later from unauthorized users on the line side.

The IP addresses of SRST endpoints are available before registration with Unified SRST, as they are configured (under `voice register pool`) for fallback from Unified CM. Hence, it is not mandatory that the endpoints are registered to Unified SRST for configuring toll fraud prevention.

The IP trust list for Unified SRST is populated based on the IP address information available under `voice register pool` configuration mode. You can find the IP address of the SIP endpoints on Unified SRST under the following commands in voice register pool configuration mode:

- **id ip** (For example, `id ip 192.168.0.0`)
- **id network** (For example, `id network 192.168.25.0 mask 255.255.255.0`)

Sometimes, IP addresses of endpoints are not available to Unified SRST before registration. Consider a scenario where `id device-id` is the CLI command configured under voice register pool configuration mode to define the device name. Then, the IP address of the device or endpoint is available to Unified SRST only during registration.

The following are the configurations of Toll Fraud Prevention in Unified SRST, 12.6:

- The CLI command `ip address trusted authentication` is enabled by default in Unified SRST. The command `ip address trusted authentication` ensures that security is enabled on the Unified SRST system.
- You can manually configure your Unified SRST endpoints as trusted by entering the IP address or subnet of the trusted phone under the `iptrust-list` configuration mode, as follows:

```
Router(config)#voice service voip
Router(config-voi-serv)#ip address trusted list
Router(config-iptrust-list)#ipv4 192.168.10.0 /16
OR
Router(config-iptrust-list)#ipv4 192.168.12.0 255.255.255.0
```

- You can verify the manually added IP address of the Unified SRST endpoint, as follows:

```
Router#show running-config | section voice service voip
voice service voip
ip address trusted list
ipv4 192.168.10.1
ipv4 192.168.10.2 255.255.0.0
ipv4 192.168.10.3 255.255.0.0
ipv4 192.168.10.4 255.255.255.0
```

- The CLI command `ip address trusted list` under `voice service voip` configuration mode supports manual configuration of trusted IP addresses.
- The CLI command `show ip address trusted check` provides information on whether a particular IP address is trusted or not.
- The CLI command `silent-discard untrusted` in `sip` configuration mode silently discards SIP requests from untrusted sources. This command is enabled by default on Unified SRST.
• The **show ip address trusted list** CLI command displays a list of trusted IP addresses. The trusted IP addresses are displayed under the following lists:
  
  – Dial Peer (only applicable for trunk side): Provides details on the IP address of the trunk that is configured under the dial-peer configuration mode.
  
  – Configured IP Address Trusted List: Provides details on the manually configured IP addresses that are trusted.
  
  – Dynamic IP Address Trusted List: Provides details on the IP address of all the phones that are configured for fallback from Unified CM. This list is introduced in Unified CME 12.6 Release.
  
  – Server Group: Provides details on the IP address of the phones that are configured under server-groups configuration mode.

```
Router>enable
Router#show ip address trusted list
IP Address Trusted Authentication
    Administration State: UP
    Operation State:      UP

    IP Address Trusted Call Block Cause: call-reject (21)

    VoIP Dial-peer IPv4 and IPv6 Session Targets:
    Peer Tag Oper State Session Target
    -------- ---------- ---------------
    4          UP         ipv4:10.65.125.155

    Configured IP Address Trusted List:
        ipv4 192.168.20.1
        ipv4 192.168.20.2 255.255.0.0
        ipv4 192.168.20.3 255.255.0.0
        ipv4 192.168.20.4 255.255.255.0

    Dynamic IP Address Trusted List:
        IP Address                                   Subnet Mask     Count Reason
            -------------------------------------------- --------------- ----- ----------------
            ipv4:8.55.0.0                                255.255.0.0         1 Pool Configured
            ipv4:192.168.0.1                             255.255.0.0         2 Pool Configured
            ipv6:2001:420:54FF:13::312:0                 119                 1 Pool Configured
            ipv4:8.55.22.15         1 Phone Registered
```

**Note** The column **Count** in Dynamic IP Address Trusted List displays the number of directory numbers (DNs) sharing the same IP address. For example, ipv4 192.168.0.1 with count 2 represents two DNs sharing the IP address 192.168.0.1.

**Note** The output of **show ip address trusted list** command displays the entry in column **Type** as ‘Phone Registered’ if **id device-id** is configured.

### Upgrade Considerations

When you upgrade to Unified SRST 12.6 version, you need not perform extra configurations for supporting toll fraud prevention. All the endpoints that are manually configured or auto-registered on Unified SRST are added to the Unified SRST IP Address Trust List. You can view the list of trusted IP addresses under the output of the CLI command **show ip address trusted list**.
Configure Toll Fraud Prevention

This section contains the following tasks.

- Configure IP Address Trusted Authentication for Incoming VoIP Calls, page 63
- Add Valid IP Addresses For Incoming VoIP Calls, page 65
- Troubleshooting Tips for Toll Fraud Prevention, page 67

Configure IP Address Trusted Authentication for Incoming VoIP Calls

Prerequisites

- Unified SRST 8.1 or a later version for secure trunk calls.
- Unified SRST 12.6 or a later version for secure line and trunk calls.
- The CLI command `silent-discard untrusted` needs to be configured for the feature to work

Restrictions

- For an incoming VoIP call, IP trusted authentication must be invoked when the IP address trusted authentication is in “UP” operational state.

SUMMARY STEPS

1. enable
2. configure terminal
3. voice service voip
4. ip address trusted authenticate
5. ip-address trusted call-block cause <code>
6. end
7. show ip address trusted list
Chapter 2  Cisco Unified SIP SRST on Cisco 4000 Series Integrated Services Router

Configure Toll Fraud Prevention

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Enter your password if prompted.</td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> voice service voip</td>
<td>Enters voice service voip configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# voice service voip</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> ip address trusted authenticate</td>
<td>Enables IP address authentication on incoming H.323 or SIP trunk calls for toll fraud prevention support.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>IP address trusted list authenticate is enabled by default.</td>
</tr>
<tr>
<td>Router(conf-voi-serv)# ip address trusted authenticate</td>
<td>Use the “no ip address trusted list authenticate” command to disable the IP address trusted list authentication.</td>
</tr>
<tr>
<td><strong>Step 5</strong> ip-address trusted call-block cause code</td>
<td>Issues a cause-code when the incoming call is rejected to the IP address trusted authentication. This command is enabled by default.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>If the IP address trusted authentication fails, a call-reject (21) cause-code is issued to disconnect the incoming VoIP call.</td>
</tr>
<tr>
<td>Router(conf-voi-serv)#ip address trusted call-block cause call-reject</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router()# end</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> show ip address trusted list</td>
<td>Verifies a list of valid IP addresses.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router# #show ip address trusted list</td>
<td></td>
</tr>
<tr>
<td>IP Address Trusted Authentication</td>
<td></td>
</tr>
<tr>
<td>Administration State: UP</td>
<td></td>
</tr>
<tr>
<td>Operation State: UP</td>
<td></td>
</tr>
<tr>
<td>IP Address Trusted Call Block Cause: call-reject (21)</td>
<td></td>
</tr>
</tbody>
</table>

Examples

Router> enable
Router#show ip address trusted list
IP Address Trusted Authentication
   Administration State: UP
   Operation State: UP

   IP Address Trusted Call Block Cause: call-reject (21)

   VoIP Dial-peer IPv4 and IPv6 Session Targets:
   Peer Tag Oper State Session Target
----------- --------------
   Configured IP Address Trusted List:
      ipv4 192.168.20.1
      ipv4 192.168.20.2 255.255.0.0
      ipv4 192.168.20.3 255.255.0.0
      ipv4 192.168.20.4 255.255.255.0

   Dynamic IP Address Trusted List:
   ----------------------------------------------- --------------- ----- ----------------
   ipv4:8.55.0.0                                    255.255.0.0     1 Pool Configured
   ipv4:192.168.0.1                                 255.255.0.0     1 Pool Configured

Add Valid IP Addresses For Incoming VoIP Calls

Prerequisites

- Cisco Unified CME 8.1 or a later version.

SUMMARY STEPS

1.  enable
2.  configure terminal
3.  voice service voip
4.  ip address trusted list
5.  ipv4 ipv4 address network mask
6.  end
7.  show ip address trusted list
Configure Toll Fraud Prevention

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>enable</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router&gt; enable</td>
</tr>
<tr>
<td>Enables privileged EXEC mode.</td>
<td></td>
</tr>
<tr>
<td>• Enter your password if prompted.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router# configure terminal</td>
</tr>
<tr>
<td>Enters global configuration mode.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>voice service voip</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config)# voice service voip</td>
</tr>
<tr>
<td>Enters voice service voip configuration mode.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>ip address trusted list</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(conf-voi-serv)# ip address trusted list</td>
</tr>
<tr>
<td>Enters ip address trusted list mode and allows to manually add additional valid IP addresses.</td>
<td></td>
</tr>
</tbody>
</table>
| **Step 5** | ipv4 {<ipv4 address> [<network mask>]}
| **Example:** | Router(cfg-iptrust-list)#ipv4 172.19.245.1 |
| Allows you to add up to 100 IPv4 addresses in **ip address trusted list**. Duplicate IP addresses are not allowed in the **ip address trusted list**. |
| • (Optional) **network mask**— allows to define a subnet IP address. |
| **Step 6** | end |
| **Example:** | Router(config-register-pool)# end |
| Returns to privileged EXEC mode. |
| **Step 7** | show ip address trusted list |
| **Example:** | Router# show shared-line |
| Displays a list of valid IP addresses for incoming H.323 or SIP trunk calls. |

Examples

The following example shows three IP addresses configured as trusted IP addresses:

```
Router#show ip address trusted list
IP Address Trusted Authentication
    Administration State: UP
    Operation State:       UP

    IP Address Trusted Call Block Cause: call-reject (21)

    Configured IP Address Trusted List:
    ipv4 192.168.20.1
    ipv4 192.168.20.2 255.255.0.0
    ipv4 192.168.20.3 255.255.0.0
    ipv4 192.168.20.4 255.255.255.0
```
Troubleshooting Tips for Toll Fraud Prevention

For troubleshooting toll fraud mechanism supported on Unified SRST, you can enable the CLI commands `debug voip iptrust debug` and `debug voip iptrust detail`, as follows:

Router#debug voip iptrust
voip iptrust debugging is on
Router#debug voip iptrust detail
voip iptrust detail debugging is on

IPv6 Support for Unified SRST SIP IP Phones

Internet Protocol version 6 (IPv6) is the latest version of the Internet Protocol (IP). IPv6 uses packets to exchange data, voice, and video traffic over digital networks. Also, IPv6 increases the number of network address bits from 32 bits in IPv4 to 128 bits. From Unified SRST Release 12.0 onwards, Unified SRST supports IPv6 protocols for SIP IP phones.

IPv6 support in Unified SRST allows the network to behave transparently in a dual-stack (IPv4 and IPv6) environment and provides additional IP address space to SIP IP phones that are connected to the network. If you do not have a dual-stack configuration, configure the CLI command `call service stop` under `voice service voip` configuration mode before changing to dual-stack mode. For an example of switching to dual-stack mode, see Examples for Configuring IPv6 Pools for SIP IP Phones, page 92.

The Cisco IP Phone 7800 Series and 8800 Series are supported on IPv6 for Unified SRST.

For more information on configuring SIP IP phones for IPv6 source address, see Configure IPv6 Pools for SIP IP Phones, page 68.

For an example of configuring IPv6 Support on Unified SRST, see Examples for Configuring IPv6 Pools for SIP IP Phones, page 92.


Feature Support for IPv6 in Unified SRST SIP IP Phones

The following basic features are supported for a IPv6 WAN down scenario:

- Basic SIP Line (IPv4 or IPv6) to SIP Line calls (IPv4 or IPv6) when Unified SRST is in dual-stack `no anat` mode.

The following supplementary services are supported as part of IPv6 in Unified SRST IP Phones:

- Hold/Resume
- Call Forward
- Call Transfer
- Three-way Conference (with BIB conferencing only)
- Line to T1/E1 Trunk and Trunk to Line with Supplementary Service Features
- Fax to and from PSTN (IPv4 ATA to ISDN T1/E1) for both T.38 Fax Relay and Fax Passthrough

Restrictions

The following are the known restrictions for IPv6 support on Unified SRST:
IPv6 Support for Unified SRST SIP IP Phones

- SIP Trunks are not supported on Unified SRST for IPv6 deployment. PSTN calls are supported only through T1/E1 trunks.
- SCCP IP Phones are not supported in a deployment of IPv6 for Unified SRST.
- SIP Phones can be either in IPv4 only or IPv6 only mode (no anat).
- Trancoding and Transrating are not supported.
- H.323 trunks are not supported.
- Secure SIP lines or trunks are not supported.
- IPv6 on Unified SRST is not supported on the Cisco IOS platform. The support is restricted to Cisco IOS XE platform with Cisco IOS Release 16.6.1 or later versions.

Configure IPv6 Pools for SIP IP Phones

Before You Begin
- Unified SRST 12.0 or a later version.
- IPv6 option only appears if protocol mode is dual-stack configured under sip-ua configuration mode or IPv6.
- Cisco Unified SRST License must be configured for the gateway to function as a Unified SRST gateway to support IPv6 functionality. For more information on licenses, see Licensing, page 40.
- Cisco Unified Communications Manager (Unified Communications Manager) is provisioned with the IPv6 address of Unified SRST. For information on configuration of Unified SRST on Unified Communications Manager, see the section Survivable Remote Site Telephony Configuration in Cisco Unified Communications Manager Administration Guide.

SUMMARY STEPS

1. enable
2. configure terminal
3. ipv6 unicast-routing
4. voice service voip
5. sip
6. no anat
7. call service stop
8. exit
9. exit
10. sip-ua
11. protocol mode {ipv4 | ipv6 | dual-stack [preference {ipv4 | ipv6}]}
12. exit
13. voice service {voip}
14. sip
15. no call service stop
16. exit
17. voice register global
18. default mode
19. **max-dn** max-directory-numbers
20. **max-pool** max-voice-register-pools
21. exit
22. voice register pool pool-tag
23. id { network address mask | ip address mask | mac address }
24. end
### IPv6 Support for Unified SRST SIP IP Phones

#### Detailed Steps

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** enable | Enables privileged EXEC mode.  
  - Enter your password if prompted. |
| **Example:**  
  Router> enable | |
| **Step 2** configure terminal | Enters global configuration mode. |
| **Example:**  
  Router#configure terminal | |
| **Step 3** ipv6 unicast-routing | Enables the forwarding of IPv6 unicast datagrams. |
| **Example:**  
  Router(config)# ipv6 unicast-routing | |
| **Step 4** voice service voip | Enters voice-service configuration mode to specify a voice encapsulation type.  
  - voip—Specifies Voice over IP (VoIP) parameters. |
| **Example:**  
  Router(config)# voice service voip | |
| **Step 5** sip | Enters SIP configuration mode. |
| **Example:**  
  Router(config-voi-serv)# sip | |
| **Step 6** no anat | Disables Alternative Network Address Types (ANAT) on a SIP trunk. |
| **Example:**  
  Router(config-serv-sip)# no anat | |
| **Step 7** call service stop | Shuts down SIP call service. |
| **Example:**  
  Router(config-serv-sip)# call service stop | |
| **Step 8** exit | Exits SIP configuration mode. |
| **Example:**  
  Router(config-serv-sip)# exit | |
### IPv6 Support for Unified SRST SIP IP Phones

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>9</td>
<td><code>exit</code></td>
<td>Exits voice service voip configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Router(config-voi-serv)# exit</code></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td><code>sip-ua</code></td>
<td>Enters SIP user-agent configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Router(config)# sip-ua</code></td>
<td></td>
</tr>
</tbody>
</table>
| 11   | `protocol mode {ipv4 | ipv6 | dual-stack}
  {preference {ipv4 | ipv6}}` | Allows phones to interact with phones on IPv6 voice gateways. You can configure phones for IPv4 addresses, IPv6 addresses, or for a dual-stack mode. |
|      | **Example:**     |         |
|      | `Router(config-sip-ua)# protocol mode dual-stack
  preference ipv6` |         |
| 12   | `exit`           | Exits SIP configuration mode. |
|      | **Example:**     |         |
|      | `Router(config-sip-ua)# exit` |         |
| 13   | `voice service {voip}` | Enters voice-service configuration mode to specify a voice encapsulation type. |
|      | **Example:**     |         |
|      | `Router(config)# voice service voip` |         |
| 14   | `sip`            | Enters SIP configuration mode. |
|      | **Example:**     |         |
|      | `Router(config-voi-serv)# sip` |         |
### IPv6 Support for Unified SRST SIP IP Phones

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 15</strong> no call service stop</td>
<td>Activates SIP call service.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-serv-sip)# call service stop</td>
</tr>
<tr>
<td><strong>Step 16</strong> exit</td>
<td>Exits SIP configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-serv-sip)# exit</td>
</tr>
<tr>
<td><strong>Step 17</strong> voice register global</td>
<td>Enters voice register global configuration mode to set parameters for all supported SIP phones in Unified SRST.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config)# voice register global</td>
</tr>
<tr>
<td><strong>Step 18</strong> default mode</td>
<td>Enables mode for provisioning SIP phones in Unified SRST. The default mode is Unified SRST itself.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-register-global)# default mode</td>
</tr>
<tr>
<td><strong>Step 19</strong> max-dn max-directory-numbers</td>
<td>Limits number of directory numbers to be supported by this router.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-register-global)# max-dn 50</td>
</tr>
<tr>
<td>• Maximum number is platform and version-specific. Type ? for value.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 20</strong> max-pool max-voice-register-pools</td>
<td>Sets maximum number of SIP phones to be supported by the Unified SRST router.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-register-global)# max-pool 40</td>
</tr>
<tr>
<td><strong>Step 21</strong> exit</td>
<td>Exits voice register global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-register-global)# exit</td>
</tr>
<tr>
<td><strong>Step 22</strong> voice register pool pool-tag</td>
<td>Enters voice register pool configuration mode to set phone-specific parameters for a SIP phone.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config)# voice register pool 1</td>
</tr>
</tbody>
</table>
Chapter 2      Cisco Unified SIP SRST on Cisco 4000 Series Integrated Services Router

Configure Unified SRST on Cisco 4000 Series Integrated Services Platform

For Unified SRST Release 10.5 and later, Unified SRST is supported on Cisco 4000 Series Integrated Services Routers. A Unified SRST system supports SIP phones with standard-based RFC 3261 feature support locally and across SIP WAN networks. With Cisco Unified SIP SRST, SIP phones can place calls across SIP networks with similar features, as SCCP phones do. For example, most SCCP phone features such as caller ID, speed dial, and redial are supported on SIP networks, that give users the opportunity to choose SCCP or SIP.

Prerequisites

- Cisco IOS XE Denali 16.3.1 or a later release.
- Cisco IP Phones 7800 Series or 8800 Series.
- An appropriate feature license to support Unified SIP SRST on the router.
- You need to configure voice register global in your router.
- You need to ensure that your router is in default mode (for Unified SRST).

Restrictions

- For a list of restrictions for Unified SIP SRST support on Cisco 4000 Series Integrated Services Routers, see Restrictions of Unified SRST on Cisco 4000 Series Integrated Services Routers, page 37.

SUMMARY STEPS

1. enable
2. configure terminal
3. voice service voip

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 23  id { network address mask mask</td>
<td>ip address mask mask</td>
</tr>
</tbody>
</table>

Example:

Router(config-register-pool)# id network 2001:420:54FF:13::901:0/117

Router(config-register-pool)# id network 10.64.88.0 mask 255.255.255.0

Step 24  end | Exits to privileged EXEC mode. |

Example:

Router(config)# end

Explicitly identifies a locally available individual SIP phone to support a degree of authentication.
4. allow-connections from-type to to-type
5. no supplementary-service sip moved-temporarily
6. no supplementary-service sip refer
7. supplementary-service media-renegotiate
8. sip
9. registrar server [expires[max sec][min sec]]
10. exit
11. exit
12. voice register global
13. default mode
14. max-dn max-directory-numbers
15. max-pool max-voice-register-pools
16. exit
17. voice register pool pool-tag
18. id [network address mask mask] | ip address mask mask
19. dtmf-relay [rtp-nte]
20. codec codec
21. no vad
22. end

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Router&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Step 2 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3 voice service voip</td>
<td>Enters voice service configuration mode and specifies voice-over-IP encapsulation.</td>
</tr>
<tr>
<td>Example: Router(config)# voice service voip</td>
<td>Enters voice register global configuration mode to set global parameters for all supported Cisco SIP IP phones in a Cisco Unified SIP SRST environment.</td>
</tr>
<tr>
<td>Step 4 allow-connections from-type to to-type</td>
<td>Allows connections between specific types of endpoints in a VoIP network.</td>
</tr>
<tr>
<td>Example: Router(config-voi-serv)# allow-connections sip to sip</td>
<td></td>
</tr>
</tbody>
</table>
### Command or Action

<table>
<thead>
<tr>
<th>Step 5</th>
<th>no supplementary-service sip moved-temporarily</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config-voi-serv)# no supplementary-service sip moved-temporarily</td>
</tr>
<tr>
<td><strong>Purpose</strong></td>
<td>Disables supplementary service for call forwarding.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 6</th>
<th>no supplementary-service sip moved-temporarily</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config-voi-serv)# no supplementary-service sip refer</td>
</tr>
<tr>
<td><strong>Purpose</strong></td>
<td>Prevents the router from forwarding a REFER message to the destination for call transfers.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 7</th>
<th>supplementary-service media-renegotiate</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config-voi-serv)# supplementary-service media-renegotiate</td>
</tr>
<tr>
<td><strong>Purpose</strong></td>
<td>Enables mid-call media renegotiation for supplementary services.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 8</th>
<th>sip</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config-voi-serv)# sip</td>
</tr>
<tr>
<td><strong>Purpose</strong></td>
<td>Enters SIP configuration mode.</td>
</tr>
</tbody>
</table>

- Required only if you perform the following step for enabling the SIP registrar function.

<table>
<thead>
<tr>
<th>Step 9</th>
<th>registrar server [expires[max sec][min sec]]</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config-serv-sip)# registrar server expires max 120 min 60</td>
</tr>
<tr>
<td><strong>Purpose</strong></td>
<td>Enables SIP registrar functionality in Unified SRST.</td>
</tr>
</tbody>
</table>

- expires: (Optional) Sets the active time for an incoming registration.
- min sec: (Optional) Minimum expiration time for a registration, in seconds. The range is from 60 to 3600. The default is 60.

<table>
<thead>
<tr>
<th>Step 10</th>
<th>exit</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config-serv-sip)# exit</td>
</tr>
<tr>
<td><strong>Purpose</strong></td>
<td>Exits SIP configuration mode.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 11</th>
<th>exit</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config-voi-serv)# exit</td>
</tr>
<tr>
<td><strong>Purpose</strong></td>
<td>Exits voice-service configuration mode.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 12</th>
<th>voice register global</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config)# voice register global</td>
</tr>
<tr>
<td><strong>Purpose</strong></td>
<td>Enters voice register global configuration mode to set parameters for all supported SIP phones in Unified SRST.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 13</th>
<th>default mode</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config-register-global)# default mode</td>
</tr>
<tr>
<td><strong>Purpose</strong></td>
<td>Enables mode for provisioning SIP phones in Unified SRST. The default mode is Unified SRST itself.</td>
</tr>
</tbody>
</table>
### Command or Action

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| 14   | max-dn max-directory-numbers | Limits number of directory numbers to be supported by this router.  
- Maximum number is platform and version-specific.  
Type ? for value. |
| 15   | max-pool max-voice-register-pools | Sets maximum number of SIP phones to be supported by the Unified SRST router.  
- Maximum number is platform and version-specific.  
Type ? for value. |
| 16   | exit | Exits voice register global configuration mode. |
| 17   | voice register pool pool-tag | Enters voice register pool configuration mode to set phone-specific parameters for a SIP phone. |
| 18   | id { network address mask mask | Explicitly identifies a locally available individual SIP phone to support a degree of authentication. |
| 19   | dtmf-relay rtp-n te | Forwards DTMF tones by using Real-Time Transport Protocol (RTP) with the Named Telephone Event (NTE) payload type and enables DTMF relay using the RFC 2833 standard method. |
| 20   | no vad | Disables voice activity detection (VAD) on the VoIP dial peer.  
- VAD is enabled by default. Because there is no comfort noise during periods of silence, the call may seem to be disconnected. You may prefer to set no vad on the SIP phone pool. |
## Configure Voice Hunt Groups on Unified SRST

To redirect calls for a specific number (pilot number) to a defined group of directory numbers on Cisco Unified SCCP and SIP IP phones, perform the following steps.

Voice Hunt Group on Unified SRST is supported for Parallel, Sequential, Peer, and Longest-Idle hunt groups. Only the basic call features such as Call, Hold or Resume are supported for Unified SRST on Cisco 4000 Series Integrated Services Routers. For support of advanced features such as Auto Logout, Members Logout, and supplementary call features, you need to configure Unified E-SRST. For more information on Voice Hunt Group support on Unified E-SRST, see Unified E-SRST with Support for Voice Hunt Group, page 96.

For a list of restrictions of Unified SRST on Cisco 4000 Series Integrated Services Routers, see Restrictions of Unified SRST on Cisco 4000 Series Integrated Services Routers, page 37

### Prerequisites

- Cisco IOS XE Denali 16.3.1 or later versions.
- Shared Lines are not supported on Unified SRST.

### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `voice hunt-group hunt-tag [longest-idle | parallel | peer | sequential]`
4. `pilot number [secondary number]`
5. `list number`
6. `final number`
7. `preference preference-order [secondary secondary-order]`
8. `timeout seconds`

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Step 21 codec codec-type [bytes] | Specifies the codec supported by a single SIP phone or a VoIP dial peer in a Cisco Unified SIP SRST environment. The `codec-type` argument specifies the preferred codec and can be one of the following:  
  - `g711alaw`: G.711 a–law 64,000 bps.  
  - `g711ulaw`: G.711 mu–law 64,000 bps.  
  - `g729r8`: G.729 8000 bps (default). The `bytes` argument is optional and specifies the number of bytes in the voice payload of each frame. |
| Step 22 end | Returns to privileged EXEC mode. |

Example:

```
Router(config-register-pool)# codec g729r8
```

Example:

```
Router(config-register-pool)# end
```

Specifies the codec supported by a single SIP phone or a VoIP dial peer in a Cisco Unified SIP SRST environment. The `codec-type` argument specifies the preferred codec and can be one of the following:

- `g711alaw`: G.711 a–law 64,000 bps.
- `g711ulaw`: G.711 mu–law 64,000 bps.
- `g729r8`: G.729 8000 bps (default).

The `bytes` argument is optional and specifies the number of bytes in the voice payload of each frame.

Returns to privileged EXEC mode.
### Configure Voice Hunt Groups on Unified SRST

9. **end**

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> voice hunt-group <strong>hunt-tag</strong> [longest-idle</td>
<td>parallel</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config)# voice hunt-group 1 longest-idle</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> pilot <strong>number</strong> [secondary <strong>number</strong>]</td>
<td>Defines the phone number that callers dial to reach a voice hunt group.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-voice-hunt-group)# pilot number 8100</td>
<td></td>
</tr>
</tbody>
</table>
### Command or Action

**Step 5**  
`list number`

**Example:**  
Router(config-voice-hunt-group)# list 8000, 8010, 8020, 8030

**Purpose:**  
Creates a list of extensions that are members of a voice hunt group. To remove a list from a router configuration, use the `no` form of this command.

- *number*—List of extensions to be added as members to the voice hunt group. Separate the extensions with commas.
- Add or delete all extensions in a hunt-group list at one time. You cannot add or delete a single number in an existing list.
- There must be from 2 to 10 extensions in the hunt-group list, and each number must be a primary or secondary number.
- Any number in the list cannot be a pilot number of a parallel hunt group.

**Step 6**  
`final number`

**Example:**  
Router(config-voice-hunt-group)# final 8888

**Purpose:**  
 Defines the last extension in a voice hunt group.

- If a final number in one hunt group is configured as a pilot number of another hunt group, the pilot number of the first hunt group cannot be configured as a final number in any other hunt group.

**Step 7**  
`preference preference-order [secondary secondary-order]`

**Example:**  
Router(config-voice-hunt-group)# preference 6

**Purpose:**  
Sets the preference order for the directory number associated with a voice hunt-group pilot number.

**Note**  
- **preference-order**—Range is 0 to 8, where 0 is the highest preference and 8 is the lowest preference. Default is 0.
- **secondary secondary-order**—(Optional) Keyword and argument combination is used to set the preference order for the secondary pilot number. Range is 1 to 8, where 0 is the highest preference and 8 is the lowest preference. Default is 7.
Configure Voice Hunt Groups on Unified SRST

Configure Feature Support on Unified SIP SRST

This section provides configuration information for some of the features supported on Unified SIP SRST.

Configure SIP-to-SIP Call Forwarding

SIP-to-SIP call forwarding (call routing) is available. Call forwarding is provided either by the phone or by using a back-to-back user agent (B2BUA), which allows call forwarding on any dial peer. Calls into a SIP device may be forwarded to other SIP or SCCP devices (including Cisco Unity, third-party voice-mail systems, or an auto attendant or IVR system such as IPCC and IPCC Express). In addition, SCCP IP phones may be forwarded to SIP phones.

Cisco Unity or other voice messaging systems connected by a SIP trunk or SIP user agent are able to pass a message-waiting indicator (MWI) when a message is left. The SIP phone then displays the MWI when indicated by the voice messaging system.

Note: SIP-to-H.323 call forwarding is not supported.

To configure SIP-to-SIP call forwarding, you must first allow connections between specific types of endpoints in a Cisco IP-to-IP gateway. The allow-connections command grants this capability. Once the SIP-to-SIP connections are allowed, you can configure call forwarding under an individual SIP phone pool. Any of the following commands can be used to configure call forwarding, according to your needs:

- Under voice register pool
  - call-forward b2bua all directory-number

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 8 hops number</td>
<td>For configuring a peer or longest-idle voice hunt group only. Defines the number of times that a call can hop to the next number in a peer or longest-idle voice hunt group before the call proceeds to the final number.</td>
</tr>
<tr>
<td>Example: Router(config-voice-hunt-group)# hops 2</td>
<td></td>
</tr>
<tr>
<td>Step 9 timeout seconds</td>
<td>Defines the number of seconds after which a call that is not answered is redirected to the next directory number in a voice hunt-group list.</td>
</tr>
<tr>
<td>Example: Router(config-voice-hunt-group)# timeout 100</td>
<td>• Default: 180 seconds.</td>
</tr>
<tr>
<td>Step 10 end</td>
<td>Exits to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Router(config-voice-hunt-group)# end</td>
<td></td>
</tr>
</tbody>
</table>
In a typical Cisco Unified SIP SRST setup, the `call-forward b2bua mailbox` command is not used; however, it is likely to be used in a Cisco Unified SIP Communications Manager Express (CME) environment. Detailed procedures for configuring the `call-forward b2bua mailbox` command are found in the *Cisco Unified Communications Manager (CallManager)* documentation on Cisco.com.

The command `call-forward b2bua all` needs to point towards the trunk.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. voice register pool `tag`
4. `call-forward b2bua all` `directory-number`
5. `call-forward b2bua busy` `directory-number`
6. `call-forward b2bua mailbox` `directory-number`
7. `call-forward b2bua noan` `directory-number` `timeout` `seconds`
8. end

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> voice register pool <code>tag</code></td>
<td>Enters voice register pool configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>• Use this command to control which phone registrations are accepted or rejected by a Cisco Unified SIP SRST device.</td>
</tr>
<tr>
<td><strong>Step 4</strong> <code>call-forward b2bua all</code> <code>directory-number</code></td>
<td>Enables call forwarding for a SIP back-to-back user agent (B2BUA) so that all incoming calls are forwarded to another non-SIP station extension (that is, SIP trunk, H.323 trunk, SCCP device or analog/digital trunk).</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>• <code>directory-number</code>: Phone number to which calls are forwarded. Represents a fully qualified E.164 number. Maximum length of the phone number is 32.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Configure Voice Hunt Groups on Unified SRST

Configure Call Blocking Based on Time of Day, Day of Week, or Date

This section applies to both SCCP and SIP SRST. Call blocking prevents the unauthorized use of phones and is implemented by matching a pattern of up to 32 digits during a specified time of day, day of week, or date. Cisco Unified SIP SRST provides SIP endpoints the same time-based call blocking mechanism that is currently provided for SCCP phones. The call blocking feature supports all incoming calls, including incoming SIP and analog FXS calls.

Note: Pin-based exemptions and the “Login” toll-bar override are not supported in Cisco Unified SIP SRST.

---

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 5 call-forward b2bua busy directory-number</td>
<td>Enables call forwarding for a SIP B2BUA so that incoming calls to a busy extension are forwarded to another extension.</td>
</tr>
<tr>
<td>Example: Router(config-register-pool)# call-forward b2bua busy 5006</td>
<td></td>
</tr>
<tr>
<td>Step 6 call-forward b2bua mailbox directory-number</td>
<td>Controls the specific voice-mail box selected in a voice-mail system at the end of a call forwarding exchange.</td>
</tr>
<tr>
<td>Example: Router(config-register-pool)# call-forward b2bua mailbox 5007</td>
<td></td>
</tr>
<tr>
<td>Step 7 call-forward b2bua noan directory-number timeout seconds</td>
<td>Enables call forwarding for a SIP B2BUA so that incoming calls to an extension that does not answer after a configured amount of time are forwarded to another extension.</td>
</tr>
<tr>
<td>Example: Router(config-register-pool)# call-forward b2bua noan 5010 timeout 10</td>
<td>This command is used if a phone is registered with a Cisco Unified SIP SRST router, but the phone is not reachable because there is no IP connectivity (there is no response to Invite requests).</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 8 end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Router(config-register-pool)# end</td>
<td></td>
</tr>
</tbody>
</table>
The commands used for SIP phone call blocking are the same commands that are used for SCCP phones on your Cisco Unified SRST system. The Cisco SRST session application accesses the current after-hours configuration under call-manager-fallback mode and applies it to calls originated by Cisco SIP phones that are registered to the Cisco SRST router. The commands used in call-manager-fallback mode that set block criteria (time/date/block pattern) are the following:

- **after-hours block pattern** pattern-tag pattern [7-24]
- **after-hours day** day start-time stop-time
- **after-hours date** month date start-time stop-time

When a user attempts to place a call to digits that match a pattern that has been specified for call blocking during a time period that has been defined for call blocking, the call is immediately terminated and the caller hears a fast busy.

In SRST (call-manager-fallback configuration mode), there is no phone- or pin-based exemption to after-hours call blocking. However, in Cisco Unified SIP SRST (voice register pool mode), individual IP phones can be exempted from all call blocking using the `after-hours exempt` command.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. call-manager-fallback
4. after-hours block pattern tag pattern [7-24]
5. after-hours day day start-time stop-time
6. after-hours date month date start-time stop-time
7. exit
8. voice register pool tag
9. after-hour exempt
10. end

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
</tbody>
</table>
### Configure Voice Hunt Groups on Unified SRST

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 3</strong> call-manager-fallback</td>
<td>Enters call-manager-fallback configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config)# call-manager-fallback</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> after-hours block pattern tag pattern [7-24]</td>
<td>Defines a pattern of outgoing digits to be blocked. Up to 32 patterns can be defined, using individual commands.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-cm-fallback)# after-hours block pattern 1 91900</td>
<td>• If the 7-24 keyword is specified, the pattern is always blocked, 7 days a week, 24 hours a day.</td>
</tr>
<tr>
<td></td>
<td>• If the 7-24 keyword is not specified, the pattern is blocked during the days and dates that are defined using the after-hours day and after-hours date commands.</td>
</tr>
<tr>
<td><strong>Step 5</strong> after-hours day day start-time stop-time</td>
<td>Defines a recurring time period based on the day of the week during which calls are blocked to outgoing dial patterns that are defined using the after-hours block pattern command.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-cm-fallback)# after-hours day mon 19:00 07:00</td>
<td>• day: Day of the week abbreviation. The following are valid day abbreviations: sun, mon, tue, wed, thu, fri, sat.</td>
</tr>
<tr>
<td></td>
<td>• start-time stop-time: Beginning and ending times for call blocking, in an HH:MM format using a 24-hour clock. If the stop time is a smaller value than the start time, the stop time occurs on the day following the start time. For example, “mon 19:00 07:00” means “from Monday at 7 p.m. until Tuesday at 7 a.m.”</td>
</tr>
<tr>
<td></td>
<td>The value 24:00 is not valid. If 00:00 is entered as a stop time, it is changed to 23:59. If 00:00 is entered for both start time and stop time, calls are blocked for the entire 24-hour period on the specified date.</td>
</tr>
<tr>
<td><strong>Step 6</strong> after-hours date month date start-time stop-time</td>
<td>Defines a recurring time period based on month and date during which calls are blocked to outgoing dial patterns that are defined using the after-hours block pattern command.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-cm-fallback)# after-hours date jan 1 00:00 00:00</td>
<td>• month: Month abbreviation. The following are valid month abbreviations: jan, feb, mar, apr, may, jun, jul, aug, sep, oct, nov, dec.</td>
</tr>
<tr>
<td></td>
<td>• date: Date of the month. Range is from 1 to 31.</td>
</tr>
<tr>
<td></td>
<td>• start-time stop-time: Beginning and ending times for call blocking, in an HH:MM format using a 24-hour clock. The stop time must be larger than the start time. The value 24:00 is not valid. If 00:00 is entered as a stop time, it is changed to 23:59. If 00:00 is entered for both start time and stop time, calls are blocked for the entire 24-hour period on the specified date.</td>
</tr>
</tbody>
</table>
### Configure Voice Hunt Groups on Unified SRST

#### Verification

To verify the feature's configuration, enter one of the following commands:

- **show voice register dial-peer**: Displays all the dial peers created dynamically by phones that have registered. This command also displays configurations for after hours blocking and call forwarding.
- **show voice register pool <tag>**: Displays information about a specific pool.
- **debug ccsip message**: Debugs basic B2BUA calls.

For more information about these commands, see *Cisco Unified SRST and Cisco Unified SIP SRST Command Reference (All Versions)*.

---

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 7</strong> exit</td>
<td>Exits call-manager-fallback configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-cm-fallback)# exit</td>
<td></td>
</tr>
</tbody>
</table>

| **Step 8** voice register pool tag | Enters voice register pool configuration mode.  
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td>Use this command to control which registrations are accepted or rejected by a Cisco Unified SIP SRST device.</td>
</tr>
<tr>
<td>Router(config)# voice register pool 12</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Step 9</strong> after-hour exempt</th>
<th>Specifies that for a particular voice register pool, none of its outgoing calls are blocked although call blocking is enabled.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-register-pool)# after-hour exempt</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Step 10</strong> end</th>
<th>Returns to privileged EXEC mode.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-register-pool)# end</td>
<td></td>
</tr>
</tbody>
</table>
SIP Call Hold and Resume

Unified SRST supports the ability for SIP phones to place calls on hold and to resume from calls placed on hold. This also includes support for a consultative hold where A calls B, B places A on hold, B calls C, and B disconnects from C and then resumes with A. Support for call hold is signaled by SIP phones using “re-INVITE c=0.0.0.0” and also by the receive-only mechanism.

No configuration is necessary.

Configure Music On Hold for Unified SRST

Unified SRST supports the ability for SIP phones to play music for calls placed on hold. The following is the recommended configuration for Music On Hold (MOH) on a SIP Phone that falls back to Unified SRST.

SUMMARY STEPS

1. enable
2. configure terminal
3. no telephony-service
4. call-manager-fallback
5. moh enable-g711 "flash:filename"
6. moh g729 "flash:filename"
7. end

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router&gt; enable</td>
</tr>
<tr>
<td>Step 2 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router# configure terminal</td>
</tr>
<tr>
<td>Step 3 no telephony-service</td>
<td>Removes all the configurations for IP phones configured under the telephony-service configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router# no telephony-service</td>
</tr>
</tbody>
</table>
Enabling KPML for SIP Phones

Perform the following steps to enable KPML digit collection on a SIP phone.

Restrictions

- A dial plan assigned to a phone has priority over KPML.

SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `voice register pool pool-tag`
4. `digit collect kpml`
5. `end`
6. `show voice register dial-peer`
Configure Voice Hunt Groups on Unified SRST

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Step 2 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>• pool-tag: Unique sequence number of the SIP phone to be configured.</td>
</tr>
<tr>
<td>Step 3 voice register pool pool-tag</td>
<td>• Range is version and platform-dependent; type ? to display range.</td>
</tr>
<tr>
<td>Example:</td>
<td>• You can modify the upper limit for this argument with the max-pool</td>
</tr>
<tr>
<td>Step 4 digit collect kpml</td>
<td>Enables KPML digit collection for the SIP phone.</td>
</tr>
<tr>
<td>Example:</td>
<td>• This command is enabled by default for supported phones in Cisco</td>
</tr>
<tr>
<td>Step 5 end</td>
<td>• Exit to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>• Cisco Unified CME and Cisco Unified SRST.</td>
</tr>
<tr>
<td>Step 6 show voice register dial-peers</td>
<td>Displays details of all dynamically created VoIP dial peers</td>
</tr>
<tr>
<td>Example:</td>
<td>• associated with the Cisco Unified CME SIP register including the</td>
</tr>
<tr>
<td></td>
<td>• defined digit collection method.</td>
</tr>
</tbody>
</table>

Disabling SIP Supplementary Services for Call Forward and Call Transfer

Perform the following steps to disable REFER messages for call transfers and redirect responses for call forwarding from being sent to the destination by Unified SRST. You can disable these supplementary features if the destination gateway does not support them.

SUMMARY STEPS

1. enable
2. configure terminal
3. voice service voip
   or
dial-peer voice tag voip
4. `no supplementary-service sip {moved-temporarily | refer}`
5. `end`

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>· Enter your password if prompted.</td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> voice service voip</td>
<td>Enters voice-service configuration mode to set global parameters for VoIP features.</td>
</tr>
<tr>
<td>or</td>
<td>· Enters dial peer configuration mode to set parameters for a specific dial peer.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# voice service voip or</td>
<td></td>
</tr>
<tr>
<td>Router(config)# voice service voip</td>
<td></td>
</tr>
<tr>
<td>or</td>
<td></td>
</tr>
<tr>
<td>Router(config)# voice service voip</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> no supplementary-service sip {moved-temporarily</td>
<td>refer}</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>· moved-temporarily: SIP redirect response for call forwarding.</td>
</tr>
<tr>
<td>Router(conf-voi-serv)# no supplementary-service</td>
<td>· refer: SIP REFER message for call transfers.</td>
</tr>
<tr>
<td>sip refer</td>
<td>· Sending REFER and redirect messages to the destination is the default behavior.</td>
</tr>
<tr>
<td>or</td>
<td>Note: This command is supported for calls between SIP phones and calls between SCCP phones. It is not supported for a mixture of SCCP and SIP endpoints.</td>
</tr>
<tr>
<td>Router(config-dial-peer)# no supplementary-service sip refer</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> end</td>
<td>Exits to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-voi-serv)# end or</td>
<td></td>
</tr>
<tr>
<td>Router(config-dial-peer)# end</td>
<td></td>
</tr>
</tbody>
</table>

### Configuring Idle Prompt Status for SIP Phones

Perform the following steps to customize the message that displays on SIP phones after the phones failover to Cisco Unified SRST.
Configure Voice Hunt Groups on Unified SRST

Note
You do not need to create new configuration files with the **create profile** command and restart the phones after changing the idle status message in Cisco Unified SRST. Modifying the status message takes effect immediately in Cisco Unified SRST.

SUMMARY STEPS

1. enable
2. configure terminal
3. voice register global
4. system message *string*
5. end
6. show voice register global

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td>Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> voice register global</td>
<td>Enters voice register global configuration mode to set global parameters for all supported SIP phones in a Cisco Unified CME environment.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# voice register global</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> system message <em>string</em></td>
<td>Defines a status message that displays on SIP phones registered to Cisco Unified SRST.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-register-global)# system message fallback active</td>
<td><em>string</em>: Up to 32 alphanumeric characters. Default is “CM Fallback Service Operating.”</td>
</tr>
<tr>
<td><strong>Step 5</strong> end</td>
<td>Exits to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-register-global)# end</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> show voice register global</td>
<td>Displays all global configuration parameters associated with SIP phones.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router# show voice register global</td>
<td></td>
</tr>
</tbody>
</table>
Examples

The following are sample configurations for supporting SIP SRST on Cisco 4000 Series Integrated Services Router.

Example for Configuring Unified SIP SRST on Cisco 4000 Series Integrated Services Routers

The following example shows how to configure Unified SIP SRST on Cisco 4000 Series Integrated Services Routers.

```
voice service voip
allow-connections sip to sip
no supplementary-service sip moved-temporarily
no supplementary-service sip refer
supplementary-service media-renegotiate
sip
registrar server expires max 120 min 60
!
!
voice register global
default mode
max-dn 40
max-pool 40
!
voice register pool 1
id network 8.55.0.0 mask 255.255.0.0
dtmf-relay rtp-nre
codec g711ulaw
no vad
!
!
```

Example for Configuring Voice Hunt Groups in Unified SIP SRST

The following example shows how to configure longest-idle hunt group 20 with pilot number 4701, final number 5000, and 6 numbers in the list. After a call is redirected six times (makes 6 hops), it is redirected to the final number 5000.

```
Router(config)# voice hunt-group 20 longest-idle
Router(config-voice-hunt-group)# pilot 4701
Router(config-voice-hunt-group)# list 4001, 4002, 4023, 4028, 4045, 4062
Router(config-voice-hunt-group)# final 5000
Router(config-voice-hunt-group)# hops 6
Router(config-voice-hunt-group)# timeout 20
Router(config-voice-hunt-group)# exit
```
Examples for Configuring IPv6 Pools for SIP IP Phones

The following example provides configuration of IPv6 pools for SIP IP Phones:

```
ipv6 unicast-routing
voice service voip
sip
no anat
call service stop
exit
exit
sip-ua
protocol mode dual-stack
exit
voice service voip
sip
no call service stop
exit
voice register global
default mode
max-dn 50
max-pool 40
exit
voice register pool 1
id network 2001:420:54FF:13::901:0/117
end
```

The following example provides interface configuration for IPv6 supported on Unified SRST:

```
configure terminal
interface GigabitEthernet0/0/1
ip address 10.64.86.229 255.255.255.0
negotiation auto
ipv6 address 2001:420:54FF:13::312:82/119
ipv6 enable
```

The following example provides IP route configuration for IPv6 supported on Unified SRST:

```
```

The following example displays output when SIP call service is shut down with the `call service stop` CLI command:

```
Router# show sip service
SIP service is shut
under 'voice service voip', 'sip' submode
```

The following example displays output when SIP call service is active with the `no call service stop` CLI command:

```
Router# show sip-ua service
SIP Service is up
under 'voice service voip', 'sip' submode
```
Example for Configuring Call Blocking Based on Time of Day, Day of Week, or Date

The following example defines several patterns of digits for which outgoing calls are blocked. Patterns 1 and 2, which block calls to external numbers that begin with 1 and 011, are blocked on Monday through Friday before 7 a.m. and after 7 p.m. Pattern 3 blocks calls to 900 numbers 7 days a week, 24 hours a day.

call-manager-fallback
  after-hours block pattern 1 91
  after-hours block pattern 2 9011
  after-hours block pattern 3 91900 7-24
  after-hours day mon 19:00 07:00
  after-hours day tue 19:00 07:00
  after-hours day wed 19:00 07:00
  after-hours day thu 19:00 07:00
  after-hours day fri 19:00 07:00

The following example exempts a Cisco SIP phone pool from the configured blocking criteria:

voice register pool 1
  after-hour exempt

Example for Configuring Music On Hold for Unified SIP SRST

The following example shows how to configure Music On Hold (MOH) for Unified SIP SRST on Cisco 4000 Series Integrated Services Routers.

enable
configure terminal
no telephony-service
call-manager-fallback
moh enable-g711 "flash:music-on-hold.au"
moh g729 "flash:SampleAudioSource.g729.wav"

Example for Configuring SIP-to-SIP Call Forwarding on Unified SRST

The following is a sample configuration for SIP-to-SIP Call Forwarding on Unified SRST.

enable
configure terminal
voice register pool 15
call-forward b2bua busy 5006
call-forward b2bua mailbox 5007
call-forward b2bua noan 5010 timeout 8

Example for Configuring Idle Prompt Status for SIP Phones

The following is a sample configuration for idle prompt status for SIP phones on Unified SRST.

enable
configure terminal
voice register global
system message fallback active
end
Example for Disabling SIP Supplementary Services for Call Forward and Call Transfer

The following is a sample configuration for disabling SIP supplementary services for call forward and call transfer on Unified SRST.

```
enable
configure terminal
voice service voip
no supplementary-service sip {moved-temporarily | refer}
end
```