Cisco Unified SRST Manager Administration Guide

First Published: August, 2012
Last Updated: March 30, 2018

Cisco Systems, Inc.
www.cisco.com

Cisco has more than 200 offices worldwide.
Addresses, phone numbers, and fax numbers
are listed on the Cisco website at
www.cisco.com/go/offices.

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

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

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

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

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

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

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

Cisco Unified SRST Manager Administration Guide
© 2018 Cisco Systems, Inc. All rights reserved.

CONTENTS

Preface

This preface describes the audience and conventions of the *Cisco Unified SRST Manager Administration Guide*. It also describes the available product documentation and provides information on how to obtain documentation and technical assistance.

Audience

This guide is intended primarily for network administrators and channel partners.

Conventions

This guide uses the following conventions:

Item	Convention
Commands and keywords.	**boldface** font
Variables for which you supply values.	*italic* font
Optional command keywords. You do not have to select any options.	[enclosed in brackets]
Required command keyword to be selected from a set of options. You must choose one option.	{options enclosed in braces | separated by vertical bar}
Displayed session and system information.	`screen` font
Information you enter.	**`boldface screen`** `font`
Variables you enter.	*`italic screen`* font
Menu items and button names.	**boldface** font
Choosing a menu item.	**Option > Network Preferences**

Note Means *reader take note*.

Tip Means *the following information will help you solve a problem*.

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

Timesaver Means *the described action saves time*. You can save time by performing the action described in the paragraph.

Warning **Means *reader be warned*. In this situation, you might perform an action that could result in bodily injury.**

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

Feature History

This section lists the features documented in the *Cisco Unified SRST Manager Administration Guide* and maps them to the modules in which they appear.

Note Cisco Unified Survivable Remote Site Telephony (SRST) Manager is **End-of-Life (EOL)**. Hence, provisioning for Unified E-SRST through Unified SRST Manager is not supported for Unified E-SRST Release 12.2 and later releases. For more information, see Migration from Unified SRST Manager to Unified E-SRST, page 9.

Feature and Release Support

Table -1 lists the Cisco Unified Survivable Remote Site Telephony (SRST) Manager version that introduced support for a given feature. Unless noted otherwise, subsequent versions of Cisco Unified SRST Manager supports that feature. The features that were introduced or modified in Cisco Unified SRST Manager 9.0.6 and later appear in the table.

Note Not all features may be supported in your Cisco Unified SRST Manager version.

To determine the correct Cisco Unified Communications Manager version and Cisco Unified Survivable Remote Site Telephony (SRST/ESRST) release that supports a specific Cisco Unified SRST Manager version, see the *Cisco Unified SRST Manager Compatibility Matrix* at: http://docwiki.cisco.com/wiki/Cisco_Unified_SRST_Manager_Compatibility_Matrix

Table -1 Supported Cisco Unified SRST Manager Features

Version	Feature Name	Feature Description	Documented In
11.0	Configuration Changes	Users can view the list of CLIs that are pushed to router by Cisco Unified SRST Manager.	Viewing Configuration Changes
	AXL Upgrade	Administrative XML (AXL) support is upgraded to 9.0 from Cisco Unified SRST Manager 11.0 onwards.	Supported Phones and Platforms
	Rollback	In case of a provisioning failure, the Cisco Unified SRST Manager restores the router back to the original configuration state by removing all the new CLIs that were added before the failure.	Changing the Information for a Single Cisco Unified SRST Site
	Intelligent Provisioning	The Cisco Unified SRST Manager triggers provisioning if there are configuration changes from the last successful provisioning.	About Scheduled Provisioning
	ESRST Scalability	From Cisco Unified SRST Manager Release 11.0 onwards, the scale of Enhanced SRST (ESRST) mode is increased to match the scale of classic SRST for both Session Initiation Protocol (SIP) and Signaling Connection Control Protocol (SCCP) phones.	*Cisco Unified Survivable Remote Site Telephony and Cisco Unified Enhanced Survivable Remote Site Telephony Version 11.0 Data Sheet*
	New Phone Support	Cisco Unified SRST Manager Release 11.0 supports new phone models.	*Cisco Unified SRST Manager Compatibility Matrix*
	Alert Enhancement	Error messages are made more meaningful to enhance the debug ability.	System Alerts
	DNS Enhancement	Entering the DNS server details is optional while configuring Cisco Unified Communications Manager from Cisco Unified SRST Manager.	Using the Central Call Agent Wizard to Add Cisco Unified Communications Manager Information
	User Management	Enables Cisco Unified SRST Manager with multiple user support.	Configuring Users for Cisco Unified SRST Manager
	Fast Track Support	Fast track is supported from Cisco Unified SRST Manager 11.0 onwards for SIP phones in ESRST mode.	*Cisco Unified SRST Manager Compatibility Matrix*
	Jabber CSF Client Support	Support is provided for Cisco Jabber - Client Services Framework (CSF) Client.	*Cisco Unified SRST Manager Compatibility Matrix*
	Scheduling	From Cisco Unified SRST Manager 11.0 onwards, scheduled provisioning is optional.	Using the Central Call Agent Wizard to Add Cisco Unified Communications Manager Information
	New Platform Support	Cisco Unified SRST Manager 11.0 supports five new platforms.	*Cisco Unified SRST Manager Compatibility Matrix*
	ESXi 5.1 and ESXi 5.5 Support	Cisco Unified SRST Manager 11.0 supports ESXi 5.1 and ESXi 5.5.	Cisco Unified SRST Manager Overview

Table -1 Supported Cisco Unified SRST Manager Features (continued)

Version	Feature Name	Feature Description	Documented In
9.0.6	No Dial Plan Support	Dial Plan is not supported from Cisco Unified SRST Manager 9.0.6. A note has been added in the applicable sections.	Cisco Unified SRST Manager Overview
	AXL Upgrade	Administrative XML (AXL) support is upgraded to 8.5 from Cisco Unified SRST Manager 9.0.6 onwards.	Supported Phones and Platforms

Cisco Unified SRST Manager Workflow

This section provides the steps to be followed to set up the Cisco Unified SRST Manager and provision the routers.

Step 1 Download the Open Virtual Appliance (OVA) file from Cisco.com and deploy it on your local system using VMware vSphere.

Step 2 Configure the IP address, Netmask, Gateway, Location, and User and Admin credentials.

Step 3 Log in to the Cisco Unified SRST Manager using the credentials configured in Step 2.

Step 4 Choose **System > Trusted TLS Certificates > Add**, enter the required details and click **Update**.

Step 5 Secure the communication between the Cisco Unified SRST Manager and Branch Office.

Note If you opt for secure communication, you should create a secure configuration in the branch router.

Step 6 Choose **Setup Wizards > Add Central Call Agent** and update the necessary details.

Step 7 Choose **Configure > Sites** and click **Retrieve SRST References** to view the Cisco Unified Communication Manager site information.

Step 8 Choose **Configure > Sites**. Click the corresponding router name, provide the details, and click **Update**.

Step 9 Choos**e Troubleshoot > Network Connectivity** and click **Start Network Connectivity Test** to test the connectivity for the configured site.

Step 10 Choose **Configure > Sites**, select the router name, and click **Provision** to provision the site.

Step 11 Choose **Reports > Site Provisioning History** to check the provisioning status.

PART 1

Overview and Initial Configuration

Cisco Unified SRST Manager Overview

This module provides an overview of Cisco Unified SRST Manager Release, and technical information that you need for using and maintaining Cisco Unified SRST Manager.

Migration from Unified SRST Manager to Unified E-SRST

Cisco Unified Survivable Remote Site Telephony (SRST) Manager is **End-of-Life (EOL)**. Hence, provisioning for Unified E-SRST through Unified SRST Manager is not supported for Unified E-SRST Release 12.2 and later releases. Unified E-SRST is provisioned only using CLI commands (manual provisioning) to support fall back of phones registered to Unified Communications Manager. For more information on configuring Unified E-SRST, see *Cisco Unified SCCP and SIP SRST System Administrator Guide (All Versions)*.

Overview

Note Cisco Unified SRST Manager software does not support provisioning Media Gateway Control Protocol (MGCP) dial plan. Cisco has removed the support for this feature due to the complexity of and differences between dial plans across the globe. These complexities and differences must be analyzed by a Cisco engineering team member to understand whether the Cisco Unified SRST Manager dial plan logic can meet customer requirements. If you are interested in automatic dial plan provisioning, contact srstmgr@cisco.com. The Cisco engineering team member requires a copy of your Cisco Unified Communications Manager dial plan (.tar file) for analysis. After analysis, a private build of the Cisco Unified SRST Manager with the dial plan provisioning feature enabled will be delivered.

Cisco Unified SRST Manager Release operates within a virtual machine, running in the VMware ESXi (4.1, 5.0, 5.1, or 5.5) hypervisor environment. The software is packaged as an open virtualization archive (OVA) template for installation within the VM environment. The OVA file includes the Cisco Unified SRST Manager software, as well as the virtual machine system settings preconfigured to operate with Cisco Unified SRST Manager.

Cisco Unified SRST Manager includes the following features:

- Support for traditional SRST and enhanced E-SRST.
- Failover support for SCCP and SIP phones.
- Management of the dial plan configuration on SRST routers, enabling internal/external dialing in survival mode (supported with MGCP gateways only).

- Advanced features, such as hunt groups, call park/group call park, and call pickup (on E-SRST routers).
- Advanced scheduling options to configure exactly when Cisco Unified SRST Manager retrieves configuration information from CUCM and provisions the branch office routers.
- Option to configure the branch router as a traditional SRST or E-SRST. Traditional SRST supports basic telephony features and a higher count of phones and extensions. E-SRST provides enhanced features, with more limited scalability.

Enhanced Survivable Remote Site Telephony (E-SRST)

This section describes the Cisco Enhanced Survivable Remote Site Telephony (E-SRST) solution.

- Overview of E-SRST Telephony
- Prerequisites
- E-SRST Limitations
- Cisco Unified SRST Manager Limitations
- Cisco Unified SRST Manager Telephony Features Limitations
- Cisco Unified SRST Manager Support of VMware Features

Overview of E-SRST Telephony

Cisco Unified SRST Manager operates as part of the Cisco Enhanced Survivable Remote Site Telephony (E-SRST) solution. Survivable Remote Site Telephony (SRST) and E-SRST solutions provide telephone functionality in remote branch sites during temporary WAN outages that prevent communication between the central site and the branch site.

Table 1 describes the features of the Cisco Unified SRST and Cisco Unified E-SRST solutions.

Table 1 Cisco Unified SRST and Cisco Unified E-SRST Features

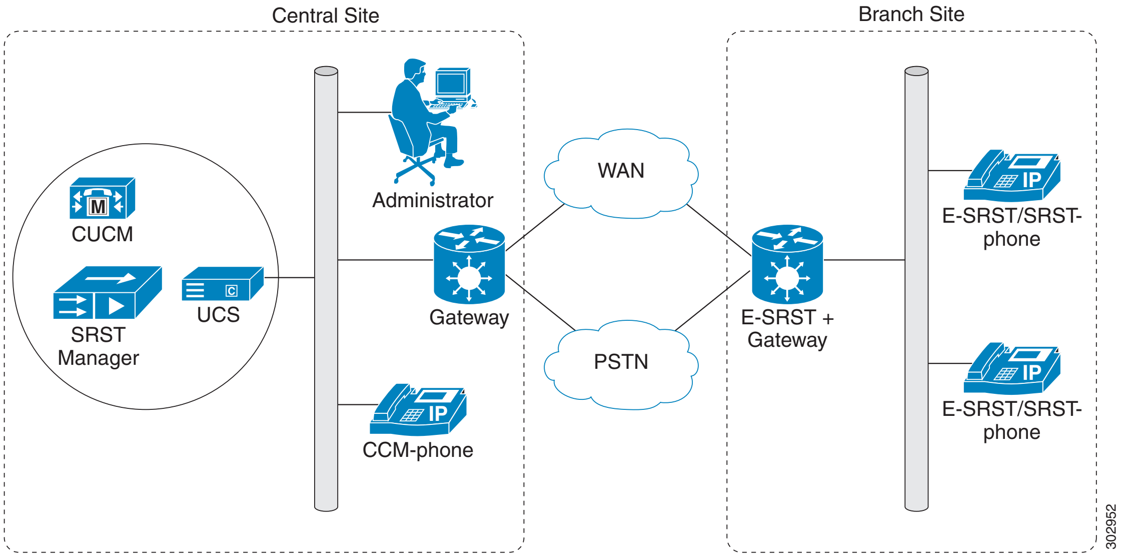
Cisco Unified SRST Solution	Cisco Unified E-SRST Solution
Features	
Basic telephone features during failover	Advanced telephone feature support during failover Simplified administration Automated provisioning and deployment Improved security features
Telephone Support	
Support of SIP and SCCP phones	Support of SIP and SCCP phones
Call Manager Support	
Cisco Unified Communications Manager Cisco Business Edition 6000	Cisco Unified Communications Manager Cisco Business Edition 6000

The E-SRST solution supports advanced Cisco Unified Communications Manager Express (CUCME) telephony features such as hunt groups and pick-up groups, but reduces the complex and manual configuration required at the branch site.

In the E-SRST solution, Cisco Unified SRST Manager resides at the central site and collects information from Cisco Unified Communications Manager. Cisco Unified SRST Manager collects configuration information required for advanced features such as hunt groups and pick-up groups, and distributes the configuration information to the branch sites. In the event of a WAN outage, when the E-SRST service running on the branch office routers takes over call processing, it applies the configuration provisioned by Cisco Unified SRST Manager to provide enhanced telephony services at the branch sites.

Figure 1 shows the supported topology model for E-SRST on a branch site.

Figure 1 E-SRST Topology



For Cisco Unified E-SRST deployments, the branch office is configured in Cisco Unified Communications Manager Express-as-SRST mode on a Cisco Integrated Services Router (ISR) or a Cisco Integrated Services Router Generation 2 (ISR G2). The number of phones supported for SRST mode and E-SRST mode are available in the datasheet at *Cisco Unified Survivable Remote Site Telephony and Cisco Unified Enhanced Survivable Remote Site Telephony Version 11.0 Data Sheet*.

The E-SRST feature provides automated remote site provisioning of the following advanced telephony features in survivable mode by collecting the configuration information from Cisco Unified Communications Manager:

- After-hours
- Call pickup and group pickup
- Call routing restrictions (local and long distance, and time of day)
- Class of restrictions
- Dial Plan
- Hunt groups
- Phones and extensions (speed dials, lines, softkeys)
- Pick-up groups

Cisco Unified SRST Manager enables you to set up provisioning schedules for defining when and how often to retrieve configuration information from Cisco Unified Communications Manager and provision the branch site E-SRST routers. You can also perform provisioning on-demand to synchronize a specific E-SRST router with the Cisco Unified Communications Manager information.

The E-SRST solution enables a phone in Cisco Unified SRST mode to operate similarly to when the system is in normal Cisco Unified Communications Manager mode. The look and feel of the phone displays and softkeys in Cisco Unified E-SRST mode are similar to those in normal Cisco Unified Communications Manager mode.

For more information about Cisco Unified Survivable Remote Site Telephony, see:

Cisco Unified SCCP and SIP SRST System Administrator Guide (All Versions)

Prerequisites

Cisco Unified SRST Manager works only with the Primary Node Publisher of the Cisco Unified Communications Manager (CUCM) cluster. More then one cluster is not supported.

E-SRST Limitations

- E-SRST requires Cisco Unified Communications Manager Express Release 8.6 and later.
- E-SRST does not support secure Cisco Unified SRST.
- E-SRST does not support special characters such as @, !, +
- COR lists can be applied to a maximum of 4 DNs on a SIP phone (voice register pool).

Cisco Unified SRST Manager Limitations

- Extension mobility on Cisco Unified Communications Manager is not supported.
- Dial plan provisioning is supported only for MGCP gateways.
- Supports only button layouts that have line numbers first, followed by speed dials. Interleaving of speed dials and line numbers is not supported.
- Cisco Unified SRST Manager Release does not support IPv6 addressing.
- VMware tools are part of the system and cannot be upgraded.
- Only one network interface (vNIC) is supported. Do not add additional network interfaces.
- If clock sync to hardware is enabled for the Cisco Unified SRST Manager VM on the vSphere/vCenter application, disable NTP configuration on Cisco Unified SRST Manager.
- When a Cisco Unified SRST Manager user initiates a browser session, the previous session is terminated automatically.

Cisco Unified SRST Manager Telephony Features Limitations

After Hours

- Supports single partition only.

Call Park

- Supports general purpose call park only
- A maximum of 10 park slots can be created
- It is recommended to create only one park slot range. In case of multiple call park slot numbers or range configured, only one of them gets picked up randomly. Determining which call park got picked up is not supported.

COR

- Calling privileges (CSS and partition) in translation pattern is not supported. Translation patterns are configured as number expansions in E-SRST and configuring calling privileges in number expansions is not supported.

Dial Plan

Note Cisco Unified SRST Manager software does not support provisioning Media Gateway Control Protocol (MGCP) dial plan. Cisco has removed the support for this feature due to the complexity of and differences between dial plans across the globe. These complexities and differences must be analyzed by a Cisco engineering team member to understand whether the Cisco Unified SRST Manager dial plan logic can meet customer requirements. If you are interested in automatic dial plan provisioning, contact srstmgr@cisco.com. The Cisco engineering team member requires a copy of your Cisco Unified Communications Manager dial plan (.tar file) for analysis. After analysis, a private build of the Cisco Unified SRST Manager with the dial plan provisioning feature enabled will be delivered.

- The @ wildcard in the route pattern is not supported. Cisco Unified SRST Manager converts the @ wildcard to T. In Cisco Unified Communications Manager, the @ wildcard is a special macro function that expands into a series of patterns representing the entire national numbering plan for a certain country. For example, configuring a single unfiltered route pattern such as 9.@ with the North American Numbering Plan really adds 166 individual route patterns to the Unified CM internal dial plan database.
- PreDot is the only Digit Discard Instruction (DDI) supported. All the other configured DDIs are ignored.
- Calling party transformation in translation pattern is ignored. Translation patterns are configured as number expansions in E-SRST and there is no way to configure calling party transformation using number expansion.
- A maximum of 250 translation patterns are supported because E-SRST supports a maximum of 250 number expansions.
- Calling number transformation is configured in the router using voice translation rules. If an external phone number mask is selected in the calling number transformation and if the external phone number mask is not same for all the DNs in Cisco Unified SRST Manager, then the calling number transformation is ignored.
- The following items in the device pool of all DNs for a site must be the same: SRST reference, external phone number mask, local route group, calling/called party settings, and so on. Otherwise dial plan will not be provisioned correctly.
- Caller ID, Num Digits or Prefix Dn from the port configuration of a T1 CAS port is only used if these configurations are same for all the ports in a T1 CAS.

Hunt Groups

- The E-SRST Hunt Group feature is based on the Cisco Unified Call Manager Express (CME) Voice Hunt Group feature. The hunt group membership is configured within CME using the Cisco IOS **list** command within the "voice hunt-group" CLI sub-mode. The **list** command typically limits the number of hunt group members to a maximum of 32. Limits may vary, depending on the specific IOS release version running on the router. If the Cisco Unified Communications Manager hunt group has more than this number of hunt group members, only the first 32 members will be configured on the E-SRST router.

  For current details on the CME CLI limitations of the voice hunt-group list command, see:

  http://www.cisco.com/en/US/docs/voice_ip_comm/cucme/command/reference/cme_l1ht.html#wp1045524

Phones

- One user per phone. The Cisco Unified Call Manager Express (CME) router does not support using the same username on multiple ephones. Phones will be provisioned by using MAC address as the username.
- Softkeys on SIP phone do not survive after failover. Some of the softkey features are disabled in the phone firmware. As a result any features that requires softkeys will not function, such as call-park, call-pickup, and so on.
- Cisco Unified SRST Manager does not support softkey template for SIP phones.
- For the list of supported phones, see *Cisco Unified SRST Manager Supported Phones and Platforms*

Voicemail

- When Cisco Unified Communications Manager has the same voicemail pilot configured for all of the phones in a branch router, Cisco Unified SRST Manager will provision the voicemail pilot in the router. When Cisco Unified Communications Manager has different voicemail pilots configured on difference phones in a branch router, Cisco Unified SRST Manager cannot determine only one vmpilot, and it deletes the voicemail from the branch router.
- Only numeric characters [0-9] are supported for voicemail pilot number.
- If voicemail is configured in both Cisco Unified Communications Manager and Cisco Unified SRST Manager then, voicemail from Cisco Unified SRST Manager is configured on the router.
- Default voicemail profile from Cisco Unified Communications Manager is configured on router if there is at least one phone associated for that Cisco Unified SRST reference.
- If none of the phones of Cisco Unified SRST reference is associated with any voicemail then, default voicemail is configured on the router.

Shared Line

- Shared line provides SIP-SIP, SCCP-SCCP, and SIP-SCCP support.
- Shared line support is available only in ESRST mode.
- Need to have phone firmware which supports version negotiation features on phone.
- Shared line between SIP-SIP and SIP-SCCP is supported from SRST 10.0, IOS version 15.3(3)M.
- All instances of shared lines that share a particular extension should have same name and label. If the name and label are not same across all instances of a shared line, it results in incorrect name and label.

Video

Video and camera is not supported in SRST (classic as well as ESRST mode).

Call Park/Pickup

- Call park/pickup configurations are provisioned by Cisco Unified SRST Manager. However, due to SIP phone softkey firmware limitations during failover, call park/pickup on SIP phones do not work during failover mode.

Music-On-Hold (MOH)

- Music On Hold (MOH) on SIP phones is only supported with SIP phone firmware load 9.2.
- The default Music On Hold audio file is “cusm-music-on-hold.au”. MOH is provisioned regardless of the Cisco Unified Communications Manager configuration. Provisioning can be disabled using the Cisco Unified SRST Manager GUI.

Single Number Reach (SNR)

- SIP SNR is only supported with CME 9.0.
- SNR is not supported for DNs that are shared.
- SNR mobility softkeys in the phone do not survive during failover mode. Current phone firmware defaults to its own phone softkeys defaults during failover.

Cisco Unified SRST Manager Support of VMware Features

Table 2 describes the Cisco Unified SRST Manager support of VMware features.

Table 2 Support of VMware Features

Feature	Support
VM Templates (OVAs)	Yes
Copy Virtual Machine	Yes
Restart Virtual Machine on Different ESXi Host	Yes
Resize Virtual Machine	No
VMware Hot Add	No
Multiple Physical NICs and vNICs	Yes for pNICs, only 1 vNIC
VMware High Availability (HA)	No
VMware Site Recovery Manager (SRM)	No
VMware vNetwork Distributed Switch	Yes
VMware vMotion	No
VMware Dynamic Resource Scheduler (DRS)	No
VMware Dynamic Power Management	No
Long Distance vMotion	No
VMware Storage vMotion	No
VMware vCenter Update Manager (VUM)	No

Table 2 Support of VMware Features

Feature	Support
VMware Consolidated Backup (VCB)	No
VMware Data Recovery (DR, VDR)	No
VMware Snapshots	Yes
VMware Fault Tolerance (FT)	No
VMware vCenter Converter	No
VMsafe	No
VMware vShield	No
Virtual Appliance Packaging of UC apps	No
3rd-party VM-based backup tools (for example, Veeam, Viziocore, esXpress)	No
3rd-party VM-based deployment tools (for example, rPath, Platespin)	No
3rd-party Physical To Virtual (P2V) Migration Tools	No
Identity	No
VMware Boot from SAN	No
All other vSphere features	No

Cisco Unified SRST Manager Administration Interfaces

Cisco Unified SRST Manager Release utilizes CLI, GUI and REST interface. This chapter describes these interfaces, contains the following sections.

CLI

The CLI is a text-based interface accessed through a secure session (ssh) session to the server hosting the Cisco Unified SRST Manager VM. Those familiar with Cisco IOS command structure and routers will see similarities.

The Cisco Unified SRST Manager commands are structured much like the Cisco IOS CLI commands. However, the Cisco Unified SRST Manager CLI commands do not affect Cisco IOS configurations.

See How to Use the Cisco Unified SRST Manager CLI for the instructions to enter the Cisco Unified SRST Manager CLI environment.

The CLI is accessible from a PC or server anywhere in the IP network.

CLI commands can also be used for routine monitoring and maintenance of the Cisco Unified SRST Manager system.

GUI

Cisco Unified SRST Manager provides a GUI. For information on using the GUI, see the online help in the application or the relevant sections in this guide.

About the Cisco Unified SRST Manager GUI

Tip When you use the Cisco Unified SRST Manager GUI, you can use the Back and Forward buttons on your browser to view information in another window, but if you make changes in that window and submit your changes, you will receive an error and your changes will **not** be saved. **Do not submit information after using your browser's navigation tools to move to another window**. Click the appropriate button or menu to reach the window in which you want to enter information.

About the Cisco Unified SRST Manager Dashboard

You should periodically monitor the status of the system to ensure that the deployment remains ready for failover events. You can monitor the system from the Cisco Unified SRST Manager dashboard.

The Cisco Unified SRST Manager dashboard provides an at-a-glance view of the state of the system. The dashboard contains a summary of items that would typically require the attention of the administrator, such as error and warning messages. When the system is functioning normally, with no alerts or activity, the dashboard shows minimal information.

You can return to the dashboard from anywhere in the system by clicking **Dashboard** on the top right.

The dashboard includes two areas:

- **Provisioning Status:** Displays a summary of the results of the most recent provisioning cycle. If all sites have been successfully provisioned, a single success message is displayed. If any sites are disabled, have failed provisioning, or have never been provisioned, the provisioning status panes displays a site count for each provisioning outcome respectively. For provisioning failures, the system generates a system alert message for each site that indicates the reason for the failure. To review site specific results by status, click the corresponding report link.
- **System Alerts:** Displays the number of critical, warning, error, and informational alert messages that require attention. To review system alert details by level, click the corresponding link. See System Alerts for more information about alerts.

Overview of Initial Configuration Tasks

The following is a high-level overview of the tasks required before you can use the Cisco Unified SRST Manager GUI to configure Enhanced Survivable Remote Site Telephony (E-SRST).

Task	Where to find more information
Before You Begin	
Install and configure Cisco Unified Communications Manager.	Installation guide for your release of Cisco Unified Communications Manager. See http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_installation_guides_list.html
Install Cisco Unified SRST at the branch office, including security certificates. The supported options are: • Sites using original SRST. • Sites using E-SRST require CUCME.	For original SRST, see http://www.cisco.com/en/US/docs/voice_ip_comm/cusrst/admin/srst/configuration/guide/srst41/srst41sa.html For CUCME, see http://www.cisco.com/en/US/docs/voice_ip_comm/cucme/admin/configuration/guide/cmeadm.html
Install Cisco Unified SRST Manager Release 11.0.	*Installation and Upgrade Guide for Cisco Unified SRST Manager Release 11.0*
Accept the license agreement.	*Installation and Upgrade Guide for Cisco Unified SRST Manager Release 11.0*
Configure the networking.	*Installation and Upgrade Guide for Cisco Unified SRST Manager Release 11.0*
Create an administrator account.	*Installation and Upgrade Guide for Cisco Unified SRST Manager Release 11.0*
Log into Cisco Unified SRST Manager.	Logging In to the Cisco Unified SRST Manager Graphical User Interface
Global Configuration	
Configure global settings for Cisco Unified SRST Manager, including importing security certificates.	• Using the Setup Wizard • Configuring Backup and Restore • Working With Network Time and Time Zone Settings

Task	Where to find more information
Configuring Central Call Agents	
Import the TLS certificates.	Working With Trusted TLS Certificates
Configure a central call agent, such as Cisco Unified Communications Manager, in Cisco Unified SRST Manager.	Using the Central Call Agent Wizard to Add Cisco Unified Communications Manager Information
Configure advanced telephony features on Cisco Unified Communications Manager such as softkeys, hunt groups, call routing restrictions, and call pickups. When a branch site is selected to enable E-SRST provisioning using the Cisco Unified SRST Manager GUI, the configuration for these advanced telephony features are downloaded to the branch site.	See the Cisco Unified Communications Manager: http://www.cisco.com/en/US/products/sw/voicesw/ps556/tsd_products_support_series_home.html
Configuring Branch Sites	
Create and configure site templates for Cisco Unified SRST Manager.	Using Site Templates
Import SRST sites by retrieving SRST references from Cisco Unified Communications Manager.	Viewing the Cisco Unified SRST References
Configure sites, if needed.	Viewing and Provisioning Sites
Configure provisioning for one or more sites.	• Changing the Information for a Single Cisco Unified SRST Site • Changing the Information for Multiple Cisco Unified SRST Sites at Once
Configuring Users for Cisco Unified SRST Manager	• Configuring Users for Cisco Unified SRST Manager
Provisioning Tasks	
Provision sites.	Viewing and Provisioning Sites
Monitor provisioning and understand the error messages associated with provisioning failure.	• Monitoring the Provisioning Status of a Branch Device • System Alerts
Changes as Needed	
Update the domain name settings.	Working With DNS Servers
Monitoring	
Monitor the status of the Cisco Unified SRST Manager system.	• About the Cisco Unified SRST Manager Dashboard • Monitoring the Learned Cisco Unified Communications Manager Express Routers • Monitoring the Provisioning Status of a Branch Device • Viewing Reports

Task	Where to find more information
Maintenance	
Periodically back up the Cisco Unified SRST Manager system. Restore it as needed.	Configuring Backup and Restore
Troubleshooting	
Troubleshoot the Cisco Unified SRST Manager system as necessary.	• Troubleshooting Using the GUI • For information about troubleshooting using the CLI, see: *Administration Guide for Cisco Unified SRST Manager 11.0*

Logging In to the Cisco Unified SRST Manager Graphical User Interface

Restrictions

The Cisco Unified SRST Manager graphical user interface (GUI) supports the following web browsers:

- Internet Explorer Releases 6 or later
- Mozilla Firefox

Cookies must be enabled.

Before You Begin

- Install Cisco Unified SRST Manager software. See *Installation and Upgrade Guide for Cisco Unified SRST Manager Release 11.0* for information.
- Gather the administrator username and password that you entered during the installation.

Procedure

Step 1 Open a web browser.

Step 2 Enter the IP address of the Cisco Unified SRST Manager system.

The GUI login screen appears.

Step 3 Enter the administrator user name and password.

Step 4 Click **Log In**.

The Cisco Unified SRST Manager dashboard appears.

About the Cisco Unified SRST Manager Dashboard

Monitor the status of the system periodically to ensure that the deployment remains ready for failover events. You can monitor the system from the Cisco Unified SRST Manager dashboard.

The dashboard provides an at-a-glance view of the state of the system. The dashboard contains a summary of items that would typically require the attention of the administrator, such as error and warning messages. When the system is functioning normally, with no alerts or activity, the dashboard shows minimal information.

You can return to the dashboard from anywhere in the system by clicking **Dashboard** on the top right.

The dashboard is comprised of the following areas:

- **Provisioning Status:** Displays a summary of the results of the most recent provisioning cycle. If all sites have been successfully provisioned, a single success message is displayed. If any sites are disabled, have failed provisioning, or have never been provisioned, the provisioning status panes displays a site count for each provisioning outcome respectively. For provisioning failures, the system generates a system alert message for each site that indicates the reason for the failure. To review site specific results by status, click the corresponding report link.
- **System Alerts:** Displays the number of critical, warning, error, and informational alert messages that require attention. To review system alert details by level, click the corresponding link. See System Alerts for more description of the alerts.

Configuring E-SRST Site Provisioning

When enabled on a site, the Cisco Unified SRST Manager E-SRST functionality provides automated remote site provisioning of the following advanced telephony features in survivable mode by gathering the information from Cisco Unified Communications Manager:

- After-hours
- Call pickup and group pickup
- Call routing restrictions (local and long distance, and time of day)
- Class of restrictions
- Dial Plan
- Hunt groups
- Phones and extensions (speed dials, lines, softkeys)
- Pick-up groups

Note Cisco Unified SRST Manager software does not support provisioning Media Gateway Control Protocol (MGCP) dial plan. Cisco has removed the support for this feature due to the complexity of and differences between dial plans across the globe. These complexities and differences must be analyzed by a Cisco engineering team member to understand whether the Cisco Unified SRST Manager dial plan logic can meet customer requirements. If you are interested in automatic dial plan provisioning, contact srstmgr@cisco.com. The Cisco engineering team member requires a copy of your Cisco Unified Communications Manager dial plan (.tar file) for analysis. After analysis, a private build of the Cisco Unified SRST Manager with the dial plan provisioning feature enabled will be delivered.

This section describes the high-level tasks required to configure a site to support E-SRST. Enabling E-SRST requires configuration on Cisco Unified SRST Manager, the Cisco Unified Communications Manager central call agent, and on the CUCME call agent at the branch site. Most of the configuration on Cisco Unified SRST Manager is handled using the GUI.

This procedure assumes that the security certificates have been installed on Cisco Unified SRST Manager. For more information, see About Security for Cisco Unified SRST Manager.

Using E-SRST to Pull an Advanced Telephony Configuration from CUCM to the Branch Site

This section describes the high-level configuration tasks required to pull advanced telephony configuration information from Cisco Unified Communications Manager to the remote site.

- Initial Configuration Using the Cisco Unified SRST Manager GUI, page 28
- Preparing the Central Cisco Unified Communications Manager Call Agent for E-SRST Provisioning, page 28
- Configuring the Cisco Unified Communications Manager Express Branch Call Agent to Prepare for E-SRST Provisioning, page 30
- Enabling E-SRST Provisioning on the Site Using the Cisco Unified SRST Manager GUI, page 32
- Verifying the Updated Configuration on the Branch Call Agent Router, page 33

Initial Configuration Using the Cisco Unified SRST Manager GUI

Before you can configure Cisco Unified SRST Manager to support E-SRST on branch sites, you must first perform the following high-level tasks using the GUI:

1. Configure the Cisco Unified SRST Manager initial values using the setup wizard. For more information, see Using the Setup Wizard.
2. Add the central call agent using the Central Call Agent wizard. For more information, see Using the Central Call Agent Wizard to Add Cisco Unified Communications Manager Information.
3. Retrieve the Cisco Unified SRST sites. For more information, see Viewing the Cisco Unified SRST References.

Preparing the Central Cisco Unified Communications Manager Call Agent for E-SRST Provisioning

This section assumes that the advanced telephony features have already been configured on Cisco Unified Communications Manager. For more information, see the Cisco Unified Communications Manager documentation at
http://www.cisco.com/en/US/products/sw/voicesw/ps556/tsd_products_support_series_home.html.

To configure Cisco Unified Communications Manager to prepare for E-SRST provisioning, perform the following steps on Cisco Unified Communications Manager.

Procedure

Step 1 Configure the Cisco Unified SRST references on Cisco Unified Communications Manager with the following:

- Site name
- Port number for CUCME
- IP address of the router

Step 2 Create a device pool in Cisco Unified Communications Manager that has the SRST reference. Collect the following information:

- Device pool name
- Cisco Unified SRST reference, which must match the site name
- Devices and phones. For each phone that you want to be registered for survivable mode, set the device pool to match the device pool configured in the previous step.

Step 3 Configure the advanced telephony configuration on Cisco Unified Communications Manager that will be downloaded to the branch site using E-SRST provisioning.

Cisco Unified SRST Manager supports selected Cisco Unified Communications Manager features to be downloaded using E-SRST site provisioning, and operates in survivable fallback mode. Table 3 lists the supported features and instructions for preparing for the E-SRST site provisioning.

Table 3 Cisco Unified Communications Manager Advanced Telephony Features Supported in Cisco Unified SRST Manager

Cisco Unified Communications Manager Advanced Telephony Configuration	Instructions for Preparing the Cisco Unified Communications Manager Feature for E-SRST Site Provisioning
Calling search space (CSS) and partitions	Cisco Unified SRST Manager converts the CSS and partitions into cor lists on the branch routers. Calling search space and partitions on CUCM are typically used to apply restrictions on calling, such as internal, local, national, and international calling restrictions. Cisco Unified SRST Manager applies the configured restrictions using cor lists on the branch routers.
Call pickup and group pickup	
Hunt groups	1. Select the Hunt Pilot setting. 2. Select **Hunt Pilot**. 3. Select **Hunt List**. 4. Select **Device Settings --> Softkey Templates**. Assign this template to all ephones. In fallback mode, these templates are translated into an ephone template, and assigned to the ephones as well. As a result, the same softkey templates that appear in normal connected mode will appear in fallback mode.

Table 4 lists the softkey states and keys that E-SRST provisioning supports.

Table 4 ***Softkeys Supported for E-SRST Provisioning***

Phone States	Softkey
Alerting	Endcall
Connected	Endcall, HLog, Hold, Join, Park, RmLstC, Select, TrnsfVM, Trnsfer
Hold	Join, Newcall, Resume, Select
Idle	Cfwdall, Dnd, Gpickup, Hlog, Join, Newcall, Pickup, Redial, RmLstC
Remote-in-use	Cbarge, Newcall
Ringing	Answer, Dnd, Hlog
Seized	CallBack, Cfwdall, Endcall, Gpickup, Hlog, Pickup, Redial

Configuring the Cisco Unified Communications Manager Express Branch Call Agent to Prepare for E-SRST Provisioning

The E-SRST solution requires that Cisco Unified Communications Manager Express (CUCME) be configured in Cisco Unified SRST fallback mode. For more information, see the *Cisco Unified Communications Manager Express Administrator Guide*.

The Cisco Unified Communications Manager Express site must also be configured with additional CLI commands to ensure that Cisco Unified SRST Manager can contact the Cisco Unified Communications Manager Express site. This enables Cisco Unified SRST Manager to transfer configuration information from the Cisco Unified Communications Manager to the branch site.

The communication between Cisco Unified SRST Manager and Cisco Unified Communications Manager Express can use local authentication or HTTPS authentication. The following sections describe the procedures for preparing CUCME:

- Configuring Communication with CUCME by Local Authentication
- Configuring Communication with CUCME by HTTPS Authentication

Configuring Communication with CUCME by Local Authentication

Perform the following procedure in CUCME to configure communication between Cisco Unified SRST Manager and CUCME using local authentication:

Procedure for Using Local Authentication

Step 1 Configure the user telnet name and password for the interface that connects back to Cisco Unified SRST Manager.

username *name* **privilege 15 password** *password*

Note Privilege 15 is required for Cisco Unified SRST Manager to push the configurations to the branch site.

Step 2 Enter the line terminal configuration and enter line configuration mode.

line vty 0 4

Step 3 Enable local password checking at login.

login local

Step 4 Define which protocol to use to connect to the branch call agent.

- If TLS is not enabled on Cisco Unified SRST Manager, enter the following command:

  transport input telnet

- If TLS is enabled on Cisco Unified SRST Manager, enter the following command:

  transport input ssh

Step 5 Enable the IP HTTP server using the following command:

ip http server

Step 6 Set the IP HTTP authentication to the local setting using the following command:

ip http authentication local

Step 7 Enable or disable the HTTPS secure server, depending on whether TLS is enabled on the Cisco Unified SRST Manager:

- If TLS is enabled on Cisco Unified SRST Manager, enter the following command:

  ip http secure-server

- If TLS is disabled on Cisco Unified SRST Manager, enter the following command:

  no ip http secure-server

  If TLS is disabled on Cisco Unified SRST Manager, this setting is required for the Cisco Unified Communications Manager voice configuration to be downloaded to the branch router.

Step 8 Set the IP HTTP flash (include the colon ":" at the end of the command).

ip http path flash:

Step 9 Set the IP HTTP timeout policy using the following command:

ip http timeout policy

Configuring Communication with CUCME by HTTPS Authentication

Perform the following procedure in CUCME to configure communication between Cisco Unified SRST Manager and CUCME using HTTPS authentication:

Procedure for Using HTTPS Authentication

Step 1 Configure the user telnet name and password for the interface that connects back to Cisco Unified SRST Manager.

username *name* **privilege 15 password** *password*

Note Privilege 15 is required for Cisco Unified SRST Manager to push the configurations to the branch site.

Step 2 Enter the line terminal configuration and enter line configuration mode.

```
line vty 0 4
```

Step 3 Enable AAA login authentication.

```
login authentication https
```

Step 4 Define ssh as the connection protocol for connecting to the branch call agent.

```
transport input ssh
```

Step 5 Enter the following commands individually to configure AAA authentication.

```
aaa new-model
aaa authentication login https group tacacs+
aaa authorization exec https group tacacs+ if-authenticated
aaa session-id common
ip tacacs source-interface GigabitEthernet0/1
tacacs server ACS
address ipv4 100.100.100.200
key cisco123
single-connection
```

Step 6 Enable the IP HTTP server using the following command:

```
ip http server
```

Step 7 Set IP HTTP AAA authentication.

```
ip http authentication aaa login-authentication https
ip http authentication aaa exec-authorization https
```

Step 8 Enable the HTTPS secure server with TLS enabled on the Cisco Unified SRST Manager.

```
ip http secure-server
```

Step 9 Set the IP HTTP flash (include the colon ":" at the end of the command).

```
ip http path flash:
```

Step 10 Set the IP HTTP timeout policy using the following command:

```
ip http timeout policy
```

Enabling E-SRST Provisioning on the Site Using the Cisco Unified SRST Manager GUI

You must enable E-SRST provisioning using the Cisco Unified SRST Manager GUI for each branch site that will download Cisco Unified Communications Manager telephony configuration during the provisioning process. You can either perform on-demand site provisioning for the site, or configure Cisco Unified SRST Manager to perform scheduled provisioning on the site.

For information, see Viewing and Provisioning Sites.

Verifying the Updated Configuration on the Branch Call Agent Router

After the E-SRST provisioning is complete, the dial plan and ephone configuration settings configured on the central call agent should be propagated to the branch call agent router. Verify that the updated settings are configured on the site by viewing the dial peer and ephone configuration settings.

Using the Setup Wizard

Use the Setup Wizard to set initial values for the Cisco Unified SRST Manager system.

Before You Begin

Gather the following information before you run the Setup Wizard:

Table 5 System Setup Parameters

Parameter	Description
Voicemail Pilot	
Auto-Learn Call Forwarding Settings	Determines whether the system should auto-learn the call forwarding settings.
Pilot Number	The voicemail pilot number for the branch office call agent. The system saves this number to the default site template. If the "Autolearn call forward settings" option is set to "Yes," the voicemail pilot number is automatically retrieved from the central call agent during the provisioning process. Enter the voicemail pilot number if you want to override the retrieved pilot number.
TLS Security	
TLS Security	Enables security between Cisco Unified SRST Manager and devices at the branch. • If TLS security is set to On, Cisco Unified SRST Manager uses https and ssh. Ensure that the branch site has generated an encryption certificate. • If TLS security is set to Off, Cisco Unified SRST Manager uses http and telnet.

Procedure

Step 1 Select **Setup Wizards > Setup**.

The system displays the Introduction page of the setup wizard.

Step 2 Click **Next** to begin the wizard. See Table 5 for descriptions of the parameters configured in the wizard.

Related Topics

- Using the Central Call Agent Wizard to Add Cisco Unified Communications Manager Information

Configuring Users for Cisco Unified SRST Manager

This section provides the information related to configuring users and contains the following:

- Viewing the List of Users
- Adding a New User
- Displaying or Modifying a User Profile
- Displaying or Modifying Group Subscriptions
- Finding a User
- Deleting a User

Viewing the List of Users

Procedure

Step 1 Choose **Configure** > **Users**.
The Configure Users window is displayed and contains the following fields:

- User ID—By default, the system displays Users IDs in alphabetical order from A to Z. Click **User ID** to sort from Z to A.
- Display Name—To display the list of users in alphabetical order by display name, click **Display Name**.

Related Topics

- Adding a New User
- Displaying or Modifying a User Profile
- Displaying or Modifying Group Subscriptions
- Finding a User
- Deleting a User

Back to Configuring Users for Cisco Unified SRST Manager main menu.

Adding a New User

Procedure

Step 1 Choose **Configure** > **Users**.
The Configure Users window is displayed.

Step 2 Click **Add**.
The Add a New User window is displayed.

Step 3 Enter information in the following fields:

- User ID
- Password options
- Password
- Confirm Password—Enter the password again for confirmation.

Note Assigning the user to a specific group is mandatory for the user to get access to Cisco Unified SRST Manager. For more information. refer to "Displaying or Modifying Group Subscriptions" section on page 39

Step 4 Click **Add** to save your changes.

Note If you selected a random password or PIN, a message appears with the new password or PIN. Write these values in a secure place to give it to the user. They are also displayed on the User Profile page (see "Displaying or Modifying a User Profile" section on page 39).

Related Topics

- Viewing the List of Users
- Displaying or Modifying a User Profile
- Displaying or Modifying Group Subscriptions
- Finding a User
- Deleting a User

Back to Configuring Users for Cisco Unified SRST Manager main menu.

Displaying or Modifying a User Profile

Procedure

Step 1 To view a user's profile, choose **Configure** > **Users**.
The Configure Users window is displayed.

Note If you cannot locate the user, click **Find** to search for the user (see "Finding a User" section on page 40).

Step 2 Click the corresponding User ID.
The user profile window is displayed with the following fields shown:

- User ID
- Password options (enabled by default)
- Password
- Confirm Password—Enter the password again for confirmation.

Step 3 Click **Apply** to save the changes made to this user profile.

Additional User Profile Options

In this window, you can also click the following tabs:

- Groups—Change a user's groups. See Displaying or Modifying Group Subscriptions.

Related Topics

- Viewing the List of Users
- Adding a New User
- Displaying or Modifying Group Subscriptions
- Finding a User
- Deleting a User

Back to Configuring Users for Cisco Unified SRST Manager main menu.

Displaying or Modifying Group Subscriptions

Procedure

Step 1 Choose **Configure** > **Users**.
The Configure Users window is displayed.

Step 2 Click the name of the user whose group subscription you want to view or modify.
The User Profile window is displayed.

Step 3 Click the **Groups** tab. The following fields are displayed:

- Group ID
- Rights
- Description

Step 4 To subscribe the user to another group, click **Subscribe as member**.
The Find window appears.

Step 5 Click **Find** to view the groups available for subscription.

Note **Admin** and **Guest** are the two groups available in Cisco Unified SRST Manager.

Step 6 Check the check box corresponding to the group this user should be a member of and click **Select row(s)**.

Step 7 (Optional) To unsubscribe the user from a group, Check the **Group Name** check box and click **Unsubscribe**.

Step 8 Click **Cancel** to close the window.

Related Topics

- Viewing the List of Users
- Adding a New User
- Displaying or Modifying a User Profile
- Finding a User
- Deleting a User

Back to Configuring Users for Cisco Unified SRST Manager main menu.

Finding a User

Note Only users with Administrator permissions, can view the Users window (Configure > Users.)

Procedure

Step 1 Choose **Configure** > **Users**.
The Configure Users window is displayed.

Step 2 Click **Find**.
The following optional fields are displayed:

- User ID
- Name
- Extension

Step 3 Click **Find**.
The User Configuration window displays the results of your search.

Related Topics

- Viewing the List of Users
- Adding a New User
- Displaying or Modifying a User Profile
- Displaying or Modifying Group Subscriptions
- Deleting a User

Back to Configuring Users for Cisco Unified SRST Manager main menu.

Deleting a User

Procedure

Step 1 Choose **Configure** > **Users**.

Step 2 Check the check box adjacent the user ID that you want to delete.

Step 3 Click **Delete**.

Step 4 Click **Ok** to confirm the deletion.

Related Topics

- Viewing the List of Users
- Adding a New User
- Displaying or Modifying a User Profile
- Displaying or Modifying Group Subscriptions
- Finding a User

Back to Configuring Users for Cisco Unified SRST Manager main menu.

Using the Central Call Agent Wizard to Add Cisco Unified Communications Manager Information

The Add Central Call Agent Wizard adds Cisco Unified Communications Manager information that identifies Cisco Unified Communications Manager to Cisco Unified Survivable Remote Site Telephony (SRST) Manager. No changes are made to the Cisco Unified Communications Manager configuration.

Note When deploying Cisco Unified Enhanced-Survivable Remote Site Telephony, Cisco Unified SRST Manager can be configured for only one central call agent. Do not configure more than one installation of Cisco Unified SRST Manager to access the same Cisco Unified Communications Manager, which is the only central call agent that Cisco Unified SRST Manager supports for E-SRST.

Before You Begin

Collect the following information before you add a Cisco Unified Communications Manager:

Table 6 Central Call Agent Parameters

Parameter	Description
CUCM Hostname	
Hostname or IP Address	Identifies the Cisco Unified Communications Manager to Cisco Unified SRST Manager. Configuring DNS server is optional. You can enter either a hostname or IP address. If you enter an IP address, the system performs a DNS reverse look-up to store the Cisco Unified Communications Manager by hostname. **Note** The DNS server forward and reverse tables should be set up with the IP address and hostname of Cisco Unified Communications Manager.
CUCM AXL Interface	
AXL Username	The user name that Cisco Unified SRST Manager uses to access the Cisco Unified Communications Manager AXL interface. This user name must exist on the Cisco Unified Communications Manager as an “application user” and be assigned the role of “standard AXL API access” or “standard CUCM super users.”

Table 6 Central Call Agent Parameters (continued)

Parameter	Description
AXL Password	The password that corresponds to the Cisco Unified Communications Manager AXL interface user. This password must correspond to the password configured on Cisco Unified Communications Manager for this user name. **Note** If the password changes on Cisco Unified Communications Manager, you must also change the password in Cisco Unified SRST Manager. There is no automatic password synchronization for AXL credentials.
CUCM Cluster	
Cluster Name	A descriptive name that uniquely identifies this Cisco Unified Communications Manager cluster. By default, the system uses the hostname that you entered at the beginning of this wizard as the cluster name.
Secondary Node	A second member of the Cisco Unified Communications Manager cluster to be used by Cisco Unified SRST Manager provisioning when the Cisco Unified SRST Manager cannot contact the primary Cisco Unified Communications Manager.
CUCM Schedule	
Defines how often you want Cisco Unified SRST Manager to contact Cisco Unified Communications Manager to synchronize configuration data. **Tip** We recommend that you schedule Cisco Unified SRST Manager to contact the Cisco Unified Communications Manager during off-peak hours.	
Schedule	Enable or disable scheduled provisioning. **Note** By default, schedule provisioning is enabled and set to at 12 a.m. EST everyday. If schedule provisioning is disabled, the default schedule is not effective and other schedule parameters fields are grayed out.
Daily	Frequency in days. Enter the number of days between provisioning cycles.
Weekly	Frequency in weeks. Enter the number of weeks between provisioning cycles and the day of the week.
Monthly	Frequency in months. Enter the day of the month. **Note** If the day of the month is beyond the number of days the month contains, the provisioning occurs on the last day of that month. (For example if you configure provisioning for the 31st day of every month, provisioning for February occurs on the last day of the month.) Enter the number of months between provisioning cycles.

Table 6 Central Call Agent Parameters (continued)

Parameter	Description
Start Time	Start time for the provisioning cycle. This indicates the time of day at which Cisco Unified SRST Manager initiates contact to Cisco Unified Communications Manager.
End Time	(Optional) Indicates whether Cisco Unified SRST Manager should suspend provisioning at a certain time. If you do not enter an end time, the system continues provisioning until all sites have been processed. If you enter an end time, and the end time is reached during a provisioning cycle, the system suspends provisioning and waits until the next provisioning cycle to continue, at which time any sites not yet provisioned from the previous cycle will be processed first.
Call Agent Time Zone	Indicates the time zone in which the Cisco Unified Communications Manager is physically located. This enables the start and end times to be specified relative to the Cisco Unified Communications Manager time so that peak call load hours can be avoided.

Procedure

Step 1 Select **Setup Wizards > Add Central Call Agent**.

The system displays the Introduction page of the Add Central Call Agent Wizard.

Step 2 Click **Next**.

The system displays the Unified Communications Manager Hostname page of the Add Central Call Agent Wizard.

Step 3 Enter the Cisco Unified Communications Manager hostname or IP address.

Step 4 Click **Next**.

The system displays the Unified Communications Manager AXL Interface page of the Add Central Call Agent Wizard.

Step 5 Enter the following information:

- AXL Username
- AXL Password
- Confirm the AXL Password

Step 6 Click **Next**.

The system displays a message stating that it will contact the Cisco Unified Communications Manager and downloads all the configured cluster nodes. This can take a few minutes.

Step 7 Click **OK** at the warning message.

The system displays the Unified Communications Manager Cluster page of the Add Central Call Agent Wizard.

Step 8 Enter the Cisco Unified Communications Manager cluster name and select a secondary node.

- Cluster Name

- Secondary Node

Step 9 Click **Next**.

The system displays the Unified Communications Manager Schedule page of the Add Central Call Agent Wizard.

Step 10 Enter information about how often Cisco Unified SRST Manager should contact Cisco Unified Communications Manager to retrieve configuration information. See CUCM Schedule.

Step 11 Enter a start time. You can optionally enter an end time.

Step 12 Enter a time zone.

Step 13 Click **Next**.

The system displays the CUCM Enable page of the Add Central Call Agent Wizard. You can set Enable Provisioning to either On or Off. If Off is selected, scheduled provisioning is not activated.

Step 14 Set Enable Provisioning to On to enable Cisco Unified SRST Manager to access Cisco Unified Communications Manager.

Step 15 Click **Finish** to complete the Central Call Agent Wizard and save this information.

Related Topics

- Viewing, Adding, and Removing the Central Call Agent
- Viewing and Updating the Central Call Agent
- Viewing the Cisco Unified SRST References
- Viewing the Cluster Nodes Associated With a Central Call Agent
- Supported AXL Versions
- Supported Phones and Platforms

Supported AXL Versions

The following AXL versions are supported for Cisco Unified SRST Manager:

Table 7 Supported AXL Versions

Cisco Unified SRST Manager Version	Supported Cisco Unified CM Versions	Supported AXL Versions
9.0.4	9.1, 9.0, and 8.5	7.0.1
9.0.6	10.5, 10.0, 9.1, 9.0 and 8.5	8.5
11.0	11.0,10.5, 10.0, 9.1, and 9.0	9.0

Supported Phones and Platforms

Refer to Cisco Unified SRST Manager Compatibility Matrix for more information on the following:

- Supported Phones

This section lists all the phone models supported by Cisco Unified SRST Manager.

- Supported Administrative XML (AXL) versions

  This section provides the list of AXL versions supported by Cisco Unified SRST Manager.
- ESRST Scalability

  This section provides the information on increase in scalability for E-SRST.
- New Platforms Supported

  This section provides the list of platforms that are newly supported from Cisco Unified SRST Manager 11.0.0 Release.
- Fast track support

  Fast track is supported only for SIP phones available from Cisco IOS Release 15.3(3)M, or Cisco Unified Communications Manager Express 10.0 or Cisco Unified SRST 10.0. Some phones are natively supported in Cisco Unified Communications Manager Express, Cisco Unified SRST or Cisco Unified E-SRST, which is known as inbuilt support.

  For information on fast track use cases for Cisco Unified SRST Manager phone configuration, see Cisco Unified SRST Manager Compatibility Matrix.

Viewing and Updating the Central Call Agent

You can change information about the central call agent that you previously configured.

Before You Begin

Enter initial values by using the Add Central Call Agent Wizard. See Using the Central Call Agent Wizard to Add Cisco Unified Communications Manager Information.

Procedure

Step 1 Select **Configure > Central Call Agents**.

The system displays the Central Call Agents page, containing the name of the central call agent that you have configured.

Step 2 To view the details of the central call agent, click its underlined name.

The system displays the CUCM Profile page with the Profile tab highlighted.

Step 3 Update the information on the page. See Table 6 for a description of the parameters.

Step 4 Click **Update** to save this information.

Related Topics

- Viewing, Adding, and Removing the Central Call Agent
- Viewing the Cisco Unified SRST References
- Viewing the Cluster Nodes Associated With a Central Call Agent

Viewing the Cisco Unified SRST References

Procedure

Step 1 Select **Configure > Central Call Agents**.

The system displays the Central Call Agents page, containing the name of the central call agent that you have configured.

Step 2 To view the details of the central call agent, click the underlined name.

The system displays the CUCM Profile page. Click the **SRST References** tab to view a list of the Cisco Unified SRST references.

Step 3 To retrieve additional Cisco Unified SRST references, do the following:

a. Click **Retrieve SRST References**. The system displays a warning message stating that the system will automatically contact the Cisco Unified Communications Manager and download all configured SRST references.

b. Click **OK** to retrieve the references.

The system automatically creates new branch office sites for each Cisco Unified SRST reference.

Note When Cisco Unified SRST Manager retrieves a new SRST reference from the Cisco Unified Communications Manager, provisioning for the new site is disabled by default. An administrator must enable provisioning for the site manually. See Changing the Information for a Single Cisco Unified SRST Site and Changing the Information for Multiple Cisco Unified SRST Sites at Once.

When finished, the system displays the Sites page. (You can also select **Configure > Sites** to view the Sites page.)

The page contains the following information for each site:

- Site name
- Indication of whether provisioning is enabled
- Branch Call Agent
- Site Template Name
- SRST Type
- Indication of whether dial plan configuration is enabled

For more information about the information displayed on the Sites page, see Viewing and Provisioning Sites.

Related Topics

- Viewing, Adding, and Removing the Central Call Agent
- Viewing the Cluster Nodes Associated With a Central Call Agent

Viewing, Adding, and Removing the Central Call Agent

Restriction

You can only configure one central call agent per system.

Procedure

Step 1 Select **Configure > Central Call Agents**.

The system displays the Central Call Agents page, containing the name of the central call agent that you have configured.

Step 2 To view the details of the central call agent, click the underlined name.

The CUCM Profile page appears. The page contains several tabs that provide information about the central call agent:

- Profile (selected by default)

  This tab displays the parameters configured when the central call agent was added. For more information, see Table 6 in Using the Central Call Agent Wizard to Add Cisco Unified Communications Manager Information.

  To change parameters in the Profile tab, enter new values and click the **Update** button.

- SRST References

  This tab displays a list of the SRST references for the central call agent. Below the list is a **Retrieve SRST References** button that updates the list of references and opens the Sites page. For more information, see Viewing the Cisco Unified SRST References.

- Cluster Nodes

  This tab displays the cluster nodes associated with the central call agent. For more information, see Viewing the Cluster Nodes Associated With a Central Call Agent.

Step 3 To add a central call agent, click **Add**.

Note You can only configure one central call agent per system. If one is already configured, the Add button is grayed out.

The system displays the Add Central Call Agent Wizard. See Using the Central Call Agent Wizard to Add Cisco Unified Communications Manager Information.

Step 4 To remove a central call agent, do the following:

a. Select the central call agent.

b. Click **Remove**.

c. Click **OK** at the warning message.

Viewing the Cluster Nodes Associated With a Central Call Agent

Procedure

Step 1 Select **Configure > Central Call Agents**.

The system displays the Central Call Agents page, containing the name of the central call agent that you have configured.

Step 2 To view the cluster nodes associated with the central call agent, click the underlined name of the call agent.

The system displays the CUCM Profile page with the Profile tab highlighted.

Step 3 Click the **Cluster Nodes** tab.

The system displays the CUCM Profile page with the cluster nodes that have been configured.

Step 4 To retrieve a node, do the following:

a. Click **Retrieve Nodes**. The system displays a warning message stating that the system will automatically contact Cisco Unified Communications Manager and download all configured cluster nodes.

b. Click **OK** to retrieve the nodes.

Related Topics

- Viewing, Adding, and Removing the Central Call Agent
- Viewing the Cisco Unified SRST References

Viewing and Provisioning Sites

Before You Begin

Import at least one site. See Viewing the Cisco Unified SRST References.

Note If provisioning is not enabled on a site, the site will not be provisioned.

Procedure

Step 1 Select **Configure > Sites**.

The system displays the Sites page, listing the sites that have been added to Cisco Unified SRST Manager. For each site, the following information is listed:

Parameter	Description
Site	Name of the site.
Provisioning Enabled	Displays a green check mark if provisioning is enabled. **Note** By default, provisioning is not enabled for new SRST references retrieved from the Cisco Unified Communications Manager. See Changing the Information for a Single Cisco Unified SRST Site and Changing the Information for Multiple Cisco Unified SRST Sites at Once.
Branch Call Agent	Indicates the branch call agent for the site.
Site Template Name	Name of the site template associated with the site. See Using Site Templates.
SRST Type	Enhanced SRST (Cisco Unified CME) or Classic SRST.
Dial Plan Configuration Enabled	If a check mark appears, then dial plan configuration will be provisioned for the site.

Step 2 To filter the list of sites, do the following:

a. Select a filter from the Filter drop-down list.

b. Select a condition from the Match if drop-down list.

c. Enter a keyword.

d. Click **Go**.

To clear the values, click **Clear Filter** and click **Go**.

Step 3 To provision sites, do the following:

a. Select the check box next to the name of the site or sites that you want to provision.

b. Click **Provision Selected Sites**. The system displays a warning message stating that the system will immediately contact the Cisco Unified Communications Manager system and download all the information about the selected sites.

c. Click **OK** to continue. The Provisioning Status page appears, displaying the site provisioning status.

Note For more information about provisioning, including the difference between automatic (scheduled) and manual provisioning, see About Provisioning Branch Site Devices.

Step 4 To view provisioning status or edit information about sites, do one of the following:

- To view the status of the provisioning at any time, select **Monitor > Provisioning Status**. See Monitoring the Provisioning Status of a Branch Device.
- To view or edit information about a specific site, click the underlined name of the site. See Changing the Information for a Single Cisco Unified SRST Site.
- To edit more than one site at a time, select the check boxes for more than one site, and click **Bulk Edit Selected Sites**. See Changing the Information for Multiple Cisco Unified SRST Sites at Once.

About Provisioning Branch Site Devices

Cisco Unified SRST Manager provisions branch call agents.

There are two ways you can provision a branch device: automatically according to a schedule or manually.

Typically, provisioning takes place based on the Cisco Unified Communications Manager provisioning schedule. The schedule defines a recurrence frequency that dictates how often the Cisco Unified SRST Manager will synchronize configuration data from the central office to the branch office.

Configuration Requirements for Branch Site Devices

To operate with E-SRST functionality, branch site devices require the following:

- A username/password configuration used for connecting to the branch router by telnet or ssh. It is recommended not to use cisco/cisco as the username/password for a branch router.
- Configuration for an http server and for https.
- Configuration of lines with:
  - Privilege level 15
  - Transport protocols—minimally, telnet, http, and ssh (for modules)

For branch routers with access lists configured, verify that Cisco Unified SRST Manager can access the branch router.

  - If you are not using TLS, verify that Cisco Unified SRST Manager can access the branch router using telnet.
  - If you are using TLS, verify that Cisco Unified SRST Manager can access the branch router using ssh.

Note For additional information, see Configuring the Cisco Unified Communications Manager Express Branch Call Agent to Prepare for E-SRST Provisioning.

About Scheduled Provisioning

Cisco Unified SRST Manager scheduled provisioning can be enabled or disabled based on your requirement. If scheduled provisioning is enabled, then Cisco Unified SRST Manager initiates the provisioning based on the schedule configured. Provisioning scheduled times are relative to the time zone of the Cisco Unified Communications Manager. This enables you to accurately select the time of day when the Cisco Unified Communications Manager call load is the lowest. Cisco Unified SRST Manager automatically adjusts the provisioning start and end times based on the time difference between the Cisco Unified SRST Manager and the configured call agent time zone.

For example, if Cisco Unified SRST Manager is in the U.S. EST time zone and the Cisco Unified Communications Manager is in the U.S. PST time zone, if the provisioning schedule is configured to run at 1:00 a.m. daily, Cisco Unified SRST Manager will wait until 4:00 a.m. EST to provision sites.

Cisco Unified SRST Manager checks the need for provisioning and only then triggers the provisioning. The provisioning is triggered based on the following factors:

- If there is a change in the configuration to Cisco Unified SRST reference such as phone is added or deleted in the Cisco Unified Communications Manager, name change or DNS change.
- If there are any changes in the mode, which is SRST to ESRST and vice-versa on the site
- If there are any changes in the call forward number

If the above mentioned factors are not present, then the provisioning is not triggered.

See Table 6 for more information about the provisioning schedule.

Manually Provisioning a Site

You can manually provision sites from the **Configure > Sites** page. During the provisioning cycle, the system contacts the Cisco Unified Communications Manager. We recommend that you perform this procedure when the central systems are not busy.

Changing the Information for a Single Cisco Unified SRST Site

Before You Begin

You must have imported at least one site. See Viewing the Cisco Unified SRST References.

Procedure

Step 1 Select **Configure > Sites**.

The system displays the Sites page.

Step 2 Click the underlined name of the site for which you want to update the information.

The system displays the Site Profile page. This page contains several categories of information about the site and you can edit many of the details.

Step 3 Update fields.

Table 8 Update Site Parameters

Parameter	Description
Site	
Name	The Cisco Unified SRST reference name retrieved from the Cisco Unified Communications Manager. This field is read-only.
Telephony	
Central Call Agent	Name of the central call agent associated with the site. This field is read-only.
SRST Reference	IP address of the SRST site. This field is read-only.
Site Provisioning	
Site Provisioning Enable	Enable or disable provisioning for the site.
Template	Defines the name of the site template to be used when provisioning the branch device. See Using Site Templates.
Rollback	

Table 8 Update Site Parameters (continued)

Parameter	Description
Restore Last Working Configuration	Enable or disable command restore for the site. In case of a provisioning failure, Cisco Unified SRST Manager restores router back to the original configuration state by removing all the new CLI that were added before the failure. **Note** By default, command rollback is enabled on all the routers.
Router Login Credentials	
Username	Defines the username login credentials for the device at the site. The login credentials are configured by an administrator for the branch router. The account must have privilege level 15. **Note** It is strongly recommended not to use the weak username/password combination of cisco/cisco.
Password	Defines the password login credentials for the device at the site.
Confirm Password	Confirmation of the password login credentials for the device at the site.

Step 4 Click **Update** to save this information.

Related Topics

- Viewing and Provisioning Sites
- Changing the Information for Multiple Cisco Unified SRST Sites at Once

Changing the Information for Multiple Cisco Unified SRST Sites at Once

Before You Begin

You must have imported at least one site. See Viewing the Cisco Unified SRST References.

Restrictions

- You must configure all Cisco Unified SRST sites with a user name and password for provisioning to succeed.
- Do not use the Bulk Edit Selected Sites feature if each Cisco Unified SRST site has a unique user name and password. When you use the Bulk Edit Selected Sites feature, the system changes each Cisco Unified SRST site user name and password on Cisco Unified SRST Manager to the same values. These new values must match the values configured on the individual Cisco Unified SRST sites.

Procedure

Step 1 Select **Configure > Sites**.

The system displays the Sites page.

Step 2 Select the check boxes next to the sites that you want to modify.

Step 3 Click **Bulk Edit Selected Sites**.

The system displays the Site Profile Bulk Edit page.

Step 4 To make changes, select the checkbox next to a field name and enter a value for any or all of the following:

- Site Provisioning Enable
- Restore Last Working Configuration
- Template
- Router Login Credentials: Username
- Router Login Credentials: Password

Step 5 Click **Update**.

The system applies the changes to each of the sites.

Related Topics

- Viewing and Provisioning Sites
- Changing the Information for a Single Cisco Unified SRST Site

Using Site Templates

Because many sites have common sets of information, Cisco Unified SRST Manager provides site templates. Use these templates to apply configuration settings to new sites.

By default, Cisco Unified SRST Manager includes the following site templates:

- default

  You cannot change the name of this site template or delete it, but you can edit its values.
- ESRST_and_Dialplan
- ESRST_only
- SRST_and_Dialplan
- SRST_only

You can also create custom site templates. Table 9 describes the features configured for the default set of site templates. For details about each feature, see Table 10.

Table 9 Default Site Template Parameters

Site Template	Provision Site as Classic SRST	Auto-Learn Call Forward Settings	Enable Dial Plan configuration	Enable Music on Hold configuration	Enable Hunt Group configuration	Enable Call Park configuration	Enable Call Pickup configuration	Enable Calling Privileges configuration	Enable After Hours configuration	Enable Single Number Reach configuration
default	—	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
ESRST_and_Dialplan	—	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
ESRST_only	—	Yes	—	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SRST_and_Dialplan	Yes	Yes	Yes	Yes	—	—	—	—	—	—
SRST_only	Yes	Yes	—	Yes	—	—	—	—	—	—

Procedure

Step 1 Select **Configure > Site Templates**.

The system displays the Site Templates page, containing a list of the site templates configured in Cisco Unified SRST Manager.

Step 2 To create a new site template, update an existing site template, or view the details of an existing site template, see Creating, Changing, and Viewing a Site Template.

Step 3 To remove a site template, do the following:

a. Select the site template to delete.

b. Click **Remove**.

c. Click **OK** at the warning message.

Related Topics

- Creating, Changing, and Viewing a Site Template

Creating, Changing, and Viewing a Site Template

Procedure

Step 1 Select **Configure > Site Templates**.

The system displays the Site Templates page, containing a list of the site templates configured in Cisco Unified SRST Manager.

Step 2 Do one of the following:

- To create a new site template, click **Add**.

Note You can create a maximum of 10 site templates.

- To view the details of an existing site template or to change a site template, click the underlined name of the site template.

The system displays the Site Template Profile page, including the following information.

Note Some of the parameters are hidden in the initial view. Click the “Show Individual Feature Configuration” link to display all of the parameters.

Note Ensure that there are no active calls on a gateway when switching a site template from Cisco Unified SRST to E-SRST.

Table 10 Site Template Profile Parameters

Parameter	Description
Template	
Name	The name of the site template. Restriction: The name cannot have spaces in it.
Site Feature Configuration	
Provision Site as Classic SRST	Provision the site as classic SRST. The larger feature set that E-SRST enables will not be provisioned.

Table 10 Site Template Profile Parameters (continued)

Parameter	Description
Auto-Learn Call Forward Settings	Cisco Unified SRST Manager retrieves call forward settings from Cisco Unified Communications Manager and provisions the settings on the site. If disabled, specify a number in the “Call Forward Number” field for Cisco Unified SRST Manager to use to provision on the site.
Call Forward Number	If Auto Learn Call Forward Settings is disabled, the number specified here (instead of the voicemail pilot on CUCM) will be used by Cisco Unified SRST Manager to configure the call forward settings on the site. If using a centralized voicemail server, consider entering the number of a local receptionist to ensure that forwarded calls are handled correctly when the WAN link is down and the central voicemail server is unreachable.
Enable Dial Plan configuration	Cisco Unified SRST Manager retrieves dial plan information from the CUCM and provisions the dial plan configuration on the site branch router.
Enable Music on Hold configuration	Cisco Unified SRST Manager provisions the music on hold (MOH) configuration on the site branch router.
Enable Hunt Group configuration	Cisco Unified SRST Manager retrieves hunt group information from the CUCM and provisions the hunt group configuration on the site branch router.
Enable Call Park configuration	Cisco Unified SRST Manager retrieves call park information from the CUCM and provisions the call park configuration on the site branch router.
Enable Call Pickup configuration	Cisco Unified SRST Manager retrieves call pickup information from the CUCM and provisions the call pickup configuration on the site branch router.
Enable Calling Privileges configuration	Cisco Unified SRST Manager retrieves call restrictions (calling search spaces, partitions, and so on) information from the CUCM and provisions the call restriction configuration on the site branch router.
Enable After Hours configuration	Cisco Unified SRST Manager retrieves time-based calling restrictions information from the CUCM and provisions the configuration on the site branch router.
Enable Single Number Reach configuration	Cisco Unified SRST Manager retrieves single number reach information from the CUCM and provisions the single number reach configuration on the site branch router.

Step 3 Enter information in the fields. See Table 10.

Step 4 Click **Update**.

Related Topics

- Using Site Templates

PART 2

Making Updates to the System

Working With DNS Servers

Restriction

You can have a maximum of four DNS servers.

Note DNS server configuration is optional in the Cisco Unified SRST Manger version 11.0. If DNS server is not configured, then it is highly recommended to provide IP address of the Cisco Unified Communications Manager (CUCM) in the GUI at the time of adding CUCM. If host name of the CUCM is provided then ensure that IP address of the CUCM is present in the certificate under alternate host name.

Procedure

Step 1 Select **System** > **Domain Name System Settings**.

The system displays the Domain Name System Settings page.

Step 2 To update the domain name settings, enter values for one or both of the following:

- The hostname of the Cisco Unified SRST Manager system.
- The domain name. **Example**: Cisco.com

Step 3 To add a DNS server, do the following:

a. Click **Add**.

b. Enter the IP address of the DNS server.

c. Click **Add**.

Step 4 To remove a DNS server, do the following:

a. Select the check box next to the DNS server to delete.

b. Click **Delete**.

c. At the prompt, click **OK**.

What To Do Next

If you have made any changes, save and then reload the configuration. See Saving and Reloading the Cisco Unified SRST Manager Configuration.

Working With Network Time and Time Zone Settings

You must add an NTP server to Cisco Unified SRST Manager and configure the time zone to ensure that system processes have the correct date and time associated with them.

Restriction

You can have a maximum of four NTP servers.

Procedure

Step 1 Select **System** > **Network Time & Time Zone Settings**.

The system displays the Network Time & Time Zone Settings page.

Step 2 To add an NTP server, do the following:

a. Click **Add**. The system displays the Add a NTP Server page.

b. Enter the IP address of the NTP server.

c. Select the Preferred check box to make this the preferred NTP server.

d. Click **Add**.

Step 3 To remove an NTP server, do the following:

a. Select the check box next to the NTP server that you want to delete.

b. Click **Delete**.

c. At the prompt, click **OK**.

Step 4 To update the time zone settings, change the values for the country or time zone where the Cisco Unified SRST Manager system resides. Click **Apply**.

What To Do Next

If you have made any changes, save and then reload the configuration. See Saving and Reloading the Cisco Unified SRST Manager Configuration.

Displaying System Information

Procedure

Step 1 To display the System Information page, select **System** > **System Information**.

The system displays the System Information page.

The System Information page displays the following:

Parameter	Description
Module SKU	SKU for Cisco Unified SRST Manager.
Number of Processors	Number of processors allocated to the Cisco Unified SRST Manager VM.
CPU Model	CPU model of the processor(s) allocated to the Cisco Unified SRST Manager VM.
CPU Speed (MHz)	CPU speed of the processor(s) allocated to the Cisco Unified SRST Manager VM.
CPU Cache (KByte)	CPU cache size of the processor(s) allocated to the Cisco Unified SRST Manager VM.
Software Version	Version of Cisco Unified SRST Manager software that is running on this system.
Uptime	Amount of time that the Cisco Unified SRST Manager system has been running.
SDRAM	Amount of memory allocated to the Cisco Unified SRST Manager VM.
Disk Size(s)	Hard disk storage space allocated to the Cisco Unified SRST Manager VM.

About Security for Cisco Unified SRST Manager

About Security

Security certificates are required to provide a secure connection between systems. Security is needed for the following:

- Between Cisco Unified Communications Manager and Cisco Unified SRST Manager
- Between Cisco Unified SRST Manager and the Cisco Unified SRST or CUCME device at the branch site

About Security Certificates

Use one of these methods to generate and sign security certificates:

- Trust chains. Trust chains use Certificate Authorities (CAs) to simplify large deployments. Install security certificates for the Cisco Unified Communications Manager and Cisco Unified SRST Manager that were all signed by a CA and the connections are all part of a trusted chain.
- Self-signed certificates. Use self-signed certificates for each device. In this case, Cisco Unified SRST Manager needs the security certificate from each device to which it connects.

The TLS security certificate can be represented in one of two formats: distinguished encoding rules (DER) and privacy-enhanced mode (PEM).

Retrieving Security Certificates from Cisco Unified Communications Manager

Note Use this method to retrieve the certificates from the Cisco Unified Communications Manager system. You will later add this certificate to the Cisco Unified SRST Manager system.

Procedure

Step 1 Log in to the Cisco Unified OS Administration interface.

Step 2 Select **Security > Certificate Management**.

Step 3 Click **Find** to show the certificates.

Step 4 Click the *.pem or *.der link for the desired certificate.

Step 5 Click **Download** to save the certificate to the local file system.

Working With Trusted TLS Certificates

- Viewing and Removing Trusted TLS Certificates
- Adding a Trusted TLS Certificate
- Viewing a Trusted TLS Certificate

Viewing and Removing Trusted TLS Certificates

Restriction

Trusted TLS certificates cannot be edited.

Procedure

Step 1 Select **System** > **Trusted TLS Certificates**.

The system displays the Trusted TLS Certificates page with the following information:

- Label
- Owner
- Issuer

Step 2 To add a trusted TLS certificate, click **Add**. See Adding a Trusted TLS Certificate.

Step 3 To see more information about a trusted TLS certificate, click the underlined name of the certificate. See Viewing a Trusted TLS Certificate.

Step 4 To remove a trusted TLS certificate, do the following:

a. Select the check box next to the trusted TLS certificate to remove.

b. Click **Remove**.

Related Topics

- Back to the Working With Trusted TLS Certificates menu page
- Adding a Trusted TLS Certificate
- Viewing a Trusted TLS Certificate

Adding a Trusted TLS Certificate

Add a trusted TLS certificate either by uploading a file or by uploading text.

Before You Begin

If uploading a file, upload the trusted TLS certificate to a location where you can find it easily.

Restriction

TLS certificates that you paste into the text window must be in PEM format. Certificate files that you upload to Cisco Unified SRST Manager may be in PEM or DER format.

Procedure

Step 1 Select **System** > **Trusted TLS Certificates**.

The system displays the Trusted TLS Certificates page.

Step 2 Click **Add**.

The system displays the Add Trusted TLS Certificate page.

Step 3 Enter the keystore label for this trusted TLS certificate. This is a unique identifier for this certificate.

Step 4 Select **Certificate File** if the trusted TLS certificate will be a file or select **Certificate Text** if the certificate will be uploaded as plain text.

Step 5 Do one of the following:

- If you selected Certificate File, click **Browse**. Navigate to the file, highlight it, and click **Open**.
- If you selected Certificate Text, paste the contents of the trusted TLS certificate in the text box.

Step 6 Click **Update**.

Related Topics

- Back to the Working With Trusted TLS Certificates menu page
- Viewing and Removing Trusted TLS Certificates
- Viewing a Trusted TLS Certificate

Viewing a Trusted TLS Certificate

Procedure

Step 1 Select **System** > **Trusted TLS Certificates**.

The system displays the Trusted TLS Certificates page.

Step 2 To see more information about a trusted TLS certificate, click the underlined name of the certificate. The system displays the <*name_of_trusted_TLS_certificate*> Trusted Certificate Entry page with the following information:

Parameter	Description
Owner Info	
Common Name (CN)	The X.500 common name attribute, which contains the name of an object. If the object corresponds to a person, it is typically the person's full name. This is usually the hostname of the server to which you are talking.
Organization (O)	The name of an organization.
Organization (OU)	The name of an organizational unit.
Location (L)	The name of a locality, such as a city, county or other geographic region.
State (ST)	The full name of a state or province.
Country (C)	The country name. A two-letter ISO 3166 country code.
Issuer Info—The entity that verified the information and issued the certificate.	
Common Name (CN)	The X.500 common name attribute, which contains the name of an object. If the object corresponds to a person, it is typically the person's full name. This is usually the hostname of the server to which you are talking.
Organization (O)	The name of an organization.
Organization (OU)	The name of an organizational unit.
Location (L)	The name of a locality, such as a city, county or other geographic region.
State (ST)	The full name of a state or province.
Country (C)	The country name. A two-letter ISO 3166 country code.
Validity	
Valid From	The date from which the certificate is first valid.
Expires On	The date on which the certificate expires.

Parameter	Description
Fingerprint	
MD5	The fingerprint (also known as thumbprint) is a cryptographic hash value that uniquely identifies the certificate. The MD5 message-digest algorithm is a widely used cryptographic hash function with a 128-bit (16-byte) hash value. Specified in RFC 1321, MD5 has been employed in a wide variety of security applications, and is also commonly used to check the integrity of files.

Step 3 To return to the Trusted TLS Certificates page, click **Back**.

Related Topics

- Back to the Working With Trusted TLS Certificates menu page
- Viewing and Removing Trusted TLS Certificates
- Adding a Trusted TLS Certificate

PART 3

Monitoring and Maintaining the System

Monitoring the Provisioning Status of a Branch Device

While Cisco Unified SRST Manager is actively provisioning branch call agent devices, you can view the realtime status of the provisioning process. To view the status, select **Monitor > Provisioning Status**. If the provisioning cycle was started manually, the system automatically displays the provisioning monitor page.

The system automatically refreshes the Provisioning Status page until all the selected sites have finished the provisioning cycle. During this time, you can navigate away from this page and return later to review the updated status. If the provisioning has not finished, the page will display the updated status for individual sites.

- Site—The name of the site being provisioned.
- Progress—The current state of provisioning:
  - Not Started
  - In Progress
  - Complete
- Result—Indicates the outcome of the provisioning process for the site (or indicates that the provisioning is still in progress):
  - In Progress
  - Success
  - Failed

If the system is not currently provisioning any sites, the system displays an informational message stating this.

Related Topics

- For information about generating the Site Provisioning report, see Viewing the Site Provisioning History Report.
- For descriptions of all alerts, see System Alerts.

Monitoring the Learned Cisco Unified Communications Manager Express Routers

Procedure

Step 1 Select **Monitor > Learned CUCME Routers**.

The system displays the Learned CUCME Routers page listing all the Cisco Unified Communications Manager Express routers that have been added to Cisco Unified SRST Manager. For each router, the system lists the following information:

Parameter	Description
Site	Name of the site where the learned Cisco Unified Communications Manager Express device resides.
CUCME IP Address	IP address for the learned Cisco Unified Communications Manager Express device.
Platform	Hardware platform on which the learned Cisco Unified Communications Manager Express site is installed.
CUCME Version	Version of Cisco Unified Communications Manager Express installed.

Step 2 To filter the list of routers, do the following:

a. Select a filter from the Filter drop-down list.

b. Select a condition from the Match if drop-down list.

c. Enter a keyword.

d. Click **Go**.

e. To clear the values, click **Clear Filter** and click **Go**.

Viewing Configuration Changes

After provisioning a cisco router successfully, you can view the configuration changes associated with the router under **Reports > Site Provisioning History** in Cisco Unified SRST Manager GUI. The following columns under Site Provisioning History provides the details of configuration changes associated with a router:

- Latest Configuration Changes
- Complete Configuration Changes

The configuration changes file is created for both Cisco Unified SRST routers and Cisco Unified E-SRST routers. It contains the details of the mode and the time stamp. The configuration changes file can store data to a maximum of 2MB. If configuration changes exceeds 2MB, then the data is overwritten.

Latest Configuration Changes

Latest Configuration Changes log file provides the list of CLI which are pushed to the router between the latest two successful provisioning. If there are no new CLIs added between the last successful provisioning and the current successful provisioning, then the latest configuration changes section will be empty. If the current provisioning fails, then there is no content in the latest configuration changes. Check the time stamp to confirm the latest configuration changes.

Complete Configuration Changes

Complete Configuration Changes log file provides details of all the CLI that are pushed to the router from Cisco Unified SRST Manager at any point of time.

Cisco Unified SRST Manager gets the CLI information from the router. Hence, there is possibility that some CLI, which automatically comes with the parent CLI may also be listed. If you have configured some CLI manually, then those CLIs will also be listed.

Viewing the Configuration Changes

To viewing the CLI log file, refer to Viewing the Site Provisioning History Report, page 109.

Maintaining the Cisco Unified SRST Manager System

Copying Configurations

Use Cisco Unified SRST Manager EXEC commands to copy the startup configuration and running configuration to and from the hard disk on the Cisco Unified SRST Manager VM, the network FTP server, and the network TFTP server.

Note Depending on the specific TFTP server you are using, you might need to create a file with the same name on the TFTP server and verify that the file has the correct permissions before transferring the running configuration to the TFTP server.

Copying the Startup Configuration from the Hard Disk to Another Location

Starting in Cisco Unified SRST Manager EXEC mode, use the following command to copy the startup configuration on the hard disk to another location:

copy startup-config {**ftp:** *user-id:password@ftp-server-url* | **tftp**:*tftp-server-url*}

Syntax Description

ftp: *user-id*:*password@*	Username and password for the FTP server. Include the colon (:) and the “at” sign (@) in your entry.
ftp-server-url	URL of the FTP server including directory and filename (for example, ftps://server/dir/filename)
tftp:*tftp-server-url*	URL of the TFTP server including directory and filename (for example, tftps://server/dir/filename)

This command is interactive and prompts for the required information. You cannot enter the parameters in one line. The following examples illustrate this process.

In this example, the startup configuration is copied to the FTP server, which requires a username and password to transfer files. The startup configuration file is saved on the FTP server with the filename **start**.

```
srstmgr-1# copy startup-config ftp
Address or name of remote host? admin:messaging@ftps://server/dir/start
Source filename? temp_start
```

The following example shows the startup configuration copied to the TFTP server, which does not require a username and password. The startup configuration is saved in the TFTP directory **configs** as filename **temp_start**.

```
srstmgr-1# copy startup-config tftp
Address or name of remote host? tftps://server/dir/temp_start
Source filename? temp_start
```

Note Depending on the specific TFTP server, you might need to create a file with the same name on the TFTP server and verify that the file has the correct permissions before transferring the running configuration to the TFTP server.

Copying the Startup Configuration from the Network FTP Server to Another Location

Starting in Cisco Unified SRST Manager EXEC mode, use the following command to copy the startup configuration on the network FTP server to another location:

copy ftp: {running-config | startup-config} *user-id:password@ftps://server/dir/filename*

Syntax Description

running-config	Active configuration on hard disk.
startup-config	Startup configuration on hard disk.
*user-id***:***password@*	Username and password for the FTP server. Include the colon (:) and the at sign (@) in your entry.
ftp-server-url	URL of the FTP server.

This command is interactive and prompts you for the information. You cannot enter the parameters in one line. The following example illustrates this process.

Examples

In this example, the FTP server requires a username and password. The file **start** in the FTP server configs directory is copied to the startup configuration.

```
srstmgr-1# copy ftp: startup-config
!!!WARNING!!! This operation will overwrite your startup configuration.
Do you wish to continue[y]? y
Address or name or remote host? admin:messaging@tftps://server/configs
Source filename? start
```

Note Depending on the specific TFTP server, you might need to create a file with the same name on the TFTP server and verify that the file has the correct permissions before transferring the running configuration to the TFTP server.

Copying the Running Configuration from the Hard Disk to Another Location

Starting in Cisco Unified SRST Manager EXEC mode, use the following command to copy the running configuration on the hard disk to another location:

copy running-config {ftp: *user-id:password@***ftps://***server/dir/filename* |
startup-config | **tftp:tftps://***server/dir/filename* **}**

Syntax Description

ftp: *user-id***:***password@*	Username and password for the FTP server. Include the colon (:) and the at sign (@) in your entry.
ftp-server-url	URL of the FTP server including directory and filename..
startup-config	Startup configuration on hard disk.
tftp-server-url	URL of the TFTP server including directory and filename.

When you copy the running configuration to the startup configuration, enter the command on one line.

When you copy to the FTP or TFTP server, this command becomes interactive and prompts you for the information. You cannot enter the parameters in one line. The following example illustrates this process.

Examples

In the following example, the running configuration is copied to the FTP server, which requires a username and password. The running configuration is copied to the configs directory as file **saved_start**.

```
srstmgr-1# copy running-config ftp:
Address or name of remote host? admin:messaging@ftps://server/configs
Source filename? saved_start
```

In the following example, the running configuration is copied to the startup configuration. In this instance, enter the command on a single line.

```
srstmgr-1# copy running-config startup-config
```

Note Depending on the specific TFTP server, you might need to create a file with the same name on the TFTP server and verify that the file has the correct permissions before transferring the running configuration to the TFTP server.

Copying the Running Configuration from the Network TFTP Server to Another Location

Starting in Cisco Unified SRST Manager EXEC mode, use the following command to copy the running configuration from the network TFTP server to another location:

copy tftp: {**running-config** | **startup-config**} **tftps:**//*server/dir/filename*

Syntax Description

running-config	Active configuration on hard disk.
startup-config	Startup configuration on hard disk.
tftp-server-url	URL of the TFTP server.

This command is interactive and prompts you for the information. You cannot enter the parameters in one line. The following example illustrates this process.

Examples

In this example, the file **start** in directory **configs** on the TFTP server is copied to the startup configuration.

```
srstmgr-1# copy tftp: startup-config
!!!WARNING!!! This operation will overwrite your startup configuration.
Do you wish to continue[y]? y
Address or name of remote host? tftps://server/configs
Source filename? start
```

Note Depending on the specific TFTP server, you might need to create a file with the same name on the TFTP server and verify that the file has the correct permissions before transferring the running configuration to the TFTP server.

Restoring Factory Default Values

Cisco Unified SRST Manager provides a command to restore the factory default values for the entire system. Restoring the system to the factory defaults erases the current configuration. This function is available in offline mode. When the system is clean, a message appears indicating that the system will reload, and the system begins to reload. When the reload is complete, the system prompts you to start the post-installation process.

Caution This operation is irreversible. All data and configuration files are erased. Use this feature with caution. We recommend that you do a full system backup before proceeding with this feature.

Procedure

Step 1 Enter the following to put the system into offline mode:

```
srstmgr-1# offline
```

Step 2 Enter the following:

```
srstmgr-1(offline)# restore factory default
```

The system displays a message stating that this will cause all the configuration and data on the system to be erased and this is not reversible, and asks if you want to continue.

Step 3 Do one of the following:

- Enter **n** to retain the system configuration and data.

  The operation is cancelled, but the system remains in offline mode. To return to online mode, enter **continue**.

- Enter **y** to erase the system configuration and data.

  When the system is clean, a message appears indicating that the system will start to reload. When the reload is complete, a prompt appears to start the post-installation process.

Going Offline, Reloading, Rebooting, Shutting Down, and Going Back Online

You must take the Cisco Unified SRST Manager system offline before you can back up, reload, or restore the system; however, you do not need to take the system offline to shut down the system.

Shut down Cisco Unified SRST Manager from the console or CLI interface before powering off the virtual machine from the vSphere client/vCenter application.

- Taking the Cisco Unified SRST Manager System Offline, page 97
- Restarting the Cisco Unified SRST Manager System, page 98
- Shutting Down the Cisco Unified SRST Manager System, page 98

Taking the Cisco Unified SRST Manager System Offline

Using the **offline** command in Cisco Unified SRST Manager EXEC mode takes the system into offline/administration mode. When you use the **offline** command, the system prompts you for confirmation. The default is “no,” so to confirm, you must enter **y** for “yes.”

Procedure

Step 1 Enter the following command:

offline

Step 2 Enter **y** to confirm.

Example

```
srstmgr-1# offline
!!!WARNING!!!: If you are going
offline to do a backup, it is
recommended
that you save the current
running configuration using the
‘write’ command,
prior to going to the offline
state.
Putting the system offline will
terminate all end user sessions.
Are you sure you want to go
offline[n]? :y
srstmgr-1(offline)
```

Restarting the Cisco Unified SRST Manager System

To restart the system using the starting configuration, use the **reload** command in Cisco Unified SRST Manager offline/administration mode. Restarting the system will terminate all end-user sessions and cause any unsaved configuration data to be lost.

Procedure

Step 1 Enter the following command:

reload

Example

```
srstmgr-1(offline) reload
srstmgr-1(offline)>
MONITOR SHUTDOWN...
EXITED: probe exit status 0
EXITED: SQL_startup.sh exit status 0
EXITED: LDAP_startup.sh exit status 0
[...]
Booting from Secure secondary boot loader..., please wait.

[BOOT-ASM]


Please enter '***' to change boot configuration:
[...]
STARTED: /bin/products/umg/umg_startup.sh

 waiting 70 ...
SYSTEM ONLINE
srstmgr-1#
```

Shutting Down the Cisco Unified SRST Manager System

To halt the system, use the **shutdown** command in Cisco Unified SRST Manager EXEC mode.

⚠ **Caution** You must shut down the software before you shut down the VM.

- Shutting Down the Software, page 99
- Shutting Down the VM, page 99

Shutting Down the Software

Procedure

Step 1 Enter the following command:

shutdown

Shutting Down the VM

Power off the VM using the VMware management application.

Viewing Reports

- Viewing the Alert History Report
- System Alerts
- Viewing the Site Provisioning History Report
- Viewing the Backup History Report
- Viewing the Restore History Report
- Viewing the Network Time Protocol Report
- Viewing Site Dial Peer Details

Viewing the Alert History Report

The Alert History Report displays a list of all system alert messages that have occurred on the system. The alerts include critical, error, warning, and informational messages. The messages are grouped by alert level, and appear in chronological order. You can filter the alerts according to alert level by selecting specific check boxes at the top of the report and clicking **Go**.

Procedure

Step 1 Select **Reports** > **Alert History**.

The Alert History Report contains the following fields:

- Level—Alert level. Can be critical, error, warning, or informational.
- System—The system originating the alert message.
- Date and Time—Date and time when the system created the alert.
- Description—Description of the alert. See System Alerts for a list of all the alerts.
- Help—Additional information about the alert. To see the details, click **details**.

Step 2 To delete all of the alerts, click **Delete Alert History**.

Related Topics

- Back to the Viewing Reports menu page
- System Alerts

System Alerts

The following tables list all the alerts:

- Table 11: System Alerts – Warnings
- Table 12: System Alerts – Errors
- Table 13: System Alerts – Informational Messages

Table 11 System Alerts – Warnings

Alert Name	Description
CcmFailoverToSecondary	The primary central call agent was unavailable for provisioning, but the secondary central call agent was successfully utilized.
CcmUnreachableForProvisioning	Cisco Unified SRST Manager was unable to pull provisioning information from the configured telephony service server because it could not be reached on the network. Typically telephony service is provided by a central call agent like Cisco Unified Communications Manager.
ProvisioningCycleSuspended	Cisco Unified SRST Manager has suspended the process of provisioning remote sites based on the central site configuration.
SiteProvisioningSkipped	Provisioning for a site was skipped due to incomplete configuration.
SrstCSSNameConflictFound	A name conflict was found for Cisco Unified Communications Manager Calling Search Space names when applied to the Cisco Unified Communications Manager Express class of restriction lists.
SrstDialPeerMatchingToCUCMRoutePatternNotFound	Unable to find a matching dial peer to a Cisco Unified Communications Manager route pattern.
SrstLongHuntGroupChainFound	Hunt group configuration: Unable to configure long hunt pilot.
SrstMultipleTimeZonesFound	Multiple time zones for a site were found on the central Cisco Unified Communications Manager.
SrstPartitionNameConflictFound	A name conflict was found for Cisco Unified Communications Manager partition names when applied to the Cisco Unified Communications Manager Express class of restriction names.

Table 11 System Alerts – Warnings (continued)

Alert Name	Description
SrstTimeBasedPartitionsDayOfMonthLimitReached	After hours configuration: Cisco Unified SRST Manager was unable to add more day of month schedules because the Cisco Unified Communications Manager Express time-based-partitions day of month limit has been reached.
SrstWarning	Cisco Unified SRST Manager has indicated a warning. Refer to the log files for details about the warning.
TlsCredentialExpired	A TLS credential on Cisco Unified SRST Manager has expired.
UmgProvisioningWarnings	Provisioning of the secondary Cisco Unified SRST Manager has some anomalies. **Note** The details link for this alert contains a list of all the provisioning errors seen for the Cisco Unified SRST Manager aggregated into a single alert.
UmgUnreachableForProvisioning	Cisco Unified SRST Manager was unable to provision a secondary Cisco Unified SRST Manager because it was unable to create a connection to the device. Possible causes for the failure include Cisco Unified SRST Manager TLS configuration, router line VTY configuration, or a network problem.

Table 12 System Alerts – Errors

Alert Name	Description
CcmGlobalDataRetrievalFailure	Cisco Unified SRST Manager was unable to update the global Cisco Unified SRST data from Cisco Unified Communications Manager. See the logs for more details.
CcmProvisiningFail	Cisco Unified SRST Manager could not provision because of a communications problem with the central call agent.
CcmProvisioningFailAuth	Cisco Unified SRST Manager could not provision because of bad central call agent AXL credentials. Update the AXL username and password for the central call agent and try again.

Table 12 System Alerts – Errors (continued)

Alert Name	Description
CcmProvisioningFailTls	Cisco Unified SRST Manager could not provision because of a bad central call agent public TLS certificate. Add the central call agent's TLS certificate to Cisco Unified SRST Manager and try again.
CcmSrstReferenceDataRetrievalFailure	Cisco Unified SRST Manager was unable to update site-specific Cisco Unified SRST data from Cisco Unified Communications Manager. See the logs for more details.
LocalhostDnsFailure	The Cisco Unified SRST Manager host cannot be resolved by the DNS server.
SrstAfterHourNoExemptFailure	Unable to get After Hours no Exempt for the specified site. See the logs for more details.
SrstAfterHoursBlockPatternFailed	The after-hours configuration was unable to configure some after hours block patterns. See the logs for more details.
SrstAfterHoursConfigurationFailed	The after-hours configuration failed. See the logs for failure details.
SrstAfterHoursCreationFailed	Cisco Unified SRST Manager was unable to create after hours. See the logs for more details.
SrstCallParkConfigurationFailed	One or more errors were seen while trying to configure call park entries. See the logs for more details.
SrstCcpDiscoveryFailure	Cisco Unified SRST Manager was unable to execute configuration discovery for the Cisco Unified SRST site. See the logs for more details.
SrstCMENotSupportedFailure	Cisco Unified Communications Manager Express voice is not supported on the router. Check the router version and image.
SrstCreateDnFailure	Cisco Unified SRST Manager was unable to create the DN in Cisco Unified SRST. See the logs for more details.
SrstCreateExternalCallRoutingFailure	Cisco Unified SRST Manager was unable to create the external call routing configuration in Cisco Unified SRST.
SrstCreatePhoneFailure	Cisco Unified SRST Manager was unable to create a phone in Cisco Unified SRST. See the logs for more details.
SrstCreateSoftkeyTemplateFailure	Cisco Unified SRST Manager was unable to create a softkey template in Cisco Unified SRST. See the logs for more details.

Table 12 System Alerts – Errors (continued)

Alert Name	Description
SrstCreateSpeedDialFailure	Cisco Unified SRST Manager was unable to create speed dial in Cisco Unified SRST. See the logs for more details.
SrstCreateTranslationRulesFailure	Cisco Unified SRST Manager was unable to create translation rules in Cisco Unified SRST.
SrstCritical	Cisco Unified SRST Manager has experienced a critical error. Refer to the log files for details about the error.
SrstDeleteDnFailure	Cisco Unified SRST Manager was unable to delete the DN in Cisco Unified SRST. See the logs for more details.
SrstDeleteExternalCallRoutingFailure	Cisco Unified SRST Manager was unable to delete the external call routing configuration in Cisco Unified SRST.
SrstDeletePhoneFailure	Cisco Unified SRST Manager was unable to delete a phone in Cisco Unified SRST. See the logs for more details.
SrstDeleteSokftKeyTemplateExceeded	The maximum number of configured softkey templates was exceeded.
SrstDeleteSokftKeyTemplateFailure	Cisco Unified SRST Manager was unable to delete the softkey template in Cisco Unified SRST. See the logs for more details.
SrstDeleteSpeedDialFailure	Cisco Unified SRST Manager was unable to delete speed dial in Cisco Unified SRST. See the logs for more details.
SrstDeleteTranslationRulesFailure	Cisco Unified SRST Manager was unable to delete translation rules in Cisco Unified SRST.
SrstError	Cisco Unified SRST Manager has experienced an error. Refer to the log files for details about the error.
SrstFetchingCcmSRSTConfigurationFailure	Cisco Unified SRST Manager was unable to fetch the Cisco Unified SRST configuration from Cisco Unified Communications Manager. See the logs for more details.
SrstFetchingHardwareConfigurationFailure	Cisco Unified SRST Manager was unable to provision the site because it was unable to get hardware information for the site. See the logs for more details.

Table 12 System Alerts – Errors (continued)

Alert Name	Description
SrstFetchingMappingConfigurationFailure	Cisco Unified SRST Manager was unable to fetch the Cisco Unified SRST mapping configuration from the database. See the logs for more details.
SrstFetchingPlatformInformationFailure	Cisco Unified SRST Manager was unable to provision the site because it was unable to get hardware platform information based on the hardware. Ensure that this hardware is supported.
SrstFetchingSRSTConfigurationFailure	Cisco Unified SRST Manager was unable to fetch the Cisco Unified SRST configuration from the router. See the logs for more details.
SrstFetchingTelephonyConfigurationFailure	Cisco Unified SRST Manager was unable to fetch the telephony configuration from the router. See the logs for more details.
SrstFetchTranslationRulesFailure	Cisco Unified SRST Manager was unable to fetch translation rules from Cisco Unified SRST.
SrstGettingCSSContainingPartitionFailed	Cisco Unified SRST Manager was unable to get CSS Containing Partition. See the logs for more details.
SrstHuntGroupConfigurationFailed	The hunt groups configuration failed. See the logs for failure details.
SrstHuntGroupLongPilotFound	The hunt group configuration was unable to configure a long-chained hunt pilot.
SrstInvalidDateFormatFound	Cisco Unified SRST Manager was unable to provision the date format because an invalid or unsupported date format was found.
SrstInvalidTimeZoneFound	Cisco Unified SRST Manager was unable to provision the time zone because an invalid or unsupported time zone was found.
SrstMaxConfiguredCoRExceeded	The maximum configured class of restrictions was exceeded.
SrstMaxConfiguredPhoneExceeded	The number of maximum configured phones was exceeded.
SrstMaxConfiguredSpeedDialsExceeded	The maximum configured speed dials was exceeded in the phone.
SrstMaxConfiguredDnExceeded	The number of maximum configured DNs was exceeded.
SrstMOHProvisioningFailure	Unable to do MOH provisioning. See the logs for more details.

Table 12 System Alerts – Errors (continued)

Alert Name	Description
SrstMultipleExternalPhoneNumMaskFound	Multiple external phone number masks were found in Cisco Unified Communications Manager.
SrstMultipleTimeBasedPartitionsFound	The after-hours configuration was unable to configure a site because multiple time-based partitions were found on Cisco Unified Communications Manager.
SrstMultipleVMPilotsFound	Multiple voicemail pilots for a site were found on Cisco Unified Communications Manager.
SrstPhoneProvisioningFailed	Cisco Unified SRST Manager was unable to create or update the phone in Cisco Unified SRST. See the logs for more details.
SrstPickupGroupConfigurationFailed	One or more errors was seen while trying to configure pickup group entries. See the logs for more details.
SrstProvisioningFailed	Cisco Unified SRST Manager was unable to provision a Cisco Unified SRST site. See the logs for more details.
SrstRouterModeDetectionFailure	Cisco Unified SRST Manager was unable to detect the router properties. See the logs for more details.
SrstSNRProvisioningFailed	Unable to do SNR provisioning for the specified site. See the logs for more details.
SrstSNRUpdateFailed	Unable to update SNR for the specified site. See the logs for more details.
SrstSoftkeyTemplateProvisioningFailure	Cisco Unified SRST Manager was unable to provision Softkey Template in Cisco Unified SRST. See the logs for more details.
SrstSystemInSRSTModeFailure	Cisco Unified SRST Manager was unable to provision a site because the site is in Cisco Unified SRST mode. Remove the “call-manager-fallback” configuration and try again.
SrstUnsupportedCMEVersionFailure	Cisco Unified SRST Manager was unable to provision the site because the version of Cisco Unified Communications Manager Express found is unsupported. Check the router version and image.
SrstUpdateDnFailure	Cisco Unified SRST Manager was unable to update the DN in Cisco Unified SRST. See the logs for more details.

Table 12 System Alerts – Errors (continued)

Alert Name	Description
SrstUpdatePhoneFailure	Cisco Unified SRST Manager was unable to update a phone in Cisco Unified SRST. See the logs for more details.
SrstWritingMappingConfigurationFailure	Cisco Unified SRST Manager was unable to write the Cisco Unified SRST mapping configuration to the database. See the logs for more details.
TlsCredentialSigningFailed	There was a failed TLS credential signing request to an external SCEP certificate authority.
TlsCredentialSigningTimeout	There was a failed TLS credential signing request to an external SCEP certificate authority because the certificate authority never completed the transaction and returned the signed credentials.
UmgProvisioningFailed	Problems were encountered while provisioning the secondary Cisco Unified SRST Manager. **Note** The details link for this alert contains a list of all the provisioning errors seen for the Cisco Unified SRST Manager aggregated into a single alert.

Table 13 System Alerts – Informational Messages

Alert Name	Description
NewSrstReferenceDetected	A new Cisco Unified SRST reference has been detected on the central telephony server (Cisco Unified Communications Manager). This could be an indication of a new Cisco Unified SRST Manager site to prepare.
ProvisioningCycleComplete	Completed the process of provisioning remote sites based on the central site configuration.
ProvisioningCycleResuming	Restarted the process of learning of any configuration changes from the central site to complete the configuration that must be pushed down to SRSV-CUE devices on a remote site.
ProvisioningCycleStarted	Starting the process of learning of any configuration changes from the central site that must be pushed down to SRSV-CUE devices on a remote site.
SrstInfo	Cisco Unified SRST Manager has provided an informational message. Refer to the log files for message details.

Table 13 System Alerts – Informational Messages (continued)

Alert Name	Description
TlsCredentialRenewed	A TLS credential on Cisco Unified SRST Manager has expired but has been automatically renewed through a SCEP certificate authority.
UmgProvisioningInfo	This message is an indication that provisioning of the secondary Cisco Unified SRST Manager has some additional information to convey. **Note** The details link for this alert contains a list of all the provisioning errors seen for the Cisco Unified SRST Manager aggregated into a single alert.

Related Topics

- Back to the Viewing Reports menu page
- About the Cisco Unified SRST Manager Dashboard

Viewing the Site Provisioning History Report

The Site Provisioning History Report shows the results of the most recent successful site provisioning cycle. These results cannot be cleared or deleted.

Procedure

Step 1 Select **Reports** > **Site Provisioning History**.

The Site Provisioning History Report contains the following fields:

- Site—The site name. The report displays every site known to Cisco Unified SRST Manager.
- Last Attempt—Indicates the outcome of the most recent provisioning attempt made by Cisco Unified SRST Manager for that site. Results can include never, success, failed, or disabled.
  - "Never" indicates that the site has never been provisioned. The site may be newly created and neither the manual nor scheduled provisioning has occurred yet.
  - "Disabled" indicates that the site was administratively disabled for provisioning during the last provisioning cycle. You can enable a disabled site on the Site Profile page. See Changing the Information for a Single Cisco Unified SRST Site.
  - If the last attempt field is set to "Failed," the system displays the date and time of the failure, and generates an alert. The system also increments the failed provisioning status count on the dashboard. To see the alert details, click **Reports > Alert History**.

Note Site provisioning failures are severe. Correct the failure as soon as possible by reviewing the corresponding alert.

- Date and Time—The date and time of the last provisioning attempt. This field is blank if the Last Attempt field is Never or Disabled.
- Last Successful—Indicates the last time that Cisco Unified SRST Manager successfully provisioned the branch device. Can be either "Success" or "Never."

- Date and Time—If the status of the Last Successful field is Success, the report shows the date and time (relative to the branch device) when the successful provisioning was completed.
- Ephones Controlled—Displays the number of ephones being controlled by the CUCME device. The number should be consistent with the number of ephones provided by Cisco Unified Communications Manager.

Note Ephone data is shown only if E-SRST is enabled on the site.

- Latest Configuration Changes—If there is any change in the configuration between the current and previous successful provisioning, then a file containing the CLI difference will be available to view. Click **Details** to view the CLI differences.
- Complete Configuration Changes—Click **Details** to view the complete list of CLI running on Cisco Unified SRST Manager.

Step 2 To filter by status, such as success, failed, or never, select the check box next to a status and click **Go**.

Step 3 To view the Site Dial Peer Details page for a site in the report, click the site name in the report. See Viewing Site Dial Peer Details.

Related Topics

- Back to the Viewing Reports menu page
- About the Cisco Unified SRST Manager Dashboard
- Monitoring the Provisioning Status of a Branch Device
- Viewing and Provisioning Sites
- Viewing Site Dial Peer Details

Viewing the Backup History Report

Procedure

Step 1 Select **Reports** > **Backup History**.

If there is any backup history to report, the Backup History report contains the following fields:

- ID—ID of the backup.
- Server URL—The server where the backup history is stored.
- Backup Time and Date—Date and time when the system was last backed up.
- Version—The version of the Cisco Unified SRST Manager software that is installed.
- Description—A description of the backup.
- Result—Displays the status of the last backup procedure for system configuration information and for data. Values can be either Success or Fail.

Step 2 To sort backup reports, click any of the headers.

Related Topics

- Back to the Viewing Reports menu page
- Configuring Backup and Restore

Viewing the Restore History Report

The Restore History report shows the history of all the restore processes done on the current system since installation.

Procedure

Step 1 Select **Reports** > **Restore History**.

If there is any restore history to report, the Restore History report contains the following fields:

- ID—ID of the restore.
- Server URL—The server where the restore history is stored.
- Restore Time and Date—Date and time when the system was last backed up.
- Version—The version of Cisco Unified SRST Manager software that is installed.
- Result—Status of the last restore procedure. Result shows Success or Fail for the components that were restored.

Step 2 To sort restore history reports, click any of the headers.

Related Topics

- Back to the Viewing Reports menu page
- Configuring Backup and Restore

Viewing the Network Time Protocol Report

Procedure

Step 1 Choose **Reports** > **Network Time Protocol**.

The system displays the Network Time Protocol Report with the following fields:

- #—The prioritized number of the NTP server. The system attempts to synchronize its time starting with NTP server number one.
- NTP Server—IP address or hostname of the NTP server.
- Status—Indicates if the NTP server connected with Cisco Unified SRST Manager or if it was rejected.
- Time Difference (secs)—Time offset between the NTP server and the client.

- Time Jitter (secs)—Estimated time error of the system clock, measured as an exponential average of RMS time differences.

Related Topics

- Back to the Viewing Reports menu page
- Working With Network Time and Time Zone Settings

Viewing Site Dial Peer Details

This Site Dial Peer Details page displays a list of dial peers for a specific site and details about each dial peer.

Procedure

Step 1 Choose **Reports** > **Site Provisioning History** to display a report of the results of the most recent site provisioning cycle. The report includes each site known to Cisco Unified SRST Manager.

Step 2 Click the name of a site in the report.

The system displays the Site Dial Peer Details page for the site. The page contains the following information for each dial peer:

- Dial Peer tag—Digit that uniquely identifies a dial peer.
- Type—Category that identifies the type of dial peer.
- Destination Pattern—A pattern that the router uses to match the called number of incoming calls. If an incoming call conforms to the destination pattern for the dial peer, the router directs the call to that dial peer.
- Port—Voice port associated with the given dial peer.
- Preference—Preferred selection order of a dial peer within a hunt group.
- Created by SRST Manager—Indicates whether the dial peer was created by SRST Manager.

Related Topics

- Back to the Viewing Reports menu page

Backing Up and Restoring Data

Cisco Unified SRST Manager backup and restore functions use an FTP server to store and retrieve data. The backup function copies the files from Cisco Unified SRST Manager to the FTP server and the restore function copies the files from the FTP server to Cisco Unified SRST Manager. The FTP server can reside anywhere in the network as long as the backup and restore functions can access it with an IP address or hostname.

Tip It is recommended that you back up your configuration files whenever you make changes to the system or application files. Do backups regularly to preserve configuration data.

The system supports two types of backup: data and configuration. You can select one or both.

- Configuration—Backs up the system configuration, including registration credentials, configuration templates, central call agent, and so on.
- Data—Backs up system data.

Note It is strongly discouraged to back up only the data because of the potential of introducing inconsistency between configuration and data files.

Backups are performed only in offline mode. The system displays a message before performing the backup alerting you that the system will be taken offline.

Cisco Unified SRST Manager automatically numbers and dates the backup files. Performing different backup types at various times causes different backup IDs for data backups and configuration backups. For example, the last data backup ID might be 3, and the last configuration backup might be 4. Performing an “all” backup might result in a backup ID of 5 for both data and configuration.

When restoring the files, refer to the backup ID for the backup file that you want to use.

Note It is recommended that you back up your configuration files whenever changes are made to the system or application files. Back up data files, which contain voice messages, regularly, to minimize data loss, such as from a hardware failure.

Restrictions for Backing Up and Restoring Data

- Both the backing up and restoring functions require that the system be in offline mode, so we recommend performing this task when call traffic is least impacted.

- Cisco Unified SRST Manager supports only full backup and restore. This feature does not support backing up or restoring select details of a configuration.
- If you change a configuration, then perform a system restore, the restore process will overwrite the changes to the configuration.

Configuring Backup and Restore

Configuring the Backup Server

Before you begin the backup process, set the backup configuration parameters.

Procedure

Step 1 Select **Administration** > **Backup / Restore** > **Configuration**.

The system displays the Backup / Restore Configuration page.

Step 2 Enter the information shown in the following fields:

- Server URL—The URL of the server on the network where the backup files are stored. The format should be *ftp://<server/directory>/* where <*server/directory*> is the IP address or hostname of the server.
- User ID—The account name or user ID on the backup server. You must have an account on the system to which you are backing up your data. Do not use an anonymous user ID.
- Password—The password for the account name or user ID on the backup server.
- Maximum revisions—The maximum number of revisions of the backup data to keep on the server. The maximum number is 50. The default value is 5.

Step 3 Click **Apply** to save the information.

Manually Starting a Backup

Before You Begin

- Configure the server used to back up the data. See Configuring the Backup Server.
- Save your Cisco Unified SRST Manager configuration. See Saving and Reloading the Cisco Unified SRST Manager Configuration.

Procedure

Step 1 Select **Administration** > **Backup / Restore** > **Start Backup**.

The system displays the Backup / Restore Start Backup page and automatically generates a backup ID. The backup ID increases by 1 every time you back up the server.

Step 2 Enter a description of the backup file; for example, "backupdata2012-10-01."

Step 3 Select the check box for the types of data that you want to save. You can choose one or both:

- Configuration—Saves the system and application settings.
- Data—Saves the application data.

Step 4 Click **Start Backup**.

Step 5 Click **OK** at the confirmation message.

Viewing and Removing Scheduled Backups

Procedure

Step 1 Select **Administration** > **Backup / Restore** > **Scheduled Backups**.

If one or more backups have been scheduled, the system displays the Backup / Restore Scheduled Backups page with the following information:

- Name
- Description
- Schedule
- Next Run
- Categories of backup (type of data to save)

Step 2 To sort scheduled backups, click any of the headers.

Step 3 To modify an existing scheduled backup, click the underlined schedule name, edit the parameters, and click **Apply**.

Step 4 To add a new scheduled backup, click **Schedule Backup**. See Adding a Scheduled Backup.

Step 5 To disable all existing scheduled backups, which means that the system ignores all scheduled backups and does not collect any backup data, click **Bulk Disable**. See Disabling Scheduled Backups.

Note Disabling scheduled backups allows you to temporarily turn off backups without deleting the backup schedule.

Step 6 To remove a scheduled backup, do the following:

a. Select the check box next to the name of the backup.

b. Click **Delete**.

c. Click **OK** at the confirmation message.

Adding a Scheduled Backup

You can configure scheduled backups to occur once or recurring jobs that repeat:

- Every *n* days at a specific time
- Every *n* weeks on specific day and time
- Every *n* months on a specific day of the month and time
- Every *n* years on specific day and time

Before You Begin

You must do the following before starting a backup:

- Configure the server used to back up the data. See Configuring the Backup Server.
- Save the Cisco Unified SRST Manager configuration. See Saving and Reloading the Cisco Unified SRST Manager Configuration.

Procedure

Step 1 Select **Administration** > **Backup / Restore** > **Scheduled Backups**.

The system displays the Backup / Restore Scheduled Backups page.

Step 2 Click **Schedule Backup**.

The system displays the Backup / Restore Scheduled Backups page.

Step 3 Enter a name for the scheduled backup.

Step 4 Enter a description of the scheduled backup—for example, “backupdata2012-09-01.”

Step 5 Select the check box for the type of data that you want to save. You can select one or both:

- Configuration—Saves the configurations of the system and applications.
- Data—Saves your application data messages.

Step 6 Select whether the scheduled backup will occur:

- Once
- Daily
- Weekly
- Monthly
- Yearly

Step 7 Select whether the scheduled backup will start:

- Immediately
- On a specific date and time. If you choose this option, enter the date and time.

Step 8 Optionally, you can select the Disabled check box to disable the backup. The backup remains configured, but is not active. See Disabling Scheduled Backups.

Step 9 Click **Add**.

Step 10 If you choose Immediately, the system displays a message stating that running a backup will put the system in offline mode and disable management interfaces. Click **OK** to continue.

Disabling Scheduled Backups

Procedure

Step 1 Select **Administration** > **Backup/Restore** > **Scheduled Backups**.

The system displays the Backup / Restore Scheduled Backups page listing all the backups that are scheduled.

Step 2 To disable a single scheduled backup, do the following:

a. Click the underlined name of the scheduled backup. The system displays the Scheduled Backups page with information about this scheduled backup.

b. Select the **Disabled** check box.

c. Click **Apply**.

Step 3 To disable all scheduled backups, do the following:

a. Click **Bulk Disable**. The system displays the Scheduled Backups page with disabling information.

b. Select **Disabled Range** and enter a date range for when the scheduled backups will be disabled.

c. Click **Apply**.

Starting a Restore

After you have backed up your configuration and data, you can restore it for a new installation or upgrade.

Restriction

After you perform a restore, you cannot run the Setup Wizard.

Before You Begin

Configure a backup server. See Configuring the Backup Server.

Procedure

Step 1 Select **Administration** > **Backup / Restore** > **Start Restore**.

The system displays the Backup / Restore Start Restore page with the following fields:

- Backup ID—The backup ID of previous backups.
- Version—Version
- Description—Name of this backup.
- Backup Time and Date—Date and time when this backup was made.
- Categories—The type of data that you want to restore.

Step 2 Select the row containing the configuration that you want to restore.

Step 3 Select the check box for the type of data that you want to save. You can choose one or both:

- Configuration—Saves the configurations of the system and applications.
- Data—Saves your application data.

Step 4 Click **Start Restore**.

Step 5 After restoring the backup, you might need to console into Cisco Unified SRST Manager from the vSphere client/vCenter application, and re-configure the network credentials (interface Ethernet 0, and IP default gateway) before the system is ready for use.

Note In some cases, the backup includes the configuration of network credentials and no further configuration of network credentials is necessary after restoring the backup.

If the backup does not include the network credentials, or if it has incorrect credentials, you will not be able to reach the Cisco Unified SRST Manager GUI remotely. You can access Cisco Unified SRST Manager using the VMware manager console.

Backing Up and Restoring Data Using the CLI

Backup and Restore Using SFTP

Overview

You can transfer files from any Cisco Unified SRST Manager application to and from the backup server using Secure File Transfer Protocol (SFTP). SFTP provides data integrity and confidentiality that is not provided by FTP.

Because SFTP is based on Secure Shell tunnel version 2 (SSHv2), only SSHv2 servers are supported for this feature.

To run backup and restore over SFTP, you must configure the URL of the backup server in the form of sftp://*hostname*/*dir*, in addition to the username and password to log in to the server. The backup server must have an SSH daemon running with the SFTP subsystem enabled. The SSH protocol allows various user authentication schemes.

Performing Backup and Restore Using SFTP

Prerequisites

Cisco Unified SRST Manager 9.0 or a later version.

Required Data for This Procedure

There is no data required.

SUMMARY STEPS

1. **config t**
2. **backup** {**revisions** *number* | **server url** *sftp-url* **username** *sftp-username* **password** *sftp-password*}
3. **end**

DETAILED STEPS

	Command or Action	Purpose

Step 1	`config t`
	Example:
	`srstmgr-1# config t`
		Enters configuration mode.

Step 2	**backup** {**revisions** *number* | **server url** *sftp-url* **username** *sftp-username* **password** *sftp-password*}
	Example:
	`srstmgr-1(config)# backup server url sftp://branch/vmbackups username admin password mainserver`
		Performs a backup to the specified SFTP or FTP server. To use SFTP, the URL must be of the form sftp://*hostname*/*directory*.

Step 3	`end`
	Example:
	`srstmgr-1(config)# end`
		Returns to EXEC mode.

Backup Server Authentication Using a SSH Host Key

- Overview, page 121
- Configuring Backup Server Authentication Without Using the SSH Host Key, page 123
- Configuring Backup Server Authentication Using the SSH Host Key, page 124

Overview

You can authenticate the backup server using the SSH protocol before starting a backup/restore operation. The SSH protocol uses public key cryptography for server authentication.

This feature provides two methods of authenticating a server:

- Establishing a secure connection based only on the URL of a trusted backup server.
- Obtaining the fingerprint of the backup server and using it to establish a secure connection. This fingerprint is also known as the host key or private key.

The first method is easier than the second method, but it is less secure because it does not depend on knowledge of the backup server's private host key. However, if you know the URL of a trusted backup server, it is generally safe. In this case, the backup server securely provides the client with its private host key.

In both cases, when server authentication is enabled, the system validates the SSH server's private host key by comparing the fingerprint of the key received from the server with a preconfigured string. If the two fingerprints do not match, the SSH handshake fails, and the backup/restore operation does not occur.

You cannot use the GUI to configure this feature; you must use the CLI.

Both methods are explained in the following sections.

Configuring Backup Server Authentication Without Using the SSH Host Key

Prerequisites

Cisco Unified SRST Manager 9.0 or a later version

Required Data for This Procedure

To enable SSH authentication of a backup server without knowing the server's fingerprint (private host key), you must know the URL of a trusted backup server.

SUMMARY STEPS

1. **config t**
2. **backup server url sftp://***url*
3. **backup server authenticate**
4. **end**
5. **show security ssh knownhost**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**config t** **Example:** `srstmgr-1# config t`	Enters configuration mode.
Step 2	**backup server url sftp://***url* **Example:** `srstmgr-1(config)# backup server url sftp://company.com/server22`	Establishes an initial connection with the backup server.
Step 3	**backup server authenticate** **Example:** `srstmgr-1(config)# backup server authenticate`	Retrieves the fingerprint of the backup server's host key and establishes a secure SSH connection.

	Command or Action	Purpose

Step 4	`end`
	Example:
	`srstmgr-1(config)# end`
		Returns to EXEC mode.

Step 5	`show security ssh knownhost`
	Example:
	`srstmgr-1(config)# show security ssh knownhost`
		Displays a list of configured SSH servers and their fingerprints.

Configuring Backup Server Authentication Using the SSH Host Key

Prerequisites

Cisco Unified SRST Manager 9.0 or a later version

Required Data for This Procedure

To use a backup server's fingerprint (private host key) to enable SSH authentication, you must first retrieve the fingerprint "out-of-band" by running the **ssh-keygen** routine on the backup server. This routine is included in the OpenSSH package. The following example shows the command and its output:

ssh-keygen -l -f /etc/ssh/ssh_host_dsa_key.pub

1024 4d:5c:be:1d:93:7b:7c:da:56:83:e0:02:ba:ee:37:c1 /etc/ssh/ssh_host_dsa_key.pub

SUMMARY STEPS

1. **config t**
2. **security ssh knownhost** *host* **{ssh-rsa | ssh-dsa}** *fingerprint-string*
3. **end**
4. **show security ssh knowhost**

DETAILED STEPS

	Command or Action	Purpose

Step 1	`config t`
	Example:
	`srstmgr-1# config t`
		Enters configuration mode.

	Command or Action	Purpose
Step 2	**security ssh knownhost** *host* {**ssh-rsa** | **ssh-dsa**} *fingerprint-string* **Example:** `srstmgr-1(config)# security ssh knownhost server.cisco.com ssh-rsa a5:3a:12:6d:e9:48:a3:34:be:8f:ee:50:30:e5:e6:c3`	Configures the MD5 fingerprint of the SSH server's host key using the following arguments and keywords: *host* — Fully qualified hostname or IP address of the SSH server. **ssh-rsa** — RSA algorithm was used to create this fingerprint for a SSH server's host key. **ssh-dsa** — DSA algorithm was used to create this fingerprint for a SSH server's host key. *fingerprint-string* — MD5 fingerprint string.

Step 3	**end**
	Example:
	`srstmgr-1(config)# end`
		Returns to EXEC mode.

Step 4	**show security ssh knownhost** **Example:** `srstmgr-1(config)# show security ssh knownhost`	Displays a list of configured SSH servers and their fingerprints.

Encrypting and Signing of Backup Content on the Server

- Overview, page 125
- Configuring the Encryption and Signing of Backup Content on the Server, page 126

Overview

You can protect backed up configuration and data files using signing and encryption before the files are transferred to the backup server.

To enable this feature, you must configure a master key from which the encryption and signing key (known as the session key) are derived. The backup files are encrypted and signed before they are sent to the backup server. When restoring the files, the master key is used to validate the integrity of the files and decrypt them accordingly. You can also restore the backup files to any other machine running Cisco Unified SRST Manager 9.0 or later versions, if you configure the same master key before you begin the restore process. To make it easier to automate a scheduled backup, the master key is stored securely on the hosting device. It is not included in the backup content.

During the restore process, if the system detects that backup content has been tampered with, the restore process aborts. The system also halts and waits for the administrator to take some action, such as restoring using a different revision.

For backward compatibility, you can allow unsigned backup files to be restored if the risk is acceptable.

Configuring the Encryption and Signing of Backup Content on the Server

Prerequisites

Cisco Unified SRST Manager 9.0 or a later version

Required Data for This Procedure

There is no data required.

SUMMARY STEPS

1. **config t**
2. **backup security key generate**
3. **backup security protected**
4. **backup security enforced**
5. **end**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**`config t`**
	Example:
	`srstmgr-1# config t`
		Enters configuration mode.

Step 2	**`backup security key generate`**
	Example:
	`srstmgr-1(config)# backup security key generate`
		Creates the master key used for encrypting and signing the backup files.

Step 3	**`backup security protected`**
	Example:
	`srstmgr-1(config)# backup security protected`
		Enables secure mode for backups. In secure mode, all backup files are protected using encryption and a signature.

Step 4	**`backup security enforced`**
	Example:
	`srstmgr-1(config)# backup security enforced`
		Specifies that only protected and untampered backup files are restored.

Step 5	**`end`**
	Example:
	`srstmgr-1(config)# end`
		Returns to EXEC mode.

Saving and Reloading the Cisco Unified SRST Manager Configuration

Restriction

Reloading the system terminates all user sessions and lose all unsaved data.

Procedure

Step 1 Select **Administration** > **Control Panel**.

The system displays the Administration Control Panel page.

Step 2 To save the current configuration, do the following:

a. Click **Save Configuration**.

b. If the system displays a warning or confirmation message, click **OK**.

Step 3 To reload the saved configuration, do the following:

a. Click **Reload**. The system displays a warning message stating that this will terminate all user sessions and you will lose any unsaved data.

b. Click **OK**.

PART 4

Troubleshooting

Troubleshooting Using the GUI

Running a Network Connectivity Test

You can run a network connectivity test to initiate a connection between Cisco Unified SRST Manager and all the systems that are configured on the system, including the central call agent and branch call agents.

The test may take several minutes to complete. During the test, the status page will refresh automatically. You can either wait for the test to complete or go to other pages and later return to this page to see the test results.

Procedure

Step 1 Select **Troubleshoot** > **Network Connectivity and Audit**.

The system displays the Network Connectivity Test page.

Step 2 To start a network connectivity test, click **Start Network Connectivity Test**.

When the test is complete, the system displays a message stating that the test is complete and shows the results. See Viewing Results from a Network Connectivity Test. If the connectivity test fails, the system displays a brief indication of the cause of the failure. You can find additional failure diagnostic information in the trace buffer or message log.

Step 3 To cancel the network connectivity test that is currently running, click **Cancel Network Connectivity Test**.

Step 4 To see the results of previous network connectivity tests, click **Click here for results of previously run test**. The system displays the results. See Viewing Results from a Network Connectivity Test.

Note Results of previous tests are only available for the current login session.

Step 5 To restart a previous network connectivity test, click **Restart Network Connectivity Test**.

Related Topics

Back to the Troubleshooting Using the GUI menu page

Viewing Results from a Network Connectivity Test

After you run a network connectivity test (see Running a Network Connectivity Test), the system displays the results. If a connectivity test was run previously, you can view the results by selecting **Troubleshoot** > **Network Connectivity and Audit** and clicking "Click here for results of previously run test."

Table 14 Network Connectivity Test Result Parameters

Parameter	Description
Central Call Agents	
Cluster Name	Name of the central call agent cluster.
Hostname	Hostname of the central call agent to which Cisco Unified SRST Manager system tried to connect.
Result	Result of the network connectivity test. Can be either Success or Failed.
Time (ms)	The amount of time, in milliseconds, that it took to connect.
Details	Any additional details about this network connectivity test.
Branch Call Agents	
Hostname	Hostname of the branch call agent to which Cisco Unified SRST Manager tried to connect.
Result	Result of the network connectivity test. Can be either Success or Failed.
Time (ms)	The amount of time, in milliseconds, that it took to connect.
Details	Any additional details about this network connectivity test.

Configuring Trace Settings

Use this procedure to enable traces, or debug message output, for components in the Cisco Unified SRST Manager system. Components are modules, entities, and activities in the system. You can review the output by selecting **Troubleshoot > View > Trace Buffer**. See Viewing a Trace Buffer.

Restriction

Enabling too many traces can adversely affect the system performance.

Procedure

Step 1 Select **Troubleshoot** > **Traces**.

The system displays the Traces page, with a hierarchical listing of the system components.

Step 2 To enable a trace on a system component, select the check box next to the name of the component.

Step 3 To expand the listing of components, click the + sign next to the upper-level components.

Step 4 Select the check box next to an upper-level component (a module or entity) to enable the traces for all of the components under that component. Deselect the check box next to an upper-level component to disable the traces for all of the components under that component.

Step 5 Click **Apply** to save your changes.

Step 6 Click **OK** in the confirmation window.

Related Topics

Back to the Troubleshooting Using the GUI menu page

Viewing Tech Support Information

Procedure

Step 1 Select **Troubleshoot > View > Tech Support**.

The system displays the Tech Support page and shows a collection of configuration data.

Step 2 To save the tech support information, click **Download Tech Support** and save the file to a convenient location.

Related Topics

Back to the Troubleshooting Using the GUI menu page

Viewing a Trace Buffer

You can enable traces, or debug message output, for components in the Cisco Unified SRST Manager system. For details on configuring the trace, see Configuring Trace Settings. Use the following procedure to view the trace output.

Procedure

Step 1 Select **Troubleshoot > View > Trace Buffer**.

The system displays the Trace Buffer page and shows the contents of the trace buffer.

Step 2 To save the trace buffer information, click **Download Trace Buffer** and save the file to a convenient location.

Step 3 To clear the trace buffer information, do the following:

a. Click **Clear Trace Buffer**.

b. Click **OK** at the confirmation message.

Related Topics

Back to the Troubleshooting Using the GUI menu page

Viewing a Log File

Procedure

Step 1 Select **Troubleshoot > View > Log File**.

The system displays the Log File page and shows the contents of the log file.

Step 2 To save the log file, click **Download Log File Bundle** and save the file to a convenient location.

Related Topics

Back to the Troubleshooting Using the GUI menu page

Troubleshooting Using the CLI

Cisco technical support personnel may request that you run one or more of these commands when troubleshooting a problem. Cisco technical support personnel will provide additional information about the commands at that time.

Caution Some of these commands may impact the performance of your system. It is strongly recommended that you not use these commands unless directed to do so by Cisco Technical Support.

Log and Trace Files

About Logging

To check the log and trace files on the hard disk, use the **show logs** command in EXEC mode. This command displays the list of logs available, their size, and their dates of most recent modification.

When the log file reaches its maximum length, Cisco Unified SRST Manager renames the file and creates a new logging file.

For a detailed list of all the arguments associated with the **trace** command, see trace.

Note Logs for E-SRST are turned on by default.

Example of Log Output

The following is an example of the **show logs** output:

```
se-100-1-1-100# show logs
     SIZE             LAST_MODIFIED_TIME                                NAME
    14872   Thu Aug 09 06:10:07 PDT 2012                               dmesg
  3753146   Sun Aug 12 22:00:46 PDT 2012                          atrace.log
      200   Thu Aug 09 06:10:08 PDT 2012                    debug_server.log
     1258   Thu Aug 09 06:10:08 PDT 2012                            sshd.log
     2435   Thu Aug 09 06:10:08 PDT 2012                          syslog.log
    25197   Thu Aug 09 06:10:15 PDT 2012                         install.log
  2654089   Mon Aug 13 11:33:40 PDT 2012                        messages.log
      494   Thu Aug 09 06:10:10 PDT 2012                            klog.log
     8332   Thu Aug 09 06:10:22 PDT 2012                        postgres.log
     4289   Thu Aug 09 06:10:28 PDT 2012                             csl.log
    10415   Wed Aug 08 09:48:20 PDT 2012                   postgres.log.prev
      461   Thu Aug 09 06:10:32 PDT 2012    HttpServ_management_registry.log
        0   Wed Aug 08 10:22:50 PDT 2012                    _cpftpserver.log
   741308   Fri Aug 10 09:07:54 PDT 2012                      _cpgeneric.log
      602   Fri Aug 10 09:07:53 PDT 2012                       _cpnotify.log
   298191   Fri Aug 10 09:07:54 PDT 2012                       _cppstats.log
   508407   Fri Aug 10 09:07:54 PDT 2012                    _cptransport.log
    72512   Fri Aug 10 09:07:02 PDT 2012                   _cpconversion.log
        0   Wed Aug 08 10:22:50 PDT 2012                     _cpunittest.log
        0   Wed Aug 08 10:22:50 PDT 2012                _cpunittestError.log
   537262   Fri Aug 10 09:06:57 PDT 2012                       _cploader.log
   110899   Fri Aug 10 09:06:43 PDT 2012                  _cpperformance.log
        0   Wed Aug 08 10:22:50 PDT 2012                       _cplegacy.log
        0   Wed Aug 08 10:22:50 PDT 2012                          _cpxdm.log
        0   Wed Aug 08 10:22:50 PDT 2012                         _cptest.log
        0   Wed Aug 08 10:22:50 PDT 2012                          _cpapp.log
        0   Wed Aug 08 10:22:50 PDT 2012                           _cpui.log
        0   Wed Aug 08 10:22:50 PDT 2012                _cpuiperformance.log
        0   Wed Aug 08 10:22:50 PDT 2012                     _cpuinotify.log
   123693   Fri Aug 10 09:06:56 PDT 2012                    _cphibernate.log
   404019   Fri Aug 10 09:07:49 PDT 2012                     _cpcommands.log
  1047488   Thu Aug 09 06:07:44 PDT 2012                     atrace_save.log
```

Log Commands in Configuration Mode

- **log console errors**—Displays error messages (severity=3)
- **log console info**—Displays information messages (severity=6)
- **log console notice**—Displays notices (severity=5)
- **log console warning**—Displays warning messages (severity=4)
- **log server address** *a.b.c.d*

log trace

- **log trace local enable**
- **log trace server enable**
- **log trace server url** *ftp-url*

Log Commands in EXEC Mode

- **log console monitor**
- **log trace boot**
- **log trace buffer save**

Saving and Viewing Log Files

Problem You must be able to save log files to a remote location.

Recommended Action Log files are saved to a disk by default. You can configure Cisco Unified SRST Manager to store the log files on a separate server by using the **log server address** command. Also, you can copy log files on the disk to a separate server if they need to be kept for history purposes, for example:

```
copy log filename.log url ftp://ftp-user-id:ftp-user-passwd@ftp-ip-address/directory
```

```
srstmgr# copy log messages.log url ftp://admin:messaging@172.168.0.5/log_history
```

Problem You cannot display the contents of the log files.

Recommended Action Copy the log files from Cisco Unified SRST Manager to an external server and use a text editor, such as **vi**, to display the content.

Using Trace Commands

To troubleshoot network configuration in Cisco Unified SRST Manager, use the **trace** command in EXEC mode. For a detailed list of all the arguments associated with the trace command, see trace.

PART 5

CLI Reference Information

How to Use the Cisco Unified SRST Manager CLI

This chapter provides helpful tips for understanding and configuring the Cisco Unified SRST Manager software using the CLI.

About the Cisco Unified SRST Manager CLI

The Cisco Unified SRST Manager command line interface (CLI) provides additional administrative functionality beyond the GUI. Access the CLI using a secure shell (ssh) client.

Cisco Unified SRST Manager CLI commands have a structure similar to that of Cisco IOS CLI commands. For both interfaces, standard Cisco IOS navigation and command-completion conventions apply. For example, **?** lists options, **TAB** completes a command, and **|** directs **show** command output.

The following are differences between the Cisco Unified SRST Manager CLI and the Cisco IOS CLI:

- Standard command names and options do *not* necessarily apply. A notable example is the command for accessing global configuration mode: the Cisco IOS command is **configure terminal**; the network module command is **config terminal** or **config t**.
- Cisco Unified SRST Manager employs a last-one-wins rule. For example, if two users both try to set the IP address for the same entity at the same time, the system starts and completes one operation before it starts the next. The last IP address set is the final result.
- The Cisco Unified SRST Manager command modes, EXEC and configuration operate similarly to the EXEC and configuration modes in the Cisco IOS CLI.
- After you enter configuration mode, all the CLI commands can be used in the **no** form. Example:

  no hostname <*hostname*>

  This command deletes the configured hostname.

Understanding Command Modes

The Cisco Unified SRST Manager command environment is divided into two basic modes:

- EXEC—This is the mode that you are in after you log in to the Cisco Unified SRST Manager command environment. Some Cisco Unified SRST Manager EXEC commands only display or clear parameter values, stop or start the entire system, or start troubleshooting procedures. However, unlike Cisco IOS EXEC mode, Cisco Unified SRST Manager EXEC mode has a few commands that change parameter values.
- Configuration—This mode enables you to make system configuration changes, which are stored in the running configuration. If you later save the running configuration to the startup configuration, the changes made with the configuration commands are restored when you reboot the software.

  Cisco Unified SRST Manager configuration mode has various subconfiguration levels. The global configuration mode changes the command environment from EXEC to configuration. You can modify many software parameters at this level. However, certain configuration commands change the environment to more specific configuration modes where modifications to the system are entered. For example, the **interface ethernet 0** command changes the environment from config to config-interface. At this point, you can enter or modify interface parameter values.

The commands available to you at any given time depend on the current mode. Entering a question mark (**?**) at the CLI prompt displays a list of commands available for each command mode. The descriptions in this command reference indicate each command's environment mode.

Table 15 describes how to access and exit various common command modes of the Cisco Unified SRST Manager software. It also shows examples of the prompts displayed for each mode.

Table 15 Accessing and Exiting Command Modes

Command Mode	Release	Access Method	Prompt	Exit Method

EXEC	9.0 and later	When the prompt appears, you can enter the **enable** command, but it is not necessary.	**`with enable:`**
			`srstmgr#`
			`without enable:`
			`srstmgr>`
				Press **CTRL-SHIFT-6** and then enter **x**.

configuration	9.0 and later	From EXEC mode, use the **configure terminal** command.	`srstmgr(config)#`	To return to EXEC mode from configuration mode, use the **end** or **exit** command.
AAA accounting	8.0 and later	From configuration mode, use the **aaa accounting server remote** command.	`srstmgr-1(aaa-accounting)#`	To return to configuration mode, use the **end** or **exit** command.
AAA accounting event	8.0 and later	From configuration mode, use the **aaa accounting event** command.	`srstmgr-1(aaa-accounting-event)#`	To return to configuration mode, use the **end** or **exit** command.
AAA accounting policy	8.0 and later	From configuration mode, use the **aaa policy** command.	`srstmgr-1(aaa-policy)#`	To return to configuration mode, use the **end** or **exit** command.

Table 15 Accessing and Exiting Command Modes (continued)

Command Mode	Release	Access Method	Prompt	Exit Method
backup schedule	9.0 and later	From EXEC mode, use the **backup schedule** command.	`srstmgr(backup-schedule)#`	To return to EXEC mode, use the **end** or **exit** command.
kron-schedule	9.0 and later	From EXEC mode, use the **kron schedule** command.	`srstmgr(kron-schedule)#`	To return to EXEC mode, use the **end** or **exit** command.

Entering the Command Environment

After you install Cisco Unified SRST Manager and establish IP connectivity with it, use this procedure to enter the command environment.

Note This procedure describes how to enter the Cisco Unified SRST Manager command environment remotely. From the server hosting the Cisco Unified SRST Manager VM, it is possible to enter the command environment by opening a console window for the VM within the vSphere client. When using this method, the IP address, username, and password are not required.

- Prerequisites, page 143
- Summary Steps, page 143
- Detailed Steps, page 144

Prerequisites

The following information is required to enter the command environment:

- IP address of the Cisco Unified SRST Manager VM
- Username and password to log in to Cisco Unified SRST Manager

Summary Steps

1. Connect to Cisco Unified SRST Manager using ssh:

   ssh *username@IP_address*

2. When prompted, enter the Cisco Unified SRST Manager password.

Detailed Steps

	Command or Action	Purpose

Step 1	Connect to Cisco Unified SRST Manager using ssh:
	`ssh` *`username`*`@`*`IP_address`*
	Example:
	`C:\> ssh admin@10.0.0.0`
		Use a secure shell client to connect.
		username—User name for Cisco Unified SRST Manager
		IP_address—IP address of the Cisco Unified SRST Manager VM

Step 2	When prompted, enter the Cisco Unified SRST Manager password.
	Example:
	`Password:`
	`se-10-0-0-0#`
		After entering the password, Cisco Unified SRST Manager displays the command prompt.

Exiting the Command Environment

To leave the Cisco Unified SRST Manager command environment, in EXEC mode enter the **exit** command once to exit EXEC mode, and again to exit the application.

The following example illustrates the exit procedure:

```
se-10-0-0-0# exit
```

Getting Help

Entering a question mark (**?**) at the CLI prompt displays a list of commands available for each command mode. You can also get a list of keywords and arguments associated with any command by using the context-sensitive help feature.

To get help specific to a command mode, a command, a keyword, or an argument, use one of the following commands:

Command	Purpose
`help`	Provides a brief description of the help system in any command mode.
*`abbreviated-command-entry`***`?`**	Provides a list of commands that begin with a particular character string. (No space between command and question mark.)
`abbreviated-command-entry``<`**`Tab`**`>`	Completes a partial command name.
`?`	Lists all commands available for a particular command mode.
`command` **`?`**	Lists the keywords or arguments that you must enter next on the command line. (Space between command and question mark.)

Using the no and default Forms of Commands

Where available, use the **no** form of a command to disable a function. Use the command without the **no** keyword to reenable a disabled function or to enable a function that is disabled by default. The command reference entry for each command provides the complete syntax for the configuration commands and describes what the **no** form of a command does.

Configuration commands can also have a **default** form, which returns the command settings to the default values. In those cases where a command is disabled by default, using the **default** form has the same result as using the **no** form of the command. However, some commands are enabled by default and have variables set to certain default values. In these cases, the **default** form of the command enables the command and sets the variables to their default values. Where available, the command reference entry describes the effect of the **default** form of a command if the command does not function the same way as the **no** form.

Saving Configuration Changes

Starting in EXEC mode, use the following command to copy the running configuration in flash memory to another location:

copy running-config {**ftp:***user-id***:***password*@*ftp-server-address*[*/directory*] |
startup-config | **tftp:***tftp-server-address*} *filename*

Keyword or Argument	Description
ftp:*user-id***:***password*@	Username and password for the FTP server. Include the colon (:) and the at sign (@) in your entry.
ftp-server-address	IP address of the FTP server.
/directory	(Optional) Directory on the FTP server where the copied file will reside. If you use it, precede the name with the forward slash (/).
startup-config	Startup configuration in flash memory.
tftp:*tftp-server-address*	IP address of the TFTP server.
filename	Name of the destination file that will contain the copied running configuration.

When you copy the running configuration to the startup configuration, enter the command on one line. In the following example, the running configuration is copied to the startup configuration as a file start. In this instance, enter the command on a single line.

```
srstmgr-1# copy running-config startup-config
```

When you copy to the FTP or TFTP server, this command becomes interactive and prompts you for the information. You cannot enter the parameters on one line. The following example illustrates this process. In the following example, the running configuration is copied to the FTP server, which requires a username and password. The IP address of the FTP server is 192.0.2.24. The running configuration is copied to the configs directory as file saved_start.

```
srstmgr-1# copy running-config ftp:
Address or name of remote host? admin:voice@192.0.2.24/configs
Source filename? saved_start
```

Troubleshooting Configuration Changes

Problem You lost some configuration data.

Recommended Action Copy your changes to the running configuration at frequent intervals. See the "Copying Configurations" section on page 93.

Problem You lost configuration data when you rebooted the system.

Explanation You did not save the data before the reboot.

Recommended Action Issue a **copy running-config startup-config** command to copy your changes from the running configuration to the startup configuration. When Cisco Unified SRST Manager reboots, it reloads the startup configuration.

Note All configuration changes require an explicit "save configuration" operation to preserve them in the startup configuration.

Scheduling CLI Commands

Cisco Unified SRST Manager enables you to schedule the execution of a block of CLI commands. Blocks of commands are entered interactively, using a symbol delimiter character to start and stop the execution. The execution of the block of commands begins in EXEC mode, but mode-changing commands are allowed in the command block.

The following limitations apply in Cisco Unified SRST Manager Release 11.0:

- The maximum size of the block of commands is 1024 characters, including new lines.
- Commands in the block cannot use the comma "," character or the delimiter character. For example, if the delimiter character is configured to be "#", that character cannot be used in the command blocks.
- Only system administrators can schedule the execution of blocks of commands.
- CLI commands are executed under system super-user privileges.
- Notification for the execution of these command blocks is not available. Error messages and results are available in log files only.

Caution Use caution when scheduling CLI commands. Interactive commands will cause the execution to hang. Some commands might cause system instability.

SUMMARY STEPS

1. **kron schedule** [*name*]
2. **description**
3. **repeat every {***number* **days at** *time* |*number* **weeks on** *day* | *number* **months on day** *date* | *number* **years on month** *month***} at** *time*

Note Instead of the **repeat every** command, you can optionally use one of the following commands:

- **repeat once at** *time*
- **repeat daily at** *time*
- **repeat monthly on day** *date* **at** *time*
- **repeat weekly on** *day* **at** *time*
- **repeat yearly on month** *month* **at** *time*

4. **start-date** *date*
5. **stop-date** *date*
6. **commands** *delimiter*
7. **exit**
8. **show kron schedules**
9. **show kron schedule detail job**

DETAILED STEPS

	Command or Action	Purpose

Step 1	`kron schedule [name]`
	Example:
	`srstmgr-1# kron schedule kron1011`
		Enters kron schedule configuration mode.

Step 2	`description description`
	Example:
	`srstmgr-1(kron-schedule)# description backup`
		(Optional) Enters a description for the scheduled kron job.

Step 3	`repeat every {number days |number weeks on day | number months on day date | number years on month month} at time time`
	Example:
	`srstmgr-1(kron-schedule)# repeat every 2 days at time 10:00`
		Specifies how often a recurring scheduled kron job occurs. To configure a one-time kron job, use the **repeat once** command. You can also optionally use one of the other **repeat** commands listed in the previous note.

Step 4	`start-date date`
	Example:
	`srstmgr-1(kron-schedule)# start-date 08/30/2012`
		Specifies the start date for the recurring scheduled kron job to occur.

Step 5	`stop-date date`
	Example:
	`srstmgr-1(kron-schedule)# stop-date 11/20/2012`
		Specifies the stop date for the recurring scheduled kron job to occur.

	Command or Action	Purpose

Step 6	**`commands`** *`delimiter`*
	Example:
	`srstmgr-1(kron-schedule)# commands %`
	`Enter CLI commands to be executed. End with the character ‘%’. Maximum size is 1024 characters, it may not contain symbol %.`
	`%show version`
	`show running-config`
	`config t`
	`hostname aaa`
	`%`
	`srstmgr-1(kron-schedule)#`
		Enters an interactive mode where commands in the the command block can be entered for the scheduled kron job. Use the delimiter character to delimit the command block.
		Note Any symbol can be a delimiter. The “%” symbol is shown for example purposes only.

Step 7	**`exit`**	Exits kron schedule configuration mode.

Step 8	**`show kron schedules`**
	Example:
	`srstmgr-1# show kron schedule`
		Displays a list of scheduled kron jobs.

Step 9	**`show kron schedule detail job`** *`name`*
	Example:
	`srstmgr-1# show kron schedule detail job kron1011`
		Displays information about a specific scheduled kron job.

Examples

The following is sample output from the **show kron schedules** command:

```
srstmgr-1# show kron schedules
Name          Schedule                          Commands
krj1          Every 1 days at 12:34             show ver,sh run,conf t,host...
Total: 1
```

The following is sample output from the **show kron schedule detail job** command:

```
srstmgr-1# show kron schedule detail job krj1
Job Name        krj1
Description
Schedule        NOT SET
Last Run        NEVER
Last Result
Next Run        NEVER
Active          from Feb 15, 2010 until INDEFINITE
Disabled
CLI Commands
                show ver
                sh run
                conf t
                hostname aaa
srstmgr-1#
```

C

Note For information about other CLI commands that are not listed in this document, see the *Cisco Unity Express Command Reference for 3.0 and Later Versions.*

clear counters interfaces

To clear interface counters, use the **clear counters interfaces** command in EXEC mode.

clear counters interfaces

Syntax Description

This command has no arguments or keywords.

Command Default

None. Interface counters are not cleared.

Command Modes

EXEC

Command History

Version	Modification
9.0	This command was introduced.

Usage Guidelines

Use this command when you have interface counters you want to clear, for example, the general debug counters. This command clears all counters, including statistics counters.

Examples

The following example illustrates the use of the **clear counters interfaces** command.

```
srstmgr-1> enable
srstmgr-1# clear counters interfaces
srstmgr-1# show interfaces ide 0
IDE hd0 is up, line protocol is up
     0 reads, 0 bytes
     0 read errors
     0 write, 0 bytes
     0 write errors
srstmgr-1#
```

Related Commands

Command	Description
clear crashbuffer	Clears the kernel crash buffer.

clear crashbuffer

To clear the kernel crash buffer, use the **clear crashbuffer** command in EXEC mode.

clear crashbuffer

Syntax Description

This command has no arguments or keywords.

Command Default

None. Crash buffer is not cleared.

Command Modes

EXEC

Command History

Version	Modification
9.0	This command was introduced.

Usage Guidelines

Use this command to clear the kernel crash buffer after the reasons for a crash are fully investigated.

Examples

The following example illustrates the use of the **clear crashbuffer** command.

```
srstmgr-1 enable>
srstmgr-1# clear crashbuffer
srstmgr-1#
```

Related Commands

Command	Description
clear counters interfaces	Clears the interface counters.

copy url

To add support for new phone types to Cisco Unified SRST Manager, use the **copy url** command in EXEC mode to upload the phonetype.jar file containing updated information for supported phone types.

copy url [*ftp_sitename*]/[*directory_path*]/[*file_name*] **phone-config username** [*username*] **password** [*password*]

no copy url

Syntax Description

ftp_sitename	Name of the ftp site containing the JAR file.
directory_path	Path to the file on the ftp site.
file_name	Name of the JAR file on the ftp site.
username	User name of ftp site account.
password	Password for the ftp site account.

Command Default

None.

Command Modes

EXEC

Command History

Version	Modification
9.0	This command was introduced.

Usage Guidelines

Use this command to upload phonetype.jar, a Java archive (JAR) file containing updated information for phone types supported by Cisco Unified SRST Manager. The updated JAR file can include new phone types to add to Cisco Unified SRST Manager.

JAR File Contents

The uploaded phonetype.jar file must contain the following files:

usr/bin/products/umg/CusmPhoneModels.xml

usr/ccp/classes/PhoneModels.xml

META-INF/MANIFEST.MF

Examples

The following example illustrates the use of the **copy url** command.

```
srstmgr-1# copy url ftp://192.1.1.2/tmpdir/phonetype.jar phone-config username johndoe
password mypassword
```

S

Note For information about other CLI commands that are not listed in this document, see *Cisco Unity Express Command Reference for 3.0 and Later Versions.*

show clock

To display clock statistics, use the **show clock** command in EXEC mode.

show clock

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Version	Modification
9.0	This command was introduced.

Usage Guidelines

Cisco Unified SRST Manager uses the Network Time Protocol (NTP) server for clocking functions. Use the **show clock** command to display the Cisco Unified SRST Manager clock status.

Examples

The following is sample output for the **show clock** command:

```
srstmgr-1# show clock

19:20:33.724 PST Wed Mar 17 1993
time zone:                                America/Los_Angeles
clock state:                              unsync
delta from reference (microsec):          0
estimated error (microsec):               175431
time resolution (microsec):               1
clock interrupt period (microsec):        10000
time of day (sec):                        732424833
time of day (microsec):                   760817
```

Table 16 describes the significant fields shown in the display.

Table 16 show clock Field Descriptions

Field	Description
time zone	Current time zone setting.
clock state	Synchronization state of the clock.
delta from reference (ms)	Difference between the module clock and the NTP reference clock.
time of day (sec)	Current time of day in seconds.
time of day (ms)	Current time of day in microseconds.

Related Commands

Command	Description
ntp server	Specifies the NTP server for Cisco Unified SRST Manager.
show ntp	Displays the time source for an NTP server.

show configuration

To display the contents of the non-volatile memory, use the **show configuration** command in EXEC mode.

show configuration

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Version	Modification
9.0	This command was introduced.

Usage Guidelines

Use this command for troubleshooting.

Examples

The following is sample output for the **show configuration** command:

```
se-1-100-100-100# show configuration
!
! This adds all the platform CLI commands
!

! host name
hostname se-1-100-100-100

! domain name
ip domain-name localdomain

! DNS Servers
ip name-server 1.100.100.100

! Timezone Settings
clock timezone America/Los_Angeles

! NTP Servers
!VAR_NTP_SERVER

! INTERFACE_F0
interface Ethernet 0
 ip address 1.100.100.100 255.255.0.0
 end interface


! DEFAULT GATEWAY
ip default-gateway 1.100.100.100

End
```

Related Commands

Command	Description
backup category	Specifies the type of data to be backed up and initiates the backup process.
hostname	Specifies the hostname of the current messaging gateway.
ip domain-name	Specifies the local messaging gateway's domain name and/or domain name server.
restore factory default	Restores factory default settings.

show interfaces

To display the IP configuration and statistics for the Ethernet interface, use the **show interfaces** command in privileged EXEC mode.

show interfaces

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Version	Modification
9.0	This command was introduced.

Examples

The following is sample output for the **show interfaces** command:

```
se-192-100-1-1# show interfaces
Ethernet 0 is up, line protocol is up
  Internet address is 192.100.1.1 mask 255.255.255.0 (configured locally)
     5188306 packets input, 0 bytes
     25113 input errors, 0 dropped, 0 overrun, 0 frame errors
     10791446 packets output, 0 bytes
     20301 output errors, 0 dropped, 0 overrun, 0 collision errors
     0 output carrier detect errors
```

Related Commands

Command	Description
ip name-server	Specifies the domain name server.

show ip dns cache

To display the DNS cache, use the **show ip dns cache** command in EXEC mode.

show ip dns cache

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Version	Modification
9.0	This command was introduced.

Examples

The following is sample output for the **show ip dns cache** command:

```
srstmgr-1> show ip dns cache


srstmgr-1.unspecified.       2147483647 IN A         192.0.2.24
localhost.\(none\).      2147483647 IN A         192.0.2.23
192.0.2.22.in-addr.arpa. 2147483647 IN PTR               localhost.
stress-umg1-192.0.2.24.example.com.  2147483647 IN A     192.0.2.24
192.0.2.24.in-addr.arpa.             2147483647 IN PTR   192.0.2.24.te
mp.com.
se-192.0.2.24.localdomain.      2147483647 IN A          192.0.2.24
sundial1-umg-se-192.0.2.24.localdomain. 2147483647 IN A         10.1.12.95
localhost.temp.com.     2147483647 IN A         192.0.2.18
192.0.2.24.temp.com.    2147483647 IN A         192.0.2.24
192.0.2.24.\(none\).    2147483647 IN A         192.0.2.24
stress-umg1-192.0.2.24.example.com.    2147483647 IN A       192.0.2.24
localhost.                             2147483647 IN A       192.0.2.20
stress-umg1-192.0.2.22.\(none\).       2147483647 IN A       192.0.2.24
se-192.0.2.24.example.com.             2147483647 IN A       192.0.2.24
localhost.cisco.com.                   2147483647 IN A       192.0.2.23


se-10-1-12-95>
```

Related Commands

Command	Description
hostname	Specifies the hostname for the current configuring Cisco Unified SRST Manager.
ip name-server	Specifies the domain name server.
ntp server	Specifies the NTP clocking server.
show hosts	Displays all configured hosts.

show license status

To display the license agreement, use the **show license status** command in EXEC mode.

show license status

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Version	Modification
9.0	This command was introduced.

Examples

The following is sample output for the **show license status** command:

```
se-1-100-80-203# show license status

LICENSE AGREEMENT
            =================
PLEASE  READ THE  FOLLOWING TERMS  CAREFULLY. INSTALLING THE LICENSE OR
LICENSE  KEY  PROVIDED FOR  ANY CISCO  PRODUCT  FEATURE  OR  USING SUCH
PRODUCT  FEATURE  CONSTITUTES  YOUR  FULL ACCEPTANCE  OF  THE FOLLOWING
TERMS. YOU MUST NOT PROCEED FURTHER IF YOU ARE NOT WILLING TO  BE BOUND
BOUND BY ALL THE TERMS SET FORTH HEREIN.

You hereby  acknowledge  and  agree that  the  product feature  license
is terminable and that the product  feature  enabled  by  such  license
may  be  shut  down or  terminated by  Cisco  after  expiration of  the
applicable  term  of  the license  (e.g., 30-day  trial  period). Cisco
reserves the  right to terminate or shut down  any such product feature
electronically  or by  any other  means available. While alerts or such
messages  may  be provided, it is  your sole  responsibility to monitor
your terminable  usage of any  product  feature enabled by  the license
and to ensure that your systems and  networks are prepared for the shut
down of the product feature. You acknowledge  and agree that Cisco will
not have any liability  whatsoever for  any damages, including, but not
limited to, direct, indirect, special, or consequential damages related
to any product  feature  being shutdown or terminated.
```

show log name

To display logging data, use the **show log name** command in EXEC mode.

show log name *word* [**containing** *expression* | **paged** | **tail**]

Syntax Description

word	The name of the log file to display. Use the **show logs** command to display a list of available log files.
containing *expression*	Only displays events that match a search expression.
paged	Displays in paged mode.
tail	Displays the latest events as they occur.

Command Modes

EXEC

Command History

Version	Modification
9.0	This command was introduced.

Usage Guidelines

This command has the following filtering options:

- **show begin**: Begins the output of any **show** command from a specified string.
- **show exclude**: Filters **show** command output so that it excludes lines that contain a particular regular expression.
- **show include**: Filters **show** command output so that it displays only lines that contain a particular regular expression.

Examples

The following partial output for the **show log name** command displays the dmesg log:

```
srstmgr-1# show log name dmesg

Press <CTRL-C> to exit...
Linux version 2.4.24 (bld_adm@bld-system) (gcc version 2.95.3 20010315 (version4
Platform: nm
setup.c: handling flash window at [15MB..16MB]
setup.c: handling kernel log buf at [245.5MB]
setup.c: handling trace buf at [246MB]
BIOS-provided physical RAM map:
 BIOS-e820: 0000000000000000 - 000000000009f400 (usable)
 BIOS-e820: 000000000009f400 - 00000000000a0000 (reserved)
 BIOS-e820: 00000000000e0800 - 0000000000100000 (reserved)
 BIOS-e820: 0000000000100000 - 0000000000f00000 (usable)
 BIOS-e820: 0000000000f00000 - 0000000001000000 (reserved)
 BIOS-e820: 0000000001000000 - 000000000f580000 (usable)
 BIOS-e820: 000000000f580000 - 000000000f600000 (reserved)
 BIOS-e820: 000000000f600000 - 0000000010000000 (reserved)
 BIOS-e820: 00000000fff00000 - 0000000100000000 (reserved)
245MB LOWMEM available.
On node 0 totalpages: 62848
```

```
zone(0): 4096 pages.
zone(1): 58752 pages.
zone(2): 0 pages.
DMI not present.
Kernel command line: root=/dev/hda1 ro plat=nm
Initializing CPU#0
Detected 498.674 MHz processor.
Calibrating delay loop... 996.14 BogoMIPS
Memory: 245128k/251392k available (1164k kernel code, 4852k reserved, 667k data)
kdb version 4.3 by Keith Owens, Scott Lurndal. Copyright SGI, All Rights Reservd
in atrace_init
log_head: h: 0, t: 8429274, l: 0, w: 0, s: 10484672
Using existing trace log
log_head: h: 0, t: 8429274, l: 0, w: 0, s: 10484672
Dentry cache hash table entries: 32768 (order: 6, 262144 bytes)
Inode cache hash table entries: 16384 (order: 5, 131072 bytes)
Mount cache hash table entries: 512 (order: 0, 4096 bytes)
Buffer cache hash table entries: 16384 (order: 4, 65536 bytes)
Page-cache hash table entries: 65536 (order: 6, 262144 bytes)
CPU: L1 I cache: 16K, L1 D cache: 16K
CPU: L2 cache: 256K
CPU serial number disabled.
```

The following sample output for the **show log** command displays the dmesg log using a search string:

```
srstmgr-1# show log name dmesg containing setup

Press <CTRL-C> to exit...
setup.c: handling flash window at [15MB..16MB]
setup.c: handling kernel log buf at [245.5MB]
setup.c: handling trace buf at [246MB]
srstmgr-1#
```

The following partial output for the **show log** command displays the dmesg log in paged mode:

```
srstmgr-1# show log name dmesg paged

Linux version 2.4.24 (bld_adm@bld-system) (gcc version 2.95.3 20010315 (version
)) #1 Tue Nov 30 23:07:21 PST 2007
Platform: nm
setup.c: handling flash window at [15MB..16MB]
setup.c: handling kernel log buf at [245.5MB]
setup.c: handling trace buf at [246MB]
BIOS-provided physical RAM map:
 BIOS-e820: 0000000000000000 - 000000000009f400 (usable)
 BIOS-e820: 000000000009f400 - 00000000000a0000 (reserved)
 BIOS-e820: 00000000000e0800 - 0000000000100000 (reserved)
 BIOS-e820: 0000000000100000 - 0000000000f00000 (usable)
 BIOS-e820: 0000000000f00000 - 0000000001000000 (reserved)
 BIOS-e820: 0000000001000000 - 000000000f580000 (usable)
 BIOS-e820: 000000000f580000 - 000000000f600000 (reserved)
 BIOS-e820: 000000000f600000 - 0000000010000000 (reserved)
 BIOS-e820: 00000000fff00000 - 0000000100000000 (reserved)
245MB LOWMEM available.
On node 0 totalpages: 62848
zone(0): 4096 pages.
zone(1): 58752 pages.
zone(2): 0 pages.
DMI not present.
Kernel command line: root=/dev/hda1 ro plat=nm
Initializing CPU#0
 -- More --
```

The following output for the **show log name** command displays the current dmesg log as events are being entered:

```
srstmgr-1# show log name dmesg tail

Press <CTRL-C> to exit...
Freeing unused kernel memory: 88k freed
```

The following partial output for the **show log name** command displays the dmesg log beginning with the first line starting with ide0:

```
srstmgr-1# show log name dmesg | begin ide0

    ide0: BM-DMA at 0xfc00-0xfc07, BIOS settings: hda:pio, hdb:pio
    ide1: BM-DMA at 0xfc08-0xfc0f, BIOS settings: hdc:pio, hdd:pio
hda: C/H/S=50127/232/176 from BIOS ignored
hdb: C/H/S=0/0/0 from BIOS ignored
hda: IC25N020ATMR04-0, ATA DISK drive
blk: queue c030c160, I/O limit 4095Mb (mask 0xffffffff)
ide0 at 0x1f0-0x1f7,0x3f6 on irq 14
hda: attached ide-disk driver.
hda: host protected area => 1
hda: 39070080 sectors (20004 MB) w/1740KiB Cache, CHS=2432/255/63, UDMA(33)
init unit number == 0
```

Related Commands.

Command	Description
log console	Configures the types of messages to be displayed on the console.
log console monitor	Displays system messages on the console.
log server address	Specifies an external server for saving log messages.
log trace boot	Saves the trace configuration on rebooting.
log trace buffer save	Saves the current trace information.
show logging	Shows the types of messages that are displayed on the console.
show logs	Displays the list of available logs.

show ntp

To display the time source for a Network Time Protocol (NTP) server, use the **show ntp** command in EXEC mode.

show ntp [**detail**]

Syntax Description

detail	Displays detailed information about the NTP servers.

Command Modes

EXEC

Command History

Version	Modification
9.0	This command was introduced.

Usage Guidelines

This command displays the chain of NTP servers back to their primary time source, starting from the local host.

Examples

The following is sample output for the **show ntp** command:

```
srstmgr-1# show ntp

192.0.2.24: stratum 9, offset 0.000015, synch distance 0.03047
192.0.2.23: stratum 8, offset -0.001124, synch distance 0.00003
```

Table 17 describes the significant fields shown in the display.

Table 17 show ntp Field Descriptions

Field	Description
(first field)	IP address of the host.
stratum	Server hop count to the primary clock source. Valid values are: • 0—Unspecified • 1—Primary clock reference • 2–255—Secondary reference via NTP
offset	Time offset between the host and the local host, in seconds.
synch distance	Host synchronization distance, which is the estimated error relative to the primary source.

The following is sample output for the **show ntp detail** command:

```
srstmgr-1# show ntp detail

server 192.0.2.24, port 123
```

```
stratum 9, precision -17, leap 00
refid [192.0.2.22] delay 0.00012, dispersion 0.00000 offset 0.000011
rootdelay 0.00058, rootdispersion 0.03111, synch dist 0.03140
reference time:      af4a3ff7.926698bb  Thu, Mar 11 1993 14:47:19.571
originate timestamp: af4a4041.bf991bc5  Thu, Mar 11 1993 14:48:33.748
transmit timestamp:  af4a4041.bf90a782  Thu, Mar 11 1993 14:48:33.748

server 192.0.2.23, port 123
stratum 8, precision -18, leap 00
refid [192.0.2.21] delay 0.00024, dispersion 0.00000 offset -0.001130
rootdelay 0.00000, rootdispersion 0.00003, synch dist 0.00003
reference time:      af4a402e.f46eaea6  Thu, Mar 11 1993 14:48:14.954
originate timestamp: af4a4041.bf6fb4d4  Thu, Mar 11 1993 14:48:33.747
transmit timestamp:  af4a4041.bfb0d51f  Thu, Mar 11 1993 14:48:33.748
```

Table 18 describes the significant fields shown in the display.

Table 18 show ntp detail Field Descriptions

Field	Description
server	IP address of the host server.
port	Port number of the host server.
stratum	Server hop count to the primary clock source. Valid values are: • 0—Unspecified • 1—Primary clock reference • 2–255—Secondary reference via NTP
precision	Precision of the clock, in seconds to the power of two.
leap	Two-bit code warning of an impending leap second to be inserted in the NTP time scale. Valid values are: • 00—No warning • 01—Last minute was 61 seconds • 10—Last minute was 59 seconds • 11—Alarm condition (clock not synchronized)
refid	IP address of the peer selected for synchronization.
delay	Round-trip delay of the packet, in milliseconds.
dispersion	Measure, in milliseconds, of how scattered the time offsets have been from a given time server.
offset	Time offset between the host and the local host, in seconds.
rootdelay	Total round-trip delay, in seconds, to the primary reference source at the root of the synchronization subnet.
rootdispersion	Maximum error, in seconds, relative to the primary reference source at the root of the synchronization subnet.
synch dist	Host synchronization distance, which is the estimated error relative to the primary source.
reference time	Local time, in time-stamp format, when the local clock was last updated. If the local clock has never been synchronized, the value is zero.

Table 18 show ntp detail Field Descriptions (continued)

Field	Description
originate timestamp	Local time, in time-stamp format, at the peer when its latest NTP message was sent. If the peer becomes unreachable, the value is zero.
transmit timestamp	Local time, in time-stamp format, when the latest NTP message from the peer arrived. If the peer becomes unreachable, the value is zero.

Related Commands

Command	Description
ntp server	Configures the Network Time Protocol (NTP) server to keep the system time synchronized with the NTP server.
show clock	Displays clock statistics.

show srsx central-call-agent

To display the list of configured Cisco Unified Communications Manager systems or details for the specified Cisco Unified Communications Manager system, use the **show srsx central-call-agent** command.

show srsx central-call-agent [*hostname* [**srst-references** | **nodes**]]

Syntax Description

hostname	Hostname of a specific Cisco Unified Communications Manager system.
srst-references	Displays the Cisco Unified SRST references for the specified Cisco Unified Communications Manager system.
nodes	Displays all the nodes discovered for the Cisco Unified Communications Manager system.

Command Modes

EXEC mode

Command History

Version	Modification
9.0	This command was introduced.

Usage Guidelines

This information is also available in the Cisco Unified SRST Manager graphical user interface, which we recommend that you use as the primary administrative interface.

Examples

The following is an example of the **show srsx central-call-agent** command:

```
srstmgr-1# show srsx central-call-agent
Name |Provisioning|SRST-References
__________________________________
CUCM8|enabled     |7
```

The following is an example of the **show srsx central-call-agent** command with a central call agent specified:

```
srstmgr-1# show srsx central-call-agent CUCM8

Name:                         CUCM8
AXL Username:                 Administrator
AXL Password:                 *******
AXL Pacing:                   0 (milliseconds)
Provisioning Schedule:        Every day at 12:00 am
Default Voicemail:            CUC 8.5
Provisioning:                 enabled
Site Provision Enable Default:enabled
Primary Node:                 CentralCA.srst.bxb.lab
Secondary Node:               CentralCA2.srst.bxb.lab
```

The following is an example of the **show srsx central-call-agent** command with a central call agent specified and asking for a list of the Cisco Unified SRST references:

```
srstmgr-1# show srsx central-call-agent ccm ccm.cisco.com srst-references
```

```
SRST-references           |IP Address
________________________________________
branch-bos-srst           |192.168.1.2
branch-nyc-srst           |192.168.1.4
branch-sj-srst            |192.168.1.5
```

The following is an example of the **show srsx central-call-agent** command with a central call agent specified and asking for a list of the nodes discovered for the central call agent:

```
srstmgr-1# show srsx central-call-agent CUCM8 nodes

Nodes
________________________________________
CentralCA.srsv.bxb.lab
CentralCA2.srsv.bxb.lab
```

Related Commands

Command	Description
show srsx site	Displays the sites on the Cisco Unified SRST system.

show srsx provisioning-history

To display the provisioning history for all sites, use the **show srsx provisioning-history** command.

show srsx provisioning-history

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC mode

Command History

Version	Modification
9.0	This command was introduced.

Usage Guidelines

This information is also available in the Cisco Unified SRST Manager graphical user interface, which we recommend that you use as the primary administrative interface.

Examples

The following is an example of the **show srsx provisioning-history** command in Cisco Unified SRST Manager 9.0:

```
srstmgr-1# show srsx provisioning-history

Site           |Last Result|Date                 |Last Success         |Users Provisioned
_________________________________________________________________________________________
branch-bos-srst|Success    |Mon, Mar 22, 09:24 AM|Mon, Mar 22, 09:24 AM|21
branch-nyc-srst|unknown    |                     |                     |0
branch-sj-srst |unknown    |                     |                     |0
```

The following is an example of the **show srsx provisioning-history** command in Cisco Unified SRST Manager 9.0:

```
srstmgr-1# show srsx provisioning-history

Site           |Last Result|Date                 |Last Success         |Users Provisioned
_________________________________________________________________________________________
branch-bos-srst|Success    |Mon, Mar 22, 09:24 AM|Mon, Mar 22, 09:24 AM|21
branch-nyc-srst|unknown    |                     |                     |0
branch-sj-srst |unknown    |                     |                     |0
```

Related Commands

Command	Description
show srsx central-call-agent	Displays the central call agents available on the Cisco Unified SRST system.
show srsx site	Displays the sites on the Cisco Unified SRST system.

show srsx site

To display the list of sites managed by the Cisco Unified SRST Manager or to see details for the specified site, use the **show srsx site** command.

show srsx site [*sitename*]

Syntax Description

sitename	Name of a specific site.

Command Modes

EXEC mode

Command History

Version	Modification
9.0	This command was introduced.

Usage Guidelines

This information is also available in the Cisco Unified SRST Manager graphical user interface, which we recommend that you use as the primary administrative interface.

Examples

The following is an example of the **show srsx site** command:

```
srstmgr-1# show srsx site

Site    |Provisioning|Call Agent  |SRST            |SRST
------------------------------------------------------------------------------------------
srst1   |enabled      |CUCM8      |192.168.1.2      |bos-srst.srst.lab
srst1   |enabled      |CUCM8      |192.168.1.4      |bos-srst.srst.lab
srst2   |enabled      |CUCM7      |192.168.1.5      |bos-srst.srst.lab
```

The following is an example of the **show srsx site** command with a site specified:

```
srstmgr-1# show srsx site srst1

Sitename:                 srst1
Central Call Agent:       CUCM8
Central Voicemail Server: CUC 8.5
Srst Reference:        srst1
Srst Address:             192.168.28.131
Template:                 default
Provisioning:             enabled
SRST provisioning         enabled
Router login username     bxb100 admin
Router login password     *******
```

Related Commands

Command	Description
show srsx central-call-agent	Displays the central call agents available on the Cisco Unified SRST system.

show srsx site-template

To display the site provisioning templates used when provisioning Cisco Unified SRST Manager devices, use the **show srsx site-template** command.

show srsx site-template [**default**] | [*name*] | [**auto-learned**]

Syntax Description

default	Displays default site provisioning templates.
name	Displays details for the selected template.
auto-learned	Displays site provisioning templates for auto-learned sites.

Command Modes

EXEC mode

Command History

Version	Modification
9.0	This command was introduced.

Usage Guidelines

This information is also available in the Cisco Unified SRST Manager graphical user interface, which we recommend that you use as the primary administrative interface.

Examples

The following is an example of the **show srsx site-template** command in which the voicemail pilot has been auto-learned:

```
se-1-100-100-100# show srsx site-template
Name              |Voicemail Pilot|
___________________________________
default           |Auto-Learned   |
ESRST_and_Dialplan|Auto-Learned   |
ESRST_only        |Auto-Learned   |
SRST_and_Dialplan |Auto-Learned   |
SRST_only         |Auto-Learned   |
```

Related Commands

Command	Description
show srsx central-call-agent	Displays the central call agents available on the Cisco Unified SRST system.
show srsx site	Displays the sites on the Cisco Unified SRST system.

show srsx system-settings

To display the global Cisco Unified survivable remote system configuration values, use the **show srsx system-settings** command.

show srsx system-settings

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC mode

Command History

Version	Modification
9.0	This command was introduced.

Usage Guidelines

This information is also available in the Cisco Unified SRST Manager GUI, which we recommend that you use as the primary administrative interface.

Examples

The following is an example of the **show srsx system-settings** command:

```
srstmgr-1# show srsx system-settings

Use TLS Security: Off
```

Related Commands

Command	Description
show srsx central-call-agent	Displays the central call agents available on the Cisco Unified SRST Manager system.
show srsx site	Displays the sites on the Cisco Unified SRST Manager system.

T

Note For information about other CLI commands that are not listed in this document, see *Cisco Unity Express Command Reference for 3.0 and Later Versions.*

trace

trace

To view trace messages, use the **trace** command in EXEC mode.

trace *{module {entity {activity}}}*

Syntax Description

module	Trace module values. Can be any combination of the values listed in Table 19. Entering **all** gives information for all the modules.
entity	Entity values. Each module has one or more entity values associated with it. Can be any combination of the values for that particular module. See Table 19. Entering **all** gives information for all the entities.
activity	Activity values. Each entity has one or more activity values associated with it. Can be any combination of the values for that particular entity. See Table 19. Entering **all** gives information for all the activities.

Table 19 lists all the modules, entities, and activities.

Table 19 Module, Entity, and Activity Values

Module Name	Entity Name	Activity Name	Description
aaa	authorization	jaas	Used for authentication, authorization, and accounting (AAA) debugging
		pam	
	authentication	jaas	
		pam	
	acct	service	
		queue	
		library	
dns	cache	daemon	Domain Name Service (DNS) debugging
		localzone	
		startup	
		ethconfig	
	enablecheck	dns_check	
		debug	
		ipv4_check	
		hostname_check	
		results	
		dns_query	
	resolver	send	
		receive	
	server	ask	
		answer	

Table 19 Module, Entity, and Activity Values (continued)

Module Name	Entity Name	Activity Name	Description
management	agent	debug	Management debugging
webInterface	group	save	GUI debugging
		delete	
		read	
	user	save	
		delete	
		read	
	aaa	read	
	privileges	action	
	axl	delete	
		post	
		read	
	backupRestore	serverConfiguration	
		restore	
		backup	
	controller	startup	
		request	
	session	login	
		logout	
webInterface (continued)	sysdb	get	GUI debugging (continued)
		set	
		providerStart	
		providerGet	
		providerStop	
		providerSet	
	database	query	
		connection	
		results	

Table 19 Module, Entity, and Activity Values (continued)

Module Name	Entity Name	Activity Name	Description
sysdb	producer	nodeDetach	Interprocess communication debugging
		nodeAttach	
		timeLimit	
		nodeHandle	
		mkdir	
		attrCreate	
		attrDelete	
		rmdir	
	lock	acquire	
		release	
		wait	
	traversal	directory	
		attribute	
		node	
	misc	allocation	
	provider	stop	
		other	
		events	
		deadline	
		get	
		startup	
		commit	
		check	
	utility	metaInfo	
		dealloc	
		chdir	
		nameLookup	
	consumer	set	Interprocess communication debugging (continued)
		get	
		nameLookup	

Table 19 Module, Entity, and Activity Values (continued)

Module Name	Entity Name	Activity Name	Description
limitsManager	platform	xdebug	System limits debugging
		debug	
		info	
		warning	
		crash	
		error	
	cli	xdebug	
		debug	
		info	
		warning	
		crash	
		error	
	api	xdebug	
		debug	
		info	
		warning	
		crash	
		error	
	sysdb	xdebug	
		debug	
		info	
		warning	
		crash	
		error	
	license	xdebug	
		debug	
		info	
		warning	
		crash	
		error	
	utilities	xdebug	
		debug	
		info	
		warning	
		crash	
		error	

Table 19 Module, Entity, and Activity Values (continued)

Module Name	Entity Name	Activity Name	Description
limitsManager (continued)	feature	xdebug	System limits debugging (continued)
		debug	
		info	
		warning	
		crash	
		error	
	mainthread	xdebug	
		debug	
		info	
		warning	
		crash	
		error	
operation	manager	ucid	Command authorization debugging
		operation	
license	debug	core_errors	CSL debugging
		events	
		core_events	
		ipc	
		errors	
		agent_info	
		agent_error	
		agent_all	
		core_all	
	monitor	monitor-license	
BackupRestore	BackupRestore	CONF	Backup and restore debugging
		SERVER	
		INIT	
		OPERATION	
		HISTORY	

Table 19 Module, Entity, and Activity Values (continued)

Module Name	Entity Name	Activity Name	Description
dbclient	debug	level0	Database client debugging
		level1	
		level2	
		level3	
		level4	
		level5	
	sysdb	set	
		get	
		commit	
	database	transaction	
		query	
		garbageCollect	
		connection	
		largeobject	
		mgmt	
		execute	
		results	
superthread	main	startup	Core Java services debugging
	parser	parse	
snmp	JNI	Net-SNMP	SNMP debugging
	agent	debug	
rest	base_resources	info	Common REST interface debugging
		warn	
		error	
	common	info	
		warn	
		error	
security	policy	password	PIN and password authentication policy debugging
		pin	

Table 19 Module, Entity, and Activity Values (continued)

Module Name	Entity Name	Activity Name	Description
ntp	ntp	loopstatus	Network time protocol debugging
		clkselect	
		clkadj	
		clockstatus	
		packets	
		clkvalidity	
		peerstats	
		event	
		loopfilter	
srsx	gui	actions	SRSx GUI debugging
		error	
	cli	debug	SRSx CLI debugging
		error	
	mgmt	debug	SRSx management interface debugging
		error	
	service-point	info	SRSx service point debugging
		trace	
		debug	
		warning	
		error	
	site-manager	info	SRSx site manager debugging
		trace	
		debug	
		warning	
		error	
	srst-engine	info	E-SRST provisioning engine debugging
		trace	
		debug	
		warning	
		error	
		all	

Command Modes

EXEC

Command History

Version	Modification
9.0	This command was introduced.

Examples

The following example illustrates the use of the **trace srsx srst-engine** command:

```
se-192-1-1-149# trace srsx srst-engine all
```

Related Commands

Command	Description
log console monitor	Enables log monitor events for debugging.

GLOSSARY

A

AAA Authentication, authorization, and accounting. Specifies the failover functionality that you can optionally configure for the authentication server.

B

backup and restore Captures the configuration of Cisco Unified SRST Manager so that it can be restored later in case the Cisco Unified SRST Manager configuration becomes corrupted.

C

capability Defines what functions a group can perform.

central call agent Generic term for the Cisco Unified Communications Manager.

central voicemail server Generic term for the Cisco Unity Connection.

Cisco Unified SRST Manager GUI Provides the primary administrative interface for configuring Cisco Unified SRST Manager or Enhanced Survivable Remote Site Telephony (E-SRST). You can access the Cisco Unified SRST Manager graphical user interface from either Firefox or Internet Explorer.

Cisco Unified Communications Manager A call agent.

Cisco Unified SRST Cisco Unified Survivable Remote Site Telephony. A system, made up of a central office and one or more branch offices, that provides telephony services during a WAN outage.

cluster A group of connected devices, such as Cisco Unity Connection, that are managed as a single entity. The devices can be in the same location, or they can be distributed across a network. Any server in the cluster can do the job of any other server in the cluster.

D

DER A binary TLS certificate type.

Display Name User’s name displayed within Cisco Unified SRST Manager applications.

Domain name system (DNS) server The DNS server provides translation from hostnames to IP addresses.

E

Enhanced Survivable Remote Site Telephony (E-SRST) Provides automated remote site provisioning of the following advanced telephony features in survivable mode by gathering the information from Cisco Unified Communications Manager about:

- End-user phones and extensions (speed dials, lines, softkeys)
- Voicemail and call forward configuration
- Call routing restrictions (local and long distance, and time of day)
- Call park and group call park
- Call pickup
- Hunt groups

G

Group ID Name of a group of users, usually created to assign members to a Cisco Unified SRST Manager.

L

log file A file that lists actions that have occurred.

N

NAT Network Address Translation

Network time protocol (NTP) Used to set the system time to avoid manual configuration of the time. Using NTP helps the system to keep the system time synchronized with the NTP server in case there is a drift in the system clock. NTP typically provides accuracy within a millisecond on LANs and up to a few tens of milliseconds on WANs relative to Coordinated Universal Time. Typical NTP configurations utilize multiple redundant servers and diverse network paths to achieve high accuracy and reliability.

O

operation A set of CLI commands or GUI functions.

P

Password A Cisco Unified SRST Manager password consists of letters and numbers and is at least 3 characters but not more than 32 characters long.

Password options For the password used by the user to access the Cisco Unified SRST Manager GUI, select one of the following:

Generate a Random Password—To have Cisco Unified SRST Manager generate a random password.

Blank Password—To leave the password blank.

Password Specified Below—To specify a password for the user. (Default and Recommended)

PAT Port Address Translation. Network address translation (NAT) variant where a single public address is shared for multiple private network devices and port translation is used to expose private services to the public network.

PEM Privacy Enhanced Mail. A TLS certificate type. It is a Base64 encoded DER certificate, enclosed between "-----BEGIN CERTIFICATE-----" and "-----END CERTIFICATE-----".

pilot number The number used to reach a desired service such as voicemail or auto attendant. Typically this number is not visible on IP phones as it is hidden behind the voicemail button on the phone which dials the pilot automatically.

Primary E.164 number User or group's primary telephone number, including area code.

privilege A set of operations that are grouped together. Privileges are assigned to users.

provisioning The processing performed by Cisco Unified SRST Manager to configure branch site devices for SRST or E-SRST services. The process involves retrieving information from Cisco Unified Communications Manager and converting it to IOS commands for the branch router.

R

REST A programmatic interface.

Rights Member or Owner.

S

secondary node A replica of the primary node. It is configured for use in case the primary node fails.

site A site is created on Cisco Unified SRST Manager based on the existence of a Cisco Unified SRST reference configured on the Cisco Unified Communications Manager.

SMTP Simple Mail Transfer Protocol (SMTP). standard for e-mail transmissions across the Internet. Formally SMTP is defined in RFC 821 (STD 10) as amended by RFC 1123 (STD 3) chapter 5. The protocol used today is also known as ESMTP and defined in RFC 2821.

SRST See Cisco Unified SRST.

SRST reference A gateway that can provide limited Cisco Unified Communications Manager functionality when all other Cisco Unified Communications Manager servers for a device are unreachable.

T

trace buffer Collection of debug traces for system activity.

U

User ID Alphanumeric user identifier.