Cisco Emergency Responder Administration Guide, Release 15 and SUs

First Published: 2023-12-18

Last Modified: 2024-03-28

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

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

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

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

Preface

Overview

This document provides you with the required information to install, configure, manage, and use Cisco Emergency Responder (Emergency Responder).

Audience

Network engineers, system administrators, and telecom engineers should review this guide to learn the steps required to properly set up Emergency Responder in the network. Because of the close interaction of Emergency Responder with CiscoUnifiedCommunicationsManager, you should be familiar with CiscoUnifiedCommunicationsManager before deploying Emergency Responder.

Security personnel should also read this document.

Organization

The following table details how this guide is organized:

Topic	Description
Plan for Cisco Emergency Responder, on page 5	Provides information to help you understand emergency call ordinances, how Emergency Responder helps you meet the ordinances, and what you must do to deploy Emergency Responder successfully.

Topic	Description
Configure Cisco Unified Communications Manager, on page 83	Describes the configuration procedures for Unified CM for Emergency Responder.
Configure Cisco Emergency Responder, on page 107	Describes the configuration procedure for Emergency Responder.
Configure Emergency Responder and National E911 Service Provider Enterprise Services , on page 183	Describes how to configure Emergency Responder to interoperate with National E911 Service Provider Enterprise.
Configure Cisco Emergency Responder Serviceability, on page 195	Describes how to configure and use Emergency Responder Serviceability features.
Configure Cisco Unified Operating System, on page 205	Describes how to configure and use the Cisco Unified Communications Operating System, which is bundled with Emergency Responder.
Configure Cisco Emergency Responder Disaster Recovery System, on page 237	Describes how to configure the Cisco Emergency Responder Disaster Recovery System.
Cisco Emergency Responder Admin Utility, on page 305	Describes how to use the Cisco Emergency Responder Admin Utility.
Cisco Emergency Responder User Preparation , on page 309	Describes the various roles for Emergency Responder users.
Troubleshoot Cisco Emergency Responder, on page 323	Addresses problems you might encounter with Emergency Responder and provides ways to resolve them; also includes other tasks associated with problem identification and resolution.
ALI Formatting Tool, on page 315	Describes the ALI Formatting Tool (AFT) and provides information about how to use and troubleshoot the AFT.
Cisco Emergency Responder Administration Web Interface, on page 361	Describes the fields on the pages of the Emergency Responder administrator web interface.
Cisco Emergency Responder Serviceability Web Interface , on page 509	Describes the Emergency Responder serviceability web interface.
Cisco Unified Operating System Administration Web Interface , on page 527	Describes the Cisco Unified Operating System (OS) Administration web interface.
Disaster Recovery System Web Interface , on page 563	Describes the Cisco Emergency Responder Disaster Recovery System Administration web interface.
Admin Utility Web Interface for Cisco Emergency Responder , on page 573	Describes the Cisco Emergency Responder Admin Utility web interface.
Using AFT for Specific Service Providers , on page 577	Provides service-provider specific information for use in conjunction with the AFT.

Topic	Description
Event Log Messages , on page 585	Provides Emergency Responder based Event Log messages and administrative alerts.
Cisco Emergency Responder Port Usage , on page 593	Provides information about the ports used by Emergency Responder.

Related Documentation

For additional information about Cisco Emergency Responder (Emergency Responder) and Cisco Unified Communications Manager, see the following publications.

- All Cisco Emergency Responder documents are available at:

  http://www.cisco.com/en/US/products/sw/voicesw/ps842/tsd_products_support_series_home.html

- Cisco Unified Communications Manager installation documents are available at:

  http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_installation_guides_list.html

- Cisco Unified Communications Manager operating system installation documents and backup and restore documents are available at:

  http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html

- Information about Cisco Unified Operations Manager is available at:

  http://www.cisco.com/en/US/products/ps6535/index.html

Cisco Product Security Overview

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

Further information regarding U.S. export regulations may be found at the U.S. Bureau of Industry and Security's Export Administration Regulation Downloadable Files web page.

Acknowledgments

This product includes software developed by Justin Wells and Semiotek Inc. for use in the WebMacro Servlet Framework (http://www.webmacro.org).

You may use WebMacro for use under the GNU General Public License. You may also use WebMacro under the terms of the Semiotek Public License. The terms of the Semiotek Public License are as follows:

Copyright (c) 1997, 1998, 1999, 2000, 2011 Semiotek Inc.

All rights reserved.

CHAPTER 1

New and Changed Information

New and Changed Information

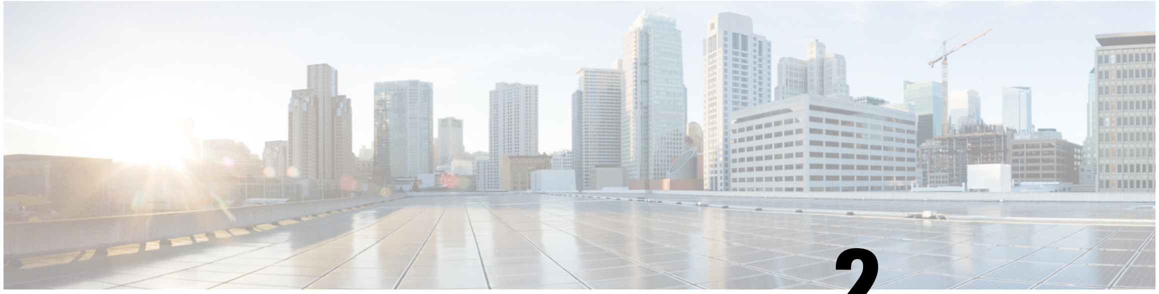
The following table provides an overview of the significant changes to the features in this guide up to this current release. The table doesn't provide an exhaustive list of all changes made to the guide or of the new features up to this release.

Table 1: New Features and Changed Behavior in Emergency Responder

Date	Description	See
March 28, 2024	IPv6 Subnet Support for Release 15SU1	• Configure IPv4 Subnet, on page 450 • Configure IPv6 Subnet (Applicable from Release 15SU1 Onwards), on page 451
December 18, 2023	Migration of All Applications to 64-Bit System	Cisco Emergency Responder and all applications have moved to a 64-biy architecture. Some of the affected areas are: • Hardware and EXSi specifications for upgrades and migrations • Upgrade Paths • Floppy Drive is replaced with CDROM for unattended installation.

PART I

Deployment and Planning



CHAPTER 2

Plan for Cisco Emergency Responder

Plan for Cisco Emergency Responder Overview

Cisco Emergency Responder (Emergency Responder) helps you manage emergency calls in your telephony network so that you can respond to these calls effectively and so that you can comply with local ordinances concerning the handling of emergency calls. In North America, these local ordinances are called “enhanced 911,” or E911. Other countries and locales have similar ordinances.

Because emergency call ordinances can differ from location to location within a country, region, state, or even metropolitan area, Emergency Responder gives you the flexibility to configure your emergency call configuration to specific local requirements. However, ordinances differ from location to location, and security requirements differ from company to company, so you must research your security and legal needs before deploying Emergency Responder.

Understanding Enhanced 911 (E911)

Enhanced 911, or E911, is an extension of the basic 911 emergency call standard in North America. The information in the following sections describe E911 requirements and terminology.

Overview of Enhanced 911 Requirements

Enhanced 911 (E911) extends the basic 911 emergency call standard to make it more reliable.

When using basic 911 in North America, if a caller dials 911, the call is routed to a Public Safety Answering Point (PSAP), also called the 911 operator. The PSAP talks to the caller and arranges the appropriate emergency response, such as sending police, fire, or ambulance teams.

E911 extends this standard with these requirements:

- The emergency call must be routed to the local PSAP based on the location of the caller. In basic 911, the call is routed to a PSAP, but not necessarily the local one.
- The caller location information must be displayed at the emergency operator terminal. This information is obtained by querying an automatic location information (ALI) database.

In E911, the location of the caller is determined by the Emergency Location Identification Number (ELIN), which is a phone number the PSAP can dial to reconnect to the emergency caller if the emergency call is cut off or if the PSAP needs to talk to the caller again. The emergency call is routed to the PSAP based on the location information associated with this number. For multiline phone systems, such as an office system, the ELIN can be associated with more than one telephone by grouping the phones in an Emergency Response Location (ERL). In this case, the location the PSAP receives that would be the address of an office building. For large buildings, the location would include additional information such as floor or region on a floor. Each ERL requires a unique ELIN.

In addition to these general E911 requirements, each locality can further extend or limit these requirements. For example, a city ordinance might include specific limitations on the size of an ERL (such as, no larger than 7000 square feet), or on the number of phones that can be included in an ERL (such as, no more than 48 phones). You must work with your service provider and local government to determine the exact E911 requirements in your area.

Related Topics

E911 and Cisco Emergency Responder Terminology , on page 6

Understanding Cisco Emergency Responder, on page 9

E911 and Cisco Emergency Responder Terminology

The following list defines some of the key terminology used in this document.

ALI

Automatic location information. Information that connects an ELIN to a location, is used to route emergency calls from that ELIN to the correct local PSAP, and is provided to the PSAP to help the PSAP locate the emergency caller. In Emergency Responder, you fill in ALI data for each ERL and submit the ALI data to your service provider for inclusion in the ALI database.

ANI

Automatic number identification. ANI is another name for ELIN. This document uses ELIN instead of ANI.

CAMA

Centralized automated message accounting. An analog phone trunk that connects directly to an E911 selective router, bypassing the Public Switched Telephone Network (PSTN).

DID

Direct inward dial. A telephone number obtained from your service provider that can be used to dial into your telephone network. DID numbers are used for ELIN.

ELIN

Emergency location identification number. A phone number that routes the emergency call to the local PSAP, and which the PSAP can use to call back the emergency caller. The PSAP might need to call the number if the emergency call is cut off, or if the PSAP needs additional information after normally ending the emergency call. See ALI.

Emergency Call

A call made to the local emergency number, such as 911. Emergency Responder routes the call to the service provider's network where the call is routed to the local PSAP.

Emergency Caller

The person who places the emergency call. The caller might require help for a personal emergency, or might be reporting a more general emergency (fire, theft, accident, and so forth).

ERL

Emergency response location. The area from which an emergency call is placed. The ERL is not necessarily the location of the emergency. If an emergency caller is reporting a general emergency, the actual emergency might be in a different area. In Emergency Responder, you assign switch ports and phones to ERLs, and ERL definitions include ALI data.

ESN

Emergency service number.

ESZ

Emergency service zone. The area covered by a given PSAP. This area usually includes several police and fire departments. For example, a city and its suburbs might be serviced by one PSAP.

Each ESZ is assigned a unique ESN to identify it.

MSAG

Master street address guide. A database of ALIs that enables proper routing of emergency calls to the correct PSAP. In Emergency Responder, you export your ALI definitions and transmit them to your service provider, who ensures that the MSAG is updated. You must negotiate this service with your service provider — it is not a service provided directly through Emergency Responder.

NENA

National Emergency Number Association. The organization that recommends data and file formats for ALI definitions and other emergency call requirements in the United States. Emergency Responder uses the NENA formats for ALI data export files. Your service provider has additional restrictions on data format, so ensure that your ALI entries comply with your service provider's rules.

PSAP

Public safety answering point. The PSAP is the organization that receives emergency calls (for example, the 911 operator) and is staffed by people trained in handling emergency calls. The PSAP talks to the emergency caller and notifies the appropriate public service organizations (such as police, fire, or ambulance) of the emergency and its location.

Related Topics

Overview of Enhanced 911 Requirements , on page 5
Understanding Cisco Emergency Responder, on page 9

FCC Emergency Call Regulations

The United States Federal Communications Commission (FCC) adopted rules to help ensure people who call 911 from Multi Line Telephone Systems (MLTS) like Unified Communications Manager can reach 911 directly and be quickly located by first responders. The FCC’s rules also impose requirements for transmitting dispatchable location information and require a notification be sent to a central location in the organizations when a 911 call is initiated.

Cisco Emergency Responder provides advanced Emergency Calling functionality to Cisco Unified Communications Manager. It assures that Unified CM will send emergency calls to the appropriate public safety answering point (PSAP) for the caller's location, and that the PSAP can identify the caller's location and return the call if necessary. In addition, the system automatically tracks and updates phone moves and changes. It provides local onsite notification through several methods, including phone alert, web portal alert, email, and text alert. Deploying this capability helps ensure compliance with FCC rules.

Direct 911 dial pattern

The Cisco Emergency Responder effectively manages emergency calls originating in Unified Communications Manager. To handle emergency calls, you must configure the emergency call numbers (such as 911) in Unified Communications Manager with CTI Route Points so that Emergency Responder intercepts them and provide correct treatment. That is, routing instructions based on location of the caller and that PSAP can callback the user if initial call is disconnected.

For more information, see Configure Cisco Unified Communications Manager.

Local Onsite Notification

Cisco Emergency Responder while managing 911 call routing provides ability to configure Onsite Security Users who can be notified about the emergency call through several methods:

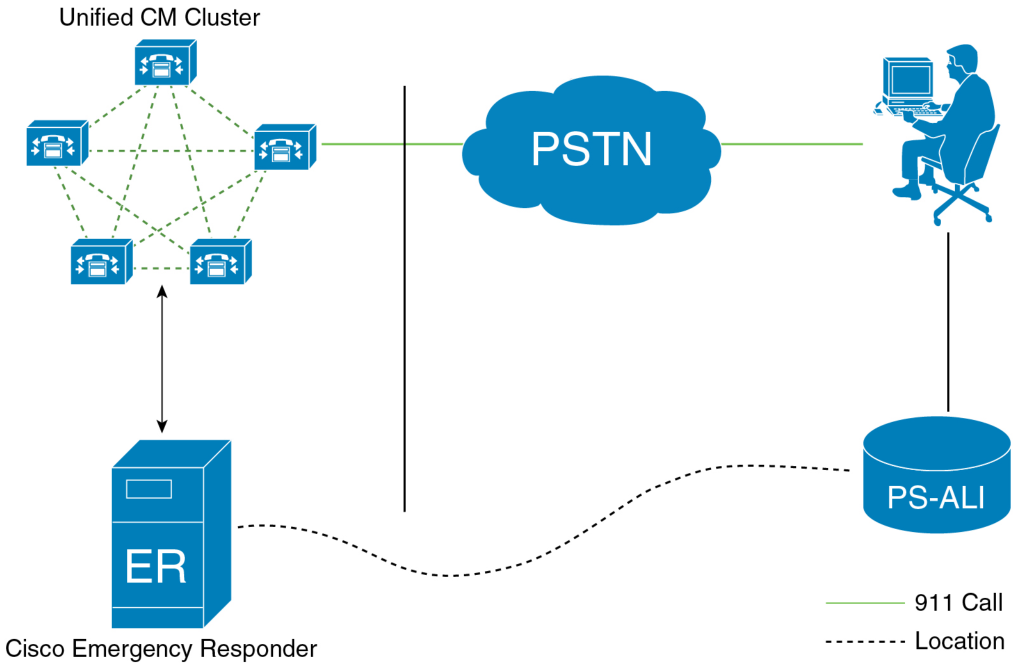
- **Telephone Call to Preconfigured DN**—Includes information like Calling Line Number and time of the 911 call.
- **Web-Notification to Authenticated Users**—Includes information like Calling Line Number, name of the originator, location, and time of the 911 call.
- **Email Notification to Configured Users**—Includes information like Calling Line Number, name of the originator, location, and time of the 911 call.
- **Text Alerts to Configured Users**—Includes information like Calling Line Number, name of the originator, location, and time of the 911 call.

For more information on how to configure these notification methods, see Configure Cisco Emergency Responder, on page 107.

In case an Onsite Security personnel is managing multiple sites (Emergency Response Locations); the Onsite Security personnel can configure Emergency Responder to get alerts from all the ERLs or only from specific ERL. See the "Configure Cisco Emergency Responder Onsite Alerts" chapter for more information.

Location Dispatch

Cisco Emergency Responder assures that Unified CM sends emergency calls to the appropriate Public Safety Answering Point (PSAP) for the caller's location, and that the PSAP can identify the caller's location and return the call if necessary.



Cisco Emergency Responder represents location through Emergency Response Location (ERL). An ERL defines the area in which an emergency call is made. ERL can be identified by the Emergency Location Identification Number (ELIN), which is a phone number the PSAP can dial to reconnect to the emergency caller if the emergency call is cut off or if the PSAP needs to talk to the caller again. For MLTS, such as an office system, the ELIN can be associated with more than one telephone by grouping the phones in an Emergency Response Location (ERL).

Cisco Emergency Responder provides ability to export PS-ALI record and update through traditional LEC (Local Exchange Carrier) Service. For more information on PS-ALI Export, see Set Up Individual ERL and Automatic Location Information (ALI) , on page 140.

Cisco Emergency Responder supports integrating with an E911 National Service Provider (like National E911 Service Provider) as an alternative to direct connection with the Local Exchange Carrier (LEC). The integration could be used to provide emergency services to phones that are on the corporate network (on-premise) and phones that are located away from the corporate network (off-premise). See Configure Emergency Responder and National E911 Service Provider Enterprise Services , on page 183.

Understanding Cisco Emergency Responder

The following topics provide an overview of Emergency Responder and how you can use it in your network.

Features

See the Release Notes for Cisco Emergency Responder for a list of the new and enhanced features. The Emergency Responder Release Notes are located at:

http://www.cisco.com/en/US/partner/products/sw/voicesw/ps842/prod_release_notes_list.html

Network Hardware and Software Requirements

Emergency Responder supports a variety of hardware and software components. For the complete list of supported hardware and software, see the Release Notes for Cisco Emergency Responder located at http://www.cisco.com/en/US/products/sw/voicesw/ps842/prod_release_notes_list.html.

Cisco Smart Software Licensing

Cisco Smart Software Licensing is a new way of thinking about licensing. It adds flexibility to your licensing and simplifies it across the enterprise. It also delivers visibility into your license ownership and consumption.

Cisco Smart Software Licensing helps you to procure, deploy, and manage licenses easily where devices self-register and report license consumption, removing the need for product activation keys (PAK). It pools license entitlements in a single account and allow you to move licenses freely through the network, wherever you need them. It is enabled across Cisco products and managed by a direct cloud-based or mediated deployment model.

This service registers the product instance, reports license usage, and obtains the necessary authorization from Cisco Smart Software Manager or Cisco Smart Software Manager satellite.

You can use Cisco Smart Licensing to:

- Register with Cisco Smart Software Manager, on page 10 or Cisco Smart Software Manager Satellite, on page 11
- See the license usage and count
- See the product licenses available on Cisco Smart Software Manager or Cisco Smart Software Manager satellite
- Renew License Authorization with Cisco Smart Software Manager or Cisco Smart Software Manager satellite
- Renew the License Registration
- Deregister with Cisco Smart Software Manager or Cisco Smart Software Manager satellite

Cisco Emergency Responder license is of single-type user and one license is required for each endpoint. Any endpoint capable of making an emergency call requires an Emergency Responder User License. For example, IP phones, analog phones, video endpoints, and clients all require an Emergency Responder User License.

Cisco Smart Software Manager replaces Prime License Manager in Cisco Emergency Responder Release 12.0 and later versions.

Note Cisco Emergency Responder is not part of Cisco Unified Workspace Licensing (UWL) or Cisco User Connect Licensing (UCL).

Cisco Smart Software Manager

Cisco Smart Software Manager is hosted on software.cisco.com, allowing product instances to register and report license consumption to it.

You can use Cisco Smart Software Manager to:

- Manage and track licenses
- Move licenses across virtual account
- Remove registered product instance

Note If you are upgrading Cisco Emergency Responder registered to Cisco Smart Software Manager from Pre-15 releases to Release 15 or higher, Cisco Emergency Responder will not update the product version to 15 in the Cisco Smart Software Manager UI for the Product Instance. Refer to CSCwf94088 for more details.

For more information about Cisco Smart Software Manager, see https://software.cisco.com/.

Cisco Smart Software Manager Satellite

Cisco Smart Software Manager Satellite is a component of Cisco Smart Licensing that manages product registrations and monitoring of smart license usage for Cisco products. If you do not want to manage Cisco products directly using Cisco Smart Software Manager, either for policy or network availability reasons, you can choose to install Cisco Smart Software Manager satellite on-premises. Products register and report license consumption to the Cisco Smart Software Manager Satellite as it does on Cisco Smart Software Manager.

Note If you are upgrading Cisco Emergency Responder registered to Cisco Smart Software Manager Satellite from Pre-15 releases to Release 15 or higher, Cisco Emergency Responder will not update the product version to 15 in the Cisco Smart Software Manager UI for the Product Instance. Refer to CSCwf94088 for more details.

For more information about Cisco Smart Software Manager Satellite, see http://www.cisco.com/web/ordering/smart-software-manager/smart-software-manager-satellite.html.

Product Instance Evaluation Mode

After installation Cisco Emergency Responder runs under the 90-day evaluation period. During this period, you can use all features in this product. Register Cisco Emergency Responder with Cisco Smart Software Manager or Cisco Smart Software Manager satellite to report the license usage to Cisco and obtain the necessary authorization for entitlement usage. After the evaluation period expires, Cisco Phone Tracking Engine of Cisco Emergency Responder stops until you register with Cisco Smart Software Manager or Cisco Smart Software Manager satellite.

Note Evaluation period is before the product is registered.

License Compliance

When first installed, the Emergency Responder is fully operational in evaluation mode for 90 days until it has successfully synchronized with the Cisco Smart Software Manager or Cisco Smart Software Manager satellite, and also new licenses are installed on Cisco Smart Software Manager or Cisco Smart Software Manager satellite. After the Cisco Emergency Responder is registered with Cisco Smart Software Manager or Cisco Smart Software Manager satellite and licenses are installed, synchronization with Cisco Smart Software Manager or Cisco Smart Software Manager satellite takes place. The Emergency Responder communicates with Cisco Smart Software Manager or Cisco Smart Software Manager satellite daily.

Emergency Responder reports the total license requirements to the Cisco Smart Software Manager or Cisco Smart Software Manager satellite. The Cisco Smart Software Manager or Cisco Smart Software Manager satellite totals the license requirements for all connected Emergency Responder product instances and compares this total license requirement to the total available installed licenses. The Cisco Smart Software Manager or Cisco Smart Software Manager satellite then reports the status back to the product instance as Authorized or as Out of Compliance.

Out of Compliance occurs when the number of licenses are insufficient.

Authorization Expired occurs when the product has not communicated with Cisco Smart Software Manager or Cisco Smart Software Manager satellite for 90 continuous days. In this state, Cisco Emergency Responder allows you to run in Authorization Expired state for another 90 more days. After which Cisco Phone Tracking Engine service is stopped on the Cisco Emergency Responder node.

Warning Install new licenses within 90 days of installation or upgrade. If you do not install new licenses within 90 days, evaluation period expires and the Emergency Responder system stops tracking and updating the Phone Location.

Any endpoint capable of making an emergency call requires an Emergency Responder User License. For example, IP phones, analog phones, video endpoints, and clients all require an Emergency Responder User License.

You can choose not to track the phones in an IP Subnet. If you do not track the phones in an IP Subnet, you do not need the Emergency Responder User Licenses for them. For additional information, Configure IP Subnet.

System Licensing Prerequisites

Complete the steps to set up Smart and Virtual accounts. For more information about this process, see https://software.cisco.com/.

Smart Software Licensing Task Flow

Procedure

	Command or Action	Purpose
Step 1	Obtain the Product Instance Registration Token, on page 13.	Use this procedure to generate a product instance registration token for your virtual account.
Step 2	Configure Transport Settings, on page 13.	Perform this step to select transport settings through which Cisco Emergency Responder can connect to Cisco Smart Software Manager. **Direct** option is selected by default where the product communicates directly with Cisco licensing servers.
Step 3	Register with Cisco Smart Software Manager, on page 15.	Perform this step to register Cisco Emergency Responder with Cisco Smart Software Manager or Cisco Smart Software Manager satellite.

Obtain the Product Instance Registration Token

Before you begin

Obtain the product instance registration token from Cisco Smart Software Manager or Cisco Smart Software Manager satellite to register the product instance. Tokens can be generated with or without the Export-Controlled functionality feature being enabled.

Procedure

Step 1 Log in to your smart account in either Cisco Smart Software Manager or your Cisco Smart Software Manager satellite.

Step 2 Navigate to the virtual account with which you want to associate the Cisco Emergency Responder cluster.

Step 3 Generate a “Product Instance Registration Token”.

Note Select the **Allow export-controlled functionality on the products registered with this token** check box to turn on the Export-Controlled functionality for tokens of a product instance you wish in this smart account. By checking this check box and accepting the terms, you enable higher levels of the product encryption for products registered with this Registration Token. By default, this check box is selected. You can uncheck this check box if you wish not to allow the Export-Controlled functionality to be made available for use with this token.

Caution Use this option only if you are compliant with the Export-Controlled functionality.

Note The **Allow export-controlled functionality on the products registered with this token** check box is not displayed for the Smart Accounts that are not permitted to use the Export-Controlled functionality.

Step 4 Copy the token or save it to another location.

For more information, see https://software.cisco.com/.

What to do next

Configure Transport Settings, on page 13.

Configure Transport Settings

Use this procedure to select transport settings through which Cisco Emergency Responder register to Cisco Smart Software Manager for license management.

Before you begin

Obtain the Product Instance Registration Token, on page 13.

Procedure

Step 1 From Cisco ER Administration, choose **System** > **License Manager**.

Step 2 From the **Smart Software Licensing** section, click the **View/Edit** link.

The **Transport Settings** dialog box appears.

Step 3 Select one of the following radio buttons:

- **Direct**—Cisco Emergency Responder sends usage information directly over the internet. No additional components are needed. This is the default setting.
- **Cisco Smart Software Manager satellite**—Cisco Emergency Responder sends license usage information to an on-premises collector called Cisco Smart Software Manager Satellite which requires a periodic exchange of information with Cisco Smart Software Manager cloud service. Under the Transport settings, enter the **URL** details as given below:
  - If you are using HTTP, go to the URL: http://Satellite-ip/Transportgateway.
  - If you are using HTTPS, go to the URL: https://SatelliteFQDN-OR-IP-address/TransportGateway.

  For more information on how to register your devices using Cisco Smart Software Manager satellite, see https://community.cisco.com/t5/cisco-software-documents/how-to-register-your-device-using-https-to-satellite-smart/ta-p/3747976.

  For more information on installation or configuration of Cisco Smart Software Manager satellite, go to this URL: https://www.cisco.com/c/en/us/buy/smart-accounts/software-manager-satellite.html.
- **Proxy Server**—Cisco Emergency Responder sends usage information over the internet through a proxy server.

  Check the **Authentication needed on HTTP or HTTPS proxy** check box if want to register to Cisco Smart Software Manager using authentication based proxy server. If you enable this check box, only then the Proxy User and Proxy Password fields are enabled.

  Enter the details in the following fields:
  - Host Name/IP Address
  - Port
  - Proxy User

    Note Administrators should ensure that they enter the configured user name for proxy in the **Proxy User** field.
  - Proxy Password

Note If you choose to use direct connection, then you must configure Domain Name System (DNS) on Cisco Emergency Responder that can resolve tools.cisco.com.

Note If you choose not to configure the domain and Domain Name System (DNS) on Cisco Emergency Responder, then you can select the transport gateway or proxy server. In such case, DNS that can resolve tools.cisco.com has to be configured on either of the proxy server.

Note If you choose not to use the DNS server in your deployment and not connect to the internet, then you can select the Cisco Smart Software Manager satellite with manual synchronization in disconnected mode.

Step 4 Check the **Do not share my hostname or IP address with Cisco** check box to allow the administrator to restrict the exchange of IP Address and hostname of the Cisco Emergency Responder during the registration and synchronization to Cisco Smart Software Manager or Cisco Smart Software Manager Satellite.

Note When the check box is selected, Cisco Emergency Responder will not share the IP Address or hostname information from being sent through registration and regular license compliance synchronization activities. A unique identifier is generated for the Cisco Emergency Responder Product Instance and will need to be used for cross-referencing in Cisco Smart Software Manager.

Step 5 Click **Save**.

What to do next

Register with Cisco Smart Software Manager, on page 15.

Register with Cisco Smart Software Manager

Use this procedure to register your product with Cisco Smart Software Manager or Cisco Smart Software Manager satellite. Your product is in Evaluation Mode until then.

Before you begin

Configure Transport Settings, on page 13.

Procedure

Step 1 From Cisco ER Administration, choose **System** > **License Manager**.
The **License Manager** window appears.

Step 2 From the **Smart Software Licensing** section, click the **Register** button.
The **Smart Software Licensing Product Registration** window appears.

Step 3 In the **Product Instance Registration Token** section, paste the copied or saved “Registration Token Key” that you generated using the Cisco Smart Software Manager or Cisco Smart Software Manager satellite.

Step 4 Click **Register** to complete the registration process.

Step 5 Click **Close**. For more information, see the online help.

Step 6 In the **Request Entitlement Now** section, click **Synchronize Now** to manually update the system license usage information.

Note Usage information is updated once every 6 hours automatically. For more information, see the online help.

Smart Software Licensing Additional Operations

The available Smart Software Licensing additional operations are:

- Renew Authorization, on page 16.

  Perform this step to manually renew the License Authorization Status for all the license listed under the License Type.

Note The license authorization is renewed automatically every 30 days. The authorization status will expire after 90 days if it is not connected to Cisco Smart Software Manager or Cisco Smart Software Manager satellite.

- Renew Registration, on page 17.

  Perform this step to renew the registration information manually.

Note The initial registration is valid for one year. Renewal of registration is automatically done every six months provided the product is connected to Cisco Smart Software Manager or Cisco Smart Software Manager satellite.

- Deregister, on page 18.

  Perform this step to disconnect the Cisco Emergency Responder cluster from Cisco Smart Software Manager or Cisco Smart Software Manager satellite. The product reverts to evaluation mode as long as the evaluation period is not expired. All license entitlements used for the product are immediately released back to the virtual account and are available for other product instances to use it.

- Reregister License with Cisco Smart Software Manager, on page 18.

  Perform this step to reregister Cisco Emergency Responder with Cisco Smart Software Manager or Cisco Smart Software Manager satellite.

Note Product may migrate to a different virtual account by reregistering with token from a new virtual account.

Renew Authorization

Use this procedure to manually renew the License Authorization Status for all the licenses listed under the License Type.

Note Additional 90-days grace period is provided after authorization expires.

Before you begin

The product should be registered with Cisco Smart Software Manager or Cisco Smart Software Manager satellite.

Procedure

Step 1 From Cisco ER Administration, choose **System** > **License Manager**.
The **License Manager** window appears.

Step 2 From the **Smart Software Licensing** section, click the **Actions** drop—down list box.

Step 3 Choose **Renew Registration Now**.
The **Renew Registration** window appears.

Step 4 Click **Ok**.

Cisco Emergency Responder sends a request to Cisco Smart Software Manager or Cisco Smart Software Manager satellite to check the "License Authorization Status" and Cisco Smart Software Manager or Cisco Smart Software Manager satellite reports back the status to Cisco Emergency Responder. For more information, see the online help.

Step 5 In the **Request Entitlement Now** section, click **Synchronize Now** to manually update the system license usage information.

Note Usage information is updated once every 6 hours automatically. For more information, see the online help.

Renew Registration

During product registration to Cisco Smart Software Manager or Cisco Smart Software Manager satellite, there is a security association used to identify the product and is anchored by the registration certificate, which has a lifetime of one year (that is, registration period). This is different from the registration token ID expiration, which has the time limit for the token to be active. This registration period is automatically renewed every 6 months. However, if there is an issue, you can manually renew this registration period.

Before you begin

The product should be registered with Cisco Smart Software Manager or Cisco Smart Software Manager satellite.

Procedure

Step 1 From Cisco ER Administration, choose **System** > **License Manager**.
The **License Manager** window appears.

Step 2 From the **Smart Software Licensing** section, click the **Actions** drop—down list.

Step 3 Choose **Renew Registration Now**.
The **Renew Registration** window appears.

Step 4 Click **Ok**.

Cisco Emergency Responder sends a request to Cisco Smart Software Manager or Cisco Smart Software Manager satellite to check the "Registration Status" and Cisco Smart Software Manager or Cisco Smart Software Manager satellite reports back the status to Cisco Emergency Responder. For more information, see the online help.

Step 5 In the **Request Entitlement Now** section, click **Synchronize Now** to manually update the system license usage information.

Note Usage information is updated once every 6 hours automatically. For more information, see the online help.

Deregister

Use this procedure to unregister from Cisco Smart Software Manager or Cisco Smart Software Manager satellite and release all the licenses from the current virtual account. This procedure also disconnects Cisco Emergency Responder cluster from Cisco Smart Software Manager or Cisco Smart Software Manager satellite. All license entitlements used for the product are released back to the virtual account and is available for other product instances to use.

Before you begin

The product should be registered with Cisco Smart Software Manager or Cisco Smart Software Manager satellite.

Procedure

Step 1 From Cisco ER Administration, choose **System** > **License Manager**.
The **License Manager** window appears.

Step 2 From the **Smart Software Licensing** section, click the **Actions** drop—down list box.

Step 3 Choose **Deregister**.
The **Deregister** window appears.

Step 4 Click **Ok**.

Step 5 In the **Request Entitlement Now** section, click **Synchronize Now** to manually update the system license usage information.

Note Usage information is updated once every 6 hours automatically. For more information, see the online help.

Reregister License with Cisco Smart Software Manager

Use this procedure to reregister Cisco Emergency Responder with Cisco Smart Software Manager or Cisco Smart Software Manager satellite.

Before you begin

Obtain the Product Instance Registration Token, on page 13.

Procedure

Step 1 From Cisco ER Administration, choose **System** > **License Manager**.
The **License Manager** window appears.

Step 2 From the **Smart Software Licensing** section, click the **Register** button.

The **Registration** window appears.

Step 3 From the **Smart Software Licensing** section, click the **Actions** drop—down list box.

Step 4 Choose **Reregister**.
The **Smart Software Licensing Product Re-registration** window appears.

Step 5 Click **Ok**.

Step 6 In the **Product Instance Registration Token** section, paste the copied or saved “Registration Token Key” that you generated using the Cisco Smart Software Manager or Cisco Smart Software Manager satellite.

Step 7 Click **Register** to complete the registration process.

Step 8 Click **Close**. For more information, see the online help.

Step 9 In the **Request Entitlement Now** section, click **Synchronize Now** to manually update the system license usage information.

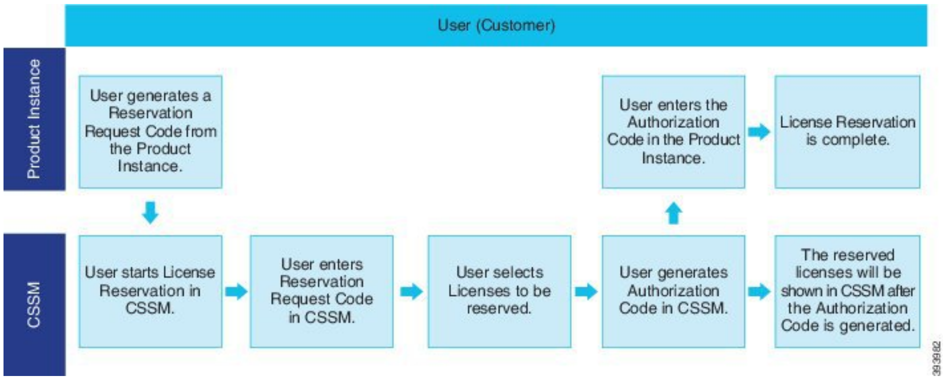
Note Usage information is updated once every 6 hours automatically. For more information, see the online help.

Specific License Reservation

Specific License Reservation is a feature that is used in highly secure networks. It provides a method for customers to deploy a software license on a device (Product Instance - Emergency Responder) without communicating usage information.

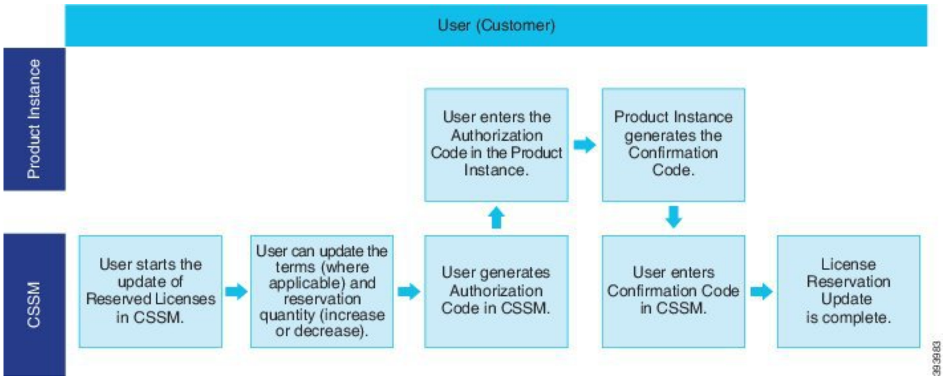
Users can specify and reserve perpetual or term-based licenses against the Emergency Responder product. No regular synchronization is required from the product once authorization code is exchanged unless there are any changes in the reservation requests. Reserved licenses remain blocked in Cisco Smart Software Manager unless released from the product with a return code.

Figure 1: Reserve Licenses


User (Customer)
Product Instance
CSSM
User generates a Reservation Request Code from the Product Instance.
User enters the Authorization Code in the Product Instance.
License Reservation is complete.
User starts License Reservation in CSSM.
User enters Reservation Request Code in CSSM.
User selects Licenses to be reserved.
User generates Authorization Code in CSSM.
The reserved licenses will be shown in CSSM after the Authorization Code is generated.
393982

An update or change in reserved licenses (increase or decrease) can be done on previously reserved licenses in Cisco Smart Software Manager. New authorization code can be installed on the product and the confirmation code obtained. The changes remain in transit status until the confirmation code from the product is installed on Cisco Smart Software Manager.

Figure 2: Update Reserve Licenses

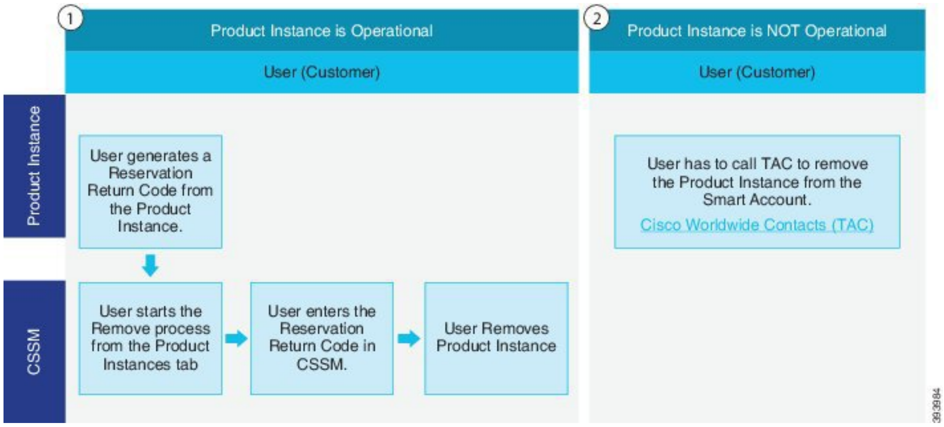

User (Customer)
Product Instance
CSSM
User enters the Authorization Code in the Product Instance.
Product Instance generates the Confirmation Code.
User starts the update of Reserved Licenses in CSSM.
User can update the terms (where applicable) and reservation quantity (increase or decrease).
User generates Authorization Code in CSSM.
User enters Confirmation Code in CSSM.
License Reservation Update is complete.
393983

When licenses are reserved on a Product Instance (Emergency Responder), there are two ways to remove your product from the smart account and release all the licenses that are reserved for that Product Instance (Emergency Responder):

- **Product Instance is operational (graceful removal)**: User can return the Specific License Reservation authorization by creating a Reservation Return code on the Product Instance (which removes the Authorization Code) and then enter the Reservation Return code into Cisco Smart Software Manager.
- **Product Instance is not operational (failure/RMA or due to destruction of VM/container)**: User should contact TAC, who can remove the Product Instance from your smart account.

Note You can only use the CLI configuration to enable Specific License Reservation.

Figure 3: Remove a Product Instance - Emergency Responder


1
Product Instance is Operational
User (Customer)
2
Product Instance is NOT Operational
User (Customer)
Product Instance
CSSM
User generates a Reservation Return Code from the Product Instance.
User starts the Remove process from the Product Instances tab
User enters the Reservation Return Code in CSSM.
User Removes Product Instance
User has to call TAC to remove the Product Instance from the Smart Account.
Cisco Worldwide Contacts (TAC)
393984

Customer entitled to License reservation feature on their Smart Account can reserve licenses from their virtual account, tie them to a devices UDI and use their device with these reserved licenses in a disconnected mode. The customer reserves specific licenses and counts for a UDI from their virtual account. The following options describe the new functionality and design elements for Specific License Reservation:

- license smart reservation enable
- license smart reservation disable

- license smart reservation request
- license smart reservation cancel
- license smart reservation install "<authorization-code>"
- license smart reservation return
- license smart reservation return-authorization "<authorization-code>"

Upgrading Specific License Reservation Enabled System to Version 14 or Later

Important Applicable from Release 14SU1 onwards.

If you are upgrading the 12.5 Emergency Responder system which is enabled for license reservation to version 14 or later, following are the scenarios need to be considered:

1. Before upgrade to version 14 or later, return the 12.x licenses using "license smart reservation return" command (Recommended).

   OR

   After upgrade to version 14 or later, return the 12.x licenses using "license smart reservation return" command.

2. Create request code using the "license smart reservation request" command. Generate authorization code with version less licenses in Cisco Smart Software Manager.

3. Install the authorization code using "license smart reservation install <auth-code>" command in Cisco Emergency Responder.

Permanent License Reservation

Cisco Emergency Responder Release 14SU1 and later provides Permanent License Reservation that allows Administrator to reserve an entitled Permanent License Tag from the Smart Account and Virtual Account against a Product instance. Administrators must provision the User Licenses as needed by the Product instance in the Smart Account and Virtual Account.

The feature is limited to FedRAMP customers. Permanent License Tag can be ordered through Cisco Commerce Workspace and is provisioned in the Smart Account and Virtual Account after Cisco approval. For ordering, see the Cisco Collaboration Flex Plan 3.0 for FedRAMP Ordering Guide available at https://www.cisco.com/c/en/us/products/collateral/unified-communications/cisco-collaboration-flex-plan/guide-c07-744596.html.

Reserving Permanent License Tag would also prompt the administrator to specify the License count the system would operate within. These can be referred on the License Management user interface and doesn't affect compliance. The administrator must have those many User Licenses provisioned in the Smart Account and Virtual Account.

Configuring Permanent License Reservation

The CLI commands available for License reservation can be used for reserving Permanent License Tag. See Specific License Reservation, on page 19.

- license smart reservation set license_count—Use this command to specify or update the license count for the system to operate within when set for Permanent License Reservation. License count set doesn't affect compliance status and is for Administrator reference only. License count set can be referred on the License Management screen.

For more information on the License reservation CLI commands, see the Command Line Interface Reference Guide for Cisco Unified Communications Solutions Release 14.

Upgrading Permanent License Reservation Enabled System to Version 15

If you are upgrading the 14 SU2 and above Emergency Responder systems which is enabled for Permanent License Reservation (PLR) to version 15, consider the following scenarios:

1. Before upgrade to version 15, return the license using the "license smart reservation return" command.
2. After upgrade, create request code using the "license smart reservation request" command. Generate authorization code with PLR license in Cisco Smart Software Manager.
3. Install the authorization code using "license smart reservation install <auth-code>" command in Emergency Responder.

Version Independent Licensing

From Release 14 onwards, Emergency Responder supports Version Independent User Licenses. The Licenses are annuity-style and issued for the subscription term. You can order these licenses through Flex EA (Enterprise Agreement) or Flex NU (Named User—Professional, Enhanced, Access). For more information, see the Ordering Guide.

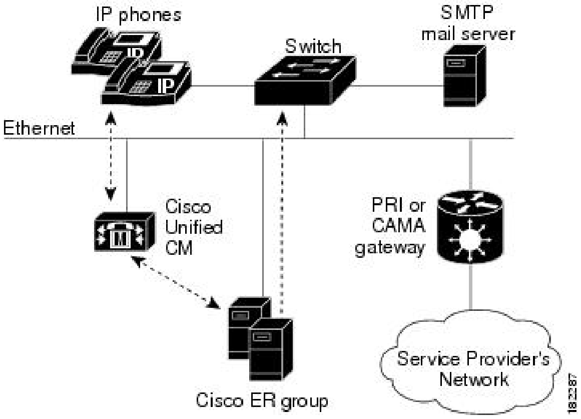
Emergency Responder continues to use the version 12.X License.

The licenses are managed on CSSM (Cisco Smart Software Manager). For more information, see the Cisco Smart Software Licensing , on page 10 section.

Emergency Responder and Your Network

The following figure shows how CiscoEmergencyResponder (Emergency Responder) fits into your network.

Figure 4: How Cisco Emergency Responder Fits Into Your Network



Emergency Responder depends on CiscoUnifiedCommunications Manager (Cisco Unified CM) for the corporate dial plan, which you must modify to send emergency calls to the Emergency Responder group.

To track phones, Emergency Responder queries Cisco Unified CM for a list of phones registered with the cluster. Emergency Responder then queries the switches on the network to determine the port used by the phones. Emergency Responder performs this operation at regular intervals throughout the day to identify phones that have changed location. See the Emergency Responder Switch Configuration , on page 148 for more information about setting up switches for Emergency Responder. See Phone Management , on page 159 for information about configuring switch ports so that Emergency Responder can send emergency calls to the correct PSAP based on port and phone location.

Note If you locate your Cisco IP Phones using a Cisco Layer 2 protocol with connected switch port discovery, then you must map and control your wiring plan. If you do not document changes in your wiring, Emergency Responder may not be able to locate a phone in your network. Update your wiring plan and your Emergency Responder configuration every time you change your wiring.

You can also have an SMTP email server in your network or with a service provider. You can then configure Emergency Responder to send an email to your onsite security personnel when an emergency call occurs. If the server is set up as an email-based paging service, the personnel are paged.

You also need a gateway with a PRI or CAMA link to the service provider's network so that Emergency Responder can route emergency calls to the local public safety answering point (PSAP).

Figure 1 shows one Emergency Responder group supporting a single CiscoUnifiedCommunicationsManager cluster. You can support more than one CiscoUnifiedCommunications Manager cluster with a single Emergency Responder group as long as the Unified CMs are running the same software version. With a larger network, you can install multiple Emergency Responder groups and create a Emergency Responder cluster.

See Emergency Call Process , on page 26 for an explanation of the path an emergency call takes when managed by Emergency Responder.

Related Topics

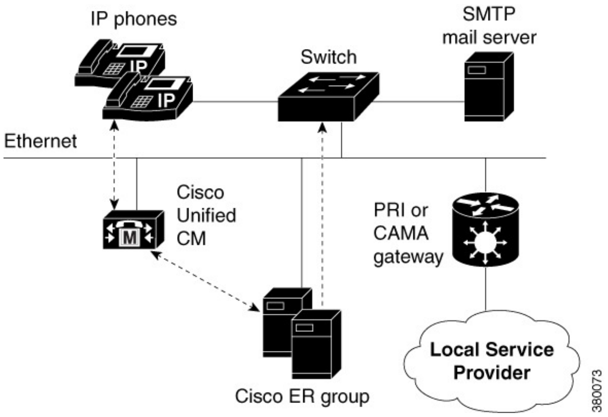
Determine Required Cisco Emergency Responder Groups , on page 33
Emergency Responder Deployment , on page 39

Emergency Responder and Your Local Service Provider

The following figure shows how Cisco Emergency Responder (Emergency Responder) interacts with your local service provider.

Figure 5: Cisco Emergency Responder and a Local Service Provider , on page 24 shows how Cisco Emergency Responder in your network interacts with local service provider. You need to have PRI/CAMA Gateway to send the Calling Party Number to your local service provider.

Figure 5: Cisco Emergency Responder and a Local Service Provider



For more details on PRI/CAMA, see CAMA and PRI Trunks , on page 36.

Instead of a local service provider, you can connect to a SIP Trunk service provider as shown in Figure 6: Cisco Emergency Responder and a SIP Trunk Service Provider , on page 24 or a dedicated National Emergency Call Delivery Service such as National E911 Service Provider as shown in Figure 7: Cisco Emergency Responder and National E911 Service Provider , on page 25.

Figure 6: Cisco Emergency Responder and a SIP Trunk Service Provider

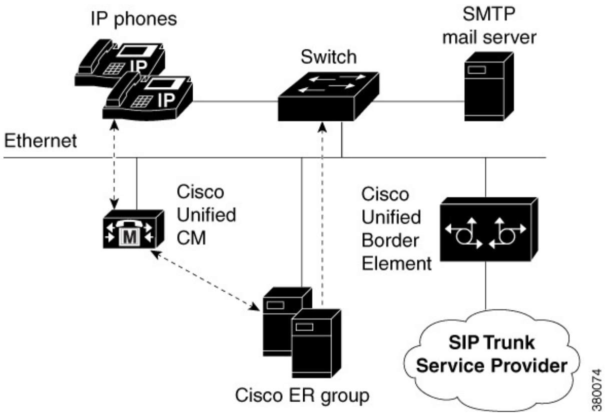


Figure 7: Cisco Emergency Responder and National E911 Service Provider

For more information on Cisco Unified Border Element, see Cisco Unified Border Element product page on Cisco.com.

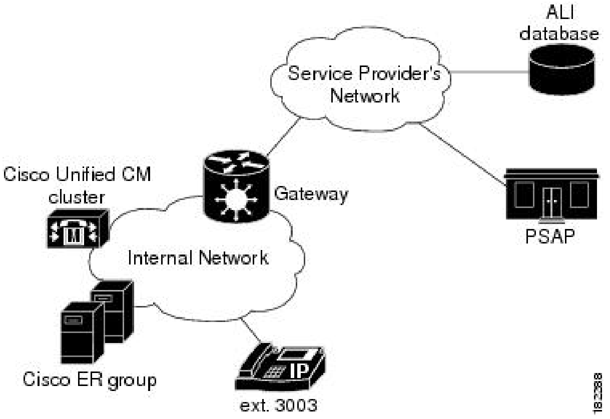
For more information on National E911 Service Provider, see Configure Emergency Responder and National E911 Service Provider Enterprise Services , on page 183.

Emergency Call Process

This topic describes the process that CiscoEmergencyResponder (Emergency Responder) uses to handle emergency calls. Understanding this process can help you set up Emergency Responder correctly and troubleshoot problems that you might encounter.

The following figure illustrates how Emergency Responder routes an emergency call.

Figure 8: How Cisco Emergency Responder Routes Emergency Calls



When someone uses extension 3003 to make an emergency call:

1. CiscoUnifiedCommunications Manager routes the call to Emergency Responder.
2. Emergency Responder gets the route pattern configured for the emergency response location (ERL) of the caller. See Call Routing Order , on page 27 for information about the order of call routing.
3. Emergency Responder converts the calling party number to the route pattern configured for the caller's ERL. This route pattern is configured to pass the appropriate emergency location identification number (ELIN) to the public safety answering point (PSAP). The ELIN is a telephone number that the PSAP can use to call back the emergency caller.
4. Emergency Responder saves a mapping between the caller's extension and the ELIN, by default, for up to three hours. The mapping might be overwritten by subsequent calls before the entry times out. You can also configure the time-out to be longer or shorter than three hours.
5. Emergency Responder routes the call using the route pattern configured for the caller's ERL. This route pattern in turn uses the configured route list to send the emergency call to the appropriate service provider's network. The service provider looks up the ELIN in the automatic location information (ALI) database, and routes the call to the appropriate local PSAP. The PSAP receives the phone call and looks up the ALI in the ALI database.
6. Concurrently, Emergency Responder sends web alerts to the Emergency Responder user. In addition, Emergency Responder calls the onsite alert (security) personnel assigned to the ERL. If you configure an

email address for the personnel, Emergency Responder also sends an email. If the address is for an email-based paging service, the personnel get pages instead of emails.

7. If an emergency call is cut off unexpectedly, the PSAP can call back the emergency caller using the ELIN. The call to the ELIN is routed to Emergency Responder, and Emergency Responder converts the ELIN to the last cached extension associated with the ELIN. The call is then routed to the extension.

To ensure proper performance and eliminate major points of failure, verify the following:

- For the emergency call to be routed correctly, the caller's phone must be assigned to the correct ERL. To check the correctness of the ERL associated with the phones, use the ERL debug tool.
- Another potential problem in not routing the call correctly relates to the ELIN definition. If you assign the ELINs route pattern to the wrong gateway, the emergency call can be routed to the wrong network and the PSAP can receive the wrong emergency call.

  Work with your service provider to determine how many gateways you need and where to connect them. These requirements are based on the service provider's network topology more than on your network's topology. In the United States, connecting to the PSTN does not ensure the correct routing of emergency calls.
- The call might be routed incorrectly in the service provider's network if the information in the ALI database is incorrect. Ensure that you export your ALI data and submit it to the service provider, and resubmit it whenever you change ELIN or location information.
- The PSAP might not be able to successfully call back an emergency caller if a lot of emergency calls are made from an ERL. Emergency Responder caches the ELIN-to-extension mapping for up to three hours. If you have two ELINs defined for an ERL, and three emergency calls are made in a three-hour window, the first ELIN is used twice: once for the first caller, then reused for the third caller. If the PSAP calls the first ELIN, the PSAP reaches the third caller, not the first caller. The likelihood of this problem arising depends on how many ELINs that you define for an ERL and the typical rate of emergency calls in the ERL.

Call Routing Order

Emergency Responder directs emergency calls based on the location of the phone from which the call is placed. The location of the phone is determined by the following methods, in order of precedence:

- Synthetic phones—The MAC address of the phone matches that of a synthetic phone and is assigned to a test Emergency Response Location (ERL). See Synthetic Phones , on page 172 and Set Up Test ERLs , on page 144.
- IP Phones tracked behind a switch port—The MAC address of the IP Phone is tracked behind a switch port assigned to an ERL. See Switch Port Configuration , on page 159.
- Access Point based tracking—Allows Cisco Emergency Responder to track the Wireless IP Phones and Soft-clients (like Cisco Jabber) behind Wireless Access Points and provides ERL treatment.
- IP Phones tracked using IP subnet—The IP address of an IP Phone belongs to an IP subnet assigned to an ERL.
- IP Phones tracked by another (remote) Emergency Responder server group in the same Emergency Responder cluster—The remote server group tracks an IP Phone behind a switch port or by IP subnet. When an emergency call is received, it is forwarded to the Cisco Unified Communications Manager cluster served by the remote Emergency Responder server group.

- Manually configured phones—The line number of the phone is manually assigned to an ERL. See Manually Define Phones , on page 168.
- Unlocated Phones—The MAC address of an IP Phone is assigned to an ERL. See Identify Unlocated Phones , on page 167.
- Default ERL—None of the preceding criteria is used to determine the phone location. The call is routed to the default ERL. See Set Up Default ERL , on page 138.

Note MAC or IP address tracking is recommended for Cisco Unified IP Phones. IP Phones that are not tracked by MAC or IP address appear as unlocated phones, even if they are assigned a location by manual line number configuration.

Note Manually configured phones can be assigned a location by Emergency Responder based on a line number that includes a leading "+". If you want Emergency Responder to assign locations to analog telephones based on line number, you can configure them with a leading "+" on Unified CM.

Customers should resolve problems that prevent IP Phones from being tracked by MAC or IP address (see Unlocated Phones , on page 324) so that IP Phones are not removed from the Unlocated Phones page. An ERL may be assigned directly to an IP Phone on the Unlocated Phones page, but this assignment does not take effect if the phone is assigned a location by manual line number configuration. Use the ERL Debug Tool to determine the ERL assignment in effect for an IP Phone that appears on the Unlocated Phones page.

Identifying Unlocated Phones

Emergency Responder defines unlocated phones as those Cisco Unified IP Phones that meet all of the following criteria:

- The IP Phone is registered to a Cisco Unified CommunicationsManager known to the Emergency Responder group.
- The MAC address of the IP Phone is not tracked behind a switch port.
- The IP address of the IP Phone is not tracked using IP subnets.
- The MAC address of the IP Phone is not defined as a synthetic phone in Emergency Responder.

Note CiscoUnified IP Phones tracked by a remote Emergency Responder server group and IP Phones having line numbers manually assigned to an ERL also appear in the Unlocated Phones screen.

Assigning ERLs to Unlocated Phones

Emergency Responder provides a procedure to assign an ERL to IP Phones that are displayed on the Unlocated Phones screen. This assignment associates the MAC address of the unlocated phone with an ERL that is selected by the administrator. These rules apply to this association:

- The association of an ERL with an IP Phone on the Unlocated Phones page does not change the status of the IP Phone; it remains on the Unlocated Phones page because the IP Phone continues to match the criteria for unlocated phones described previously.

- The ERL association is used only when the IP Phone is unlocated, as determined by Emergency Responder, using the preceding rule.

For example, Phone A is currently unlocated and appears on the Unlocated Phones page. Using the ERL assignment feature for unlocated phones, Location A is assigned as the ERL for this phone. A subsequent phone tracking cycle finds Phone A behind a switch port and it no longer appears in the Unlocated Phones page. The Phone A-to-Location-A assignment is no longer valid. Because the association is persistent, if the IP Phone is unlocated at any future time, the assignment is valid.

CTI Application Call Forwarding

If emergency calls are forwarded to 911 by computer telephony integration (CTI) applications, such as CiscoUnity, then the location used for call routing and PSAP reporting is the location of the application server, not the location of the original caller. This situation occurs even if the application retains the original calling line number. For this reason, you should dial 911 directly.

Related Topics

E911 and Cisco Emergency Responder Terminology , on page 6
Data Integrity and Reliability, on page 34
ERLs, on page 135
ELIN Numbers Emergency Calls and PSAP Callbacks , on page 93
Set Up Calling Search Space for Gateway and PSAP Connection , on page 100
Network Preparations , on page 36

Cisco Emergency Responder Groups

Deploy Cisco Emergency Responder (Emergency Responder) in your network as a pair of redundant servers. One server is designated as the Publisher server and the other as the Subscriber server. Each Emergency Responder Publisher server and Subscriber server make up an Emergency Responder Server Group.

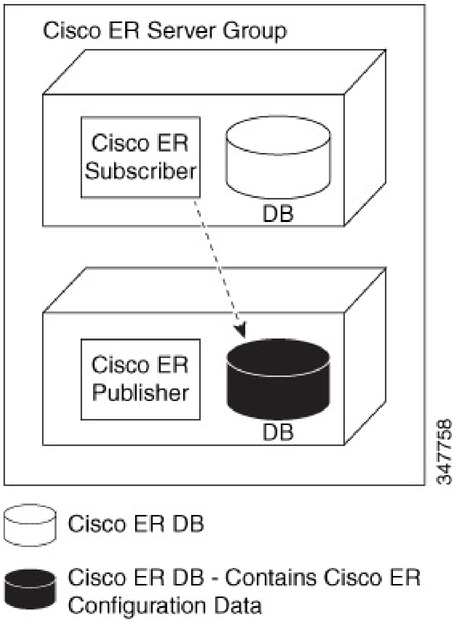
Configuration data for the server groups is stored in a database on the Publisher. This data is replicated to the Subscriber.

Note Be aware of the following when planning your Emergency Responder system:

- A single Emergency Responder group cannot support clusters with a mix of CiscoUnifiedCommunicationsManager versions.
- An Emergency Responder cluster can contain Emergency Responder groups that support different versions of CiscoUnifiedCommunicationsManager. In this way, Emergency Responder can support a mix of CiscoUnifiedCommunicationsManager versions in your telephony network.

The following figure shows an Emergency Responder Server Group.

Figure 9: Cisco Emergency Responder Server Group



Cisco Emergency Responder Clusters

An Emergency Responder cluster is a set of Emergency Responder server groups that share data to provide correct emergency call-handling capabilities. Emergency Responder cluster information is stored in a central location in the cluster called the cluster database. An Emergency Responder server group is considered part of a cluster when the group points to the same cluster database as the other server groups in that cluster.

Emergency Responder uses two separate databases:

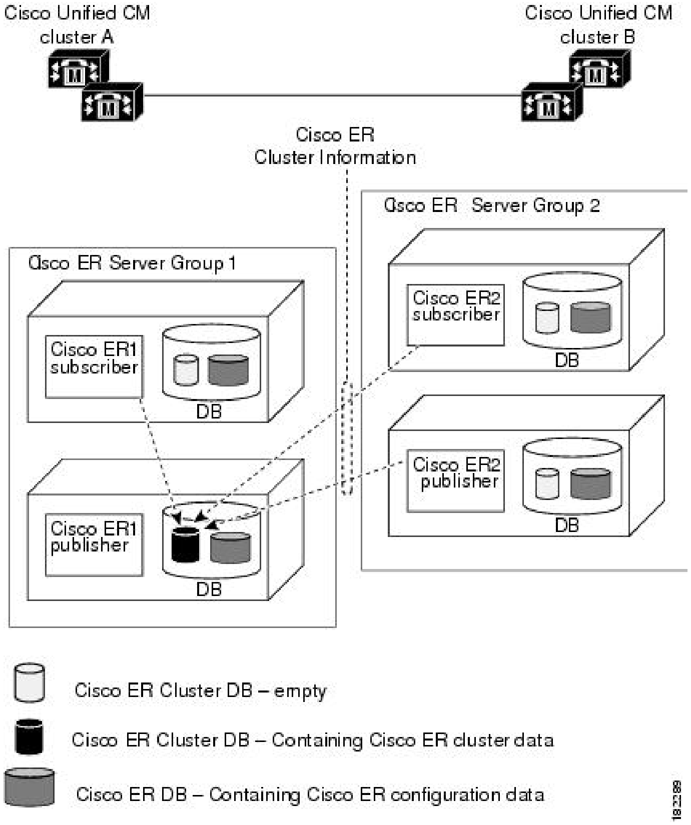
- A database that stores Emergency Responder configuration information.
- A database that stores Emergency Responder cluster information.

During installation, both databases are created on each Emergency Responder server. However, only one Emergency Responder server contains cluster data.

Note You cannot deploy different versions of Emergency Responder in the same Emergency Responder group. If you are upgrading to the latest version of Emergency Responder, make sure to upgrade both Emergency Responder servers to the same version. If phones registered with Unified CM are configured with EnergyWise Power Save Plus mode, then all the Emergency Responder Server Groups in a cluster need to be Emergency Responder Release 8.6 or later because earlier versions of Emergency Responder do not support EnergyWise. Major discovery in Emergency Responder Release 8.6 or later does not purge phones that are in EnergyWise Power Save Plus mode.

The following figure shows how CiscoEmergencyResponder (Emergency Responder) groups can be joined in a single Emergency Responder cluster.

Figure 10: Understanding the Relationship Between Cisco Emergency Responder Groups and CiscoEmergency Responder Clusters



In this example:

- There are two CiscoUnifiedCommunicationsManager clusters, Unified CMclusterA and Unified CMclusterB.
- Emergency Responder Server Group 1 and Emergency ResponderServer Group 2 form a single Emergency Responder cluster.
- Emergency Responder Server Group 1 supports Unified CMclusterA and Emergency Responder Server Group 2 supports Unified CMclusterB.
- CiscoER1 Publisher cluster database stores the Emergency Responder cluster information for both Emergency Responder server groups. Dotted lines show the Emergency Responder servers communications with the cluster database host.
- Each Emergency Responder server has a database containing the Emergency Responder configuration information.

Note For Emergency Responder intra-cluster phone tracking to work accurately, a Emergency Responder server in the cluster must be able to be found by its hostname and must be able to be reached on the network from all other Emergency Responder servers.

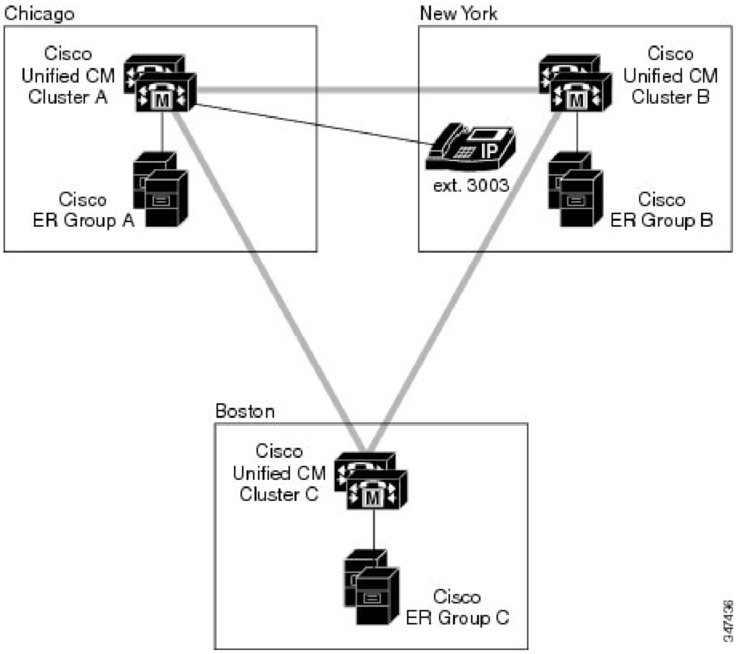
Note If you enter the system administrator email account in the System Administrator Mail ID field when you configure the Emergency Responder Server Group Settings, the system administrator receives an email notification when the standby server handles a call or when the standby server takes over for the primary server.

To complete the creation of the Emergency Responder cluster, you must navigate to the Cisco Unified CM and create inter-cluster trunks and route patterns to allow the Emergency Responder groups to hand off emergency calls between the groups and configure these route patterns in Emergency Responder.

Caution Before you create a Emergency Responder cluster, be aware that the dial plans in all CiscoUnifiedCommunicationsManager clusters supported by the Emergency Responder cluster must be unique. For example, extension 2002 can only be defined in one CiscoUnifiedCommunicationsManager cluster. With overlapping dial plans, you must have separate Emergency Responder clusters and you cannot support dynamic phone movement between those CiscoUnifiedCommunicationsManager clusters.

Track Phone Movement Across a Cluster

The following scenario illustrates how Emergency Responder clusters work and how Emergency Responder responds to phones moving between clusters:



- Cisco ER Group A has a phone (ext 3003) that is moving out to Cisco ER Group B.
  - Cisco ER Group A discovers 3003 in Cisco ER Group B.
  - The Unlocated Phones page in Cisco ER Group A display the phone in Cisco ER Group B.

  - Calls made from 3003 during this time are redirected to Cisco ER Group B and Cisco ER Group B takes the necessary steps to route this call.

- If both the Emergency Responder servers (Publisher and Subscriber) in Cisco ER Group B go down, Cisco ER Group A still displays 3003 in Cisco ER Group B.
  - Calls made from 3003 receive default Treatment as configured on Cisco UCM Cluster B.
- If 3003 moves to Cisco ER Group C:
  - It is discovered after the next incremental phone tracking on Cisco ER Group A and then in Cisco ER Group C.
  - The Unlocated Phones page changes the association of 3003 to Cisco ER Group C.
  - Calls made from 3003 during this time are redirected to Cisco ER Group C and Cisco ER Group C takes the necessary steps to route this call.
- If 3003 moves back to Cisco ER Group A:
  - It is discovered in the next incremental phone tracking and displayed under the corresponding switch port or IP subnet.
  - Calls made from 3003 during this time receive treatment from Cisco ER Group A.

Note If you make an emergency call from a Cisco Unified IP Phone using a shared line, the call may terminate on an incorrect ERL across the cluster.

Note Moving of phones discovered and associated with an ERL to a different Unified CM cluster, and tracked by a different Emergency Responder Server Group belonging to the same Emergency Responder cluster, requires the deletion of the ERLs association from the current Emergency Responder Server Group. See Step 7 of Identify Unlocated Phones , on page 167 to unassign an ERL from the current Emergency Responder Server Group.

Determine Required Cisco Emergency Responder Groups

To ensure efficient Emergency Responder performance, determine the limits that each Emergency Responder group can support when planning your Emergency Responder deployment. A single CiscoUnifiedCommunicationsManager cluster can only be supported by one Emergency Responder group, although a single Emergency Responder group can support more than one CiscoUnifiedCommunicationsManager cluster.

See the latest version of the Release Notes for Cisco Emergency Responder for the capacities of a single Emergency Responder group with your configuration. Be aware that you might meet the maximum figures for one limitation without reaching the figures for another. For example, you might define 1,000 switches, but have fewer than 30,000 switch ports.

You can install additional groups to manage larger networks. Each Emergency Responder group can work with one or more Cisco UnifiedCommunicationsManager clusters.

In addition to these per-group limits, you must also consider the territories covered by the service provider's ALI database providers. If your network extends into more than one ALI database provider's territory, you should use the ALI Formatting Tool (AFT) to export ALI records in multiple ALI database formats.

To have a single Emergency Responder group support multiple LECs, follow these steps:

Procedure

Step 1 Obtain an ALI record file output from Emergency Responder in standard NENA format. This file contains the records destined for multiple LECs.

Step 2 Make a copy of the original file for each required ALI format (one copy per LEC).

Step 3 Using the AFT of the first LEC (for example, LEC-A), load a copy of the NENA-formatted file and delete the records of all the ELINs associated with the other LECs. (For information about using the AFT, see ALI Formatting Tool, on page 315) The information to delete can usually be identified by NPA (or area code).

Step 4 Save the resulting file in the required ALI format for LEC-A, and name the file accordingly.

Step 5 Repeat steps 3 and 4 for each LEC.

If AFTs are not available for each LEC, you can achieve a similar result by editing the NENA-formatted files with a text editor.

Related Topics

Emergency Responder Deployment , on page 39
ALI Submission and Service Provider Requirements , on page 37
Export ALI Information for Submission to Your Service Provider , on page 147
ALI Formatting Tool, on page 315
ALI Formatting Tool, on page 484

Data Integrity and Reliability

The correct routing of emergency calls to the local PSAP is based on your ERL configuration. Inside your network, correct identification of the ERL for a phone determines which gateway is used to connect to the service provider's network. In the service provider's network, the routing is based on the ELIN, which is also used to look up the ALI for the caller. Your ERL configuration must be reliable so that the correct ELIN is assigned to the emergency call.

The following information will help you to maintain the reliability of your ERL configuration:

- ERLs are assigned to switch ports based on the location of the device attached to the port, not the location of the port itself. If you change the wire plugged into a port (for example, by switching wires between two or more ports), there is the potential that the device now plugged into the port is actually in a different ERL. If you do not change the ERL assigned to the port, the incorrect ELIN is used for the port, and the wrong ALI is sent to the PSAP.

  This type of change does not normally result in an incorrectly routed call, because it is unlikely that a single LAN switch connects to ERLs serviced by separate PSAPs. However, the ALI sent will be incorrect, with the possibility that your security staff will search the third floor for an emergency when the caller is actually on the fourth floor.

To prevent this problem, ensure that your wiring closets are secure, and train your networking staff to avoid swapping wires between switch ports.

- With phones that Emergency Responder cannot automatically track, you ensure that any moves, adds, or changes to these phones also result in an update to the Emergency Responder configuration. See Manually Define Phones , on page 168 for information about defining these types of phones.

Note If the switch port mapping changes, an email alert is sent.

- Before Emergency Responder1.2, if registered phones were not located behind a switch port, Emergency Responder would list the phone in the Unlocated Phones page.

  Emergency Responder1.2 and later locates these phones as follows:

  - If a registered phone is not located behind a switch port, it may be located in one of the configured IP subnets.
  - If a registered phone is not behind a switch port, or the IP subnet of the phone is not configured, or the phone is not configured as a synthetic phone, Emergency Responder lists the phone in the Unlocated Phones page.

    To determine the ERL that Emergency Responder will use for call routing, use the ERL Debug Tool to search for the phone. The search yields the current ERL used in routing the emergency call from this phone and why Emergency Responder chose that ERL. For more information, see Emergency Responder Admin Utility, on page 345.

- When you install Emergency Responder, you install a Publisher server (primary) and a Subscriber server (backup) that points to the Publisher. The Publisher server and the Subscriber server make up a Cisco Emergency Responder Server Group. This redundancy helps to ensure that the failure of one server does not affect the ability to make emergency calls. Consider installing the standby server in a physically separate location from the primary server, and on a separate subnet. This separation can protect against some types of disruption, for example, a fire in the building housing the primary server, or the loss of connectivity to the subnet hosting the primary server.

- Ensure that the Emergency Responder configuration is regularly updated as switches are added, removed, or upgraded (for example, by adding or changing modules). When you change a switch, run the switch-port and phone update process on the switch by viewing the switch in Emergency Responder and clicking **Locate Switch Ports**. See LAN Switch Identification , on page 153 for more information.

  Phones connected to undefined switches are listed as unlocated phones in Emergency Responder. If you changed a defined switch, new or changed ports become ports without an ERL association. You should assign ERLs for the new or changed switch ports. See Emergency Responder Network Administrator Role , on page 311 and Emergency Responder ERL Administrator Role , on page 310 for information about the recurring tasks involved in network changes.

- As you change your ERL/ALI configuration, you must export the information and send it to your service provider for inclusion in the ALI database. This ensures that emergency calls are routed to the correct PSAP, and that the PSAP is presented with the correct ALI. See Export ERL Information , on page 146 and Export ALI Information for Submission to Your Service Provider , on page 147 for more information.

Related Topics

Emergency Call Process , on page 26

Determine Required Cisco Emergency Responder Groups , on page 33
Cisco Emergency Responder User Preparation , on page 309

Network Preparations

The information in the following topics describe the steps you should take to prepare your network before deploying CiscoEmergencyResponder.

CAMA and PRI Trunks

To handle emergency calls, you must obtain PRI or CAMA trunks to connect to your service provider. Your service provider might support only one type of trunk. You should consult with your service provider and decide on the type of connection that works best for you.

Consider these issues:

- PRI—If you use a PRI connection for emergency calls, you can share the connection with regular telephone traffic. If you use the trunk for regular traffic, monitor trunk usage to ensure that there is sufficient available bandwidth to handle emergency calls. If your capacity is inadequate, an emergency caller might get a busy signal when trying to make the call. Ensure that you do capacity planning based on emergency call requirements.

  When you configure the PRI trunk, you must configure it so that it sends the actual calling-party number rather than a generic number (such as the main number of the site). Otherwise, the PSAP does not receive the expected ELIN, and the emergency call might not be routed to the right PSAP.

- CAMA—CAMA trunks are dedicated to emergency calls, and are available in most areas. You do not need to do capacity planning for CAMA trunks, because they are never used by regular voice traffic.

Work with your service provider to determine how many trunks are required for your network. For example, some service providers use a guideline of two CAMA trunks for 10,000 phones.

Also, the number of trunks can differ depending on the distribution of your offices with respect to the local PSAPs. For example, with offices in New York and Chicago, you would need trunks in both cities, even if your total number of telephones would require fewer trunks if your office was only in New York. Your service provider, who knows the layout of the emergency call network, can direct you on trunk requirements that are based on PSAP accessibility.

Related Topics

Set Up Calling Search Space for Gateway and PSAP Connection , on page 100

DID Service Provider Numbers

You must obtain direct inward dial (DID) numbers from your service provider for use as emergency location identification numbers (ELIN) for your emergency response locations (ERL).

In general, you must have at least one unique number per ERL. Emergency calls are routed to the local PSAP based on the ELIN of the ERL, so if you do not have unique ELINs, the call cannot be routed properly. The ALI database provider also might not accept ALIs that include duplicate ELINs.

You might want more than one ELIN per ERL. If your ERLs include more than one phone, you might have more than one emergency call made from an ERL in a short time (less than three hours). If you assign only one ELIN to the ERL, that ELIN is reused for each emergency call. For example, if four people make emergency calls within an hour, and if the PSAP calls the ELIN, the PSAP connects to the last caller. This situation might be a problem if the PSAP was trying to contact one of the earlier callers.

If you define more than one ELIN per ERL, Emergency Responder uses those ELINs in sequence until all are used, then reuses the ELINs in order. Emergency Responder maintains the link between the ELIN and the extension of the actual emergency caller for up to three hours.

Because you must purchase these DIDs from your service provider, you must balance the needs of your budget with the needs of maintaining the capability of the PSAP to reach the correct caller.

Note The number of DIDs you obtain is not related to the number of emergency calls Emergency Responder can handle. Because Emergency Responder reuses the ELINs that you define, every emergency call gets handled and routed to the correct PSAP. The number of ELINs only influences the success rate of the PSAP calling back the desired emergency caller.

Related Topics

ELIN Numbers Emergency Calls and PSAP Callbacks , on page 93

ERL Creation , on page 138

ALI Submission and Service Provider Requirements

Emergency calls are routed to the appropriate PSAP based on the emergency location identification number (ELIN) of the emergency caller. To route the call, the telephony network must have your automatic location information (ALI) that maps these ELINs to a location. Besides routing the call appropriately, the ALI database also supplies the location information that appears on the PSAPs screens to help them locate the caller.

Emergency Responder includes features to create ALIs and to export them in a variety of formats that should be acceptable to your service provider. After you create your ERL/ALI configuration, you must export the ALI data and send it to the ALI database provider.

How you send the data can vary from location to location or service provider to service provider. You must work with your service provider to determine the services you can select for submitting ALI data. At a minimum, you must know the data format they expect, and the transmission method they require.

Emergency Responder does not include automated capability for submitting ALIs.

Tip Before deploying Emergency Responder throughout your network, test the ALI submission process with your service provider. With your service provider's help, test that the PSAP can successfully call back into your network using the ALI data. Each service provider and ALI database provider has slightly different rules concerning ALI information. Emergency Responder allows you to create ALI data according to the general NENA standards, but your service provider or database provider has stricter rules.

Related Topics

ERLs, on page 135

ERL Management , on page 136

ERL Creation , on page 138

Export ERL Information , on page 146

Switch and Phone Upgrades

The most powerful capability of Emergency Responder is the ability to automatically track the addition or movement of telephones in your network. This dynamic capability helps ensure that emergency calls are routed to the local PSAP, even if a user moves a phone between cities. By automatically tracking phones, you can reduce the cost of maintaining your telephone network, and simplify moves, adds, or changes.

However, Emergency Responder only can automatically track telephone movement for certain types of phones, and for phones attached to certain types of switch ports. See Network Hardware and Software Requirements , on page 10 for a list of these phones and switches.

To achieve full automation, update your switches to supported models or software versions, and replace your telephones with supported models.

Related Topics

Emergency Responder Switch Configuration , on page 148
Phone Management , on page 159

Preparing Your Staff for Emergency Responder

Emergency Responder does not replace your existing emergency procedures. Instead, Emergency Responder is a tool you can use to augment those procedures. Before deploying Emergency Responder, consider how it fits into your procedures and how you want to use the Emergency Responder system's capabilities.

These are the main things to consider when deciding how to use Emergency Responder:

- When someone makes an emergency call, Emergency Responder notifies the assigned onsite alert (security) personnel (your emergency response teams) of the location of the caller. This information is, for the most part, the ERL name. Consider working with your emergency response teams to come up with an ERL naming strategy that helps them respond quickly to emergencies. Incorporating building names, floor numbers, and other readily understood location information in the name are the types of factors to consider.
- Emergency Responder lets you define three types of administrative user, so you can divide responsibilities for overall Emergency Responder system administration, network administration, and ERL administration. The skills and knowledge necessary for these tasks might be rare to find in one person. Consider dividing Emergency Responder configuration responsibilities according to these skills.
- The routing of emergency calls, and the transmission of the correct ALI, is only as good as the reliability of the ALI definitions you submit to your service provider and in the stability of your network topology. Ensure that your ERL administrator understands the importance of keeping the ALI data up-to-date, and that your network administrator understands the importance of maintaining a stable network. See Data Integrity and Reliability, on page 34 for more information about maintaining data integrity.

Related Topics

Emergency Responder Onsite Alert Personnel Preparations, on page 309
Emergency Responder ERL Administrator Role , on page 310
Emergency Responder Network Administrator Role , on page 311
Emergency Responder System Administrator Role , on page 312

Emergency Responder Deployment

The information in the following sections describe deployment models for various types of networks. You can use these examples as modules, combining them to form a larger, more complex network.

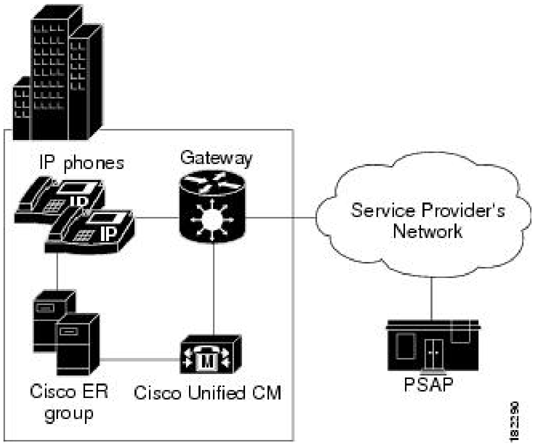
Deployment in Main Site and PSAP

To support a simple telephony network consisting of a single CiscoUnifiedCommunicationsManager cluster, install two Emergency Responder servers and configure one server as the Publisher and the other server as a Subscriber pointing to the Publisher.

Because there is only one local PSAP, you only need one gateway to the service provider's network, although capacity planning for your telephony network might require more than one gateway. Configure all route patterns to use this gateway.

The following figure shows how Emergency Responder fits into a simple telephony network with a single CiscoUnifiedCommunicationsManager cluster.

Figure 11: Deploying Cisco Emergency Responder in One Main Site with One PSAP



See these examples to extend this example to more complex networks:

- Deployment in Main Site with Two or More PSAPs, on page 40
- Deployment in Main Site with Satellite Offices , on page 41
- Deployment in Main Site Serving Multiple Sites , on page 42
- Two Main Site Deployments , on page 44

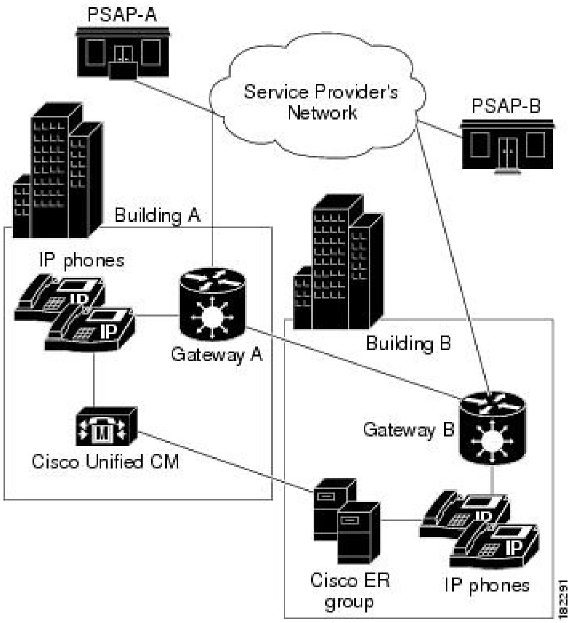
Related Topics

Emergency Call Process , on page 26
Emergency Responder and Your Network , on page 22
Determine Required Cisco Emergency Responder Groups , on page 33
Installation on a New System , on page 63
Configure Cisco Unified Communications Manager, on page 83

Deployment in Main Site with Two or More PSAPs

The following figure illustrates the Emergency Responder configuration with one main site that is served by two or more PSAPs. This example assumes you have one CiscoUnifiedCommunicationsManager cluster. If you have more than one, the setup is logically the same as the one discussed in the Two Main Site Deployments , on page 44.

Figure 12: Deploying Cisco Emergency Responder in One Main Site with Two or More PSAPs



To support this type of network, install two Emergency Responder servers and configure one server as the Publisher and the other server as a Subscriber pointing to the Publisher.

Because there are two PSAPs serving the location, you probably need more than one gateway connecting to different parts of the service provider's network. However, this depends on the layout of the service provider's network: you might only need one gateway if the PSAPs are served by a selective router that can intelligently route emergency calls to more than one PSAP. Consult with your service provider to determine the requirements for your buildings. In this example, we assume that you need two gateways; capacity planning for your telephony network might require more than one gateway for each link.

After setting up the gateways to correctly connect to the service provider's network, configure all route patterns used in Building A ERLs to use gateway A, and all route patterns used in Building B ERLs to use gateway B. As phones move between buildings, Emergency Responder dynamically updates their ERLs so that emergency calls get routed out of the desired gateway.

See these examples to extend this example to other networks:

- Deployment in Main Site and PSAP , on page 39
- Deployment in Main Site with Satellite Offices , on page 41
- Deployment in Main Site Serving Multiple Sites , on page 42
- Two Main Site Deployments , on page 44

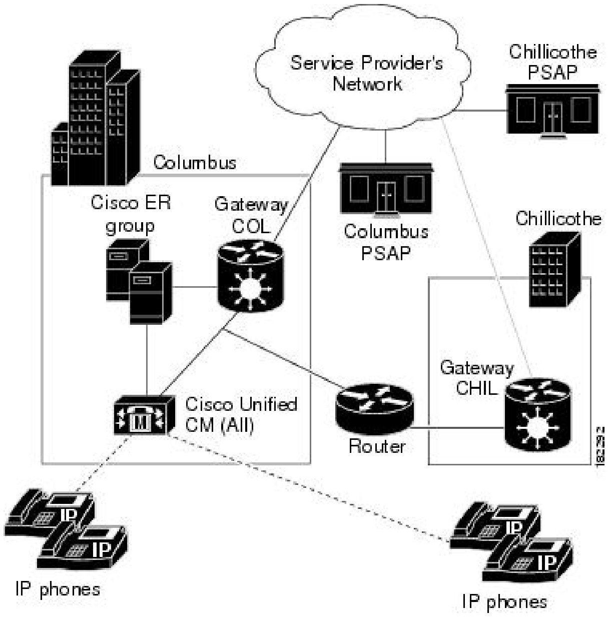
Related Topics

Emergency Call Process , on page 26
Emergency Responder and Your Network , on page 22
Determine Required Cisco Emergency Responder Groups , on page 33
Installation on a New System , on page 63
Configure Cisco Unified Communications Manager, on page 83

Deployment in Main Site with Satellite Offices

The following figure illustrates the Emergency Responder configuration with one main site that serves one or more satellite offices, that is, where the phones in the satellite office are run from the CiscoUnifiedCommunicationsManager cluster on the main site. If the satellite office has its own CiscoUnifiedCommunicationsManager cluster, see Two Main Site Deployments , on page 44.

Figure 13: Deploying Cisco Emergency Responder in One Main Site with Satellite Offices



⚠ **Caution** In this configuration, if the WAN link between the offices goes down, the people in the satellite office cannot make emergency calls with Emergency Responder support. SRST in the satellite office can provide basic support for emergency calls in case of WAN failure.

To support this type of network, install two Emergency Responder servers and configure one server as the Publisher and the other server as a Subscriber pointing to the Publisher. Install both servers in the main office.

Most likely, there are separate PSAPs serving the main (Columbus) and satellite (Chillicothe) offices. You probably need more than one gateway connecting to different parts of the service provider's network (you might have different service providers). However, this depends on the layout of the service provider's network: you might only need one gateway if the PSAPs are served by a shared switch. Consult with your service provider to determine the requirements for your buildings. In this example, we assume that you need two gateways; capacity planning for your telephony network might require more than one gateway for each link.

After setting up the gateways to correctly connect to the service provider's network, configure all route patterns used in Columbus's ERLs to use gateway COL, and all route patterns used in Chillicothe's ERLs to use gateway CHIL. As phones move between sites, Emergency Responder dynamically updates their ERLs so that emergency calls get routed out of the desired gateway.

You might also need to tune SNMP performance to account for the WAN link. Emergency Responder must do SNMP queries of the remote site switches to track phone movements there, and you might run into SNMP time-out problems if you do not allow enough time or retries to make a successful SNMP query. See Set Up SNMPv2, on page 149 for more information.

See these examples to extend this example to other networks:

- Deployment in Main Site and PSAP , on page 39
- Deployment in Main Site with Two or More PSAPs, on page 40
- Deployment in Main Site Serving Multiple Sites , on page 42
- Two Main Site Deployments , on page 44

Tip If the satellite office is small (fewer than 50 phones) and you are using survivable remote site telephony (SRST), it is probably easier to support emergency calls directly by configuring the gateway in the remote office to send 911 calls to an FXO port that has a CAMA trunk to the local PSAP rather than to Emergency Responder in the main office.

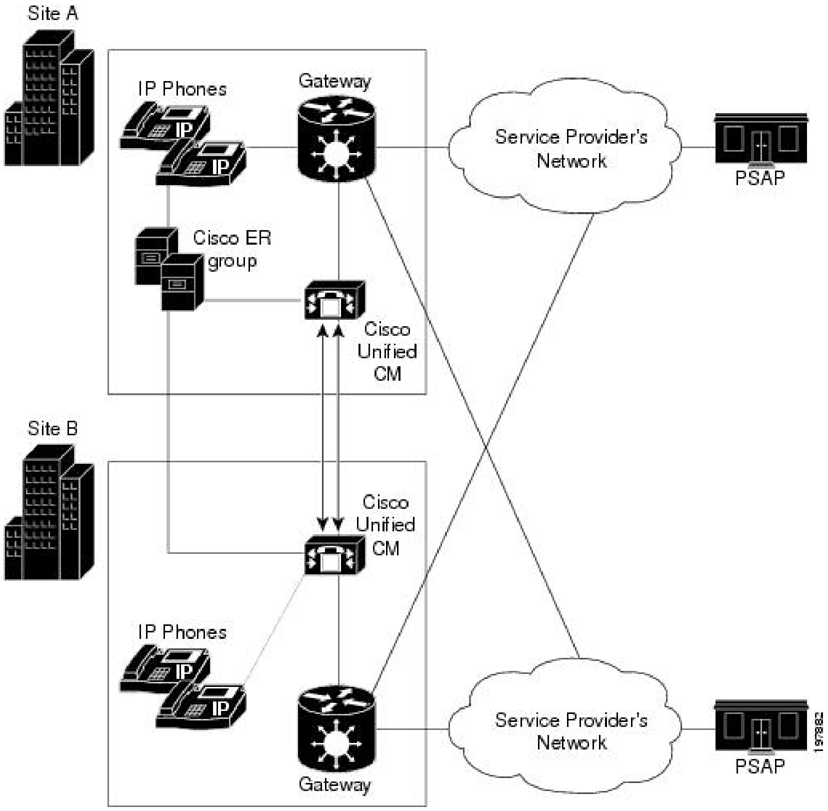
Related Topics

Emergency Call Process , on page 26
Emergency Responder and Your Network , on page 22
Determine Required Cisco Emergency Responder Groups , on page 33
Installation on a New System , on page 63
Configure Cisco Unified Communications Manager, on page 83

Deployment in Main Site Serving Multiple Sites

The following figure illustrates the Emergency Responder configuration with two or more main sites that are served by two or more PSAPs with one Unified CM cluster per site.

Figure 14: Deploying Emergency Responder in One Main Site Serving Two or More Sites



To support this type of network, install two Emergency Responder servers and configure one server as the Publisher and the other server as a Subscriber pointing to the Publisher.

Because there are two PSAPs serving the location, you probably need more than one gateway connecting to different parts of the service provider's network. However, this configuration depends on the layout of the service provider's network: you might only need one gateway if the PSAPs are served by a selective router that can intelligently route emergency calls to more than one PSAP. Consult with your service provider to determine the requirements for your buildings. In this example, assume that you need one gateway per site; capacity planning for your telephony network might require more than one gateway for each link.

After setting up the gateways to correctly connect to the service provider's network, configure all route patterns used in Site A ERLs and all route patterns used in Site B ERLs to use local site gateway. As phones move between buildings, Emergency Responder dynamically updates their ERLs so that emergency calls get routed out of the desired gateway.

In this example, Emergency Responder serves two Unified CM Clusters and facilitate the movement of phone between sites, it is required that route patterns for Site A ERLs and Site B ERLs are configured in both Site A and Site B Unified CM Clusters.

One Site Serving Multiple Sites with EMCC

Using Extension Mobility Cross Cluster (EMCC) between two Unified CM clusters enables Emergency Responder to provide enhanced support for 911 calls.

Figure 14: Deploying Emergency Responder in One Main Site Serving Two or More Sites , on page 43 illustrates how the Emergency Responder is deployed at one site and serves two or more sites with the Unified CM in each site.

In this scenario, the Emergency Responder server is shared by the EMCC user's home cluster and the visiting Unified CM cluster. For Emergency Responder to process a 911 call made by an EMCC logged-in user, the home Unified CM cluster must not use an Adjunct Calling Search Space (CSS) to direct the 911 call to the user's visiting cluster.

The shared Emergency Responder servers supporting both the clusters process the 911 call in the user's home cluster.

See these examples to extend this example to other networks:

- Deployment in Main Site and PSAP , on page 39
- Deployment in Main Site with Two or More PSAPs, on page 40
- Deployment in Main Site with Satellite Offices , on page 41
- Two Main Site Deployments , on page 44

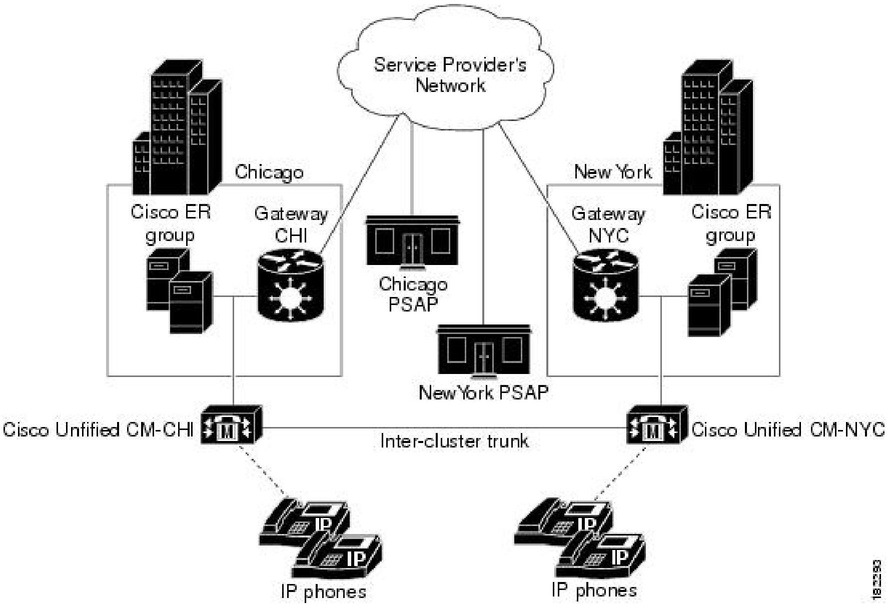
Related Topics

Emergency Call Process , on page 26
Emergency Responder and Your Network , on page 22
Determine Required Cisco Emergency Responder Groups , on page 33
Installation on a New System , on page 63
Configure Cisco Unified Communications Manager, on page 83

Two Main Site Deployments

The following figure illustrates the Emergency Responder configuration with two (or more) main sites, each served by a separate PSAP.

Figure 15: Deploying Cisco Emergency Responder in Two Main Sites



You can adapt this example to a more complex setup by combining this discussion with these examples:

- If some of your main sites have satellite offices, see Deployment in Main Site with Satellite Offices , on page 41 for information about deploying Emergency Responder in those offices.

If a main site is served by more than one PSAP, see Deployment in Main Site with Two or More PSAPs, on page 40 for information about deploying Emergency Responder in that site. To support this type of network:

- Install two Emergency Responder servers in Chicago and configure one server as the Publisher and the other server as a Subscriber pointing to the Publisher. After installation, select the Emergency Responder Publisher server in the Chicago Emergency Responder group for use as the cluster database. See Set Up Emergency Responder Cluster and Cluster DB Host , on page 134.

- Install two Emergency Responder servers in New York and configure one server as the Publisher and the other server as a Subscriber pointing to the Publisher. After installation, select the Emergency Responder Publisher server in the Chicago Emergency Responder group for use as the cluster database. See Set Up Emergency Responder Cluster and Cluster DB Host , on page 134.

Most likely, there are separate PSAPs serving your main offices. In this example, Chicago and New York use different PSAPs. You need at least one gateway in Chicago, and one in New York, to connect to different parts of the service provider's network (you might have different service providers). Consult with your service provider to determine the requirements for your buildings. Capacity planning for your telephony network might require more than one gateway in each site.

After setting up the gateways to correctly connect to the service provider's network, configure all route patterns used in Chicago's ERLs to use gateway CHI, and all route patterns used in New York's ERLs to use gateway NYC.

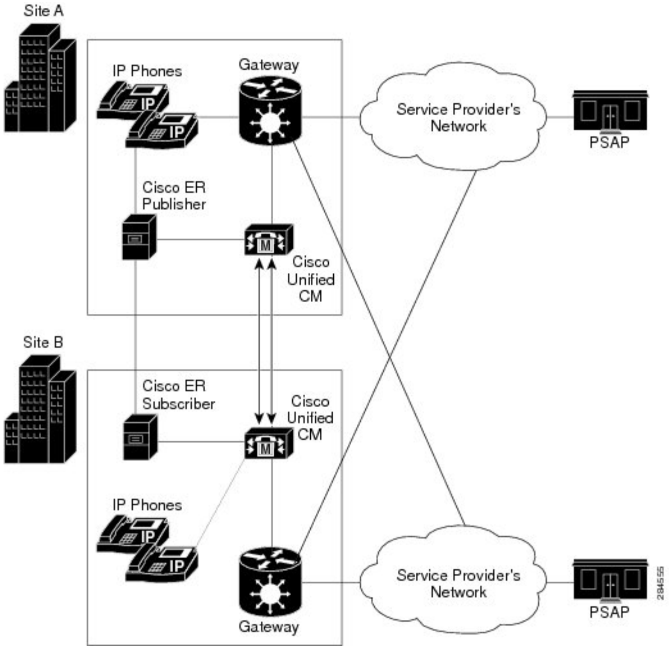
To enable phone movement between Chicago and New York, you must also configure an inter-cluster trunk to link the CiscoUnifiedCommunicationsManager clusters, and create an inter-Emergency Responder group route pattern so that Emergency Responder can transfer calls between CiscoUnifiedCommunicationsManager clusters served by separate Emergency Responder groups.

As phones move between sites, Emergency Responder dynamically updates their ERLs so that emergency calls get routed out of the desired gateway. However, if the WAN link becomes unavailable, Emergency Responder cannot track phone movement between the sites.

Deployment in Two Main Sites with Clustering Over the WAN

The following figure illustrates the Emergency Responder configuration with two main sites using Clustering over the WAN (CoW).

Figure 16: Deploying CiscoEmergency Responder in Two Main Sites with Clustering Over the WAN



To support this type of network, install one Emergency Responder server in each site and configure one server as the publisher and the other server as a subscriber. The ER publisher should be co-located with the primary Unified CM CTI manager, and the ER subscriber should be co-located with the secondary Unified CM CTI manager.

Note the following constraints:

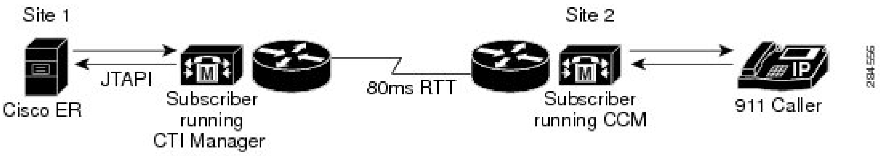
- At least 1.544 Mbps available bandwidth between ER publisher and ER subscriber (for data replication)
- No more than 80 msec RTT between any Unified CM server and either ER server

Support for CTI and JTAPI Over WAN

The following figure shows JTAPI over the WAN during routine or normal operations.

In this topology, the primary CTI manager is running on Unified CM subscriber at Site 1. Emergency calls from the Unified CM subscriber in Site 2 will reach the ER publisher in Site 1 via the primary CTI manager in Site 1, using CTI over the WAN.

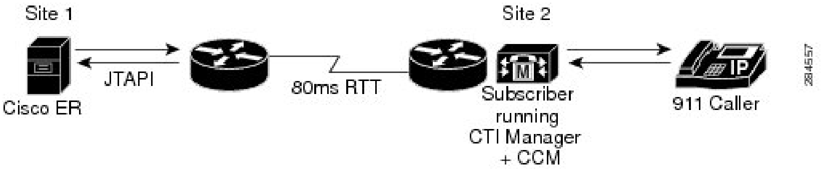
Figure 17: JTAPI Over the WAN During Normal Operations



The following figure shows JTAPI over the WAN during fail over operations.

During Emergency Responder failover operation, emergency calls from Unified CM subscriber in Site 1 will reach the Emergency Responder subscriber in Site 2 via the primary CTI manager running on Unified CM subscriber at Site 1, using JTAPI over the WAN.

Figure 18: JTAPI Over the WAN During Failover Operations



In Emergency Responder failover, the ER subscriber registers with the primary CTI manager. In Emergency Responder fallback the Emergency Responder publisher reregisters with the primary CTI manager. Emergency Responder failover and fallback takes four to five minutes. The time may vary according to the number of CTI ports configured.

Both CTI over the WAN and JTAPI over the WAN support network latency up to a 80-msec round-trip.

Cluster Deployment in Two Main Sites with EMCC

Emergency Responder can provide enhanced support for 911 calls when using Extension Mobility Cross Cluster (EMCC) between two Unified CM clusters.

Figure 15: Deploying Cisco Emergency Responder in Two Main Sites , on page 45 illustrates the Emergency Responder configuration with two (or more) main sites, each served by a separate PSAP.

In this scenario, the two clusters must be configured for EMCC. When a 911 call is made by an EMCC logged-in user, the call is offered to Emergency Responder group in the users home cluster.

Emergency Responder groups in the user's home cluster and visiting cluster form an Emergency Responder cluster. Emergency Responder group in home cluster redirects the call to visiting Emergency Responder group by using Inter-Cluster Trunk (ICT) between the two Unified CM clusters and the visiting Emergency Responder routes the call to appropriate PSAP.

Note In this scenario, the Unified CM does not have adjunct CSS configured.

See these examples to extend this example to other networks:

- Deployment in Main Site and PSAP , on page 39
- Deployment in Main Site with Two or More PSAPs, on page 40
- Deployment in Main Site with Satellite Offices , on page 41

- Deployment in Main Site Serving Multiple Sites , on page 42

Related Topics

Emergency Call Process , on page 26
Emergency Responder and Your Network , on page 22
Determine Required Cisco Emergency Responder Groups , on page 33
Installation on a New System , on page 63
Configure Cisco Unified Communications Manager, on page 83

Configure a Local Route Group in a Wide Area Network

With an Emergency Responder and Cisco Unified Communications Manager deployment that spans multiple locations over a wide area network (WAN), you may want to configure a Local Route Group (LRG) to ensure that users can make emergency calls if the connection between Emergency Responder and Cisco Unified Communications manager goes down.

While there is a communication failure between Emergency Responder and Cisco Unified Communications Manager, the following Emergency Responder features are not supported:

- Onsite alerts
- Web alerts
- Email alerts
- PSAP callback
- Device mobility

  To support device mobility, you must configure device mobility in Cisco Unified Communications Manager to route the 911 call to the new LRG location when the phones are moved from one location to another.

To configure LRG, follow these steps:

Procedure

Step 1 On Cisco Unified Communications Manager Administration, configure the LRG route pattern and route point for 911 emergency call routing.

Step 2 On Cisco Unified Communications Manager Administration, configure any destination route point that is being forwarded in the emergency call route point with the LRG route pattern.

Step 3 On Emergency Responder Administration, configure the LRG route pattern as the default ERL.

Related Topics

Emergency Call Process , on page 26
Emergency Responder and Your Network , on page 22
Determine Required Cisco Emergency Responder Groups , on page 33
Installation on a New System , on page 63
Configure Cisco Unified Communications Manager, on page 83

PART II

Installation and Upgrade

CHAPTER 3

Cisco Emergency Responder Installation

Cisco Emergency Responder Installation Overview

Cisco Emergency Responder (Emergency Responder) is distributed on an installation DVD that contains everything that is required to install Emergency Responder, including the Cisco Unified Communications Operating System software.

Hardware and Software Prerequisites

Cisco Emergency Responder requires specific hardware and software to run properly. Review the following sections before you proceed with an installation or upgrade:

- See the latest version of the Release Notes for Cisco Emergency Responder to verify that you have all the hardware and software, and in the supported versions, that you must install for Emergency Responder and to check that your CiscoUnifiedCommunicationsManager Appliance platform provides the Emergency Responder capabilities to meet your configuration needs. (You can also use equivalent Cisco-certified servers.)
- See the License Requirements section to make sure that you have all the required license keys available before you begin the installation process.

System Preparations

The Emergency Responder installation process installs both the platform software and the Emergency Responder software. During the installation, you are prompted to enter information needed by the system to complete the installation.

Note We recommend that you perform the installation or upgrade during off-peak hours. The installation or upgrade procedure completely reformats the hard disk, so Emergency Responder is unavailable for the duration of the installation or upgrade.

Review the following information before you install Cisco Emergency Responder or upgrade your system to the latest version:

- Upgrading Emergency Responder
  - Before you upgrade to the latest version of Emergency Responder, you must ensure that it is compatible with your existing version of Unified CM. You can use the Cisco Unified Communications Compatibility Tool to research this issue: http://tools.cisco.com/ITDIT/vtgsca/VTGServlet.
  - You must upgrade Emergency Responder before you upgrade Unified CM. Only after you have installed the new version of Emergency Responder can you then upgrade Unified CM.
  - After you have upgraded both Emergency Responder and Unified CM, you must then update the Unified CM Version on Emergency Responder.
  - See Table 2: Upgrading Tasks , on page 54 for the correct upgrade order and additional information about this subject.
  - If you have different security passwords in the active and inactive versions, and when you switch back to a lower version, ensure that you change the security password in the lower version to be same as the higher version. Follow these steps to change the security password:
    1. Switch the publisher node to a lower version.
    2. Change the security password of the publisher node to the new password which is same as the higher

       version.
    3. Switch the subscriber to a lower version.
    4. Change the security password of the subscriber node to the new password which is same as the higher version.
- Emergency Responder Versions
  - Different versions of Emergency Responder cannot be deployed in the same Emergency Responder group. The primary and the standby Emergency Responder servers must be running the same version of Emergency Responder. If you are upgrading to the most recent version of Emergency Responder, also make sure to upgrade both Emergency Responder servers.

Note Emergency Responder supports interoperability between two server groups in a cluster running different versions of Emergency Responder.

- Determine and list your Emergency Responder hostname and passwords.

  - The hostname for the Emergency Responder Publisher and Subscriber must not contain the underscore character (_). If you have an existing Emergency Responder server with an underscore in its hostname, change the hostname of the server before installing Emergency Responder.
  - The hostname for the Emergency Responder Publisher and Subscriber can begin with a numeric value.
  - Decide on a password for the Cisco Emergency Responder administrative user.

Note The Emergency Responder administrative users password must be at least six characters long and can contain alphanumeric characters, hyphens, and underscores. It must start with an alphanumeric character.

- Ethernet NIC speed and duplex mode:
  - Decide if you want to enable auto-negotiation of Ethernet NIC speed and duplex.
  - If yes, you do not need any additional information.
  - If no, determine what Ethernet NIC speed and duplex mode you will use.
- DHCP Configuration
  - Decide if you want to use the Dynamic Host Configuration Protocol (DHCP) to allocate IP addresses.
  - If yes, you do not need any additional information.
  - If no, you need the hostname, IP address, IP mask, and gateway address to enter for the Static Network Configuration.
- NTP Client information
  - The system prompts you to set up external Network Time Protocol (NTP) servers. We recommend that you use external NTP servers to ensure that the system time is accurate.
  - If you decide to use external NTP servers, you must enter the IP address or hostname of the servers.
  - If you do not choose to use external NTP servers, you must enter the system date and time clock information manually.

Note Use of NTP server is mandatory when installing Emergency Responder on UCS servers.

Note To avoid upgrade failures due to time sync issues with VM, disable the VM's NTP sync with the ESXi host using the workaround mentioned in the following link: http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1189.

- Database Access Security password

- The system requires a database access security password to allow the nodes in a server group to communicate. The password is shared with all nodes in the server group.
- The password must be at least six characters long and can contain alphanumeric characters, hyphens, and underscores. It must start with an alphanumeric character.

- SMTP host configuration (optional)
  - Decide if you want to use an SMTP host.
  - If yes, determine the hostname or IP address of the SMTP host.
- Caveats
  - Review the latest Release Notes for Emergency Responder before installation.

Perform the installation tasks in the order shown in this table.

Table 2: Upgrading Tasks

Installation Task	For More Information
Upgrade Emergency Responder	• Software Upgrades , on page 221
Upgrade Unified CM	• http://www.cisco.com/en/US/products/sw/voicesw/ps556/tsd_products_support_series_home.html • http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_installation_guides_list.html • Change Cisco Unified Communications Manager Version , on page 305
Update Unified CM Version	Update Cisco Unified Communications Manager Version, on page 573

Install the components for Emergency Responder in the order shown in this table.

Table 3: Installation Tasks

Installation Task	For More Information
Install Cisco Unified Communications Manager	https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-guides-list.html
Install Emergency Responder as a new installation	Installation on a New System , on page 63

Installation and Migration on the Cisco UCS Server

The information in the following sections describe the changes for installation, upgrade, and migration of the Cisco Emergency Responder on the Cisco UCS Server.

System Requirements

To run Cisco Emergency Responder on the Cisco UCS Server, your system must meet the requirements listed in the following table.

Table 4: System Requirements

System Parameter	System Parameter options
Supported Virtual Machine Configuration	See the documentation at: https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-cisco-emergency-responder.html
IOPS per virtual machine (VM)	See the documentation at: https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-cisco-emergency-responder.html
VMware version	For Emergency Responder 15 compatible/supported ESXi releases, see https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-cisco-emergency-responder.html and https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/cisco-collaboration-infrastructure.html#VMwareCompatibility. **Note** Emergency Responder 15 VM is not supported to run on any older ESXi releases. For example, ESXi 6.7/older (including 6.5, 6.0, 5.x, 4.x). **Note** Ensure that you use ESXi, rather than ESX, to run Cisco Emergency Responder on the Cisco UCS Server. However, the server can be part of a VMware vCenter that includes ESX hosts.
VMware—vMotion	No **Note** We don't support vMotion on a VM that is running. However, we support powering-down a VM. This may be helpful if you want to put a rack server into maintenance mode.
VMware—Site Recovery Manager	Yes
VMware—High Availability	Yes

System Parameter	System Parameter options
VMware—Data Recovery (VDR)	Yes
All other unlisted VMware features	Not supported

To operate Cisco Emergency Responder on the Cisco UCS Server successfully, you should have the experience and skills to manage a host server running VMware ESXi. If you do not have this experience and want to obtain the required information quickly, consider using VMware GO, a Web-based application that facilitates VMware.

Note Even if you use VMware GO, you still must use the supported VMware configuration on Cisco Emergency Responder on the Cisco UCS Server, which are documented at both http://www.cisco.com/go/swonly and https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-cisco-emergency-responder.html.

Installation on Cisco UCS Server

This following sections describe how to perform a fresh installation of a Cisco Emergency Responder on the Cisco UCS server:

- Configuration Checklist for Installing and Configuring the Server , on page 56
- Install Preparations , on page 57
- Set Up RAID , on page 58
- vSphere Client Installation , on page 59
- Aligning the Datastore Used for VMs , on page 59
- Create Virtual Machines, on page 59
- Download Virtual Machine Templates (OVA Templates) , on page 60
- Install Emergency Responder on VM, on page 61

Configuration Checklist for Installing and Configuring the Server

The following procedure provides the major steps required to install and configure Cisco Emergency Responder on the Cisco UCS Server.

Procedure

Step 1 Prepare to install the server.

For more information, see Install Preparations , on page 57.

Step 2 Physically install and connect the server.

Step 3 Power on the server and configure Cisco Integrated Management Controller (CIMC) for remote management.

Step 4 If you purchased the UCS server separately, configure the RAID settings to the following specification:

- The first two drives are configured as a RAID 1 (mirrored) drive. This drive is for ESXi installation.
- The next four drives are configured as a RAID 5 drive. This drive is for VMs.

Note Number of drives may be different in different versions of UCS servers.

For more information, see Set Up RAID , on page 58

Step 5 If you purchased the UCS server separately, configure the BIOS to the following specification:

- Disable Quiet Mode.
- Enable Enhanced SATA for CDROM access.
- Configure the following boot order:
  - SATA5:Optiarc DVD first
  - PCI Raid Adapter second

Step 6 Install and configure VMware EXSi on the smaller of the two available disks.

For more information, see the VMware ESXi documentation.

Step 7 Install vSphere Client.

For more information, see vSphere Client Installation , on page 59 and the vSphere Client documentation.

Step 8 Align the datastores for the VMs.

For more information, see Aligning the Datastore Used for VMs , on page 59.

Step 9 If you use 802.1q trunking, set the MTU size to 1472.

Step 10 Install and configure a virtual machine (VM).

For more information, see Create Virtual Machines, on page 59 and Download Virtual Machine Templates (OVA Templates) , on page 60.

Step 11 Install Cisco Emergency Responder on the VM.

For more information, see Install Emergency Responder on VM, on page 61.

Install Preparations

This section describes how to prepare to install a Cisco Emergency Responder on the Cisco UCS server in a standalone configuration, which indicates that it is not in a data center.

Allocate the following resources before installation:

- Space in a rack to receive a 2-RU UCS server
- Ethernet ports on a switch close to the UCS server:
  - One port for the CIMC
  - Two ports for the LAN on motherboard (LOM) NICs
- An IP address for the CIMC management port

- An IP address for the virtual host. The UCS server's IP address and is used by ESXi.
- A hostname, and optionally configured DNS for the virtual host's hostname
- IP addresses for the VMs

Set Up RAID

If you purchased the UCS server separately, configure the RAID settings to the following specifications:

- The first two drives are configured as a RAID 1 (mirrored) drive. This drive is for ESXi installation.
- The next four drives are configured as a RAID 5 drive. This drive is for VMs.

Note Number of drives may be different in different versions of UCS servers.

Procedure

Step 1 During server bootup, press **Ctrl+Y** to enter the preboot CLI.

Step 2 Enter the following commands to determine the current RAID configuration:

-ldinfo -l0 -a0

-ldinfo -l1 -a0

The required configuration is two drives in a RAID 1 array for logical drive 0, and four drives in a RAID 5 array for Logical drive 1. If the RAID configuration is wrong, continue with this procedure.

Note Do not continue with this procedure if RAID is configured correctly.

Step 3 Enter the command **-cfgclr -a0** to clear the RAID configuration.

Caution Clearing the RAID configuration deletes all data on the hard drives.

Step 4 Enter the following commands to configure RAID:

-cfgldadd -r1 [252:0, 252:1] -a0

-cfgldadd -r5 [252:2, 252:3, 252:4, 252:5] -a0

If the hard drives did not have a RAID configuration previously, you are done configuring RAID. If the hard drives had a RAID configuration before, continue with this procedure.

Step 5 Enter the following commands to initialize the logical volumes:

- ldinit -start -full -l0 -a0 (l0 is the letter l and the number 0, not the number 10)

- ldinit -start -full -l1 -a0 (l1 is the letter l and the number 1, not the number 11)

These commands clear data on the drives and initialize the new array.

Step 6 Allow these commands to finish running before exiting the Preboot CLI. Enter the following commands

to display the progress of the commands:

-ldinit -showprog -l0 -a0

-ldinit -showprog -l1 -a0

When both commands report that no initialization is running, it is safe to quit the Preboot CLI.

Step 7 After configuring the two logical volumes, you can exit the Preboot CLI by entering **q**.

vSphere Client Installation

When the virtual host is available on the network, you can browse to its IP address to bring up a web-based interface. The vSphere Client is Windows-based, so the download and install must be performed from a Windows PC.

After the vSphere Client is installed, you can run it and log into the virtual host using the virtual host's name or IP address, the root login ID, and the password you configured.

You can join the host to a vCenter if you want to manage it through vCenter.

Aligning the Datastore Used for VMs

When you install VMware ESXi, the second logical volume is automatically imported unaligned. VMs have better disk performance when all partitions (physical, ESXi, and VM) start on the same boundary and you will have fewer incidents of disk blocks being fragmented across the different boundaries.

To ensure that the ESXi partition used for VMs are aligned, delete the unaligned datastore (the larger disk partition, which is 407 GB), then recreate the datastore using vSphere client.

Create Virtual Machines

Cisco provides a VM template for you to download and transfer to your virtual host. Use this template to create the VM for Cisco Emergency Responder on the Cisco UCS Server installation.

Before you deploy the template and create the VM, you should have a hostname and IP address allocated for the new VM.

To create a VM and prepare to install Cisco Emergency Responder on the Cisco UCS Server, follow these steps.

Procedure

Step 1 Download the VM template for your application.

See Download Virtual Machine Templates (OVA Templates) , on page 60 for more information.

Note From Release 15 onwards, the OVA template is signed with sha512 using the Cisco authenticated certificates to ensure that there is no tampering of the OVA file.

Step 2 Upload the template to a datastore on the UCS server.

We recommend that you use the smaller datastore (with ESXi installed on it).

Step 3 Make this template available to the UCS server.

Step 4 Deploy the template file using vSphere Client. Enter the following information for the new VM:

- hostname
- datastore—Select a datastore that has enough resource.

Step 5 Complete creating the VM.

At this point a new VM is created with the correct amount of RAM, number of CPUs, size and number of disks for the intended application.

In case you are planning to upgrade any of your 12.5.x or 14 and SUs Emergency Responder to Release 15, note the following:

- Deployments with 12,000 or 20,000 users having 4GB vRAM should increase the vRAM size to 6GB before upgrading to Release 15.
- Deployments with 20000 users having 1 vCPU should increase the vCPU to 2 before upgrading to Release 15.

Table 5: Emergency Responder Release 15 VM Configuration Requirements

	Current Specifications			Recommendation for Release 15		
OVA Types	**vCPU**	**RAM**	**Disk**	**vCPU**	**RAM**	**Disk**
20, 000 users	1	4 GB	80 GB	2	6 GB	80 GB
30, 000 users	2	6 GB	110 GB	2	6 GB	110 GB
40, 000 users	4	6 GB	110 GB	4	6 GB	110 GB

Step 6 Install Cisco Emergency Responder on the Cisco UCS Server on the VM.

See Install Emergency Responder on VM, on page 61 for more information.

Download Virtual Machine Templates (OVA Templates)

The configuration of a Cisco Emergency Responder virtual machine must match a supported virtual machine template.

To obtain the virtual machine template for Cisco Emergency Responder on the Cisco UCS Server, follow these steps:

Procedure

Step 1 Select this URL in your browser:

http://www.cisco.com/cisco/software/navigator.html?mdfid=272877967

Step 2 If your browser prompts you to do so, type your Cisco.com User Name and Password in the text boxes, then click the **Log In** button.

Step 3 Select the desired version of Cisco Emergency Responder.

Step 4 Click the **Emergency Responder Virtual Machine Templates** link.

Step 5 Move your mouse over the filename and click the **Readme** link to view the virtual machine template's release information.

Step 6 Click the **Download Now** button. Follow the prompts and provide the required information to download the software.

Install Emergency Responder on VM

Procedure

Step 1 In vSphere Client, edit the VM to force entry into BIOS setup the next time the VM reboots.

Step 2 Make the Emergency Responder installation media available to the VM DVD-ROM drive.

Step 3 Power on the VM, then in BIOS setup, promote CD ROM to boot before the hard drive.

Step 4 Complete booting the VM.

The Cisco Emergency Responder installation program starts. For information about performing the installation, see the Installing Cisco Emergency Responder document.

Virtual Machine Configurations

With the virtual machine configuration for running Cisco Emergency Responder on the Cisco UCS Server, the VMware server must match the specifications described in the System Requirements, on page 55 to be supported by Cisco.

While Cisco Emergency Responder can be installed and licensed in other virtual machine configurations, Cisco does not support these configurations.

Migrate to Emergency Responder on Cisco UCS Server

Migrating from a Media Convergence Server (MCS server) to a Cisco Emergency Responder on the Cisco UCS Server follows a procedure that is very similar to replacing server hardware.

The following procedure outlines the migration process and references to other pertinent documentation.

Procedure

Step 1 Upgrade the MCS server to the most recent version of Cisco Emergency Responder.

Step 2 If the Emergency Responder VM uses a different IP address from the MCS server, change the IP address of the MCS server to the value used by the Emergency Responder VM.

Note The hostname on the Emergency Responder VM must remain the same as that on the MCS Server.

Step 3 Perform a DRS backup on the MCS server.

Step 4 Create the virtual machine (VM) on the Cisco UCS server used as the replacement for the MCS node.

For more information, see Installation on Cisco UCS Server , on page 56.

Step 5 Install the new version of Cisco Emergency Responder on the Cisco UCS server.

For more information, see Installation on Cisco UCS Server , on page 56.

Step 6 Perform a DRS restore to restore the data backed up from the MCS server to the Cisco UCS server.

Step 7 Upload the new licenses to the Cisco Emergency Responder on the Cisco UCS server.

VMWare Support

Consider the following, when using Cisco Emergency Responder on the Cisco UCS Server:

- Install, upgrade, and recovery procedures now use "soft media" such as ISO if the server does not have a DVD drive.
- USB tape backup is not supported.
- NIC teaming is configured at the VMware virtual switch.
- Hardware SNMP and syslog move to VMware and UCS Manager.
- Install logs are written only to the virtual serial port.
- Basic UPS Integration is not supported.
- Boot order is controlled by the BIOS of the VMware VM.
- Hardware BIOS, firmware, and drivers must be the required level and configured for compatibility with Cisco Emergency Responder supported VMware product and version.

For more information about the UCS C-series server, go to the following URL:

http://www.cisco.com/en/US/docs/unified_computing/ucs/c/sw/gui/config/guide/1.1.1/b_Cisco_UCS_C-Series_Servers_Integrated_Management_Controller_Configuration_Guide_1_1_1.html

To view the list of product installation and configuration guides for Cisco UCS C-Series Integrated Management Controller, go to the following URL:

http://www.cisco.com/en/US/products/ps10739/products_installation_and_configuration_guides_list.html

To view the list of product installation and configuration guides for Cisco UCS Manager, go to following URL:

http://www.cisco.com/en/US/products/ps10281/products_installation_and_configuration_guides_list.html

Emergency Responder Daily Operations on Cisco UCS Server

Daily operations for Cisco Emergency Responder on the Cisco UCS Server software applications are identical to when the application is installed on an MCS server.

There are some differences in hardware management and monitoring because Cisco Emergency Responder on the Cisco UCS Server operates in a virtual environment.

Hardware Monitoring From the VM

Applications running in a VM have no ability to monitor the physical hardware. Hardware monitoring must be done from the CIMC, ESXi plugins, vCenter, or by physical inspection (for example, for flashing LEDs.).

Hardware Monitoring From CIMC

The CIMC provides the following hardware monitoring:

- An overview of CPU, memory, and power supply health
- An overview of hardware inventory, including CPUs, memory, power supplies, and storage
- Monitoring of sensors for power supplies, fans, temperature, and voltage
- A system event log that contains BIOS and sensor entries

Hardware Monitoring From VSphere Client and VCenter

The vSphere Client provides the following monitoring features:

- When you are logged in to vCenter, the vSphere Client displays hardware and system alarms defined on the Alarms tab.
- VM resource usage is displayed on the Virtual Machines tab and on the Performance tab for each VM.
- Host performance and resource usage is displayed on the Performance tab for the Host.
- When ESXi is used standalone (without vCenter), hardware status and resource usage are available, but alarming is not possible.

Related Documentation

The *UCS RAID Controller SMI-S Reference Guide*, which describes Storage Management Initiative Specification (SMI-S) support in the Cisco UCS Servers, is available at the following URL:

http://www.cisco.com/en/US/partner/docs/unified_computing/ucs/sw/utilities/raid/reference/guide/ucs_raid_smis_reference.html

Installation on a New System

This procedure describes how to install Emergency Responder as a new installation.

You enter Emergency Responder group configuration through the Emergency Responder Administration web interface based on Publisher (primary) and Subscriber (secondary) server pairs as described in the following sections.

Note From Cisco Emergency Responder Release 14, all the certificate related operations are moved from Ipsec to Tomcat certificates. To create a trust between a publisher node and subscriber node, the Tomcat certificate should be exchanged between the publisher and subscriber for any cluster related operations to work.

Any Federal Information Processing Standards (FIPS) or hostname related changes require the same operation procedures.

Install Emergency Responder Publisher

To install Emergency Responder, you install the Publisher (primary) first, then you install the Subscriber (backup) on a separate server. You must install Emergency Responder on separate servers from CiscoUnifiedCommunicationsManager or any Cisco Unified Communications applications.

Allow approximately 1 hour to perform a new installation.

Procedure

- Insert the Emergency Responder Installation DVD.

  If the system finds the DVD, you are asked if you want to perform a media check before installation to determine if there are problems with the DVD. The system displays the checksum of the DVD and instructs you to verify this checksum on the Emergency Responder website.

  At the bottom of the screen you will see instructions for moving between elements and for selecting elements, as follows:

  - Use the **Tab** key to advance to the next element.
  - Use the **Alt-Tab** key combination to return to the previous element.
  - Use the **Space** bar to select a highlighted element.

  If you choose to perform the media check, the system performs the media check and displays the results.

  If the result of the media check is **PASS**, click **OK**. The system install begins the installation. Skip to Step 2.

  If the result of the media check is **FAIL**, obtain a new installation DVD from Cisco Systems.

- The Cisco Emergency Responder system installer starts. The Product Deployment Selection screen displays a message saying the Cisco Emergency Responder product suite is installing. Click **OK** to continue.
- The Proceed with Install page displays the current software version on the hard drive and the software version on the installation DVD.

  If you are performing a fresh installation, there will be no software on the hard drive and the system asks if you want to proceed with the installation. Click **Yes** to proceed.

  If you are performing an upgrade, the system displays the current software version and asks it you want to overwrite the hard drive. Click **Yes** to proceed.

  If you click **Yes**, the system continues with the installation and the Platform Configuration Wizard appears.

  If you click **No**, the installation is terminated.

- On the Platform Configuration Wizard page, click **Proceed** to continue with the platform installation.

  If you click **Skip**, the system installs both the platform and Emergency Responder software without prompting you to provide information during the installation. After the installation is completed and the system reboots, you are prompted to enter the required configuration details.

Note For version 8.6 and earlier, the Cisco Emergency Responder Subscriber may fail to install with unrecoverable internal error indicated in the logs. If this happens, do a Skip install by skipping the configurations step initially, proceed with the installation, and then key in the configuration details when prompted at the end of the procedure.

- Click **Continue** to proceed. The Timezone Configuration page appears.
- Choose the correct time zone to use from the list provided.

  Use the following keys to move between elements on the Timezone Configuration page:

  - **Arrow Up** or **Arrow Down** to select a time zone from the list
  - After selecting the correct time zone, click **OK**. The Auto Negotiation Configuration page appears.

- Click **Yes** to enable autonegotiation of the Ethernet NIC speed and duplex mode. The DHCP Configuration page appears. If you click **Yes**, skip to Step 10.

  If you click **No**, the NIC Speed and Duplex Configuration page appears.

- On the NIC Speed and Duplex Configuration page, do the following:

  a) Select the NIC Speed. The available options are 10 Megabit, 100 Megabit, or 1000 Megabit.
  b) Select the NIC Duplex setting. The available options are Full or Half.
  c) Click **OK**. The DHCP Configuration page appears.

- On the MTU Configuration page, you can set the maximum transmission unit (MTU) that can be sent in a network as follows:

  - Click **Yes** if you want to configure a a MTU value of less than 1500 bytes.
  - Click **No** to use the default MTU value of 1500 bytes.

- Click **Yes** if you want to use Dynamic Host Configuration Protocol (DHCP). The Administration Login Configuration page appears. Skip to Step 14.

  If you click **No**, the Static Network Configuration page appears.

- If you chose not to use DHCP, enter the following information about the Static Network Configuration page:

  - Host Name
  - IP Address
  - IP Mask
  - Gateway (GW) Address

  Click **OK**. The DNS Client Configuration page appears.

- On the DNS Client Configuration page, you are asked if you want to configure the Domain Name System (DNS) client.

Note Click the **Help** button for details about configuring DNS.

If you select **Yes**, a second DNS Client Configuration page appears.

If you select **No**, the Administration Login Configuration page appears. Skip to Step 14.

- On the second DNS Client Configuration page, you are prompted to enter the following information:
  - Primary
  - Secondary DNS (optional)
  - Domain

  Click **OK**. The Administration Login Configuration page appears.

- On the Administration Login Configuration page, enter an ID and password for the Administrator account. This password is used to access the CLI and the CiscoUnifiedOS Administration and Disaster Recovery System (DRS) websites. Click **Help** to display guidelines for creating this password.

  When you have finished, click **OK**. The Certificate Information page appears.

- Enter the following information about the Certificate Information page:
  - Organization
  - Unit
  - Location
  - State
  - Country (select from the scroll-down menu).

  Click **OK**. The Publisher Configuration page appears.

- Based on the type of installation you are performing, do one of the following:
  - If the server you are configuring is the Publisher in the server group, click **Yes**. The Network Time Protocol Client Configuration page appears. Proceed to Step 17.
  - If the server you are installing is not the Publisher in the server group, you must first configure this server on the Publisher before you can proceed. This server must also have network access to the Publisher, which must be in service for the installation to complete successfully. Click **No** only if you are configuring the Subscriber. See Install Emergency Responder Subscriber, on page 69 for information about installing the Subscriber.

- On the Network Time Protocol Client Configuration page, you are asked if you want to set up external Network Time Protocol (NTP) servers.

Note We strongly recommend that you use external NTP servers to ensure that the system time is kept accurate.

Caution For Emergency Responder install on UCS servers, it is mandatory to configure NTP server.

If you click **Yes**, the system displays a second Network Time Protocol Client Configuration page. In the fields provided, enter the IP address or hostname of the external NTP servers, then click **OK**. The Database Access Security Configuration page appears. Skip to Step 18.

If you click **No**, the Hardware Clock Configuration page appears. Enter the following information:

- Year [yyyy]
- Month [mm]
- Day [dd]
- Hour [hh]
- Minute [mm]
- Second [ss]

When you finish entering this information, click **OK**. The Database Access Security Configuration page appears.

- On the Database Access Security Configuration page, enter the security password and then confirm the password in the fields provided.

Note The security password must be at least six characters long and can contain alphanumeric characters, hyphens, and underscores. It must start with an alphanumeric character. The security password is used for secure communications between Emergency Responder server groups when performing the installation or upgrade, DRS backup or restore, and “Point to a new Publisher” operations.

Click **Help** to display guidelines. When you finish, click **OK**. The SMTP Host Configuration page appears.

- You are asked if you want to configure a Simple Mail Transport Protocol (SMTP) host. This step is optional.
  - If you click **Yes**, a second SMTP Host Configuration page appears. Click **Help** for guidelines, then enter the SMTP hostname or IP address in the field provided. When you are finished, click **OK**. The Platform Configuration Confirmation page appears.
  - If you click **No**, the Platform Configuration Confirmation page appears.
- On the Platform Configuration Confirmation page, do one of the following:
  - Select **OK** to save the platform configuration information and continue with the installation. The Cisco Emergency Responder Configuration page appears.

Note After you select **OK**, you cannot modify the platform configuration information.

  - Select **Back** if you want to return to the previous page to make modifications. Continue to select **Back** to scroll through each platform configuration page.
  - Select **Cancel** to cancel the installation.
- On the Cisco Emergency Responder Configuration page, do the following:
  - Enter the emergency number (for example, **911**).
  - Select the Cisco Unified CommunicationsManager version. Use the **Up** or **Down** arrows to select the version number and then select **OK**.

- On the Security End User Language Selection page, choose a language for the Cisco Emergency Responder web pages. The system defaults to the English language.

  The Application User Password Configuration page appears.

- On the Application User Configuration page, enter the username and password. This username and password is associated with the default administrative account and is used to log in to the Emergency Responder Administration web page. Click **Help** for guidelines.

  When you are finished, click **OK**. The Cisco Emergency Responder Configuration Confirmation page appears.

- On the Cisco Emergency Responder Configuration Confirmation page, do one of the following:
  - Select **OK** to save the Cisco Emergency Responder configuration information and continue with the installation. The system continues the installation process and then reboots.

Caution After you select **OK**, you can not modify the Cisco Emergency Responder configuration information.

  - Select **Back** if you want to return to the previous page to make modifications. Continue to select **Back** to scroll through each Emergency Responder Application User Configuration page.
  - Select **Cancel** to cancel the installation.

- After the system reboots, it checks the status of various system components. If the system finds any problems, you are prompted to correct the problem.

  If the system does not find any problems, the installation process continues. The system ejects the installation DVD, reboot, and then finishes the installation. When the installation is complete, a CLI prompt appears.

Note During this process, the system displays the MAC address of the Publisher. Write down the MAC address when it displays; you use the MAC address later to acquire Emergency Responder licenses. If you are not able to capture the MAC address during installation, you can look it up later. See the Server Licenses section for information about looking up the server MAC address.

- To bring up the Emergency Responder websites, go to any Windows system on the network, start a supported web browser, and enter the following URL:

  `http://your Emergency Responder hostname/`

  or

  `http://your Emergency Responder IP address/`

Note Make sure that the Emergency Responder is configured with DNS so that hostname is resolved to the IP address.

Install Emergency Responder Subscriber

You must install Subscriber only after you have installed the Publisher. You must install the Subscriber on a separate server from the Emergency Responder Publisher.

⚠ **Caution** You must complete the installation of the Publisher, which includes a system reboot, before you start to install the Subscriber.

Procedure

Step 1 On the Publisher server, add the details about the Subscriber server by doing the following:

a) Log in the Publisher Emergency Responder Administration website.

b) Select **System** > **Add Subscriber**. The Add Server page appears.

c) Enter the hostname of the new Subscriber and click **Insert**. The Add Subscriber page appears again.

d) In the **Configured Servers** list, check that the hostname and IP address of the new Subscriber is listed.

Step 2 Follow Steps 1 through 15 in the Installation on a New System , on page 63 section. After you complete Step 15, the Publisher Configuration page appears.

Step 3 On the Publisher Configuration page, select **No** to indicate that you are installing a Subscriber, not a Publisher. The system displays a warning saying that if this is not the Publisher, you must first configure this server using the Publisher Administration web interface before you can proceed (see Step 1 of this procedure for more information). Also, this server being added must have network access to the Publisher, which must be in service for the installation to complete successfully.

Click **OK** to close the warning.

Step 4 The Network Connectivity Test Configuration page appears. The system attempts to verify system connectivity. Click **No** to continue the installation.

Step 5 The Publisher Access Configuration page appears. Enter the following:

- Publisher hostname
- Publisher IP address
- Publisher Database/Security password

Step 6 Verify that the Publisher information is correct and click **OK**.

Step 7 The SMTP Host Configuration page appears. Choose **Yes** if you want to configure the SMTP Host.

Step 8 The Platform Configuration Complete page appears. Select one of the following options:

- If the Publisher information is correct, click **OK**.
- If the information is not correct, click the **Back** button and make the needed corrections on the Publisher Access Configuration page, then click **OK**.

The installation of the Emergency Responder Subscriber begins and takes an additional 20 to 30 minutes to complete.

Step 9 When the installation completes, go to the Emergency Responder Administration website on the Subscriber to verify that the Subscriber was installed successfully. If the installation succeeded, a message saying “Primary Cisco Emergency Responder is active” appears. This message indicates that the Subscriber was installed successfully.

Note If the Subscriber installation cannot validate the Publisher, See Cannot Validate Publisher , on page 341 in the Troubleshooting chapter.

Emergency Responder Upgrade

To upgrade from version 10.0 or a later version of Cisco Emergency Responder to the most recent version of Emergency Responder, use the Cisco Unified OS Administration web interface or Command Line Interface (CLI). See Software Upgrades , on page 221 section for information about performing upgrades.

See "Performing Software Upgrades" section of the respective *Cisco Emergency Responder Administration Guide for Emergency Responder* for information about performing upgrades to Emergency Responder.

Touchless Installation

Previous releases of Cisco Emergency Responder (Emergency Responder) cluster environment required you to install the publisher node first before you proceed to install the subscriber nodes. You had to install the subscriber node after adding this node details to the **Cisco ER Administration** > **Add Subscriber** page of the publisher node first before you proceed to install the subscriber nodes.

Touchless installation makes the installation process seamless and promotes simplified installation of Emergency Responder. With the CER server Group touchless installation, the subscriber node is configured dynamically along with the publisher node during their installation. The touchless installation proceeds without the requirement to provide any subscriber details in the installation wizard as the subscriber is not dependent on the installation of the publisher.

Note After publisher installation is complete, and if the subscriber installation does not happen automatically, you must restart the Cisco Tomcat service using the CLI command **utils service restart Cisco Tomcat** from the publisher node.

This feature has the following benefits:

- No manual intervention and scheduling during the deployment of a new cluster.
- No manual entry of the subscriber node to an existing cluster.
- No requirement to wait until the publisher node is active.

Answer File Generator

Use the Answer File Generator (AFG) tool (http://www.cisco.com/web/cuc_afg/index.html) to generate the answer files or ISO images for configuration. These files include clusterConfig.xml and platformConfig.xml files.

Start the virtual machine on which you mounted the ISO image to start the Emergency Responder installation. No manual intervention is required during installation of a standalone node. In a cluster environment, you can install both the publisher node and the subscriber node simultaneously. Sometimes, the installation of the subscriber node can stop during the installation of the publisher node. In this case, after the publisher node installation is complete, it generates a signal for the subscriber node to continue the installation.

Predefined Cluster Configurations (AFG Process)

With the implementation of this feature, the Answer File Generator (AFG) tool generates the clusterConfig.xml file along with the existing the platformConfig.xml file. If you provide the details of the subscriber node to the AFG tool, the clusterConfig.xml file includes those details. After the Emergency Responder publisher is installed, it reads the clusterConfig.xml file and if the publisher finds any subscriber node, it adds them to its cerserver tables. Adding the subscriber to cerserver tables eliminates the need to wait for the Emergency Responder publisher to finish its installation, and then manually add the subscriber on the server page. The entire installation process occurs automatically.

Preinstall Tasks for Cisco Emergency Responder

Procedure

	Command or Action	Purpose
Step 1	Planning the Installation	Make sure to review the following: • Decide on your installation method. • Decide on your cluster topology.
Step 2	Required Installation Information, on page 72	Review the installation requirements and record the configurations settings for each server that you plan to install.
Step 3	Create virtual machines.	• Get base OVA. • Run Collab Sizing Tool to get the required virtual machine count and specs of each virtual machine. If you don't want to run Collab Sizing Tool, follow the guidance in the OVA readme and the OVA wizard to select a predefined starting point, which can be changed later if needed.
Step 4	Mount the installation ISO file.	Place the installation ISO file in a location where the virtual machine can access it and edit the virtual machine's DVD drive to map to the file. Select the option to mount the DVD drive when you power on the virtual machine. When you power on the virtual machine, it mounts the ISO file and start the installation process. Do not begin the installation process until you have completed all the steps in this procedure.

	Command or Action	Purpose
Step 5	Verify the NTP status on the publisher node.	If the publisher node fails to synchronize with an NTP server, subscriber node installation can fail. On the Emergency Responder publisher node, run the `utils ntp status` CLI command.
Step 6	Complete the following firewall updates: • If a firewall is in the routing path between nodes, disable the firewall. • Increase the firewall timeout settings until after you complete the installation.	Temporarily allowing network traffic in and out of the nodes (for example, setting the firewall rule for these nodes to IP any/any) does not always suffice. The firewall might still close necessary network sessions between nodes due to timeouts.
Step 7	If you use DNS, verify that all servers on which you plan to install Emergency Responder are properly registered in DNS.	
Step 8	Cisco Smart Software Licensing , on page 10	Make sure that your system has adequate licensing.

Required Installation Information

When you install either Emergency Responder on a server, the installation process requires you to provide specific information. You can provide this information manually during the installation process or you can provide it using an answer file. For each server that you install in a cluster, you must gather this information before you begin the installation process.

The following table lists the information that you must gather before you begin the installation.

Note Because some of the fields are optional, they may not apply to your configuration. For example, if you decide not to set up an SMTP host during installation, the parameter still displays, but you do not need to enter a value.

You cannot change some of the fields after the installation without reinstalling the software, so be sure to enter the values that you want. The last column in the table shows whether you can change a parameter after installation, and if you can, it provides the appropriate menu path or Command Line Interface (CLI) command.

Table 6: Required Installation Information

Configuration Data	Description	Editable after Installation
Administrator Credentials		
Administrator Login	Specifies the name that you want to assign to the Administrator account.	No After installation, you can create additional administrator accounts, but you cannot change the original administrator account user ID.

Configuration Data	Description	Editable after Installation
Administrator Password	Specifies the password for the Administrator account.	Yes CLI: **`set password user admin`**
Application User Credentials		
Application User Username	Specifies the user ID for applications installed on the system.	Yes CLI: **`utils reset_application_ui_administrator_name`**
Application User Password	Specifies the password for applications on the system.	Yes CLI: **`utils reset_application_ui_administrator_password`**
Security Password		
Security password for Emergency Responder	Servers in the cluster use the security password to communicate with one another. Set this password on the Emergency Responder publisher node, and enter it when you install each additional node in the cluster.	Yes. You can change the security password on all nodes in the cluster using the following command: CLI: **`set password user security`**
Certificate Information		
Organization	Used to create the Certificate Signing Request.	Yes CLI: **`set web-security [orgunit] [orgname] [locality] [state] [country]`**
Unit	Used to create the Certificate Signing Request.	Yes CLI: **`set web-security [orgunit] [orgname] [locality] [state] [country]`**
Location	Used to create the Certificate Signing Request.	Yes CLI: **`set web-security [orgunit] [orgname] [locality] [state] [country]`**
State	Used to create the Certificate Signing Request.	Yes CLI: **`set web-security [orgunit] [orgname] [locality] [state] [country]`**

Configuration Data	Description	Editable after Installation
Country	Used to create the Certificate Signing Request.	Yes CLI: **`set web-security [orgunit] [orgname] [locality] [state]`**
(Optional) SMTP		
SMTP Location	Specifies the name of the SMTP host that is used for outbound email. You must fill in this field if you plan to use electronic notification. If not, you can leave it blank.	Yes • In Cisco Unified Operating System Administration Web Interface, select **Settings** > **SMTP** and enter the IP address or Hostname in the IP Address/Host Name field. • CLI: **`set smtp [host]`**
CER Emergency Number		
Emergency Number	Specifies the primary emergency number that is dial-able and is handled by Emergency Responder. All characters must either be numeric, a '*' or a '#'.	Yes
CER End User Language		
End User Language	Specifies the language the user wants to use for Emergency Responder.	Yes
CER CCM Version		
CCM Version	Indicates the version of Emergency Responder CCM.	Yes
Network Information		
DHCP (Dynamic Host Configuration Protocol)	Check the check box if you want to use DHCP to automatically configure the network settings on your server. Also, enter the hostname. If you uncheck the option, you must enter a hostname, IP Address, IP Mask, and Gateway Address.	Yes. • In Cisco Unified Operating System Administration Web Interface, select **Settings** > **IP** > **Ethernet**. • CLI: **`set network dhcp eth0 [enable]`** CLI: **`set network dhcp eth0 disable [node_ip] [net_mask] [gateway_ip]`**

Configuration Data	Description	Editable after Installation
Hostname	If DHCP is enabled, you must enter a hostname for this machine.	Yes; for Emergency Responder nodes, choose one of the following: • In Cisco Unified Operating System Administration Web Interface, select **Settings** > **IP** > **Ethernet**. • CLI: `set network hostname` You will be prompted to enter the parameters.
IP Address	If DHCP is disabled, you must enter the IP address of this machine.	Yes; for Emergency Responder nodes, choose one of the following: • In Cisco Unified Operating System Administration Web Interface, select **Settings** > **IP** > **Ethernet**. • CLI: `set network IP eth0 [ip-address] [ip-mask]`
IP Mask	If DHCP is disabled, you must enter the IP subnet mask of this machine. The subnet mask together with the IP address defines the network address and the host address. The subnet mask must use the following format: 255.255.255.0	Yes • In Cisco Unified Operating System Administration Web Interface, select **Settings** > **IP** > **Ethernet**. • CLI: `set network IP eth0 [ip-address] [ip-mask]`
Gateway Address	If DHCP is disabled, you must enter the gateway address.	Yes • In Cisco Unified Operating System Administration Web Interface, select **Settings** > **IP** > **Ethernet**. • CLI: `set network gateway [addr]`
(Optional) DNS		
Primary DNS	If you have a Domain Name Server (DNS), Emergency Responder contacts this DNS server first when attempting to resolve hostnames.	Yes CLI: `set network dns primary [address]`

Configuration Data	Description	Editable after Installation
Secondary DNS (optional)	When a primary DNS server fails, Emergency Responder will attempt to connect to the secondary DNS server.	Yes CLI: **`set network dns secondary [address]`**
Domain	Represents the name of the domain in which this machine is located	Yes CLI: **`set network domain [name]`**
Time Zone		
Region	Allows you to select a region for your time zone.	Yes
Time Zone	Reflects the local time zone and offset from Greenwich Mean Time (GMT). Select the time zone that most closely matches the location of your machine.	Yes CLI: **`set timezone [zone`**
Network Time Protocol		
NTP Server IP Address	During installation of the Emergency Responder publisher node, you must specify the IP address of an external Network Time Protocol (NTP) server. We recommend that you use the Emergency Responder publisher node as the NTP server.	Yes In Cisco Unified Operating System Administration Web Interface, select **Settings** > **NTP Servers**.
(Optional) List of Secondary Nodes	This list identifies the secondary nodes (subscribers) in the cluster by host name.	Yes

Touchless Installation Task Flow

Complete these tasks to install your Emergency Responder clusters in a single process using the touchless installation method.

Before you begin

Preinstall Tasks for Emergency Responder

Procedure

	Command or Action	Purpose
Step 1	Generate Answer Files for Touchless Install, on page 77	Use this procedure to generate the configuration files (clusterconfig.xml and platformconfig.xml) with your network settings. The touchless install process uses these files to install and configure the various cluster nodes.
Step 2	Generate ISO Images, on page 78	Use this procedure to create ISO images from the answer files. You will use the ISO image in your touchless installation.
Step 3	Upload ISO Image to Datastore, on page 78	Use this procedure to upload the ISO image to the datastore.
Step 4	Mount ISO Image to VM, on page 78	Use this procedure to mount the UC application ISO image on their corresponding VM.
Step 5	Run Touchless Install, on page 79	Begin the cluster installation. You can kick off all node installations simultaneously.

Generate Answer Files for Touchless Install

Use this procedure to generate answer files for your touchless installation of your cluster. The answer files (clusterconfig.xml and platformconfig.xml) contain the configuration information that the install process installs and configures on each cluster node.

Before you begin

You must have already planned your network topology, including addresses for your Emergency Responder cluster nodes.

Procedure

Step 1 Log in to the Cisco Emergency Responder Answer File Generator application at https://www.cisco.com/c/en/us/applicat/content/cuc-afg/index.html.

Step 2 In the **Hardware** section, choose **Virtual Machine**.

Step 3 From the **Product** section, select the product and version that you want to install.

Step 4 Complete the remaining fields under **Clusterwide Configuration** with your cluster configuration details.

Step 5 Complete the fields in the **Primary Node Configuration** with configuration details for the publisher node.

Step 6 Under **Secondary Node Configuration**, enter the node details for your subscriber node and click **Add Secondary Node**.

Step 7 Add your subscriber node.

Step 8 Click **Generate Answer Files**.

Step 9 Download the answer files to your computer.

Generate ISO Images

Use this procedure to create ISO images from the answer files. You will use the ISO images in your touchless installation.

Note This procedure describes how to use Winimage to create ISO images. You can download Winimage from http: www.winimage.com download.htm.

Procedure

Step 1 From Winimage, choose **File** > **New**.

Step 2 From the Standard format, choose **1.44 MB** and click **OK**.

Step 3 Navigate to the Menu Image, choose **Inject** and select the `platformConfig.xml` file.

Step 4 When prompted to inject the file into Winimage, click **Yes**.

Step 5 Choose **File** > **Save As**.

Step 6 Save the file as an ISO image (.iso file) using the following naming convention: `Emergency Responder—cer.iso`.

Step 7 Repeat these steps for the other Emergency Responder server groups in the cluster.

Upload ISO Image to Datastore

Use this procedure to upload the ISO images to the datastore.

Procedure

Step 1 Start the vSphere client.

Step 2 Select the **Configuration** tab.

Step 3 Select **Storage**.

Step 4 Right-click on a datastore and **Browse** the datastore.

Step 5 Navigate to the destination directory and click the **Upload files to this datastore** icon.

Step 6 Upload the ISO images to your local folder.

Step 7 At the **Upload/Download** warning, click **Yes**.

Step 8 Close the **Datastore Browser** window.

Mount ISO Image to VM

Use this procedure to mount the UC application ISO images on their corresponding virtual machine (VM).

Procedure

Step 1 In the vSphere client, choose the virtual machine.

Step 2 Open VMware Remote Console (VMRC), and click the **CD/DVD Drive 2**.

Step 3 **Browse** to the datastore and locate the ISO image.

Step 4 Select the file and click **OK**.

Step 5 Under **Device Status**, enable the **Connected and Connect at power on** option.

Step 6 Click the **Options** tab. Under **Boot Options**, check **Force entry to BIOS** and click **OK**.

Step 7 Repeat this procedure for each VM on which you want to install a node.

Run Touchless Install

After you have mounted your ISO image to your application VMs, run the touchless installation process. You can install all nodes simultaneously.

Procedure

Step 1 In vSphere client, right-click the **VM** and select **Open Console**. A console window opens.

Step 2 Click the **Power On** icon in the console toolbar to power on the virtual machine.

Step 3 When the BIOS screen appears, configure the following boot order:

a) CD-ROM
b) Hard Drive
c) Removable Devices
d) Network

Step 4 Save the settings and exit from the console. The installation commences immediately.

Step 5 Repeat these steps for each cluster node. All cluster nodes may install in parallel; you do not have to install them serially.

Step 6 After to emphasize the completion of an activity, remove the ISO configurations from the virtual machines.

PART III

Configuration

CHAPTER 4

Configure Cisco Unified Communications Manager

Configure Cisco Unified Communications Manager Overview

This chapter describes procedures for configuring Cisco Unified Communications Manager (Unified CM) for Cisco Emergency Responder (Emergency Responder).

See the Release Notes for Unified CM versions that are compatible with Cisco Emergency Responder.

The procedures describe what you must configure in Unified CM so that Emergency Responder can work in your telephone network.

They also describe a sample Unified CM setup. The names that are chosen (for example, partition and calling search space names) are not required.

Sections with examples represent an example setup, with sample values included for reference only. Your particular configuration depends on the needs of your network and your naming strategy.

For these examples, you work with the following calling search spaces and partitions:

- PhoneCSS - Includes the Phones partition.
- E911CSS - Includes the E911 and Phones partitions.

The examples are based on a single Unified CM cluster. If you have more than one cluster, you must repeat the configuration in each cluster, except for the emergency location identification number (ELIN) translation patterns. The ELIN translation patterns are only defined in the Unified CM cluster to which the gateway sends incoming calls from the public safety answering point (PSAP).

Set Up Phone Route Plans

Before configuring Emergency Responder, you must ensure that the phones that might be used to make emergency calls (typically all phones) are added and registered with Unified CM. See the documentation and online help included with Unified CM if you need assistance.

The following sections provide an example setup for your network before adding Emergency Responder.

Create Phone Partition

If you have not already created a partition for the phones, do so now.

Procedure

Step 1 Select **Call Routing** > **Class of Control** > **Partition** in Cisco Unified Communications Manager.

The Find and List Partitions page appears.

Step 2 Click **Add a New Partition**.

The Partition Configuration page appears.

Step 3 Enter a descriptive name, such as **Phones**, in the **Partition Name and Description** field. You can optionally include a description.

Step 4 Click **Insert** to add the new partition.

Related Topics

Configure Cisco Unified Communications Manager, on page 83
Create Phone Calling Search Space, on page 84
Assign Partition and Calling Search Space to Phones , on page 85

Create Phone Calling Search Space

If you do not already have a calling search space defined for the phones, follow this procedure to create one.

Procedure

Step 1 Select **Call Routing** > **Class of Control** > **Calling Search Space** in Cisco Unified Communications Manager.

The Find and List Calling Search Spaces page appears.

Step 2 Click **Add a New Calling Search Space**.

The Calling Search Space Configuration page appears.

Step 3 Enter a descriptive name, such as **PhoneCSS,** in the **Calling Search Space Name** field.

Step 4 Select the **Phones** partition in the Available Partitions list box, and click the arrow buttons between the two list boxes to add it to the Selected Partitions list box.

Step 5 Click **Insert** to add the new calling search space.

Related Topics

- Create Phone Partition, on page 84
- Configure Cisco Unified Communications Manager, on page 83
- Assign Partition and Calling Search Space to Phones , on page 85

Assign Partition and Calling Search Space to Phones

You can use the Bulk Administration Tool to change the partition and calling search space on telephones in much less time than it takes to make the changes to each phone individually. This procedure describes the phone-by-phone procedure.

After you have created the Phones partition (Create Phone Partition, on page 84) and PhonesCSS calling search space (Create Phone Calling Search Space, on page 84), configure the phones to use them.

Procedure

Step 1 Select **Device** > **Phone**.

Unified CM displays the Find and List Phones page.

Step 2 Select **Device name is not empty** in the search fields and click **Find**.

Unified CM lists all of the phones in the bottom frame.

Step 3 Click the phone with the configuration that you want to change.

Unified CM displays the Phone Configuration page.

Step 4 Change the calling search space to **PhoneCSS** and click **Update**.

Step 5 Click the line number that you want to configure in the left-hand column.

Unified CM displays the Directory Number Configuration page.

Step 6 Change the partition to **Phones**, and the calling search space to **PhoneCSS**.

Step 7 Click **Insert** to save your changes.

Related Topics

- Create Phone Partition, on page 84
- Configure Cisco Unified Communications Manager, on page 83
- Create Phone Calling Search Space, on page 84

Set Up Cisco Unified Communications Manager for Emergency Responder

To handle emergency calls, you must configure the emergency call numbers (such as 911) so that Cisco Emergency Responder (Emergency Responder) intercepts them. Emergency Responder can then route the calls to the correct public safety answering point (PSAP) and transform the call as required to route the call and to enable the PSAP operator to call back the emergency caller if the initial call is disconnected.

The following topics describe how to define the Cisco Unified Communications Manager (Unified CM) elements required for Emergency Responder.

Create Emergency Responder Partition

You must create the Emergency Responder partition E911. This partition contains the numbers used by the PSAP to call into the network and to certain other CTI route points.

Procedure

Step 1 Select **Call Routing** > **Class of Control** > **Partition** in Cisco Unified Communications Manager.

The Find and List Partitions page appears.

Step 2 Click **Add a New Partition**.

The Partition Configuration page appears.

Step 3 Enter a descriptive name, such as **E911**, in the **Partition Name** field.

Step 4 Click **Insert** to add the new partition.

Related Topics

- Create Emergency Responder Calling Search Space, on page 86
- Configure Cisco Unified Communications Manager, on page 83
- Set Up Phone Route Plans , on page 84
- Create Emergency Call Route Points, on page 87
- ELIN Numbers Emergency Calls and PSAP Callbacks , on page 93
- Create Route Patterns for Inter-Cisco Emergency Responder Group Communications, on page 100

Create Emergency Responder Calling Search Space

To create the Emergency Responder calling search space, follow these steps:

Procedure

Step 1 Select **Call Routing** > **Class of Control** > **Calling Search Space** in Cisco Unified Communications Manager.

.

The Find and List Calling Search Spaces page appears.

Step 2 Click **Add a New Calling Search Space**.

The Calling Search Space Configuration page appears.

Step 3 Enter a descriptive name, such as **E911CSS,** in the **Calling Search Space Name** field.

Step 4 In the Available Partitions list box, select the **E911** partition and then select the **Phones** partition in that order. Click the arrow buttons between the two list boxes to add them to the Selected Partitions list box. Arrange the partitions so that E911 is at the top of the list.

If you are using any other partitions, add them to this list after the E911 partition.

Note You must list the E911 partition before the Phones partition for the following reason: When the user configures the translation pattern 911 or 9.911 (see Create Translation Patterns for 9.911, on page 96), the 911 Route Point is in the E911 partition; phones cannot look into the E911 Partition. The 911 Translation Pattern is in the phones partition and gets the E911CSS. When the E911 partition is listed first, it matches the 911 Route Point and the call goes to the Emergency Responder server as intended. If you make the error of listing the Phones partition first, the Translation Pattern keeps searching, resulting in a fast busy signal.

Step 5 Click **Insert** to add the new calling search space.

Related Topics

Create Emergency Responder Partition, on page 86
Configure Cisco Unified Communications Manager, on page 83
Set Up Phone Route Plans , on page 84
Create Emergency Call Route Points, on page 87
ELIN Numbers Emergency Calls and PSAP Callbacks , on page 93
Create Alternate Emergency Call Numbers , on page 99
Set Up Calling Search Space for Gateway and PSAP Connection , on page 100

Create Emergency Call Route Points

You must configure CTI route points in Unified CM for these numbers:

- The emergency call number for your locale, such as 911.

Note If you use 9 as the access code, see Create Translation Patterns for 9.911, on page 96 to configure Emergency Responder.

- The number that your standby Emergency Responder server should listen to, such as 912.
- The number that incoming calls from the public safety answering point (PSAP) use.
- Emergency Responder modifies these calls based on your ELIN configuration to route the call to the person who initiated the emergency call, if the PSAP gets disconnected and needs to call the calling party. See ELIN Numbers Emergency Calls and PSAP Callbacks , on page 93 for information about the rest of the ELIN configuration.

Before you begin

This procedure assumes you are using 911 as the main emergency call number. If a different number is used in your locale, substitute it for 911 and make similar substitutions for other numbers based on 911 such as 912. For example, if the emergency call number in your locale is 112, use 112, and perhaps 113, 114.

When you install Emergency Responder, you are required to enter the emergency call number. In this procedure, configure the same number you specify during installation.

Note CTI route points for the 911, 912, and 913 emergency numbers must be unique. You should not have more than one CTI route point addressed to the emergency numbers used earlier.

The following table describes the emergency call route points.

Table 7: Emergency Call Route Points

Route Point Setting	Route Points		
	Primary Number (911)	**Backup Number (912)**	**ELIN (913)**
Device Name	RP911	RP912	RPELIN913
Description	The emergency call number for the area. Emergency Responder handles all calls to this number.	Route point for the Emergency Responder standby server. If the primary server is unable to handle a call, the standby server receives the call through this route point.	The destination of all incoming calls PSAP. Emergency Responder transfe calls to the emergency caller. The Rou is a prefix (913) plus a Fully Qualified Fully Qualified Number could be No American Numbering Plan or E.164 Country Code. In case the ELIN is re E.164 number with a leading plus sigr a Translation Pattern to remove the le plus sign. **Note** In case the ELIN is rece E.164 number with a leac sign (+), use a Translati Pattern to remove the lea plus sign.
Directory Number	911	912	913XXXXXXXXXX
Partition	Phones	E911	E911
Calling Search Space	E911CSS	E911CSS	E911CSS
Forward Busy	Destination: 912 CSS: E911CSS	Destination: • Route pattern for default ERL. or • Onsite security number. CSS: E911CSS	Destination: Onsite security number. CSS: E911CSS

Route Point Setting	Route Points		
	Primary Number (911)	Backup Number (912)	ELIN (913)
Forward No Answer	Destination: 912 CSS: E911CSS	Destination: • Route pattern for default ERL. or • Onsite security number. CSS: E911CSS	Destination: Onsite security num CSS: E911CSS
Forward On Failure	Destination: 912 CSS: E911CSS	Destination: • Route pattern for default ERL. or • Onsite security number. CSS: E911CSS	Destination: Onsite security num CSS: E911CSS
Voice Mail Mask	Do not configure a Voice Mail Mask for this route point.	Do not configure a Voice Mail Mask for this route point.	Do not configure a Voice Mail M route point.

Note Configuring call-forwarding numbers for the standby server ensures that calls are either routed to the PSAP servicing the default ERL, or onsite security, if the standby server cannot handle the call. If you do not install a standby server, use these settings for the primary server. Configuring call-forwarding numbers for the ELIN route point ensures that PSAP callbacks go to onsite security if Emergency Responder cannot handle the call.

Procedure

Step 1 In Unified CM, select **Device** > **CTI Route Point**.

The Find and List CTI Route Points page appears.

Step 2 Click **Add a new CTI Route Point**.

The CTI Route Point Configuration page appears.

Step 3 Fill in the CTI route point properties:

- Enter a unique name, such as **RP911**, in the **Device Name** field to identify this as the emergency call number. The Emergency call route points table above shows suggested names, but you can use any name you choose.
- Select the appropriate device pool from the **Device Pool** menu.
- Select the calling search space for the route point, as listed in the Emergency call route points table above.

Step 4 Click **Insert** to add the new CTI route point.

Unified CM adds the route point and asks if you want to configure line 1. Click **OK** to configure line 1.

Unified CM opens the Directory Number configuration page.

Step 5 Enter the configuration for the line you are creating using the information in the Emergency call route points table above.

Step 6 Click **Insert**.

Unified CM adds the line to the device. Repeat this procedure until all devices described in the Emergency call route points table above are configured.

For additional assistance, see documentation and online help included with Unified CM.

Related Topics

Create Emergency Responder Partition, on page 86
Create Emergency Responder Calling Search Space, on page 86
ELIN Numbers Emergency Calls and PSAP Callbacks , on page 93
Create Route Patterns for Inter-Cisco Emergency Responder Group Communications, on page 100
Create Alternate Emergency Call Numbers , on page 99
Create Emergency Responder Cisco Unified Communications Manager User, on page 104
Set Up Group Telephony Settings for Server , on page 129
Installation on a New System , on page 63

Create Required CTI Ports

Emergency Responder uses CTI ports to call onsite alert (security) personnel when someone makes an emergency call. You should have enough CTI ports so that each person assigned to an ERL can receive a call. The number of ports that you configure is the number of simultaneous calls Emergency Responder can make to these personnel. It does not relate to the number of emergency calls Emergency Responder can handle or forward to the PSAP. There is no configurable limitation to the number of simultaneous emergency calls that Emergency Responder can handle.

Before you begin

Emergency Responder requires that the CTI port extension numbers be in succession, so you must find a block of unused extensions. For example, if you want to create four CTI ports starting at 3001, then 3001, 3002, 3003, and 3004 must all be available.

Procedure

Step 1 Select **Device** > **Phone**.

Cisco Unified Communications Manager opens the Find and List Phones page.

Step 2 Click **Add a New Phone**.

Cisco Unified Communications Manager opens the Add a New Phone page.

Step 3 Select **CTI Port** for **Phone Type** and click **Next**.

Cisco Unified Communications Manager opens the Phone Configuration page.

Step 4 Configure the CTI Port, entering this information:

- **Device Name**- Enter something meaningful to you, for example, CTI3001.
- **Device Pool**- Select an appropriate device pool. This device pool must use the G.711 region.
- **Calling Search Space**- Select **PhoneCSS**.

Step 5 Click **Insert**.

Cisco Unified Communications Manager creates the CTI port and asks if you want to configure line 1. Click **OK**. Cisco Unified Communications Manager opens the Directory Number Configuration page.

Step 6 Configure line 1 for the CTI port, entering this information:

- **Partition**- Select **Phones**.
- **Calling Search Space**- Select **PhoneCSS**.

Note Configure only one line for each CTI port. Onsite security alert prompts may not get from one or more of these lines when the online alert notification is initiated through these ports.

Step 7 Click **Insert**.

Cisco Unified Communications Manager adds the line to the device. Repeat the procedure to create each CTI route port that you require.

Note All subsequent CTI ports you create must be consecutive from the first CTI port DN.

CTI port DN in Cisco Emergency Responder does not support E.164 dial pattern.

Related Topics

Create Emergency Responder Partition, on page 86
Create Emergency Responder Calling Search Space, on page 86
Create Emergency Responder Cisco Unified Communications Manager User, on page 104
Identify Cisco Unified Communications Manager Clusters , on page 132
ERL Creation , on page 138

Create a Cisco Unified Communications Manager Group for Cisco Emergency Responder

A Cisco Unified Communications Manager (Unified CM) Group is a list of up to three Unified CMs that are assigned to a device pool to assist with call processing. The first Unified CM in the list acts as the primary Unified CM for the Group and the other members act as secondary and tertiary or backup Unified CMs. By creating a Unified CM Group, you can balance the call process load across multiple Unified CMs and ensure a level of redundancy for your network.

Because each device pool has one Unified CM Group assigned to it, a Unified CM Group improves your load distribution across a device pool. When a device registers, it attempts to connect to the primary Unified CM in the Unified CM Group. If the primary Unified CM is not available, the device tries to connect with the secondary Unified CM. If the secondary Unified CM is not available, the device tries to connect to the tertiary Unified CM.

You must create a Unified CM Group for Emergency Responder.

Note The primary Cisco Unified CM in the Group assigned to the device pool for Cisco ER must also be the primary CTI Manager for Cisco Emergency Responder. The Group must also contain the secondary CTI manager for Cisco ER.

Procedure

Step 1 Select **System > Unified CM Group**.

The Find and List Unified CM Groups page opens.

Step 2 Click **Add New**.

The Unified CM Group Configuration page opens.

Step 3 Enter the following information in the appropriate field:

- **Name** – Enter a CM Group name that is meaningful to you; for example, Cisco Emergency Responder CM Group.
- **Auto-registration Cisco Unified Communications Manager Group** - Do not check this box for the Unified CM Group for Emergency Responder.
- **Cisco Unified Communications Managers** – Add the primary and secondary CTI Manager for Emergency Responder to the list of Selected Cisco Unified Communications Managers by selecting each from the Available Cisco Unified Communications Managers and clicking the **Down Arrow**.

Step 4 Click **Save**.

Error and System Messages

Unified CM generates several alarms to assist you in troubleshooting Emergency Responder problems. You should set up notification of Emergency Responder events so that an email notification alerts you to such important events.

The following table shows the relevant alarms.

Table 8: Relevant Unified CM Alarms

Relevant Alarms	Alarm Level	Explanation
CtiProviderOpened	Informational	Application ope
CtiProviderClosed	Informational	Application clos

Relevant Alarms	Alarm Level	Explanation
ApplicationConnectionDropped	Warning	TCP or TLS and Applicat
CtiIncompatibleProtocolVersion	Warning	The Cisco E Unified Com compatible v

By default, only Error events are posted to the event log. You should modify the event level to post warnings and set up a customer alert if the Emergency Responder user closes its applications or ports.

To do this, navigate to the Serviceability Web Page by selecting **Alarm >Configuration>Server>Service Group (CM Services)>Service (Cisco CTI Manager)**. Change the Alarm Event Level to Error to have all of the last three alarms in the above table posted to SysLog.

These alarms are systemwide alarms and not specific to Emergency Responder. So any CTI application that triggers a warning message will post to the event log and not only Emergency Responder. You should set up notification of Unified CM events relevant to Emergency Responder so that if the provider goes out of service, an email or other notification event will alert you.

ELIN Numbers Emergency Calls and PSAP Callbacks

Emergency calls are routed based on the calling party number, not the called party number. If an emergency call is disconnected for some reason (for example, the caller hangs up), the PSAP needs to be able to call back the emergency caller using the calling party number. The PSAP might also want to call back to obtain updated information after ending an emergency call normally.

Emergency Responder converts a caller extension to an emergency location identification number (ELIN), and this number is used to route the call and to enable PSAP callbacks. Emergency Responder reuses the same set of numbers, and keeps track of the internal extension of the phone from which the call was made for up to three hours. When there is no active association of an ELIN to an internal phone extension, Emergency Responder routes calls to that ELIN to on-site security.

To set up the ELIN numbers, you must first obtain direct inward dial (DID) numbers from your service provider. Because you must pay for each number, you might want to limit the number of DIDs you obtain to two or three per ERL. The DIDs must be unique for each ERL.

Emergency Responder reuses the ELIN numbers assigned to an ERL if necessary. For example, if you configure two numbers for an ERL, and three emergency calls are made within a three-hour period, the first emergency caller's ELIN mapping is replaced by the third caller's extension. If the PSAP tries to call the first caller, the PSAP reaches the third caller. This information will help as you determine the number of DIDs you need for each ERL.

See ERL Creation , on page 138 for information about how to configure the ERLs with these numbers.

Create Route Patterns for ERLs

Emergency Responder uses route patterns to route emergency calls to the local public safety answering point (PSAP). In the route pattern, you are associating a pattern with a gateway that connects to the PSAP. The gateway you choose depends on the emergency response location (ERL) to which you assign the route pattern.

You must create one route pattern for every ERL in your network. These are the direct inward dial (DID) numbers you obtain from your service provider for the purpose of allowing the PSAP to call into your network.

Before you begin

Each ERL requires unique route patterns for the ELINs. Work with the ERL administrator to get an idea of how many route patterns are needed, and the locale of the ERLs so that you can select an appropriate gateway. The ERL administrator must enter the route patterns you create into the ERL definition. See ERL Creation , on page 138 for information about ERLs.

Procedure

Step 1 Select **Call Routing** > **Route/Hunt** > **Route Pattern** in Cisco Unified Communications Manager.

Unified CM opens the Find and List Route Patterns page.

Step 2 Click **Add a New Route Pattern**.

Unified CM opens the Route Pattern Configuration page.

Step 3 Enter the information for the route pattern:

- **Route Pattern** - A pattern that you can transform to the emergency call number, typically a number, a dot, and the emergency call number. For example, 10.911, 11.911, and so forth. The pattern can only contain numbers and dots.
- **Partition** - Select **E911**.
- **Numbering Plan** - Select the numbering plan for your area.
- **Gateway/Route List** - Select the gateway to use for connecting to the local PSAP.
- **Route Option** - Select **Route this pattern**.
- **Use Calling Party's External Phone Number Mask** - Select this option.
- **Discard Digits** - Select **PreDot** if you use the suggested pattern, such as 10.911. If using a different technique, select the appropriate setting and enter a **Called Party Transform Mask** if necessary (to dial the emergency number).

Step 4 Click **Insert**.

Unified CM saves the route pattern. To add additional route patterns, return to Step 2, on page 94.

Tip Consider developing a detailed naming strategy for the route patterns because you might end up with a large number of them. For example, you could use a pattern such as xyzzaaab.911, where x is a Emergency Responder cluster identifier; y is a Emergency Responder group identifier; zz is the PSAP identifier; aaa is the ERL identifier; and b is the ELIN identifier (within the ERL).

Related Topics

Create Translation Patterns for ELINs, on page 95

Create Emergency Responder Partition, on page 86

Configure Cisco Unified Communications Manager, on page 83
ERLs, on page 135
ERL Creation , on page 138

Create Translation Patterns for ELINs

Create translation patterns that cover the direct inward dial (DID) numbers you are using for ELIN numbers. The PSAP uses these ELINs to call into your network. Emergency Responder needs to intercept these calls so it can route the call to the correct emergency caller. The translation pattern is required so that a number prefixed to the ELIN becomes the route point you configured for PSAP callbacks, as explained in the Create Emergency Call Route Points, on page 87.

Before you begin

Ensure that you have a list of all the DIDs you are using for ELINs.

Procedure

Step 1 Select **Call Routing** > **Translation Pattern** in Cisco Unified Communications Manager.

Unified CM opens the Find and List Translation Patterns page.

Step 2 Click **Add a New Translation Pattern**.

Unified CM opens the Translation Pattern Configuration page.

Step 3 Create the translation pattern:

- **Translation Pattern** - The DID you are using as an ELIN. If you can, use X variables to create a pattern that covers more than one DID (for example, 5555551XXX). If you cannot create a pattern, define translation patterns for each DID separately.
- **Partition** - Select **E911**.
- **Numbering Plan**- Select the numbering plan for your area.
- **Calling Search Space** - Select **E911CSS**.
- **Route Option** - Select **Route this pattern**.
- **Called Party Transformations, Prefix Digits (Outgoing Calls)**—Enter the digits to prefix to the number. Enter the digits you used when creating the PSAP callback route point.

Step 4 Click **Insert**.

Unified CM saves the translation pattern. To add additional translation patterns, return to Step 2, on page 95.

Related Topics

Create Route Patterns for ERLs, on page 94
Configure Cisco Unified Communications Manager, on page 83
ERLs, on page 135
ERL Creation , on page 138

Create Translation Patterns for 9.911

In systems where the external access code is 9, a CTI Route Point of 911 or 9.911 may interfere with the timing of secondary dialtone for users when they are attempting to dial external destinations. The creation of a translation pattern for 911 and 9.911 eliminates the secondary dialtone timing.

Create translation patterns so that when users dial the local system external access code of 9 plus 911, the calls are directed to the single 911 pattern previously created in the Create Emergency Call Route Points, on page 87.

Before you begin

This procedure applies to systems where the external access code is 9. If the external access code is something other than 9, this procedure may not apply.

To complete this procedure, you must have already added the partitions and the calling search space for the CiscoEmergencyResponder installation.

The following table provides translation patterns for external access code of 9.

Table 9: Translation Patterns for External Access Code of 9

Translation Pattern	911	9.911
Partition	Phones	Phones
Calling Search Space	E911CSS	E911CSS
Route Option	Route this pattern	Route this pattern
Provide outside dial tone	Check this box	Check this box
Called Party Transformations, Discard Digits (Outgoing Calls)	None	PreDot

Procedure

Step 1 Select **Call Routing** > **Translation Pattern** in Cisco Unified Communications Manager.

Unified CM opens the Find and List Translation Patterns page.

Step 2 Click **Add a New Translation Pattern**.

Unified CM opens the Translation Pattern Configuration page.

Step 3 Create the translation pattern:

- **Translation Pattern** - 911.
- **Partition** - Phones.
- **Numbering Plan** - Select the numbering plan for your area.
- **Calling Search Space** - Select **E911CSS**.
- **Route Option** - Select **Route this pattern**.
- **Provide Outside Dial Tone** - Make sure that this box is checked.
- **Called Party Transformations, Discard Digits** - Select <none>.

Step 4 Click **Insert**.

Unified CM saves the translation pattern.

Step 5 Repeat Step 2, on page 95 to Step 4, on page 95 with the following changes:

- **Translation Pattern**—9.911
- **Called Party Transformations, Discard Digits (Outgoing Calls)**—PreDot

After you have configured the 9.911 translation patterns, you must create the route points. Table 9: Translation Patterns for External Access Code of 9, on page 96 provides emergency call route points for 9.911.

Note These route points are similar to the route points that you created in the Create Emergency Call Route Points, on page 87. In this case, you enter E911 for the partition instead of Phones.

Table 10: Emergency Call Route Points for 9.911

Route Point Setting	Route Points		
	Primary Number (911)	**Backup Number (912)**	**ELIN (913)**
Device Name	RP911	RP912	RPELIN913
Description	The emergency call number for the area. Emergency Responder handles all calls to this number.	Route point for the Emergency Responder standby server. If the primary server is unable to handle a call, the standby server receives the call through this route point.	The destination of all incoming c PSAP. Emergency Responder tra calls to the emergency caller. Rou prefix (913) plus 10 Xs. Number be the same as the standard phone in your locale based on your num The number can only consist of r Xs.
Directory Number	911	912	913XXXXXXXXXX
Partition	E911	E911	E911
Calling Search Space	E911CSS	E911CSS	E911CSS
Forward Busy	Destination: 912 CSS: E911CSS	Destination: • Route pattern for default ERL. or • Onsite security number. CSS: E911CSS	Destination: Onsite security num CSS: E911CSS

Route Point Setting	Route Points		
	Primary Number (911)	Backup Number (912)	ELIN (913)
Forward No Answer	Destination: 912 CSS: E911CSS	Destination: • Route pattern for default ERL. or • Onsite security number. CSS: E911CSS	Destination: Onsite security number. CSS: E911CSS
Forward On Failure	Destination: 912 CSS: E911CSS	Destination: • Route pattern for default ERL. or • Onsite security number. CSS: E911CSS	Destination: Onsite security number. CSS: E911CSS

Note Configuring call-forwarding numbers for the standby server ensures that calls are either routed to the PSAP servicing the default ERL or to onsite security, if the standby server cannot handle the call. If you do not install a standby server, use these settings for the primary server. Configuring call-forwarding numbers for the ELIN route point ensures that PSAP callbacks go to onsite security if Emergency Responder cannot handle the call.

Related Topics

Create Route Patterns for ERLs, on page 94

Configure Cisco Unified Communications Manager, on page 83

ERLs, on page 135

Create Route Points for 9.911

Procedure

Step 1 In Unified CM, select **Device** > **CTI Route Point**.

The Find and List CTI Route Points page appears.

Step 2 Click **Add a new CTI Route Point**.

The CTI Route Point Configuration page appears.

Step 3 Fill in the CTI route point properties:

- Enter a unique name, such as **RP911**, in the **Device Name** field to identify this as the emergency call number. Table 9: Translation Patterns for External Access Code of 9, on page 96 shows suggested names, but you can use any name you choose.

- Select the appropriate device pool from the **Device Pool** menu.
- Select the calling search space for the route point, as listed in Table 9: Translation Patterns for External Access Code of 9, on page 96.

Step 4 Click **Insert** to add the new CTI route point.

- Unified CM adds the route point and asks if you want to configure line 1. Click **OK** to configure line 1.
- Unified CM opens the Directory Number configuration page.

Step 5 Enter the configuration for the line that you are creating using the information in Table 9: Translation Patterns for External Access Code of 9, on page 96.

Step 6 Click **Insert**.

Unified CM adds the line to the device. Repeat this procedure until all devices described in Table 9: Translation Patterns for External Access Code of 9, on page 96 are configured.

For additional assistance, see the documentation and online help included with Unified CM.

Related Topics

Create Route Patterns for ERLs, on page 94
Configure Cisco Unified Communications Manager, on page 83
ERLs, on page 135

Create Alternate Emergency Call Numbers

If your users are used to dialing 9 (or another number) to get an outside line, they might try to dial the emergency number by first dialing the outside line access number. For example, if the emergency number is 911, they might try to dial 9911. If you want to accommodate these possibilities, configure translation patterns for the numbers you think are likely to be used. This procedure shows how to set up 9911 as an alternate emergency call number.

Procedure

Step 1 Select **Call Routing** > **Translation Pattern**.

Unified CM opens the Find and List Translation Patterns page.

Step 2 Click **Add a New Translation Pattern**.

Unified CM opens the Translation Pattern Configuration page.

Step 3 Create the translation pattern:

- **Translation Pattern** - The number you want to support as an emergency number. In this example, 9.911.
- **Partition** - Select **Phones**.
- **Numbering Plan** - Select the numbering plan for your area.
- **Calling Search Space** - Select **E911CSS**.
- **Route Option** - Select **Route this pattern**.
- **Provide Outside Dial Tone** - Select this.
- **Called Party Transformations, Discard Digits (Outgoing Calls)** - Select **PreDot**.

Step 4 Click **Insert**.

Unified CM saves the translation pattern. To add additional translation patterns, return to Step 2, on page 95.

Related Topics

Configure Cisco Unified Communications Manager, on page 83
Create Phone Partition, on page 84
Create Phone Calling Search Space, on page 84

Set Up Calling Search Space for Gateway and PSAP Connection

You must set up a gateway to use a CAMA or PRI connection to the emergency network or PSTN so that emergency calls can be routed to the local PSAP. See the documentation for your gateway for information about setting up the gateway, and the Unified CM documentation for configuring the gateway. After you set up the gateway, you can follow this procedure to set up the calling search space for the gateway.

Procedure

Step 1 Select **Device** > **Gateway**.

Unified CM opens the Find and List Gateways page.

Step 2 Click **Find** without entering search criteria to list all of the gateways, or enter the search criteria required to list the gateway you want to configure and click **Find**.

Unified CM lists the gateways that match your criteria.

Step 3 Click the gateway you want to configure.

Unified CM opens the Gateway Configuration page.

Step 4 Select **E911CSS** for **Calling Search Space**.

Step 5 Click **Update**.

Unified CM saves your changes.

Related Topics

Create Emergency Responder Calling Search Space, on page 86
CAMA and PRI Trunks , on page 36
Emergency Responder Deployment , on page 39
Emergency Responder and Your Network , on page 22

Create Route Patterns for Inter-Cisco Emergency Responder Group Communications

If you have more than one Emergency Responder group in an Emergency Responder cluster, you must configure route patterns to enable each Emergency Responder group to route emergency calls to another Emergency Responder group if a caller's phone homes to a Unified CM cluster outside the current location of the phone. See Cisco Emergency Responder Clusters , on page 30 for a detailed explanation of how Emergency Responder groups communicate within a Emergency Responder cluster.

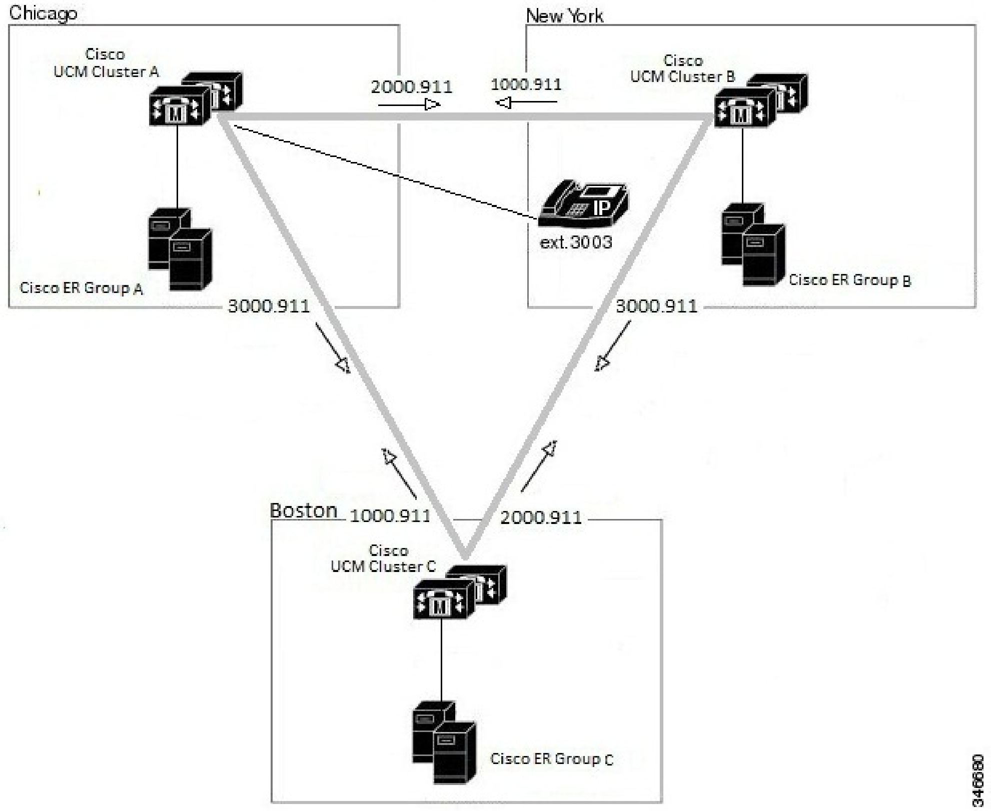
This procedure explains how to create the route pattern for one Emergency Responder group. The Inter-Cisco ER Group Route Pattern defined on a Emergency Responder Group is a route pattern for incoming Emergency Calls. Consider the network setup in the following figure.

For inter-group communications to work:

- You must define inter-cluster trunks in each Unified CM cluster to enable communications between the Unified CM clusters. See the Unified CM documentation for information about creating these types of gateways.
- Define the route pattern on the Unified CM
  - Define route pattern 2000.911 and 3000.911 in CUCM cluster A.
  - Define Route Pattern 1000.911 and 3000.911 in CUCM cluster B.
  - Define Route Pattern 1000.911 and 2000.911 in CUCM cluster C.
- Define Inter-Emergency Responder Group Route Pattern
  - In Emergency Responder Group A, define 1000.911 as the Inter-Emergency Responder Group Route Pattern.
  - In Emergency Responder Group B, define 2000.911 as the Inter-Emergency Responder Group Route Pattern.
  - In Emergency Responder Group C, define 3000.911 as the Inter Emergency Responder Group Route Pattern.

These definitions allow a call in an ERL managed by Emergency Responder Group B to be routed to Emergency Responder Group B even though the phone homes to Unified CM cluster A, which is serviced by Emergency Responder Group A.

Figure 19: Understanding Inter-Cisco Emergency Responder Group Route Patterns



Related Topics

Create Emergency Responder Partition, on page 86
Set Up Group Telephony Settings for Server , on page 129
Installation on a New System , on page 63

Create Route Patterns on Unified CM

Before you begin

The dial plans must be unique between all Unified CM clusters supported by a Emergency Responder cluster. For example, in the network shown in Create Route Patterns for Inter-Cisco Emergency Responder Group Communications, on page 100, the extension 3003 can only be defined in Unified CM cluster CUCM-A.

Procedure

Step 1 Go to Cisco Unified CM Administration. Select **Call Routing** > **Route/Hunt** > **Route Pattern**.

Unified CM opens the Find and List Route Patterns page.

Step 2 Click **Add New**.

Unified CM opens the Route Pattern Configuration page.

Step 3 Enter the information for the route pattern:

- **Route Pattern**— A pattern that you can transform to the emergency call number, typically a number, a decimal point, and the emergency call number. For example, 1000.911 or 2000.911. The pattern can only consist of numbers and decimal points.
- **Partition** — Select **E911**.
- **Numbering Plan** — Select the numbering plan for your area.
- **Gateway/Route List** — Select the inter-cluster trunk gateway to use for connecting to the Unified CM cluster supported by the Emergency Responder group whose inter-Emergency Responder group route pattern you are defining.
- **Route Option** — Select **Route this pattern**.
- **Called Party Transformations: Discard Digits** — Select **PreDot** if you use the suggested pattern, such as 1000.911. If using a different technique, select the appropriate setting and enter a **Called Party Transform Mask**, if necessary to dial the emergency number.

Step 4 Click **Save**.

Unified CM saves the route pattern. To add additional route patterns, return to Step 2, on page 94.

Note Ensure that you define the route pattern in all other Unified CM clusters serviced by Emergency Responder groups other than the Emergency Responder group whose Inter-Emergency Responder group route pattern you are defining.

Note For emergency calls to work across Emergency Responder Server Groups in a Emergency Responder cluster with Unified CM 8.5 or later, the Calling Party Selection option should be set to Originator in the **Device> Trunk Configuration** page in Unified CM Administration website.

Create an Inter-Emergency Responder Group Route Pattern

Note Ensure you define the Inter-Emergency Responder Route pattern in all other Cisco Emergency Responder groups.

Procedure

Step 1 Go to Cisco Emergency Responder Administration. Select **System** > **Telephony Settings**.

Step 2 Add the Inter-Emergency Responder Route pattern.

Step 3 Update Settings.

Create Emergency Responder Cisco Unified Communications Manager User

You must add Emergency Responder as a Unified CM user. The settings you enter here are used when you configure the Unified CM settings for Emergency Responder.

Procedure

Step 1 In Unified CM, select **User Management** > **Application User**. Click the **Add New** button.

Unified CM displays the Application User Configuration page.

Step 2 Complete the following required fields:

- **UserID**—Use a descriptive name such as "Emergency_Responder_User."
- **Password**—Enter a password for this user.
- **Confirm Password**—Reenter the password for this user.

Step 3 In the **Device Information** section, select the desired route points and CTI ports and then click the down arrow to add the selected devices to the user control list. The list of devices appears in the Controlled Devices area.

Step 4 Select the following devices:

Note You may need to use Find Phones or Find Route Points to select the desired devices.

- All CTI ports created for Cisco Emergency Responder use. For more information, see "Creating the Required CTI Ports" section.
- The primary emergency call number, for example, 911.
- The backup emergency call number, for example, 912.
- The route point used for ELINs, for example, 913XXXXXXXXXX.

Step 5 Click **Save**.

Step 6 In the Unified CM menu at the top, click **User Management** > **User Group**.

The user group search page appears.

Step 7 At search criterion, enter standard and click **Find**.

The list of user groups starting with the name standard appears.

Step 8 Click the **Standard CTI Allow Calling Number Modification** user group link to display the User Group configuration page.

Step 9 Click **Add Application Users to Group**.

The Find and List Application Users popup window appears.

Step 10 Enter the User ID and click **Find**.

The list of Applications users appears.

Step 11 Check the check box next to the user ID and click **Add Selected**.

Unified CM adds the selected user to the Standard CTI Allow Calling Number Modification user group.

Step 12 Choose **User Management** > **User Group**.

The user group search page appears.

Step 13 Enter **standard** as the search criterion and click **Find**.

The list of user groups starting with the name Standard appears.

Step 14 Click the **Standard CTI Enabled** group.

Repeat steps 9 through 11 to add the user to the Standard CTI Enabled group.

Related Topics

Create Emergency Call Route Points, on page 87

Create Required CTI Ports, on page 90

CHAPTER 5

Configure Cisco Emergency Responder

Cisco Emergency Responder Configuration Overview

After you install Cisco Emergency Responder (Emergency Responder) and configure Cisco Unified Communications Manager (Unified CM), you can configure Emergency Responder so that it begins managing emergency calls.

Configuration Overview

Emergency Responder provides several features, including expanded administrative website interfaces, role-based user management, and upload and download utilities.

Note Emergency Responder is compatible with Cisco EnergyWise, including provisions to detect user activity on powered-down phones.

Website Interfaces

Emergency Responder provides several web sites from which you can access and use different parts of the system. From the main Emergency Responder web page, you can access the following areas:

- Emergency Responder Serviceability
- Emergency Responder Administration (default home)
- CiscoUnifiedOS Administration
- Disaster Recovery System
- Emergency Responder User
- Emergency Responder Admin Utility

Each of these web sites allows a user access to different parts of the system and requires a separate login and password. Access to these web sites is controlled through the role-based user management mechanism (for more information, see Role-Based User Management , on page 108).

When the Emergency Responder system is first installed, a default Emergency Responder Administrator user is created. The default Administrator has full access to all web sites except the Cisco Unified OS Administration and Disaster Recovery System websites, and can create users, roles, and user groups. The default Administrator cannot be deleted from the system.

Related Topics

Cisco Emergency Responder Administration Web Interface
Cisco Emergency Responder Serviceability Web Interface , on page 509
Cisco Unified Operating System Administration Web Interface , on page 527
Disaster Recovery System Web Interface , on page 563

Role-Based User Management

Emergency Responder uses a role-based user management mechanism. The information in the following topics describe this mechanism.

User Management

On installation, the system creates one default user, Emergency Responder Administrator. The Emergency Responder Administrator has access to all system administration screens except the Platform Administration and Disaster Recovery System screens. By default, the Emergency Responder Administrator user is assigned to the Emergency Responder System Administrator, Emergency Responder Serviceability, Emergency Responder Admin Utility, and Emergency Responder User user groups and has access to the resources defined for the Emergency Responder System Admin, Emergency Responder Serviceability, Emergency Responder Admin Utility, and Emergency Responder User roles.

Note The default Emergency Responder Administrator user cannot be deleted.

You can add additional users. After the additional users are added, you assign them to user groups. The new user then inherits the roles that were defined for that user group.

Related Topics

- Emergency Responder User Management , on page 117
- Find and List Users, on page 463

Role Management

On installation, the system creates six default roles. The following table lists and describes the default roles.

Note Default roles cannot be deleted.

Table 11: Default Roles

Role	Description
Emergency Responder System Admin	Has access to all system administration screens.
Emergency Responder Serviceability	Has access to all serviceability screens.
Emergency Responder Admin Utility	Has access to all Admin Utility screens.
Emergency Responder Network Admin	Has access to Cisco Unified Communications Manager, LAN switch, and SNMP settings screens.
Emergency Responder ERL Admin	Has access to all ERL-related screens.
Emergency Responder User	Has access to the user screens.

When creating a new role or modifying an existing role, you specify which system resources are assigned to the role. A resource is the same thing as a web page or a menu item within the Emergency Responder administration website. For example, the **Find and List Roles** web page is a resource, as is the **User Management** > **Role menu** item.

The following table shows the resources that are available to each default role.

Note Some resources are groups of menu items. For example, the Logs menu in the Cisco Emergency Responder Serviceability website is one resource but it contains many submenus.

Table 12: Resources Assigned to Default Roles

Resource	Emergency Responder System Admin	Emergency Responder Network Admin	Emergency Responder ERL Admin	Emergency Responder Serviceability	Emergency Responder Admin Utility	Emer Resp User
Add Subscriber	x					
Admin Utility	x					
ALI Formatting Tool	x					

Resource	Emergency Responder System Admin	Emergency Responder Network Admin	Emergency Responder ERL Admin	Emergency Responder Serviceability	Emergency Responder Admin Utility	Emergen Respond User
All Logs				x		
Application User	x					
Call History	x					
Unified CM Details	x	x				
Emergency Responder Groups in Cluster	x					
Change Unified CM Version					x	
Cluster DBHost Setting					x	
Control Center				x		
CPU and Memory Usage				x		
Device SNMP Settings	x	x				
Disk Usage				x		
ERL	x		x			
ERL Audit Trail	x					
ERL Debug Tool	x					
ERL Migration	x		x			
Event Viewer				x		
File Management Utility	x					
Functional role	x					
National E911 Service Provider ERL	x		x			
National E911 Service Provider VUI Settings	x					
IP subnet	x		x			
License Management	x					
Mail Alert Configurations	x					
Manually Configured Phones	x		x			

Resource	Emergency Responder System Admin	Emergency Responder Network Admin	Emergency Responder ERL Admin	Emergency Responder Serviceability	Emergency Responder Admin Utility	Emer Resp User
MIB2 System Group Configuration				x		
Off-Premises ERL	x		x			
Onsite Contact	x		x			
Pager Alert Configurations	x		x			
Phone Search						x
Point to New Publisher					x	
Processes				x		
PS ALI Convert	x					
PS ALI Export	x					
Purge	x					
Run Tracking	x	x				
Tracking Schedule	x	x				
Server	x					
Server Group	x					
LAN Switches	x	x				
SNMP V1/V3c Configuration				x		
SNMP V3 Configuration				x		
Switch Port	x		x			
Synthetic Phone	x		x			
Telephony	x					
Unlocated Phones	x		x			
User Call History						x
User Group	x					
User Settings	x					
Web Alert						x

Related Topics

Emergency Responder Role Management , on page 121
Find and List Roles, on page 467

User Group Management

On installation, the system creates six default user groups. The following table lists and describes the default user groups.

Note Default user groups cannot be deleted.

Table 13: Default User Groups

User Group	Description
Emergency Responder System Administrator	Assigned System Administration roles
Emergency Responder Network Administrator	Assigned Network Administration role
Emergency Responder ERL Administrator	Assigned ERL Administration role
Emergency Responder Serviceability	Assigned Serviceability role
Emergency Responder Admin Utility	Assigned Admin Utility role
Emergency Responder User	Assigned User role

You can create additional user groups. When you create a user group, you assign roles and add users to the group. Multiple roles can be assigned to a single group. The users in the group have access to all the resources defined by the roles assigned to the group.

Related Topics

Emergency Responder User Group Management , on page 123
Find and List User Groups, on page 470

Upload and Download Utilities

Emergency Responder includes download and upload utilities that allow you to transfer bulk data in the form of csv files from a Emergency Responder server to a local system (download) and from a local system to a Emergency Responder server (upload).

For example, you can export database details to a csv file and then download the csv file to a local system. On the local system, you can modify the csv file, upload it the Emergency Responder server, and import the data in the csv file into the Emergency Responder database.

The following table lists the Emergency Responder administrative web pages from which you can use the upload and download utilities and gives the navigation path to each page.

Note You can upload only four file types: xml, csv, lic, and txt. Filenames must not contain spaces.

Table 14: Administrative Web Pages Containing the Upload and Download Utilities

Page Name	Navigation Path
Find Conventional ERL Data	**ERL** > **Conventional ERL**
Find Off-Premises ERL Data	**ERL** >**Off-premises ERL** >**Off-premises ERL (Search and List)**
Find National E911 Service Provider ERLs Data	**ERL** > **National E911 Service Provider ERL** > **National E911 Service Provider ERL (Search and List)**
LAN Switch Details	**Phone Tracking** > **LAN Switch Details**
Switch Port Details	**ERL Membership** > **Switch Ports**
Find and List IP subnets	**ERL Membership** > **IP subnets**
Find and List Manually Configured Phones	**ERL Membership** > **Manually Configured Phones**

Download File

Procedure

Step 1 From one of the pages listed in Table 14: Administrative Web Pages Containing the Upload and Download Utilities , on page 113, click **Export**. The Export page appears.

Step 2 If you have previously exported the data to a file, skip to Step 3. If you have not previously exported data to a file, use the **Select Export Format** pulldown menu to select the file format, then enter the name of the file to be created in the **Enter Export File Name** field. Click **Export**. The data is exported to the specified file.

Step 3 Use the Select a File to Download pulldown menu to select the file that you want to download, then click **Download**. The file is downloaded to your local system.

Upload File

Before you begin

Before beginning the procedure, make sure the file to be uploaded exists on your local system. The file can be one that was previously downloaded from a Emergency Responder server, or one that you created.

Procedure

Step 1 From one of the pages listed in Table 14: Administrative Web Pages Containing the Upload and Download Utilities , on page 113, click **Import**. The Import page appears.

Step 2 Click **Upload**. The Upload File page appears.

Step 3 Click **Browse** to select the file to be uploaded. A Choose File window opens and displays the files on your local system.

Step 4 Select the file to be uploaded and click **Open**. The pathname of the file to be uploaded appears in the **Select the file to be uploaded** field of the Upload File page.

Step 5 Click **Upload**. The file is uploaded to the Emergency Responder server. You can then import the data from the file.

Related Topics

Conventional ERL, on page 394
LAN Switch Details, on page 434
Switch Port Details, on page 438
Find and List IP Subnets (Applicable only until Release 15)
Find and List Manually Configured Phone, on page 457
File Management Utility, on page 485

Emergency Responder Configuration

The following procedure provides information about the tasks that must be completed to configure Emergency Responder and indicates which user types can complete the tasks, with pointers to more detailed information.

Note Some of the following tasks listed can be done in parallel.

Procedure

	Command or Action	Purpose
Step 1	Create and set up Emergency Responder users and groups.	This step can be completed by the System Administrator.
Step 2	Identify the switches and configure the connection to them.	This step can be completed by the Network Administrator.
Step 3	Identify the onsite alert (security) personnel, create the emergency response locations (ERLs), assign them to phones, and transmit your ALI data to your service provider.	This step can be completed by the ERL Administrator.
Step 4	Set up Emergency Responder with National E911 Service Provider for Enterprise Service.	

Related Topics

Set Up Users and Groups , on page 115
Set Up Switch Connection , on page 116
Manage Onsite Alerts, ERLs, and ALI Data , on page 116
Set Up Emergency Responder with National E911 Service Provider for Enterprise Service , on page 117

Set Up Users and Groups

The following procedure provides information about the tasks that must be completed to set up Emergency Responder users and groups. This task can be completed by a System Administrator.

Procedure

	Command or Action	Purpose
Step 1	Create the users your organization requires for Emergency Responder administration.	
Step 2	Create the Emergency Responder group.	
Step 3	Set up the Emergency Responder group telephony settings.	
Step 4	Update Emergency Responder servers to the Emergency Responder group.	
Step 5	Upload the product license key.	
Step 6	Identify and configure the Unified CM clusters whose emergency calls this Emergency Responder group handles.	The network administrator can also perform this step.
Step 7	Understand recurring system administration tasks.	
Step 8	If you use National E911 Service Provider Service Provider for Enterprise Service, configure Emergency Responder to support National E911 Service Provider Service Provider for Enterprise Service.	
Step 9	If you support off-premise users, configure AXL authentication information with Unified CM.	

Related Topics

Emergency Responder Configuration , on page 114
Emergency Responder User Management , on page 117
Log In to Emergency Responder , on page 126
Set Up a Server Group, on page 128
Set Up Group Telephony Settings for Server , on page 129
Configure Servers , on page 131
Identify Cisco Unified Communications Manager Clusters , on page 132
Emergency Responder System Administrator Role , on page 312
Set Up National E911 Service Provider VUI Settings , on page 187
Set Up AXL Authentication , on page 277

Set Up Switch Connection

The following procedure provides information about the tasks that must be completed to set up Emergency Responder switch connection. This task can be completed by a Network Administrator.

Procedure

- Enter the SNMP read community strings.
- Define the schedule Emergency Responder should use for updating information from the switches.
- Identify the switches that can have phones connected to them.
- Run the switch-port and phone update process so that Emergency Responder can identify the ports on the switches and whether phones are attached to them.
- Understand recurring network administration tasks.

Related Topics

Emergency Responder Configuration , on page 114
Set Up SNMPv2, on page 149
Define Phone Tracking and Switch Update Schedules, on page 152
LAN Switch Identification , on page 153
Manually Run the Switch-Port and Phone Update Process , on page 157
Emergency Responder Network Administrator Role , on page 311

Manage Onsite Alerts, ERLs, and ALI Data

The following procedure provides information about the tasks that must be completed to Manage onsite alerts, ERLs, and ALI data. This task can be completed by an ERL Administrator.

Procedure

- Identify the onsite alert (security) personnel that should receive alerts from Emergency Responder.
- Create the ERLs.
- Assign the ERLs to switch ports.

Note The network administrator must add the switches and run the switch-port and phone update process before you can do this task.

- Add phones that Emergency Responder does not directly support.

Note Emergency Responder does not automatically track the movement of these phones.

- Identify the unlocated phones and work with the network administrator to resolve problems that are preventing Emergency Responder from locating these phones. Assign ERLs to the phones that remain.
- Export the ALI data and transmit it to your service provider. Work with your service provider to determine transmission requirements.
- Understand recurring ERL administration tasks.

Related Topics

Emergency Responder Configuration , on page 114
ERLs, on page 135
ERL Management , on page 136
Add Onsite Security Personnel, on page 137
ERL Creation , on page 138
Switch Port Configuration , on page 159
Manually Define Phones , on page 168
Identify Unlocated Phones , on page 167
Export ERL Information , on page 146
Export ALI Information for Submission to Your Service Provider , on page 147
Emergency Responder ERL Administrator Role , on page 310

Set Up Emergency Responder with National E911 Service Provider for Enterprise Service

The following tasks apply when you use Emergency Responder with National E911 Service Provider for Enterprise Service:

Procedure

Step 1 Create National E911 Service Provider ERL and verify the validity and consistency of the ALI data for the National E911 Service Provider ERL against the National E911 Service Provider TN database.

Step 2 Assign National E911 Service Provider ERLs to switch ports, IP subnets, and unlocated phones.

Step 3 If you support off-premise users, create off-premise ERLs and assign to IP subnets and unlocated phones.

Note You cannot assign off-premise ERLs to switch ports.

Related Topics

Emergency Responder Configuration , on page 114
Reconcile ALI Discrepancies , on page 190
Switch Port Configuration , on page 159
Identify Unlocated Phones , on page 167

Emergency Responder User Management

When you install Emergency Responder, the system defines one default Emergency Responder Administrator user (see User Management , on page 108 for more information). You can also define additional users or modify existing users.

The information in the following sections describe how to add new users and how to modify and delete existing users.

Add Users

You can add users to the system and then assign them to user groups. The security levels for new users are determined by which user groups you assign them to.

In Emergency Responder, you can add a user either as a local user or a remote user. Remote users must use their Unified CM credentials or Active Directory credentials for authentication.

You can add users to either the primary and standby servers within a single Emergency Responder group. Because access is allowed based on the combination of the user groups defined on the two servers, a user that is defined only on the primary server can log into the backup server.

Before you begin

Develop a list of users for each security level. You must know the user names of all onsite alert personnel, and you should determine who should have access to each of the administration security levels.

Note You can use this procedure to add or remove users. However, you cannot remove the administrative user created at the time of Emergency Responder installation.

Procedure

Step 1 From the Emergency Responder Administration web interface, select **User Management > User**.

The Find and List Users page appears.

Step 2 Click the **Add New User** button. The User Configuration page appears.

Step 3 Enter the required information in the User Name, Authentication Mode, Password, Confirm Password and Unified CM Cluster fields.

Step 4 Click **Insert**.

Step 5 Repeat these steps to add additional users.

Step 6 To assign security levels to the new users, you must add them to one or more user groups.

Step 7 Repeat this procedure on the other Emergency Responder server in the Emergency Responder server group.

Note To remove a user from a group, you must remove the user from groups on both the primary and standby servers.

Modify Users

After you have created a user, you can change user authentication mode, change the password for a local user, or change a Unified CM cluster for a remote user.

Change User Authentication Mode

Procedure

Step 1 From the Emergency Responder Administration web interface, select **User Management** > **User**.

The Find and List Users page appears.

Step 2 Enter search criteria to find the specific user that you want to modify and click **Find**, or click **Find** without any search criteria to display all configured users. The search results are displayed.

Step 3 Click on the user name.
The User Configuration—Modify User page appears.

Step 4 Select the authentication mode that you want to assign to the user from the drop-down box:

- If you select Remote as the authentication mode, select a Unified CM Cluster from the drop-down box.
- If you select Local as the authentication mode, enter a password and reconfirm the password.

Step 5 Click **Update**.

Change Password for a Local User

Procedure

Step 1 From the Emergency Responder Administration web interface, select **User Management** > **User**.

The Find and List Users page appears.

Step 2 Enter search criteria to find the specific user that you want to modify and click **Find**, or click **Find** without any search criteria to display all configured users. The search results are displayed.

Step 3 Click on the user name.
The Modify User page, used for user configuration, appears.

Step 4 Select the authentication mode that you want to assign to the user from the drop-down box.

If you select Local as the authentication mode, enter a new password and reconfirm the new password.

Step 5 Click **Update**.

Change a Unified CM Cluster for a Remote User

In Emergency Responder, you can also change the Unified CM cluster of an existing remote user to another Unified CM Cluster.

Procedure

Step 1 From the Emergency Responder Administration web interface, select **User Management** > **User**.

The Find and List Users page appears.

Step 2 Enter search criteria to find the specific user that you want to modify and click **Find**, or click **Find** without any search criteria to display all configured users. The search results are displayed.

Step 3 If you select Remote as the authentication mode, select a Unified CM Cluster from the drop-down box. The User Configuration—Modify User page appears.

Step 4 Select the new Unified CM Cluster for all the remote users.

Step 5 Click **Update**

Delete Users

Emergency Responder enables you to perform batch operations in which you can either delete a single user or delete multiple users in bulk.

Note You cannot delete the default administrative user created at the time of installing Emergency Responder.

Procedure

Step 1 From the Emergency Responder Administration web interface, select **User Management** > **User**.

The Find and List Users page appears.

Step 2 Enter search criteria to find the specific user that you want to delete and click **Find**, or click **Find** without any search criteria to display all configured users. The search results appear.

Step 3 Find the user that you want to delete and click the **Delete** icon for that user.

The system displays a warning prompting you to confirm the deletion.

You also can select multiple users from the list, both local and remote, by checking the check box and then clicking the **Delete Users** button to delete users in bulk.

The system displays a warning prompting you to confirm the deletion.

Step 4 Click **OK**. The user is removed from the system and all User Group associations to the user are deleted.

Related Topics

Log In to Emergency Responder , on page 126

Cisco Emergency Responder User Preparation , on page 309

Changing Users to Remote in Bulk

Emergency Responder allows you to change the user to either local or remote. A remote user is authenticated using the Unified CM Cluster.

Before you begin

Note You must have system administrator or ERL administrator authority to access this page.

Procedure

Step 1 From the Emergency Responder Administration web interface, select **User Management** > **User**.

The Find and List Users page appears.

Step 2 Enter search criteria to find the specific user that you want to delete and click **Find**, or click **Find** without any search criteria to display all configured users. The search results appear.

Step 3 Click **Username**. The Modify User page, used for user configuration, appears.

Step 4 Select the authentication mode that you want to assign to the user. You can change a local user to remote user.

Step 5 Select an Unified CM Cluster from the drop-down box if you have changed the user to remote user.

Step 6 Click **Update**.

Note To change users in bulk, select the users that you want to change by checking the check box and then clicking the **Change to Remote Users** button. Select the Unified CM cluster from the drop-down box, as described in Step 6.

Emergency Responder Role Management

When you install Emergency Responder, the system defines six default roles (see Role Management , on page 109 for more information about the default roles). You can also define additional roles or modify existing roles.

The following topics describe how to add new roles and how to modify and delete existing roles.

Add Roles

You can add additional roles to the system and assign resources to them.

Note The default roles cannot be removed or modified.

Before you begin

Decide what additional roles you want to create and determine if any existing default role meets your needs.

Procedure

Step 1 From the Emergency Responder Administration web interface, select **User Management** > **Roles**.

The Find and List Roles page appears.

Step 2 Click **Add a New Role**.

The Role Configuration page appears.

Step 3 Enter the Role Name (required) and Description (optional) in the text boxes.

Step 4 From the list of resources, check the check box next to the resources to which the new role should have access.

Step 5 Click **Insert** to add the new role to the system.

Step 6 Verify that you successfully added the new role by returning to the **User Management** > **Roles** page and performing a role search. Enter search criteria to find the specific role you just created and click **Find**, or click **Find** without any search criteria to display all configured roles. The search results appear. Verify that the new role is listed.

Modify Roles

Note You cannot modify default roles.

Procedure

Step 1 From the Emergency Responder Administration web interface, select **User Management** > **Roles**.

The Find and List Roles page appears.

Step 2 Enter search criteria to find the specific role that you want to modify and click **Find**, or click **Find** without any search criteria to display all configured roles. The search results appears.

Step 3 Click the role name.

The Role Configuration—Modify Role page appears.

Step 4 If desired, modify the Role Name and Description (if one is listed) in the text boxes.

Step 5 From the list of resources, checking or unchecking the check boxes next to the resources to which the modified role should have access.

Step 6 Click **Update** to add the updated role information to the system.

Step 7 Verify that you successfully modified the new role by returning to the **User Management** > **Roles** page and perform a role search. Enter search criteria to find the specific role that you just modified and click **Find**, or click **Find** without any search criteria to display all configured roles. The search results appear. Click the role name and verify that the modified role information appears on the Role Configuration—Modify Role page.

Delete Roles

Note You cannot delete a default role.

Procedure

Step 1 From the Emergency Responder Administration web interface, select **User Management** > **Roles**.

The Find and List Roles page appears.

Step 2 Enter search criteria to find the specific role that you want to delete and click **Find**, or click **Find** without any search criteria to display all configured roles. The search results appear.

Step 3 Click the **Delete** icon for the role to be deleted.

A warning message displays asking you to verify that you want to delete the role.

Step 4 Click **OK** to delete the role.

The Find and List Roles page refresh and the roles are no longer listed in the Role Names list.

Emergency Responder User Group Management

When you install Emergency Responder, the system defines six default user groups (see User Group Management , on page 112 for more information about the default user groups). You can also define additional user groups or modify existing user groups.

You can create a user group to receive web alert from a specific ERL. You must associate this User Group with the Onsite Alert ID assigned for an ERL. For additional information, see Add Onsite Security Personnel.

Note The group members can still view all web alerts in the system, if applicable.

The following topics describe how to add new user groups and how to modify existing user groups.

Add User Groups

You can add user groups to the system and assign users and roles to each new user group.

Before you begin

Before you begin, you should decide what additional user groups that you want to create and determine if any existing default user groups meets your needs.

Procedure

Step 1 From the Emergency Responder Administration web interface, select **User Management > User Group**.

The Find and List User Groups page appears.

Step 2 Click **Add a User Group**.

The User Group Configuration—Add User Group page appears.

Step 3 Enter the User Group Name (required) and Description (optional) in the text boxes.

Step 4 Click **Add Users**.

The User Names page appears.

Step 5 Enter search criteria to find a specific user and click **Find**, or click **Find** without any search criteria to display all configured users. The search results appear.

Step 6 Check the check box to the left of the user names to be added and click **Add**.

The User Name page closes and the added names appears in the Add User to Group text box on User Group Configuration—Add User Group page.

Note To delete users from this list, select the user name and click **Remove Users**.

Step 7 Click **Add Roles**.

The Role Names page appears.

Step 8 Enter search criteria to find a specific role and click **Find**, or click **Find** without any search criteria to display all configured roles. The search results appear.

Step 9 Check the check box to the left of the roles to be added and click **Add**.

The Role Names page closes and the added roles appear in the Add Roles to Group text box on User Group Configuration page.

Note To delete roles from this list, select the user name and click **Delete Roles**.

Step 10 Click **Insert** to add the new role to the system.

Modify User Groups

Note You cannot modify default user groups.

Procedure

Step 1 From the Emergency Responder Administration web interface, select **User Management > User Group**.

The Find and List User Groups page appears.

Step 2 Enter search criteria to find the specific user group that you want to modify and click **Find**, or click **Find** without any search criteria to display all configured user groups. The search results appear.

Step 3 Click the user group name.

The User Group Configuration—Modify User Group page appears.

Step 4 (Optional) Modify the description of the User Group (if one is listed) in the **Description** text box.

Step 5 The **Add Users to Group** text box displays the names of the users currently assigned to the user group. To add additional users, follow the procedure given in the Add User Groups , on page 123.

To remove users, highlight the name of the users and click **Remove Users**.

Step 6 The **Assign Roles to Group** text box displays the names of the roles currently assigned to the user group. To add additional roles, follow the procedure given in the Add Roles , on page 121.

To remove roles, highlight the name of the roles and click **Remove Roles**.

Step 7 When you are finished, click **Update** to save the updated user group information to the system.

Step 8 Verify that you successfully modified the user group by returning to the **User Management > User Group** page and performing a search. Enter search criteria to find the specific user group that you just modified and click **Find**, or click **Find** without any search criteria to display all configured user groups. The search results appear. Click the user group name and verify that the modified user group information appears on the User Group Configuration—Modify User Group page.

Delete User Groups

Note You cannot delete the default user groups. You can only delete user groups that you have created.

Procedure

Step 1 From the Emergency Responder Administration web interface, select **User Management > User Group**.

The Find and List User Groups page appears.

Step 2 Enter search criteria to find the specific user group that you want to delete and click **Find**, or click **Find** without any search criteria to display all configured user groups. The search results appear.

Step 3 Click the **Delete** icon for the user group to be deleted.

Note You cannot delete the default user groups. You can only delete user groups that you have created.

A warning message appears asking you to verify that you want to delete the user group.

Step 4 Click **OK** to delete the user group.

The Find and List Roles page refresh and the deleted user group is no longer be listed in the User Groups list.

Cisco Emergency Responder Credential Policy

Cisco Emergency Responder includes an option to modify credential policy settings values. The system administrator can now enhance the security for all local and remote user accounts by modifying the default policy settings either in Credential Policy or in EnhancedSecurityMode Credential Policy.

For more information about the fields and their configuration options, see Credential Policy Page, on page 473.

Log In to Emergency Responder

You must log into the Emergency Responder web interfaces to view or change the system configuration. The system administrator controls access using the Role-Based User Management mechanism. See Role-Based User Management , on page 108 for more information.

Before you begin

You must have a valid user ID and password before you can log into Emergency Responder. Contact the main Emergency Responder administrator if you cannot log into the interface and you are supposed to have administrative access.

Procedure

Step 1 From an supported browser, open this URL, where servername is the DNS name or IP address of the Emergency Responder server: http://servername/ceradmin.

The browser opens the Emergency Responder Server Administration page.

Step 2 Use the Navigation pull-down menu to select the website that you want to log into. The Emergency Responder websites are as follows:

- Emergency Responder Serviceability
- Emergency Responder Administration
- CiscoUnified OS Administration
- Disaster Recovery System
- Emergency Responder User
- Emergency Responder Admin Utility

To open the Log-in page, click one of websites in the list.

Step 3 Click **Go.**

The login screen for the selected website appears.

Step 4 Enter your user name and password, and click **Login**.

Emergency Responder logs you into the selected website. Unless you log in as a system administrator, some commands in the menus may have lock icons. These locks indicate pages that you cannot view because of your authorization level.

When you are finished, click **Logout** above the menu bar to log out.

Note In Emergency Responder 8.5 and above, the validation for Username is not case sensitive.

Related Topics

Emergency Responder User Management , on page 117
Emergency Responder Role Management , on page 121
Emergency Responder User Group Management , on page 123
Cisco Emergency Responder User Preparation , on page 309

Restrict Maximum Number of Concurrent Sessions

Emergency Responder allows the administrator to restrict the maximum number of concurrent sessions that can be active at a time for any user. If this restriction is enabled, the administrator can specify a maximum limit (between 1 and15) for the number of concurrent sessions allowed.

This limit is applicable to all users configured in Emergency Responder.

Emergency Responder restricts users from creating more than the specified number of concurrent sessions. Users who attempt to create additional sessions that exceed the concurrent session limit are prevented from logging in to Emergency Responder and will see the following error message: **Session limit exceeded. Please log out of any existing sessions and try again**.

Note This limit is applicable to all users that exceed the limit.

Note This limit is imposed separately for each Emergency Responder website:

- Emergency Responder Administration
- Emergency Responder Serviceability
- Emergency Responder User
- Emergency Responder Admin Utility

Warning If a user logs in to an Emergency Responder website and closes the browser without logging out, the session remains active until it times out after a period of 30 minutes. During this period, if the user attempts to establish additional sessions beyond the prescribed limit, he will be unable to do so.

Before you begin

You must have system administrator authority to configure an Emergency Responder server group.

Procedure

Step 1 Select **System** > **CiscoER Group Settings**.

Emergency Responder opens the Emergency Responder Group Settings page.

Step 2 Check the **Limit Concurrent Sessions** check box. This option is used to enable limiting the number of concurrent sessions and enables the **Max. number of concurrent sessions** drop-down box.

Step 3 Select the maximum number of concurrent sessions that you want to impose on the Emergency Responder user, from the **Max. number of concurrent sessions** drop-down box.

Step 4 Click the **Update Settings** button to apply the new change.

Note You can disable the maximum number of concurrent settings by selecting **System** > **Emergency Responder Group Settings** and uncheck the **Limit Concurrent Sessions** check box.

Related Topics

Group Settings, on page 363

Server and Server Group Configuration

The information in the following topics describe how to configure Emergency Responder servers and server groups, and the telephony connection between the Emergency Responder groups and Unified CM.

Set Up a Server Group

To configure a Emergency Responder server group, you must connect to the administration interface on one of the servers that is part of the group. An Emergency Responder server group consists of up to two Emergency Responder servers, a primary and a standby, or backup, server. This redundancy helps ensure that Emergency Responder remains available in case one server becomes disabled.

Consider placing the two servers in a group in separate physical locations so that problems that might affect one server do not affect the other, such as a fire, flood, or network disruption. See Data Integrity and Reliability, on page 34 for more information.

Before you begin

You must have system administrator authority to configure an Emergency Responder server group.

Procedure

Step 1 Select **System** > **CiscoER Group Settings**.

Emergency Responder opens the Emergency Responder Group Settings page.

Step 2 Fill in the group settings. Many fields have defaults that should work for most networks. At minimum, you must configure these fields:

- **CiscoER Group Name**—Enter a name for the group. This name is mainly for your use, so choose a name that you find meaningful.
- **SMTP Mail Server** and **Source Mail ID**—If you want Emergency Responder to send email alerts to your Emergency Responder system administrator and onsite alert personnel (security), enter the IP address or DNS name of a mail server, and the name of an account on that server to use for sending email. If you configure email addresses for onsite alert personnel, they receive email alerts from this account when an emergency call is made in their assigned area. If their email address is for an email-based paging system, they are paged.
- **Enable Secured connection**— If you want to send mails from the SMTP Mail Server in a secure mode, ensure to configure the SMTP Mail Server in a secure mode and the SMTP server certificate is added to the Tomcat trust store of the Cisco Emergency Responder prior to enabling the Enable Secure connection checkbox. Failing to do so may result in email alert delivery failure.
- **System Administrator Mail ID**—If you want Emergency Responder to send email alerts in the case of critical errors, enter the email account information for the system contact.
- **Calling Party Modification flag**—You must set this flag if you enabled Calling Party Modification when you created Emergency Responder as a Cisco Call Manager user.
- **Enable Syslog** and **Syslog Server**—You can configure Emergency Responder to send log messages to the Syslog Server. To do this, select **Enable Syslog** and enter the fully qualified DNS name of the Syslog server.
- **Security end user web interface language**—To display the Emergency Responder User web pages in French (Canada) or Spanish(Spain), select it in the drop-down box. The default language is English(US).
- **Enable AXL & Cluster Secured connection**—To secure cluster communication and AXL communication with other products. Ensure the Cisco Unified Communications Manager tomcat-trust certificate and the Cisco Emergency Responder server group certificate is added to the Tomcat trust store of the Cisco Emergency Responder (in both publisher and subscriber). Failing to do so may result in breaking of AXL communication between Cisco Unified Communications Manager and Cisco Emergency Responder, along with the cluster communication within the Cisco Emergency Responder group.

Step 3 When you are satisfied with your settings, click **Update Settings**.

Emergency Responder creates the Emergency Responder group.

Related Topics

Configure Servers , on page 131
Group Settings, on page 363
Collect Information From Syslog , on page 356

Set Up Group Telephony Settings for Server

You must configure the telephony settings to tell Emergency Responder which phone numbers it should use for emergency calls and ELINs.

Before you begin

You must have system administrator authority to configure the telephony settings.

Before you configure these settings, create the required route points and route patterns in Unified CM. See these topics for more information:

- Create Emergency Call Route Points
- Create Route Patterns for Inter-Cisco Emergency Responder Group Communication

Procedure

Step 1 Select **System** > **Telephony Settings**.

Emergency Responder opens the Telephony Settings page.

Step 2 Enter the telephony settings, as described in the Telephony Settings , on page 368:

- **UDP Port Begin**—The first UDP port Emergency Responder can use for telephone calls. For example, 32000.
- **Inter Cisco ER Group Route Pattern**—The route pattern that other Emergency Responder groups use to route emergency calls to this group, for example, 1000.911.
- **PSAP Callback Route Point Pattern**—The CTI route point you created to receive calls from the PSAP. For example, 913XXXXXXXXXX (913 plus 10 Xs).
- **ELIN Digit Strip Pattern**—The digits to strip from the PSAP callback route point to reveal the ELIN. For example, 913.
- **Default ELIN Digit Translation**— If the Emergency Responder does not find a mapping between the caller's extension and ELIN, it will translate ELIN to Default ELIN Digit Translation Number and complete the PSAP call back.
- **Route Point for Primary Cisco ER Server**—The route point you created for the Emergency Responder primary server to use. For example, 711. You may change this number. See Modify the Emergency Number , on page 130.
- **Route Point for Standby Cisco ER Server**—The route point you created for the Emergency Responder standby server to use. For example, 912.
- **IP Type of Service (00-FF)**—The value of the type of service (ToS) byte in the IP header. The default 0xB8 implies a ToS class of Priority Queue. We recommend that this default value be used for Emergency Responder.
- **Onsite Alert Prompt Repeat Count**—The number of times a prompt is given on the onsite security phone.
- **National E911 Service Provider Route Pattern**—The route pattern for an National E911 Service Provider emergency response location (ERL).

Step 3 Click **Update Settings** to save your changes.

Modify the Emergency Number

You can configure or modify the emergency number that was automatically set at installation time by entering the number in the **Route Point for Primary CiscoER Server** field**.** Before you configure or change the emergency number, you must configure the new route point and associate it with the Emergency Responder user in Unified CM.

Caution Modify the emergency number during off-peak hours.

Procedure

Step 1 Associate the new route point with the Emergency Responder user in Unified CM. See Create Emergency Responder Cisco Unified Communications Manager User, on page 104.

Step 2 Modify the route point for the new number: enter the number in the **Route Point for Primary CiscoER Server.** field.

Step 3 Click **Update Settings**.

Note Emergency Responder can still support only one emergency number. After you change it, Emergency Responder starts routing calls received at the new emergency number route point.

Related Topics

Telephony Settings , on page 368
Create Emergency Call Route Points, on page 87
Create Route Patterns for ERLs, on page 94
Create Route Patterns for Inter-Cisco Emergency Responder Group Communications, on page 100
Identify Cisco Unified Communications Manager Clusters , on page 132

Configure Servers

After you create an Emergency Responder group, you can use the Server Settings page to update Emergency Responder server settings (for example, to change the server name or to change the trace and debug settings) and to delete servers.

Before you begin

You must have system administrator authority to update or delete a Emergency Responder server.

Procedure

Step 1 Select **System** > **Server Settings**.

Emergency Responder opens the Server Settings page.

Step 2 Select the server name in the left-hand Servers list to change the server settings (Server Name or Debug Package List, or Trace Package List settings). Emergency Responder loads the server settings into the edit boxes. Make your changes and click **Update**.

Step 3 Select the server and click **Delete** to remove a server from the group. If you are permanently removing the server from your network, ensure that you make any required changes to your telephony network so that calls are not misdirected or dropped.

Step 4 When you are satisfied with your settings, click **Update**.

Emergency Responder saves your changes and displays them in the list of servers at the top of the page.

Related Topics

Installation on a New System , on page 63

Set Up a Server Group, on page 128

Set Up Group Telephony Settings for Server , on page 129

Identify Cisco Unified Communications Manager Clusters , on page 132

Server Settings for Emergency ResponderServerGroup , on page 370

Identify Cisco Unified Communications Manager Clusters

You must identify one Unified CM server per Unified CM cluster that you want to manage with the Cisco Emergency Responder group that you are configuring. Cisco Emergency Responder obtains the list of phones registered with these Unified CM servers and tracks the movements of these phones

CiscoEmergency Responder provides three levels of CTI failover. To enable the three levels of CTI failover, enter an IP address or DNS name for the primary CTI Manager, the Backup CTI Manager 1, and the Backup CTI Manager 2.

Before you begin

You must have system administrator or network administrator authority to identify the Unified CM clusters.

You must activate Cisco Unified Communications Manager on the server before Emergency Responder can access the Unified CM cluster list. For more information, refer to CSCsx52550 using the Software Bug Toolkit.

Every Unified CM server in the Unified CM cluster must be running SNMP services so that Emergency Responder can obtain the required information from the server.

Before configuring these settings, create the required users and CTI ports. This information must be complete before Cisco Emergency Responder tries to create a provider with the Cisco Emergency Responder cluster. Cisco Emergency Responder only registers the CTI ports and route points that are associated with the user when the provider is created. See these topics for more information:

- Create Emergency Responder Cisco Unified Communications Manager User, on page 104
- Create Required CTI Ports, on page 90

To identify one Unified CM server per Unified CM cluster that you want to manage with the Cisco Emergency Responder group you are configuring, follow these steps:

Procedure

Step 1 Select **Phone Tracking** > **CiscoUnifiedCommunicationsManager Details**.

Cisco Emergency Responder opens the Unified CM Details page.

Step 2 Enter the details for the Unified CM server:

- **CiscoUnifiedCommunicationsManager**—The IP address or DNS name of the server. This server must be running Unified CM and SNMP services. Do not define more than one Unified CM server within the same Unified CM cluster in the Emergency Responder configuration.

- **CTI Manager**—The IP address or DNS name of the CTI manager for the cluster to which the server belongs.
- **CTI Manager User Name**—The user you created for CiscoEmergencyResponder. See Create Emergency Responder Cisco Unified Communications Manager User, on page 104 for more information.
- **CTI Manager Password**—The user password.
- **Backup CTI 1 Manager**—The IP address or DNS name of the first backup CTI manager for the cluster.
- **Backup CTI 2Manager**—The IP address or DNS name of the second backup CTI manager for the cluster.
- **Telephony Port Begin Address**—The first CTI port address in the sequence of ports you created for Emergency Responder use. See Create Required CTI Ports, on page 90 for more information.
- **Number of Telephony Ports**—The number of CTI ports in the sequence you created for Emergency Responder use.

Step 3 To establish secure JTAPI communications, do the following:

a) Check the **Enable Secure Connection** check box.

b) Enter the following required information:

- TFTP Server IP Address
- TFTP Server Port

Note The TFTP Server Port field is pre-populated with a default value. If in Unified CM you entered a different value for the TFTP Server Port, you must enter that value here, replacing the default value.

- CAPF Server IP Address
- CAPF Server Port

Note The CAPF Server Port field is pre-populated with a default value. If in Cisco Unified CommunicationsManager you entered a different value for the CAPF Server Port, you must enter that value here, replacing the default value.

- Instance ID for Publisher
- Secure Authentication String for Publisher
- Instance ID for Subscriber
- Secure Authentication String for Subscriber

Note You must also configure secure JTAPI communications on your Cisco Unified CommunicationsManager cluster. See Create Required CTI Ports, on page 90 for details.

Step 4 To configure the AXL Settings, do the following:

a) Enter the AXL Username configured on the Cisco Unified Communications Manager.

b) Enter the password for the AXL User.

c) Enter the Port Number. By default Port 8443 is chosen.

Step 5 Select the **SNMP Settings** checkbox if the Cisco Unified Communications Manager has SNMPv3 enabled and Emergency Responder should discover it using SNMPv3.

Step 6 Click **Insert**.

Emergency Responder adds the Unified CM server to the list of servers. Repeat this procedure if you are supporting other Unified CM clusters with this Emergency Responder group.

Tip

- To view or change a Unified CM server settings, click the server in the list of servers. The settings are loaded into the edit boxes. To change a setting, edit it and click **Update**.
- To remove a Unified CM server from the Emergency Responder configuration, click it in the list of servers, then click **Delete.**

Related Topics

Cisco Unified Communications Manager Clusters, on page 427

Set Up Emergency Responder Cluster and Cluster DB Host

Procedure

Step 1 Identify the following:

- All the Emergency Responder groups participating in the Emergency Responder cluster
- One of the Emergency Responder publishers as “Cluster DB Host”
- A password that is the same across the Cluster as “Cluster password”

Step 2 Using the Emergency Responder Admin Utility web interface, navigate to **Update** > **ClusterDB Host,** and enter the values from Step 1.

Step 3 Repeat steps 1 and 2 for each Emergency Responder server group in the cluster.

Step 4 Restart Emergency Responder services.

Note Emergency Responder server groups can communicate with Emergency Responder1.3, 2.x, 7.1 and 8.0 and later versions of Emergency Responder server groups in an Emergency Responder cluster.

Related Topics

Update Cluster DB Host, on page 574

Update Emergency Responder Cluster Database Host Details , on page 306

Cisco Unified Communications Manager Cluster Changes

If you change or upgrade the Unified CM cluster identified in Emergency Responder to a later version, you must use the Admin Utility to identify Emergency Responder with the later Unified CM version.

To change the Unified CM cluster that is identified in Emergency Responder to a different version, see Change Cisco Unified Communications Manager Version , on page 305.

Work with Emergency Responder Locations

An emergency response location (ERL) defines the area in which an emergency call is made. Security personnel and emergency response teams use ERL information to locate an emergency caller.

Note Unified CM supports alerts to onsite security personnel from Cisco Emergency Responder and PSAP Callback on phones that have the Do-Not-Disturb or Call Forwarding feature enabled. For phones with a shared line, the PSAP Callback rings on all the devices that share the same DN.

Emergency Responder system administrators or ERL administrators can create and modify ERLs. The following sections explain ERLs in greater detail and explain how to work with them in Emergency Responder.

ERLs

An emergency response location (ERL) is a building, area within a building, or outside area (if you extend phone service outdoors) that is to be considered as a single location for emergency response purposes. All telephones within the ERL are treated as coming from the same location.

When someone makes an emergency call, the public safety answering point (PSAP) and your onsite alert (security) team are notified of the ERL. If the emergency requires locating the individual who placed the emergency call, the response teams will have to find the person within the ERL. You can include more specific information using the Phone Location field for individual switch ports. This level of detail is only available for automatically tracked phones, and only appears on the Web Alert screen for onsite alert personnel.

This is similar to the way emergency calls are handled for individual home users: emergency response teams know the house from which the call was placed, but have to search from room to room until they find the caller. The bigger the house, the longer the potential search. Likewise, the larger you make your ERLs, the longer it might take a response team to find an emergency caller.

The laws relating to size of ERLs can vary for different cities, states, and countries. You are responsible for learning your local statutes and developing ERLs that satisfy those statutes. Work with your telephone service provider; they can help you understand the laws. Ultimately, you have to submit the automatic location information (ALI) for your ERLs to your service provider so that calls from your ERLs are routed to the appropriate PSAPs.

Here are some examples of possible ERLs:

- You have a 25-story building, each floor has 10,000 square feet of office space. You might create 25 ERLs, one per floor, or you could divide each floor in half and create 50 ERLs, two per floor.
- You have 5 buildings. Each building was a former home, and they are approximately 3000 square feet. You might create 5 ERLs, one per building, even though some of the buildings are multistory.
- You have a 5-story building, but the building is very large, so that each floor has 100,000 square feet of office space. You might create 20 ERLs per floor for a total of 100 ERLs, each ERL covering approximately 5,000 square feet.
- You have a high concentration of telephones, and local standards require that an ERL have no more than 48 telephones. In this case, you have to define zones based on telephone coverage, rather than on physical space. Try to create zones that are recognizable as a physical location, for example, BldJFloor5Row3.

Related Topics

ERL Management , on page 136
ERL Creation , on page 138
Export ERL Information , on page 146
E911 and Cisco Emergency Responder Terminology , on page 6
Emergency Call Process , on page 26

ERL Management

To establish a useful set of ERLs, consider following these steps:

1. Become familiar with local statutes on emergency call requirements. Local laws might have specific requirements or recommendations on the maximum size of an ERL (for example, no larger than 7,000 square feet).

2. Talk to your service provider to learn about their rules or recommendations.

3. Work with the security personnel in your organization to determine what they feel is required for them to effectively respond to an emergency call. Besides having suggestions about the size of the various zones, security personnel should also review the ERL-naming strategy because the ERL name is one of the major data points they use to locate the emergency caller.

   Security personnel also can use these fields to help locate a caller:

   - The Location field in the ALI, which you can use to clarify ERL names, for example, by including the complete street address of the building. Although security can also view the ALI from the Emergency Responder user interface, it takes a few extra steps to view the entire ALI, so including a complete address in the Location field can expedite response.

   - The Phone Location field associated to the switch port. You can use this field to fine-tune the location, for example, by specifying the office or cube number that the port serves.

4. Use Emergency Responder to enter information about your security (onsite alert) personnel. You should enter this information before defining the ERLs, because during ERL definition you assign personnel to each ERL.

5. Use Emergency Responder to define the ERLs and their ALI. See ERL Creation , on page 138 for more information.

6. Assign switch ports to the correct ERL and define the phone location for the port. See Switch Port Configuration , on page 159 for more information. Someone with network administrator authority must first add the switches to the Emergency Responder configuration before you can complete this task.

7. Define any phones that are not directly supported by Emergency Responder. See Manually Define Phones , on page 168, for more information.

8. After you are satisfied with the ERL and ALI definitions, export the ALI information and submit it to your service provider. Work with your service provider to determine the file format and submission requirements. You must submit this information so that emergency calls from your ERLs can be routed to the correct public safety answering point (PSAP). See Export ERL Information , on page 146 and the Export ALI Information for Submission to Your Service Provider , on page 147 for more information.

After you complete this task, emergency calls from your ERLs should result in the correct onsite response personnel receiving notification of an emergency call, and the correct local PSAP receiving the actual emergency call.

Note Ensure that you submit each ALI export file as you create it. The ALI export records include an indication that the record is either new or modified. If you do not submit an ALI export file, the subsequent file you submit might have incorrect status indications, which can result in your service provider rejecting some, or possibly all, of your submitted records.

9. Ensure you update the ERL, ALI, and switch port information as you:

- Add or remove switches or ports
- Add or remove manually defined phones
- Add or remove ERLs
- Update ALIs

  Any time you update the ELINs for an ERL, or the ALI, you should reexport ALI data and submit it to your service provider.

Related Topics

ERLs, on page 135
Emergency Responder ERL Administrator Role , on page 310

Add Onsite Security Personnel

You must identify your security, or onsite alert personnel so that you can assign them to your emergency response locations (ERLs). If an emergency call is made from an ERL, the associated onsite alert personnel receive:

- A web-based alert on the Emergency Responder end-user interface specific to emergency calls originating from the assigned ERL. They also can view all alerts in the system.
- An email message. If you use an email-based paging address, the message results in a page.
- A telephone call indicating that an emergency call was made.

Before you begin

You must log into Emergency Responder with system administrator or ERL administrator authority.

Collect information about all of your onsite alert personnel, including names, telephone numbers, and email addresses. Also, develop a unique identification name for each, if you do not already have one readily available (such as badge number).

Procedure

Step 1 Select **ERL** > **Onsite Alert Settings**.

Emergency Responder opens the Onsite Alert Settings page.

Step 2 Enter the unique ID, name, telephone number, email address, and pager address, and User Group of a security or onsite alert person.

Unique ID might be a badge number, email name, or other site-specific unique name. You use this ID to assign the person to an ERL, so ensure that you use a naming strategy useful to you.

You can use an email-based paging address for the email address, so that onsite alert personnel receive a page rather than an email.

Step 3 Click **Insert**.

Emergency Responder adds the person to the list of onsite personnel. Repeat until you define all security or onsite personnel.

Tip

- To delete a person, first remove the person from all ERL definitions. Then, in the Available Onsite Alerts list on the Onsite Alerts Settings page, click the **Delete** icon corresponding to that person's record.
- To modify onsite alert settings, click on the person's Onsite Alert ID, Onsite Alert Name, Onsite Alert Number, Onsite Alert Email Address or Onsite Alert Pager Address in the Available Onsite Alerts list. The information for that person displays in the Modify Onsite Alert Contact section of the page. Modify the information as needed and then click **Update**. You cannot change a person's Onsite Alert ID: to change the Onsite Alert ID, delete the person's entry and create a new one.

ERL Creation

The following sections describe how to create emergency response locations (ERLs).

Set Up Default ERL

Emergency Responder does not automatically assign new switch ports and unlocated phones to the default emergency response location (ERL). New switch ports and unlocated phones are treated as ERLs that are not configured.

You must not configure the default ERL to any of the Switch Ports, Unlocated Phones, Manually Configured Phones or IP subnets. The default ERL is used internally by Emergency Responder only if no other ERL is configured for that phone.

Emergency Responder also uses the default ERL for all emergency calls when the Emergency Responder server is first started (or restarted when there is no standby Emergency Responder server) until the initial switch port update is finished. (This process is started immediately.)

Before you begin

You must log into Emergency Responder with system administrator or ERL administrator authority.

You must first configure the required ELINs in Unified CM.

Procedure

Step 1 Select **ERL** > **Conventional ERL**.

Emergency Responder opens the Find Conventional ERL Data page.

Step 2 Click **Configure Default ERL**.

Emergency Responder opens the ERL Information for Default window.

Step 3 Fill in the ERL Information for Default window.

Step 4 Click **ALI Details**.

Emergency Responder opens the ALI Information window.

Step 5 Fill in the ALI Information window.

When finished filling in the ALI, click **Update ALI Info**. Emergency Responder saves your ALI. Click **Close** to close the window.

Step 6 Make the ERL Information for Default window the active window if it is not, and click **Update**.

Emergency Responder saves the ERL and its ALI.

Step 7 Click **Close** to close the window.

Tip You cannot delete the default ERL. In addition, you cannot configure other ERLs unless the default ERL is configured.

Related Topics

Conventional ERL, on page 394
Add New ERL , on page 396
ALI Information, on page 400
Set Up Individual ERL and Automatic Location Information (ALI) , on page 140
ERLs, on page 135
ERL Management , on page 136

Set Up ERLs for Non-PSAP Deployment

You may want to deploy Emergency Responder for on-site alerts only. That is, instead of routing emergency calls to a public safety answering point (PSAP), you route emergency calls to a specified security phone.

There are two ways to set up non-PSAP deployments:

- **Configure Security IDs Only**—In this scenario, you configure security IDs for the zones for any ERL; you do not configure route/translation patterns. All emergency calls are routed to the ERL security. If this fails, the calls are routed to the default ERL security. Emergency Responder then initiates a call to the configured security phone and plays prompts to alert security personnel to the emergency call.
- **Configure Security IDs and Route/Translation Patterns**—In this scenario, you configure security IDs for the zones for any ERL and you also configure a route/translation pattern without an ELIN number. Emergency Responder displays a popup warning message alerting you that this zone will not have an ELIN. The emergency call is routed using the route/translation pattern; If this fails, the default pattern

is used. Emergency Responder then initiates a call to the configured security phone and plays prompts to alert security personnel to the emergency call.

Note In this scenario, you must use a different route/translation pattern for each zone.

Procedure

Step 1 Identify the security personnel to be notified in case of an emergency call (see Add Onsite Security Personnel, on page 137).

For example, configure security A with directory number 1000.

Step 2 Add an ERL with no route pattern or ELIN, but only with security IDs for that ERL (see ERL Creation , on page 138).

For example, add ERL X with security A.

Step 3 Go to the switch port screen and assign discovered switch ports to the already configured ERLs (see Switch Port Configuration , on page 159).

For example, associate switch ports of switch IP Y to ERL X.

All emergency calls from any phone connected to switch IP Y use ERL X and ring on the security A directory number 1000.

Note If you use Layer 3 (IP) roaming for wireless IP phones or wireless phones register using their Wireless Access Point's IP address, then Emergency Responder cannot automatically track movement of these phones. This is because Emergency Responder uses the IP address of the phone to determine the phone's location. Do not use Layer 3 roaming if you need Emergency Responder to automatically track movement of wireless phones in your network.

Set Up Individual ERL and Automatic Location Information (ALI)

This section explains how to define a single ERL. Because several ERLs often have similar information, see "Import Several ERLs" section for strategies for simplifying the definition of similar ERLs.

Before you begin

You must log into Emergency Responder with system administrator or ERL administrator authority.

Procedure

Step 1 Select **ERL** > **Conventional ERL**.

Emergency Responder opens the Find conventional ERLs page.

Step 2 Click **Add New ERL**.

Emergency Responder opens the Add New ERL window.

Step 3 Fill in the Add New ERL window.

Step 4 Click the **Add ALI** button.

Emergency Responder opens the ALI Information window.

Step 5 Fill in the ALI Information window.

When finished filling in the ALI, click **Save and Close**.

Step 6 Make the Add New ERL window the active window if it is not, and click **Insert**.

Emergency Responder saves the ERL and its ALI.

Step 7 Click **Close** to close the window.

Tip

- To create an ERL that is similar to an existing ERL, click **Find** to list the existing ERLs, then click copy for the similar ERL. Emergency Responder creates a copy of some ERL and all ALI information, which you can modify for the new ERL.
- You can create or update tags to simplify the ALI definition process. Navigate to the ALI Information window, and look for information about the location of the samplevalidate.txt file. The sample file explains how to set up tags. When you have created or updated the desired tags, select the tag name on the ALI Information window and the ALI fields are loaded with the settings associated with the tag.

Related Topics

Conventional ERL, on page 394

Add New ERL , on page 396

ALI Information, on page 400

Import Several ERLs , on page 141

ERLs, on page 135

ERL Management , on page 136

Import Several ERLs

Rather than defining ERLs one at a time, you can create a file that contains more than one ERL definition, and import these ERLs at the same time into your Emergency Responder configuration. This is especially useful if you already have ERL definitions set up in a spreadsheet, or if you are recovering an Emergency Responder configuration using ERL data exported from Emergency Responder.

Before you begin

You must log into Emergency Responder with system administrator or ERL administrator authority.

Prepare an import file. Emergency Responder includes detailed information about the required file format on the Import ERL data page. The page also includes the location in which you must place the file to import it.

You can import conventional, off-premise, or National E911 Service Provider ERLs. Click the **Import** link in the upper-right corner of the Find Conventional ERL Data Page, Find Off-Premises ERLs Data page, and the Find National E911 Service Provider ERLs Data page.

Use the following procedure to view the format, create or update your file, copy the file to the required location, and then follow the procedure to import the file.

Procedure

Step 1 In the Find ERL page (Find Conventional ERL data page, Find Off-Premises ERLs data page, or the Find National E911 Service Provider ERLs data page), click **Import**.

Emergency Responder opens the Import ERL data page.

Step 2 Select the format of your import file (csv or xml) from the pull-down menu.

Step 3 Click **Upload** to upload the file from your local machine.

Step 4 Select your import file.

Step 5 Click **Import**.

Emergency Responder imports your ERL and associated ALI data, and displays the status of the import as it proceeds. The imported data overwrites existing conflicting data in the Emergency Responder configuration.

Step 6 Click **Close** to close the Import ERL Data window.

Related Topics

Import ERL Data, on page 406
Set Up Individual ERL and Automatic Location Information (ALI) , on page 140
ERLs, on page 135
ERL Management , on page 136
Upload File , on page 113
ERL Creation , on page 138
Set Up Off-Premise ERL
Set Up National E911 Service Provider ERLs, on page 188

Convert ALI Data

Use the PS-ALI Converter tool to generate an ERL csv (Comma Separated Value) text file that can be accepted by the Emergency Responder ERL. You must first upload an existing ALI file in NENA 2.0 format to Emergency Responder before converting it.

Before you begin

You must log into Emergency Responder with system administrator or ERL administrator authority.

To convert ALI data, follow these steps:

Procedure

Step 1 Select **Tools** > **PS-ALI Converter.**

Emergency Responder displays the PS-ALI Converter page.

Step 2 Click the **Upload PSALI file** button to upload an ERL file in NENA 2.0 format. The Upload File page appears.

Step 3 Follow the instructions in the Upload File , on page 113 to upload the ERL file.

Step 4 Select the uploaded file from pulldown menu.

Step 5 In the Output file (in csv format) Name field, enter the name of the converted csv file you want to create.

Step 6 Click **Convert** to create the csv file.

The generated csv file is in the following folder:

```
%cerroot%/import
```

You can import the file or download the file using the File Manager utility.

Step 7 Modify the converted csv file as needed. For example, add the ERL name, route pattern, and security details to update the ERL.

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

Related Topics

Import ERL Data, on page 406
Set Up Individual ERL and Automatic Location Information (ALI) , on page 140
ERLs, on page 135
ERL Management , on page 136

Set Up IP Subnet-based ERLs

In addition to supporting switch port-based ERLs, Emergency Responder supports IP subnet-based (Layer 3) ERLs. You can configure IP subnets and assign ERLs to the configured IP subnets; Cisco Emergency Responder then routes the emergency calls based on the configured IP subnet and ERL associations.

This feature is useful in environments where strict IP addressing rules are followed and cubicle-level location is not required, such as configurations with wireless phones.

Use IP subnet-based ERLs to locate and track wireless endpoints, such as Cisco Unified Wireless IP Phone 7920 series devices and Cisco clients using wireless IP connection.

Note Subnet-based tracking is limited by the IP subnet addressing plan. It cannot distinguish location within a same IP Subnet.

Note From Release 15SU1 onwards, Emergency Responder also supports IPv6 Subnets. Any specific reference to IP Subnets should be understood to mean either IPv4 or IPv6 Subnets.

Before you begin

You must have system administrator or ERL administrator authority to access this page.

Procedure

Step 1 Select **ERL Membership > IP Subnets** and click the **Add New IPv4 Subnet or Add New IPv6 Subnet** link on the Find and List IPv4 and IPv6 Subnets page.

Step 2 At the Subnet ID field, enter the IP address of the IPv4 or IPv6 subnet that you want to define. For example,the subnet ID for IPv4 is 10.76.35.0. For IPv6, subnet ID can be a normal IPv6 address or a wildcard IPv6 address like :: which is equivalent to 0:0:0:0:0:0:0:0.

Step 3 For IPv4 subnet, enter the mask of the subnet that you want to define, for example, 255.255.255.224 at the Subnet Mask field. For IPv6 subnet, enter a prefix length (mandatory, the range is 1 to 128) for the subnet.

Step 4 To select the ERL you want to assign to the subnet, click the **Search ERL** button next to the ERL Name field. The Find ERL page appears.

Step 5 Enter the ERL Search Parameters and click **Find**. The search results appear.

Step 6 Click the radio button next to the ERL that you want to assign to the subnet and click **Select ERL**. The Find ERL page closes.

Step 7 Click **Insert** to add the subnet.

A popup message requests that you force a switch port update. You can do this after all the IP subnets have been added.

Step 8 To change the fields on this page back to the last saved settings, click **Cancel Changes**.

Related Topics

Find and List Synthetic Phones, on page 461

Add New Synthetic Phone, on page 462

Set Up Test ERLs

You can use Cisco Unified Operations Manager to monitor the health and functionality of Emergency Responder.

To use Cisco Unified Operations Manager with Emergency Responder, you configure a test ERL for conventional ERLs, then add a synthetic phone and associate the synthetic phone to the test ERL. When a synthetic phone makes an emergency call, Emergency Responder uses the associated test ERL to route the call.

Note You can configure test ERLs only to synthetic phones.

Note You cannot configure test ERLs for off-premise ERLs and National E911 Service Provider ERLs.

All synthetic phones used for Emergency Responder testing must belong to one of the configured test ERLs. For phones used for test ERLs, you enter the MAC address or address range allotted for synthetic phones.

The following conditions apply to test ERLs:

- Calls from synthetic phones are not logged in Call History logs.

- Web alerts are not generated for emergency calls from synthetic phones.
- Email alerts are not generated for emergency calls from synthetic phones.
- PS-ALI records for test ERLs are not exported in NENA export files.

Tip You do not need to enter ALI data for test ERLs. Non-test ERLs must contain ALI data.

Before you begin

You must have system administrator or ERL administrator authority to reach this page.

Procedure

Step 1 Select **ERL** > **Conventional ERL** and click **Add New ERL** on the ERL Configuration page.

Step 2 At the ERL field, enter a name for the test ERL.

Step 3 At the Test ERL field, check the box to select it.

Note This setting is not available on the ERL Information for Default; default ERLs may not be used as test ERLs.

Note Do not click **ALI Details** to enter ALI data. You do not need to enter ALI data for test ERLs; only non-test ERLs must contain ALI data.

Step 4 Click **Insert** to save the test ERL and click **Close** to close the window.

Step 5 Select **ERL Membership** > **Synthetic Phones** and click **Add New Synthetic phone** on the Find and List Synthetic Phones page.

Step 6 In the MAC Address field, enter the MAC address or the range of MAC addresses allotted for synthetic phone.

Enter the MAC address in this format:

xx-xx-xx-xx-xx-xx

or

xxxxxxxxxxxx

The synthetic MAC address must be within the following range:

00059a3b7700 - 0059a3b8aff

Step 7 In the ERL Name field, enter the test ERL that you want to assign to the synthetic phone. Select the configured test ERL from the drop-down list or type in a valid test ERL name.

Step 8 Click **Insert** to add the phone to the list of defined synthetic phones.

Step 9 To change the fields on this page back to the last saved settings, click **Cancel Changes**.

Related Topics

Find and List Synthetic Phones, on page 461

Add New Synthetic Phone, on page 462

Export ERL Information

Use the Export ERL page to create ERL export files for your own use, for example, to back up or move an ERL configuration. You can export conventional, off-premise, or National E911 Service Provider ERLs. Click the **Export** link in the upper-right corner of the Find Conventional ERL Data page, Find Off-Premises ERLs Data page, and the Find National E911 Service Provider ERLs Data page.

Note Do not submit ERL export files to your service provider; they are not exported in a format that your service provider can use.

For information about exporting ALI information, see Export ALI Information for Submission to Your Service Provider , on page 147.

For information about reformating ALI data to be accepted by the ERL, see Export ALI Information for Submission to Your Service Provider , on page 147.

Before you begin

You must log into Emergency Responder with system administrator or ERL administrator authority.

Procedure

Step 1 In the Find ERL page (Find Conventional ERL Data page, Find Off-Premises ERLs Data page, or the FindNational E911 Service Provider ERLs Data page), click **Export**.

Emergency Responder opens the Export ER Data window.

Step 2 Select the Export Format (csv or xml) from the pull-down menu.

Step 3 Enter the name of the file to be exported in the Enter Export File Name field.

Step 4 Click **Export**.

Emergency Responder creates the export file, and tells you the location where the file was created and how many records were exported.

Step 5 Select the exported file from the pull-down menu and click **Download** to download it to your local machine.

Step 6 Click **Close** to close the Export ERL Data window.

Related Topics

Export ERL Data, on page 405
ERLs, on page 135
ERL Management , on page 136
ERL Creation , on page 138
Set Up Off-Premise ERL
Set Up National E911 Service Provider ERLs, on page 188

Export ALI Information for Submission to Your Service Provider

Your service provider and their database provider need your automatic location information (ALI) so that emergency calls from your conventional ERLs can be routed to the correct public safety answering point (PSAP). The PSAP can also use this information to dispatch emergency response teams (such as police, fire, medical) to deal with the emergency. As you create and update your ERLs and their ALIs, make sure that you export the data and send it to your service provider or the database provider they identify.

See ALI Formatting Tool, on page 315 chapter for information about sending ALI details to your service provider.

Before you begin

You must log into Emergency Responder with system administrator or ERL administrator authority.

⚠

Caution Ensure that you submit each ALI export file as you create it. The ALI export records include an indication that the record is either new or modified. If you do not submit an ALI export file, the subsequent file you submit might have incorrect status indications, which can result in your service provider rejecting some, or possibly all, of your submitted records.

Procedure

Step 1 Select **Tools** > **Export PS-ALI Records**.

Emergency Responder opens the Export PS-ALI Records page.

Step 2 At the **Select the NENA Format** field, choose the format required by your service provider from the drop-down list.

Step 3 At the File to Export field, enter the name of the file to export.

Step 4 At the **Company Name** field, enter your company name.

Note Emergency Responder automatically increments the Cycle Counter each time you export data. You do not need to change this counter unless you are redoing or correcting a previous exportation. However, changing the sequence number does not affect the data placed in the file. If you are redoing an export, you have to manually edit the export file to change the record status fields.

Step 5 Click **Export**.

Emergency Responder creates the export file and tells you how many records were exported.

Step 6 Click **Download** to download the file to your local machine.

Step 7 Click **Close** to close the Export ALI Records window.

Step 8 Use your service provider's method of transmitting the file to the service provider.

Related Topics

ALI Information, on page 400

Export ERL Data, on page 405

Export PS-ALI Records, on page 479

ERLs, on page 135

ERL Management , on page 136

View Audit Trail for ERL

You can view the audit trail for an ERL to determine how, when, and by whom an ERL was created or changed.

Before you begin

You must have system administrator, ERL administrator, or network administrator authority to view the audit trail.

Procedure

Step 1 Select **Reports** > **ERL Audit Trail**.

Emergency Responder opens the ERL Audit Trail page.

Step 2 Enter search criteria to select the ERLs whose audit history you want to view.

To view all ERLs, click **Find** without entering any criteria.

To narrow your search:

a) Select the field that you want to search on, select the search relationship, and enter the search string. For some fields, you can select valid strings from the right-most drop-down list.
b) To search on a combination of fields, click **More** to add additional search fields. Select **Any** at the top of the list to indicate that ERLs that match any search criteria be selected (an OR search); select **All** to indicate that only ERLs that match every criteria be selected (an AND search).
c) Click **Find** when you have entered all of the search criteria.

Emergency Responder lists the matching audit records. If there are a lot of matches, Emergency Responder uses several pages to display them. Use the links at the bottom of the list to change pages.

Tip To view the audit trail of a specific ERL, click **View** in the Audit Trail column in a list of ERLs shown on the Find and List ERLs page.

Related Topics

ERL Audit Trail, on page 478

Work with Emergency Responder Locations , on page 135

Emergency Responder Switch Configuration

Before you can assign switch ports to ERLs, you must identify the switches used in your network to Emergency Responder. The following topics describe the switch requirements and how to identify switches to Emergency Responder.

Switch Requirements for Emergency Responder

Emergency Responder uses Cisco Discovery Protocol (CDP) to locate phones, so you should enable CDP on all of your switches. If you do not enable CDP, Emergency Responder must use the Content Addressable Memory (CAM) table on the switch to track phones. Using the CAM table is less efficient than using CDP.

If some of the phones on your network do not use CDP, Emergency Responder tracks them using the CAM table.

Ensure that the switches to which phones are attached are supported by Emergency Responder, and that the switches are running the required software version. The Network Hardware and Software Requirements , on page 10 lists the supported switches and software versions.

If you are using Catalyst 3500 switch clusters, you must assign IP addresses to every switch. Emergency Responder cannot work with a switch unless the switch has an IP address.

Related Topics

Set Up SNMPv2, on page 149
Define Phone Tracking and Switch Update Schedules, on page 152
LAN Switch Identification , on page 153
Manually Run the Switch-Port and Phone Update Process , on page 157

Set Up SNMP Connection

Emergency Responder uses SNMP to obtain information about the ports on a switch. Emergency Responder must obtain this port information so that you can assign the ports to ERLs, and so that Emergency Responder can identify phones that are attached to the ports and update their ERL assignments.

Emergency Responder only reads SNMP information, it does not write changes to the switch configuration, so you only have to configure the SNMP read community strings.

When you configure the SNMP strings for your switches, you must also configure the SNMP strings for your Unified CM servers. Emergency Responder must be able to make SNMP queries of all Unified CM servers in the cluster that it supports.

If your Cisco Emergency Responder servers, Unified CM servers, and Cisco IP Phones are in a different subnet than your switches, you must either configure both the subnets for the servers and phones as well as the subnet for the switches or use *.*.*.*.

Related Topics

SNMP Settings, on page 419
LAN Switch Identification , on page 153

Set Up SNMPv2

Before you begin

You must have the system administrator or the network administrator authority to define the SNMP settings.

Obtain the read community strings from all of the switches you define in Emergency Responder. If you use different strings for different sets of switches, determine whether you can define an IP address pattern for these sets. For example, if you use the same string for all switches that begin with 10.1, and another string for switches that begin with 10.2, you can use the patterns 10.1.*.* and 10.2.*.*.

If two or more patterns match an IP address, Emergency Responder uses the SNMP string associated with the most closely matching pattern. For example, if you define *.*.*.* and 10.1.*.*, and the IP address is 10.1.12.24, Emergency Responder uses the SNMP string defined for 10.1.*.*. The sequence of entries on this page does not affect the selection.

Procedure

Step 1 Select **Phone Tracking** > **SNMPv2 Settings**.

Emergency Responder opens the SNMP Settings page.

Step 2 Enter an IP address pattern to which you want to associate an SNMP read community string.

Use the asterisk (*) as a wildcard character. You can also use number ranges for octets, such as 15—30. Because the Emergency Responder only tries to contact the switches you identify on the LAN Switch Details page (see LAN Switch Identification , on page 153 for more information), it does not matter if the IP address patterns cover devices other than switches.

Note If you are using IPv6 address, then wildcard characters are not supported. Enter the details for each switch.

- If all of your switches use the same read community string, enter *.*.*.*. You only need to create one entry.
- If subsets of your switches use the same strings, create a mask that covers those subsets, if possible. For simplicity, try to create the fewest number of patterns.
- If you use a separate string for each switch, you must enter each switch on this page.

Step 3 Enter the timeout and retries values.

These values work together to determine how often and how long Emergency Responder tries to obtain SNMP information from a switch before giving up. The first attempt lasts as long as the timeout value. If you enter 1 or higher for retries, Emergency Responder tries again, and each retry lasts twice as long as the previous try. For example, if you specify 10 for timeout, the first retry lasts for 20 seconds, the second retry lasts for 40 seconds, and so forth.

The optimal values are 10 to 15 seconds for timeout, and 2 to 3 for retries.

Step 4 Enter the read community string, for example, **public**.

Note Community string does not support special characters like angle brackets (< >), backslash (\), colon (:), quotation marks (“ “), and tilde (~).

Step 5 Click **Insert**.

Emergency Responder adds the SNMP setting to the list of settings.

Step 6 If you must create more than one setting, return to Step 2, on page 150.

If you change the SNMP read community string on a switch, you must update the associated setting in Emergency Responder:

- To change an SNMP setting, select it in the list. Emergency Responder loads the setting in the edit boxes. Make your changes and click **Update**. Then, run the switch port and phone update process on the switch after you update the SNMP setting. Select **Phone Tracking** > **LAN Switch Details**, select the switch in the LAN Switches list, and then click **Locate Switch Ports**. If you are changing the setting for many switches, run the process on all switches by selecting **Phone Tracking > Run Switch-Port & Phone Update**.

- To delete a setting, click the delete icon on the setting's entry.

Set Up SNMPv3

Procedure

Step 1 Select **Phone Tracking > SNMPv3 Settings**.

Emergency Responder opens the SNMPv3 Settings page.

Step 2 Enter the User information for which you want to provide access.

Enter an IP address pattern to which you want to associate an SNMP read community string. Use the asterisk (*) as a wildcard character. You can also use number ranges for octets, such as 15–30.

Note If you are using IPv6 address, then wildcard characters are not supported.

Step 3 To require authentication, check the **Authentication Required** check box, enter the password in the Password and Reenter Password fields, and choose the appropriate protocol.

Step 4 If you checked the **Authentication Required** check box, you can specify privacy information. To require privacy, check the **Privacy Required** check box, enter the password in the Password and Reenter Password fields, and choose the appropriate protocol.

Step 5 Enter the timeout and retries values.

These values work together to determine how often and how long Emergency Responder tries to obtain SNMP information from a switch before giving up. The first attempt lasts as long as the timeout value. If you enter 1 or higher for retries, Emergency Responder tries again, and each retry lasts twice as long as the previous try. For example, if you specify 10 for timeout, the first retry lasts for 20 seconds, the second retry lasts for 40 seconds.

The optimal values are 10 to 15 seconds for timeout, and 2 to 3 for retries.

Step 6 Click **Insert**.

Step 7 If you must create more than one setting, return to Step 2.

Whenever you change the SNMPv3 settings on a switch or Unified CM server, you must update the associated setting in Emergency Responder:

- To change an SNMPv3 setting, select it in the list. Emergency Responder loads the setting in the edit boxes. Make your changes and click **Update**. Then, run the switch port and phone update process on the switch after you update the SNMPv3 setting. Select **Phone Tracking > LAN Switch Details**, select the switch in the LAN Switches list, and then click **Locate Switch Ports**. If you are changing the setting for a large number of switches, run the process on all switches by selecting **Phone Tracking > Run Switch-Port & Phone Update**.

- To delete a setting, click the delete icon on the setting's entry.

Related Topics

SNMP Settings, on page 419

LAN Switch Identification , on page 153

Define Phone Tracking and Switch Update Schedules

To track phones successfully, Emergency Responder must periodically contact switches to obtain port and device information. Emergency Responder updates network information using two processes:

- Phone Tracking—A periodic comparison of the phones registered with Unified CM to the location information obtained from the switches. If a phone moves, Emergency Responder updates the phone's ERL. Phones that cannot be located are classified as unlocated phones (see Identify Unlocated Phones , on page 167).

Note If you do not configure a switch port phone update schedule, the default schedule runs at midnight.

- Switch-Port and Phone Update—The phone tracking process plus a more extensive check of the network switches, which can identify new or changed switch modules (additional or removed ports). Any newly-discovered ports are assigned to the Default ERL. Ensure that your ERL administrator updates the ERL assignment for new ports.

Before you begin

You must have system administrator or network administrator authority to define the schedule.

Procedure

Step 1 Select **Phone Tracking** > **Schedule**.

Emergency Responder opens the Schedule page.

Step 2 Enter the incremental phone tracking schedule in minutes and click **Update**.

Emergency Responder runs the phone tracking process this number of minutes after finishing the previous phone tracking process.

Step 3 Enter the AXL incremental location phone tracking schedule in minutes and click **Update**.

Emergency Responder runs the enhanced location phone tracking for wireless devices after this number of minutes from the start of previous location tracking process.

Note By default, Emergency Responder actively queries the Cisco Jabber client every 2 minutes through AXL discovery on receipt of the device location.

Step 4 Enter the schedule for the switch port and phone update process. You should run this process at least once per day (but not more than four times per day).

For example, if you want to run the process at midnight Monday through Friday, but at 6 PM on Saturday and Sunday, create two schedule entries:

- Select **Mon**, **Tue**, **Wed**, **Thu**, and **Fri**, and **00** for **Hour**, **00** for **Minute**, then click **Insert**. Emergency Responder adds the schedule to the list.
- Select **Sat** and **Sun**, and **18** for **Hour**, **00** for **Minute**, then click **Insert**. Emergency Responder adds the schedule to the list.

  If you define schedules that overlap, Emergency Responder only runs one process.

Note The Emergency Responder Administrator must ensure that ccmPhoneStatusUpdateStorePeriod (CISCO-CCM-MIB) value in Unified CM must be set to a value greater than the Emergency Responder incremental phone tracking interval, for tracking phone changes efficiently.

To change a switch port and phone update schedule, click the schedule in the list. Emergency Responder loads the schedule's settings in the schedule fields. Make your changes and click **Update**. To delete a schedule, click the delete icon on the schedule's list entry.

Related Topics

Phone Tracking Schedule, on page 426

Manually Run the Switch-Port and Phone Update Process , on page 157

LAN Switch Identification

You must tell CiscoEmergency Responder (Emergency Responder) which switches to manage. Emergency Responder tracks port changes, including changes to the devices connected to those ports, and can recognize which ports have phones connected to them. Identify all switches that might have phones attached to them, essentially all edge switches.

Because Emergency Responder must obtain information from the switches, you must ensure that the information you supply to Emergency Responder is correct and kept up-to-date. After you have created the initial switch list, you can make mass changes to switch definitions by exporting the switch definitions, editing the export file, and reimporting the file.

The following sections describe how to identify switches to Emergency Responder, and how to export switch information.

Identify LAN Switches One at a Time

You can enter switches into the Emergency Responder configuration one at a time. If you have a large number of switches to add, consider creating an import file to add them instead of using this procedure. See Import a Group of Switches , on page 155 for more information.

Before you begin

You must have system administrator or network administrator authority to add, remove, or change switch definitions.

Determine if your network includes phones that do not use the Cisco Discovery Protocol (CDP) to announce themselves to the network. For non-CDP phones, Emergency Responder must use the CAM information about the switch to identify phones. See Network Hardware and Software Requirements , on page 10 for information about which phones require CAM access.

Ensure that you configure the SNMP read community strings before adding switches. See Set Up SNMPv2, on page 149 for more information.

Note Emergency Responder performs a full discovery scan for all the switches when you either reboot the Emergency Responder server or while upgrading to a higher version. This process can be time consuming, depending on network size and number of switches.

Note Always delete the LAN Switches from **Emergency Responder Administration** > **Phone Tracking** > **LAN Switch Details**, if this has been removed from the network.

Procedure

Step 1 Select **Phone Tracking** > **LAN Switch Details**.

Emergency Responder opens the LAN Switch Details page.

Step 2 Enter information about the switch:

- In the **Switch Host Name/IP Address** field, enter IP address (IPv4 or IPv6) or hostname of the switch.

  Note The hostname can begin with a numerical value.

- If there might be non-CDP-enabled phones attached to the switch, select **Enable CAM-based Phone Tracking**.
- If you want to display the switch port descriptions that are configured on the switch in the locations field in Emergency Responder, select **Use port description as port location.**

Step 3 Click **Insert** to add the switch to the Emergency Responder configuration.

Emergency Responder asks if you want to run the switch port and phone update process. You must run this process so that Emergency Responder can identify the ports on the switch and so that your ERL administrator can then assign the ports to the right ERLs.

If you are adding more than one switch, you can skip running the process until you add the last switch. When you select to run the process, Emergency Responder runs the process on all switches added since the last time the switch port and phone update process was run.

If you do not choose to run the process, you can run it later by selecting **Phone Tracking** > **Run Switch-Port & Phone Update**.

In either case, newly discovered ports are assigned to the Default ERL.

Note Emergency Responder expects only one IP address or hostname per chassis and needs access to the following MIBs:

- mib-2
- IF-MIB
- CISCO-CDP-MIB
- ENTITY-MIB
- CISCO-VLAN-MEMBERSHIP-MIB
- RIDGE-MIB*
- CISCO-STACK-MIB
- Mib-2
- interface
- CISCO-2900-MIB

Click a switch in the LAN Switches list to view the switch's Emergency Responder configuration. To change the configuration, make your changes and click **Update**.

Click **Add LAN Switch** to add another switch if you are viewing an existing switch's configuration.

To delete a switch, select it from the LAN Switches list and click **Delete**. If you do not remove the switch from the network, Emergency Responder identifies any phones connected to the switch as unlocated phones.

Related Topics

Import a Group of Switches , on page 155
Export Switch Information , on page 156
LAN Switch Details, on page 434
Switch Requirements for Emergency Responder , on page 149

Import a Group of Switches

You can define a large number of switches at one time by importing a file that contains the required switch information. You can create this file by exporting switch information from your network management software, and then using a spreadsheet program to modify the records to match the Emergency Responder file format requirements (that is, by deleting columns, adding columns, rearranging columns, and so forth).

If you have a large network, importing switch definitions can save you a lot of time.

Before you begin

You must have system administrator or network administrator authority to import switch definitions.

Prepare an import file. Emergency Responder includes detailed information about the required file format on the Import LAN Switch page. The page also includes the location in which you must place the file to import it. Use the following procedure to go to the page and view the format, create your file, copy the file to the required location, and then follow the procedure to import the file.

Ensure that you configure the SNMP read community strings before adding switches. See Set Up SNMPv2, on page 149 for more information.

Procedure

Step 1 Select **Phone Tracking** > **LAN Switch Details**.

Emergency Responder opens the LAN Switch Details page.

Step 2 Click **Import** in the left-hand switch list.

Emergency Responder opens the Import LAN Switch page.

Step 3 Select the file format, and the name of the file you want to import.

Step 4 Click **Import**.

Emergency Responder asks you whether you want to run phone tracking on the imported switch. You must run phone tracking before you can configure the switch ports, so normally you should select **OK**. If you select **Cancel**, Emergency Responder imports the switches but does not run the phone tracking process.

After you make your selection, Emergency Responder adds the switch configurations and shows you the status of the import.

Step 5 Click **Close** to close the window.

Step 6 If you did not run phone tracking on the imported switches, select **Phone Tracking** > **Run Switch-Port & Phone Update**.

Emergency Responder contacts each switch to discover the ports on the switch and any phones attached to the ports.

Alternatively, you can view each switch's configuration on the LAN Switch Details page and click **Locate Switch Ports** to run the process only on the selected switch.

Related Topics

Identify LAN Switches One at a Time , on page 153

Export Switch Information , on page 156

LAN Switch Details, on page 434

Switch Requirements for Emergency Responder , on page 149

Export Switch Information

You can export your Cisco Emergency Responder (Emergency Responder) configuration. By exporting this information, you can back up your data, or create a file for updating a large number of switch definitions in Emergency Responder. You can edit the export file, make your changes, then reimport the file and overwrite the information in Emergency Responder.

Before you begin

You must have system administrator or network administrator authority to export switch definitions.

Procedure

Step 1 Select **Phone Tracking** > **LAN Switch Details**.

Emergency Responder opens the LAN Switch Details page.

Step 2 Click **Export** in the switch list.

Emergency Responder opens the Export LAN Switch page.

Step 3 Select the file type and enter the file name for the export file. Do not include a file extension.

Step 4 Click **Export**.

Emergency Responder creates the export file. Click **Close** to close the window.

Related Topics

Identify LAN Switches One at a Time , on page 153
Import a Group of Switches , on page 155
LAN Switch Details, on page 434
Switch Requirements for Emergency Responder , on page 149

Manually Run the Switch-Port and Phone Update Process

Before you can assign ERLs to switch ports, Emergency Responder must identify the ports on the switch using the switch port and phone update process. Although Emergency Responder runs this process according to the schedule you set (see Define Phone Tracking and Switch Update Schedules, on page 152 for more information), you might want to run it manually when you make a lot of changes to the switch configuration without running phone tracking on individual switches.

Because the switch port and phone update process does extensive checking, only run it if you are trying to refresh the entire Emergency Responder tracking results. Alternatively, if you are only trying to update the results for a limited number of switches, you can run phone tracking on individual switches. To run on individual switches, select **Phone Tracking** > **LAN Switch Details**, select the switch in the left-hand column then click **Locate Switch Ports**.

These are some reasons you might run phone tracking on an individual switch:

- You add a switch to Emergency Responder. When you add a switch, Emergency Responder asks if you want to run the process. If you select to run it at that time, you do not have to click **Locate Switch Ports**. Emergency Responder runs the process for all switches you added to the Emergency Responder configuration since the last time the full switch port and phone update process was run.
- You add, remove, or change a module in a switch already defined to Emergency Responder.
- You can add and delete IP subnet-based ERLs.

Manually run the switch port and the following phone update process if:

- You want to refresh the Emergency Responder tracking results.
- You add switches to Emergency Responder by importing switch definitions, as described in the Import a Group of Switches , on page 155, but you did not run phone tracking during the importation.
- If you find a large number of entries in the unlocated phones list (see Identify Unlocated Phones , on page 167), run this process to see if Emergency Responder can find some of those phones. See Unlocated Phones , on page 324 for issues you should address to help resolve these problems before running the switch-port and phone update process.

Before you begin

You must have system administrator or network administrator authority to manually run the switch port and phone update process.

Procedure

Select **Phone Tracking** > **Run Switch-Port & Phone Update**.

Emergency Responder runs the process without changing the page you are viewing. Any newly discovered ports are assigned to the Default ERL.

Note When a 911 call is placed, and the phone matches multiple ERLs via Phone Tracking, Cisco Emergency Responder will use the following hierarchy to select an ERL:

- Switch Port
- IP Subnet
- Manually configured phone

Related Topics

Define Phone Tracking and Switch Update Schedules, on page 152
Identify Unlocated Phones , on page 167
Switch Requirements for Emergency Responder , on page 149

Track Change of Switch IP Address Dynamically

Emergency Responder allows you to dynamically track the change in a LAN switch IP address managed by Emergency Responder. This feature is intended for LAN switches that have been added using the switch hostname.

Before you begin

You must have system administrator authority to enable dynamic tracking of a LAN switch IP address.

Procedure

Step 1 Select **System** > **CiscoER Group Settings**.

Emergency Responder opens the Emergency Responder Group Settings page.

Step 2 Select the **Dynamic Tracking of Switch IP Address** check box to dynamically track a switch's IP address.

Step 3 Click the **Update Settings** button to apply the change.

You must wait for the next Incremental Discovery cycle to start. During this cycle Emergency Responder detects the new IP address of the LAN switch and updates its database. You will be notified of this change detection from an entry in the Emergency Responder Event Viewer and with an administrative email alert.

Note It is recommended that you enable Dynamic Tracking of Switch IP Address only during a scheduled maintenance window when the switch is subject to an actual change of IP address. It is recommended that you disable this option during normal periods as this operation is CPU intensive.

Note For a LAN switch that has been added using the IP address, Emergency Responder cannot track any change in its IP address. In this case, you must delete the switch and add it again with the new IP address.

Related Topics

Group Settings, on page 363
Define Phone Tracking and Switch Update Schedules, on page 152

Phone Management

The following topics describe how to assign switch ports and phones to the appropriate emergency response locations (ERLs), and how to view the history of emergency calls handled by Emergency Responder.

Switch Port Configuration

After the network administrator adds switches to the Emergency Responder configuration, and runs the switch port and phone update process, you can assign the switch ports to emergency response locations (ERLs). When you assign a port to an ERL, make sure that you assign the ERL based on the location of the device attached to the port, not the location of the port itself.

For example, your wiring closet is on Floor 1. Half of its ports serve Floor 1, the other half serve Floor 2. Also, you have defined two ERLs, Floor 1 and Floor 2. Although the switch is on Floor 1, only half its ports belong in the Floor 1 ERL; the other half belong in the Floor 2 ERL.

Before you assign ports to ERLs, ensure that you have a reliable mapping of switch ports to their end points (for example, cubicle numbers or office numbers). Your assignments are only reliable if this map is kept static, that is, so long as wires are not indiscriminately moved from port to port on the switch. Work with your network administrator to ensure the integrity of the wiring closet. See Data Integrity and Reliability, on page 34 for more information.

Network devices used for switch-port tracking in Emergency Responder have limitations on the supported interface types. Only RJ45 interfaces are supported. Other interface types may not be discoverable.

Unsupported interfaces include but are not limited to SFP, SFP+, QSFP, Combo ports (RJ45 and SFP). This includes SFP GBIC transceivers to convert SFP to RJ45. Modular interfaces such as CFP, XFP, X2, CPAK, XPAK, and XENPAK are not supported. Other non-RJ45 interface types that are not listed isn't supported.

Set Up Individual Switch Ports

You can assign switch ports to ERLs a few at a time. If you have a large number of ports to map, it is much easier to create an import file to add them instead of using this procedure. See Set Up Large Number of Ports , on page 161 for more information.

Before you begin

You must have system administrator or ERL administrator authority to assign ports to ERLs.

You can only configure ports defined for the Emergency Responder group to which you are logged in.

Procedure

Step 1 Select **ERL Membership** > **Switch Ports**.

Emergency Responder opens the Switch Port Details page.

Step 2 Enter search criteria to list the ports that you want to configure.

- **Find** displays a maximum of 1,000 records. Refine your search accordingly. To limit the number of ports that are displayed, check the check box next to **Collapse search results.** The search displays the IP address or name of the switches found. To display all ports associated with a switch and display the expanded view, click the **+** button next to the switch. To display just the switch and collapse the list, click the **-** button next to the switch.
- If you want to list all ports on a specific switch, select **Switch IP Address** or **Switch Host Name**, enter the IP address or host name, and click **Find**. Emergency Responder lists all ports discovered on the switch.
- If you want to narrow your search by using multiple criteria, click the **+** button to add search fields. Select **Any** at the top of the list to indicate that ports that match any search criteria be selected (an OR search); select **All** to indicate that only ports that match every criteria be selected (an AND search).
- For all searches, select the Emergency Responder group that you want to search. If your initial search does not list the ports you are looking for, it might be because the ports are managed by a different Emergency Responder group. You can only search one Emergency Responder group at a time.

Note Emergency Responder remembers the previous search criteria for the login session.

Step 3 Assign ports to ERLs:

a) Check the check box next to the switch port that you want to assign an ERL.

If you want to assign all listed ports for a switch, select the check box for that switch. You can only assign ports on one page at a time, so if there is more than one page of ports in the listing, complete this task for each page separately.

b) Select the ERL you want to assign to the ports.

c) Optionally, enter more specific location information in the **Phone Location** field. Click **view** to open a window so that you can enter information. For example, you could enter the cubical or office number that the port serves.

This information is sent to the onsite alert (security) personnel to help them locate the emergency caller. You can only update the phone location information if you are logged into the primary Emergency Responder server in the Emergency Responder group.

d) To select the ERL you want to assign to the selected ports, click the **Search ERL** button next to the ERL Name field. The Find ERL page appears.

e) Enter the ERL Search Parameters and click **Find**. The search results appear.

f) Click the radio button next to the ERL that you want to assign to the switch ports and click **Select ERL**. The Find ERL page closes.

g) Click **Assign ERL**.

Emergency Responder assigns the ERL to the selected ports. You can continue assigning ports on this page of the ports list, but do not change the search results page before completing these steps.

Emergency Responder commits your ERL assignments. From here, you can continue to the other page of the listed ports, or click **Find** to enter new search criteria to obtain another list of ports.

Click **Edit View** to change the fields and arrangement of fields in the port list. If you want to revert to the standard view, then click **Restore Defaults**.

The phone location information is saved on the primary Emergency Responder server. Back up this data regularly.

Related Topics

Switch Port Details, on page 438
Import Switch Ports, on page 441
Set Up Large Number of Ports , on page 161
Export Switch Port Information , on page 162
Work with Emergency Responder Locations , on page 135

Set Up Large Number of Ports

You can assign a large number of ports to ERLs at one time by importing a file that contains the required information.

If you have a large network, importing port-to-ERL mappings can save you a lot of time.

Before you begin

You must have system administrator or ERL administrator authority to import switch port definitions.

Prepare an import file. The easiest way to create this file is to first export the switch port details from Emergency Responder (see Export Switch Port Information , on page 162), and then use a spreadsheet program to change the ERL to the desired ERL and add phone location information. Ensure that the switch port and phone update process is run before creating the export file, so that the file includes records for every switch port.

Before you import the file, you must copy it to the location identified on the Import Switch Port page. The following procedure explains how to get to this page. Links on the page also displays the detailed information about the required file format for the import file if you need it.

Emergency Responder must already be aware of the ports before you import the file. Ensure that all ports you are importing have been located by Emergency Responder.

You can only configure ports defined for the Emergency Responder group to which you are logged in.

Procedure

Step 1 Select **ERL Membership** > **Switch Ports** .

Emergency Responder opens the Switch Port Details page.

Step 2 Click **Import**.

Emergency Responder opens the Import Switch Ports page.

Step 3 Select the format of your import file (csv) from the pull–down menu.

Step 4 Click **Upload** to upload the file from your local machine. See Upload File , on page 113 for information about using the Upload utility.

Step 5 Select your import file using the Select File to Import pull–down menu.

Step 6 Click **Import**.

Emergency Responder imports the file and shows you the import results. The ERL-to-port mappings and port location information in the import file overwrite any existing data in the Emergency Responder configuration.

Step 7 Click **Close** to close the Import Switch Port page.

Related Topics

Switch Port Details, on page 438
Export Switch Ports, on page 440
Set Up Individual Switch Ports , on page 159
Export Switch Port Information , on page 162
Switch Requirements for Emergency Responder , on page 149

Export Switch Port Information

You can export your Emergency Responder port configuration. By exporting this information, you can back up your data, or create a file that you can use to update a large number of switch port mappings in Emergency Responder. You can edit the export file, make your changes, then reimport the file and overwrite the information in Emergency Responder.

Before you begin

You must have system administrator or ERL administrator authority to export switch port definitions.

Procedure

Step 1 Select **ERL Membership** > **Switch Ports** .

Emergency Responder opens the Switch Port Details page.

Step 2 Click **Export**.

Emergency Responder opens the Export Switch Ports page.

Step 3 Select the file format and enter the desired file name, and click **Export**.

Emergency Responder exports the file to the export location.

Step 4 To download the exported file to your local system, select the file name from the Select file to download pull–down menu and click **Download**.

Step 5 Click **Close** to close the Export Switch Port page.

Related Topics

Switch Port Details, on page 438
Set Up Individual Switch Ports , on page 159

Set Up Large Number of Ports , on page 161
Work with Emergency Responder Locations , on page 135

Switch-Port Change Reporting for Wired Cisco Unified IP Phones

Emergency Responder detects changes in the switch port association of wired CiscoUnifiedIPPhones. An incremental or full discovery cycle detects CiscoUnifiedIPPhones that have changed switch port associations or are newly discovered. Cisco UnifiedIPPhones that become missing during a complete discovery are also reported. Emergency Responder notifies the system administrator of these changes by email.

Note A missing CiscoUnifiedIPPhone is one that is registered in Cisco UnifiedCommunicationsManager but is not found behind a switch port of any switch tracked by Emergency Responder. CiscoUnifiedIPPhones that appear on the Unlocated Phones page in Emergency Responder Administration web interface are also included in the missing list. Switch-port Change Reporting reports the location changes for CiscoUnifiedIPCommunicator when it is connected to a switch that is tracked by Emergency Responder.

The change notification email contains the following information:

- The time at which the change was detected. This is the approximate completion time of the discovery cycle that detected the change.
- The previous switch IP and port number of the CiscoUnifiedIPPhone. If the CiscoUnifiedIPPhone is new, this field is blank.
- The current switch IP and port number of the CiscoUnifiedIPPhone. If the CiscoUnifiedIPPhone is missing, this field is blank.
- The details of the CiscoUnifiedIPPhone, including the MAC address, device name, Phone Type, IP address and IP phone extensions.

Procedure

Step 1 Select **System** > **Mail Alert Configurations**.

The Email Alert Settings page appears.

Step 2 In the **Misc parameters** section, check the check box to the right of Switch Port location change reporting parameter to enable or disable email alerts.

Check the **Include event viewer contents in mail check box** if you want to include the details from the event viewer in the email message.

Step 3 Click **Update Settings**.

What to do next

Note Configure the email client settings to allow line breaks in the email to improve readability.

Supported CiscoUnifiedIPPhones—This feature supports only wired CiscoUnifiedIPPhones that meet both of these conditions:

- Wired CiscoUnifiedIPPhones discovered behind a LAN switch port using Cisco Discovery Protocol (CDP) tracking or Content-Addressable Memory (CAM) tracking.
- Wired CiscoUnifiedIPPhones actively registered in Unified CM. The only exception for this rule is CiscoUnifiedIPPhones previously registered in Unified CM. These CiscoUnifiedIPPhones are reported as missing.

Cluster Scenario—The active server in each server group within a cluster sends separate notifications for the CiscoUnifiedIPPhones it discovers and tracks.

Server Group Scenario—Within a server group, Emergency Responder performs change detection and notification on the active Emergency Responder server only.

Feature Activation—The change detection and notification feature requires manual activation.

Change Notification conditions - Emergency Responder sends change notification email when a full discovery cycle completes under any of these circumstances:

- During a normally scheduled discovery.
- After a manual start from the Emergency Responder Administrator web interface.
- Because of a Unified CM addition from the web interface by the system administrator.

Similarly, a partial discovery cycle sends email notifications under these circumstances:

- During a normally scheduled discovery.
- Because of a LAN switch addition to Emergency Responder the system administrator starts the discovery process.
- Because the system administrator selecting the **Locate Switch Ports** button on the LAN switch details page.

Note An Incremental Discovery does not locate missing CiscoUnifiedIPPhones from Unified CM if no phone registrations take place during the discovery cycle. A full discovery detects all missing CiscoUnifiedIPPhones that are located since the previous full discovery.

The following events do not result in a change notification:

- When the Emergency Responder Server starts following the first discovery cycle.
- When a Publisher returns to an online state following the first discovery cycle.
- When no phone location changes occur following a discovery cycle.

Related Topics

Set Up a Server Group, on page 128

Access Point Configuration and Discovery

An Access Point is a standalone device which connects to a router through a wired network. It can also be an essential component of the router. Each Access Point is identified through a Service Set Identifier (SSID) or Basic Service Set Identifier (BSSID). Wireless phones connect to the network over Wi-Fi or any equivalent standard through an Access Point.

SSID— The Service Set Identifier (SSID) is a unique name assigned to each WLAN network. A unique name is assigned to each WLAN as multiple WLANs can coexist in one airspace.

BSSID—The Basic service set identifier (BSSID) identifies access points and their associated clients within a WLAN network when there are multiple access points present within each WLAN. BSSID is included in all the wireless packets.

Cisco Unified Communications Manager, provides support to sync Access Points through a Wireless Controller.

Cisco Emergency Responder via the configured Cisco Unified Communications Manager identifies all the " Access Points", either through direct Cisco Unified Communications Manager database access during a Major Discovery or AXL Change Notification every two minutes.

Cisco Emergency Responder administrator can assign ERLs to the Access Points. For more information on Access Point details, see the Related Topics section.

EnergyWise

Cisco EnergyWise allows administrators to measure and reduce the energy consumption of devices connected to a Cisco network, such as IP telephones. Because each telephone reports its power consumption to a switch or router, you can monitor energy consumption across a network. You can then manage the power state of a phone by determining what phones are powered up, when they receive power, and how much power they receive.

Cisco EnergyWise Phone User Experience

When a phone enters Power Save Plus mode, it becomes unregistered from Unified CM and powers down after negotiating with the EnergyWise switch. Administrators configure the sleep and wakeup times, which are communicated to the switch by the phone.

Users can wake up the Cisco Unified IP Phone 6900, 8900, and 9900 series phones from Power Save Plus mode but cannot wake up the Cisco Unified IP Phone 7900 series.

Phone Discovery Scenarios Common to EnergyWise Users

The following three phone discovery scenarios are common to EnergyWise users. These scenarios can help you to understand this feature.

Scenario 1 — When the phone is connected to a switch that is configured on Emergency Responder for discovery:

- A phone is configured with EnergyWise on the Unified CM.
- The phone is connected to the switch and is discovered by Emergency Responder. The phone is displayed on the Switch Port page, connected to a switch port.
- Before the next Major Discovery, the phone enters Power Save Plus mode and it becomes unregistered with Unified CM.
- During the next Major discovery, Emergency Responder retains the phone location information. It is listed on the Switch Port page as being connected to the same switch port.
- When the phone is powered up again, the correct location is available if the user can make a 911 call without waiting for the next Incremental or Major discovery.

Note When a phone in Power Save Plus mode is unplugged, the EnergyWise configurations on the switch are lost. And if a Major Discovery takes place, the phone location information is lost also. Even if the phone is plugged back into the same port, powers up and registers with the switch, Emergency Responder treats this phone as a newly registered phone in the next discovery cycle.

Note If an EnergyWise phone is connected to a supported switch that is configured on Emergency Responder for discovery, the phone must be discovered at least once before entering Power Save Plus mode. This ensures that Emergency Responder retains the phone location and configuration information into the next Major Discovery. If the phone enters Power Save Plus mode without being discovered, it is not listed on the Switch page. But instead the phone is listed on the IP Subnet page (if configured) or the Unlocated Phone page in the next discovery. When it wakes up, registers with the switch and is discovered, the phone is listed on the Switch Port page.

Scenario 2 — IP subnet-based phone discovery in Emergency Responder:

- The phone is configured with EnergyWise on the Unified CM.
- The phone is discovered by Emergency Responder, based on the IP subnet. It is listed on the IP Subnet page.
- Before the next Major Discovery, the phone enters Power Save Plus mode and becomes unregistered with Unified CM.
- During the next Major Discovery, Emergency Responder retains the phone location information and the phone is listed on the IP Subnet page.
- When the phone is powered up again, the correct location is available if the user makes a 911 call without waiting for the next Incremental or Major discovery.

Scenario 3 — Unlocated phones in Emergency Responder:

- The phone is configured with EnergyWise on Unified CM.
- The phone is listed on the Unlocated Phones page in Emergency Responder after discovery.
- Before the next Major discovery, the phone enters Power Save Plus mode and it becomes unregistered with Unified CM.
- During the next Major discovery, Emergency Responder retains the phone location information. It is listed on the Unlocated Phones page.
- When the phone is powered up again, users can make a 911 call without waiting for the next Incremental or Major discovery. But the phone is in the default ERL or the ERL assigned to the Unlocated Phone switch.

Power Save Plus Mode Limitations

Consider the following limitations for users making 911 calls from phones in Power Save Plus mode:

- Users cannot wake up Cisco Unified IP Phones 7900 series that are in Power Save Plus mode because the sleep and wake-up times are configured on the Unified CM. The phone location information is not deleted from Emergency Responder, but users cannot make a 911 call until the phone reaches the configured wake-up time.

- Users can wake up Cisco Unified IP Phones 6900, 8900, 9900 in Power Save Plus mode. But the phone takes a few minutes to wake up and register with Unified CM and you should consider this delay during emergencies.
- You can track phones connected to a switch on the Emergency Responder page. But if the phones go into Power Save Plus mode before they are discovered, they are considered unlocated and are listed on the Unlocated Phones page.
- If a network has a standalone Emergency Responder with no backup subscriber, you should consider the impact of a system or Emergency Responder restart. Because there is no backup server, the existing discovery data is lost when the system is restarted. And when discovery occurs, it is considered a fresh discovery and Emergency Responder does not identify the switch location information for any phones that entered Power Save Plus mode before the restart.

  In Emergency Responder, these phones are listed on the Unlocated Phones page or IP Subnet page (if configured). When the phones are powered up and are discovered, they are listed on the Switch Port page. Consider these sleeping phones and their wake-up time when you assign the ERL.

  To avoid losing phones in the Power Save Plus mode when Emergency Responder is stopped, we recommend that you configure a backup Emergency Responder subscriber. If the publisher Emergency Responder service is stopped or the server goes down, the subscriber accesses the backup version of the discovery data, including the phones in Power Save Plus Mode. And when a restart occurs, the discovery data is retrieved from the subscriber and the phones in Power Save Plus mode are not lost.

Identify Unlocated Phones

If Emergency Responder cannot locate a phone, it places the phone in the Default ERL and puts it in a list of unlocated phones. Using this list, you can reassign the phones to a different ERL, or you can use the list to help identify the problems that are preventing Emergency Responder from locating the phones.

These are some things that can prevent Emergency Responder from locating a phone:

- The phone is attached to a switch that is not defined in Emergency Responder.
- The phone is connected to an unsupported device, such as a router port, a hub connected to a router, or an unsupported switch.
- The switch to which the phone is connected is currently unreachable, for example, it does not respond to SNMP queries.
- The phone has moved to a switch served by a different Emergency Responder group. If this is the case, the Emergency Responder group name is shown for the phone in the unlocated phones list.
- No IP subnet is configured for the phone.

Because Emergency Responder cannot assign an unlocated phone to the appropriate ERL, try to identify and resolve all problems that are preventing Emergency Responder from locating these phones on your network. If you cannot resolve the problems by defining switches in Emergency Responder, or by moving phones to supported switch ports, you can manually assign a phone to an ERL. See Unlocated Phones , on page 324 for more detailed information about resolving these problems.

In addition, Emergency Responder also displays the following in the unlocated phone list:

- The phone that was manually assigned.
- The phone that was previously identified as an unlocated phone and assigned an ERL.

Before you begin

You must have system administrator or ERL administrator authority to view or configure unlocated phones.

Procedure

Step 1 Select **ERL Membership** > **Unlocated Phones**.

Emergency Responder opens the Unlocated Phones page.

Step 2 Enter search criteria to list the unlocated phones.

Step 3 Check the check box next to the phone that you want to assign an ERL.

Step 4 Click the Search **ERL button** next to the ERL Name field to select the ERL you want to assign to the selected phone. The Find ERL page appears.

Step 5 Enter the ERL Search Parameters and click **Find**. The search results appear.

Step 6 Click the radio button next to the ERL that you want to assign to the unlocated phones and click **Select ERL**. The Find ERL page closes.

Step 7 Click the **Assign ERL** button.

Emergency Responder assigns the phone to the ERL, but leaves it in this list. If you later resolve the problem that is preventing Emergency Responder from locating this phone, Emergency Responder removes it from the list and assigns it the correct ERL based on port assignment.

Note To unassign a ERL, select the phones and click on **Unassign ERL** button.

You can select all the phones on the displayed page by selecting the check box in the list title. You can only assign phones to ERLs on a single page at a time. If there is more than one page of phones, use the links at the bottom of the list to move from page to page.

Note Emergency Responder does not automatically discover analog phones or phones connected to PBXs. As a result, these phones do not appear on the Unlocated Phones list. These phones must be manually configured. See Manually Define Phones , on page 168 for more information.

Related Topics

IP Subnet Phones, on page 452

Switch Port Configuration , on page 159

Manually Define Phones , on page 168

Manually Define Phones

To manage all emergency calls in your network, Emergency Responder must know about every phone whose calls are routed by Unified CM, even if Emergency Responder does not directly support the phone. Emergency Responder handles emergency calls from these manually defined phones in the same way it handles calls from phones attached to supported switch ports. The only difference is that Emergency Responder cannot dynamically change the ERL of a manually defined phone if that phone is moved.

You must manually define a phone if any of these conditions apply:

- The phone is hosted on an unsupported port, such as a router port, a hub connected to a router, or a port on an unsupported switch.

- No IP subnet is configured for the phone.

For any phones you must manually define, you should regularly audit the location of those phones to determine if you must update the ERL assignment for the phone in Emergency Responder.

Note New switch ports and unlocated phones are NOT associated to Default ERLs automatically. They are treated as "ERL not configured." The Default ERL is used only internally by Emergency Responder if no other ERL is configured for that phone. Emergency Responder will not allow the Default ERL to be configured to switch ports, unlocated phones, manually configured phones, or IP subnets.

Note You cannot manually add a phone that is used with Unified CM Extension Mobility. With Unified CM Extension Mobility, a user can log into a phone and the phone is assigned the user's extension. However, with manually defined phones, you are defining the phone based on extension, not on device, so the extension of the logged-in person does not get assigned the appropriate ERL. Ensure that all phones used with Unified CM Extension Mobility are connected to supported switch ports.

Before you begin

You must have system administrator or ERL administrator authority to manually define phones.

Note Manually configured phones can have E.164 and non-E.164 line numbers.

Procedure

Step 1 Select **ERL Membership > Manually Configured Phones**.

Emergency Responder opens a new page, the Find and List Manually Configured Phones page.

Step 2 Enter the extension and click **Find** to search for phones that you must modify. Emergency Responder performs a search and displays the results of your search.

From the search result on the Find and List Manually Configured Phones page, you can remove a phone, change an existing phone or add a new phone:

Step 3 Click the **Delete** icon on the phone entry to remove a phone.

Step 4 To change an existing phone:

a) Click the phone entry in the list. Emergency Responder opens the Add/Modify Phones page with the phone information displayed in the edit boxes.
b) Make your changes and click **Update**. Emergency Responder updates the phone.
c) Click **Back to Phone Search** to return to the Find and List Manually Configured Phones page.

Step 5 To add a new phone:

a) Click **Add New Manual Phone**. Emergency Responder opens the Add New Manual Phone page.

b) Enter information about the phone you want to define. You must enter the line number and select an ERL. If the phone is an IP phone, you must also enter the IPv4 address or IPv6 address and MAC address for the phone. Other fields are optional and are mainly for your information.
c) To select the ERL you want to assign to the selected ports, click the **Search ERL** button next to the ERL Name field. The Find ERL page appears.
d) Enter the ERL Search Parameters and click **Find**. The search results appear.
e) Click the radio button next to the ERL that you want to assign to the manual phone and click **Select ERL**. The Find ERL page close.
f) Click **Insert**. Emergency Responder adds the phone to the list of manually defined phones.
g) Click **Back to Phone Search** to return to the Find and List Manually Configured Phones page.

Related Topics

Add New Manual Phone, on page 458
Identify Unlocated Phones , on page 167
Network Hardware and Software Requirements , on page 10
Assign Large Number of Manually Configured Phones to ERLs , on page 170
Export Manually Configured Phone Information , on page 171

Assign Large Number of Manually Configured Phones to ERLs

You can assign a large number of manually configured phones to ERLs at one time by importing a file that contains the required information.

If you have a large network, importing a manually configured phone to ERL mappings can save you a lot of time.

Before you begin

You must have system administrator or ERL administrator authority to import switch port definitions.

Prepare an import file. The easiest way to create this file is to first export the manually configured phone details from Emergency Responder (see Export Manually Configured Phone Information , on page 171), and then use a spreadsheet program to change the ERL to the desired ERL and add phone location information. Ensure that the manual phone configuration and phone update process is run before creating the export file, so that the file includes records for every manually configured phone.

Before you import the file, you must copy it to the location identified on the Import Manual Phones page. The following procedure explains how to get to this page. Links on the page also display the detailed information about the required file format for the import file if you need it.

Emergency Responder must already be aware of the manually configured phones before you import the file. Ensure that all manually configured phones you are importing have been located by Emergency Responder.

You can only configure manually configured phones defined for the Emergency Responder group to which you are logged in.

Procedure

Step 1 Select **ERL Membership** > **Manually Configured Phones**.

The Find and List Manually Configured Phones page appears.

Step 2 Click **Import**.

The Import Manually Configured Phones page appears.

Step 3 Select the Import Format (csv) using the pull-down menu.

Step 4 Click **Upload** to upload the file from your local machine. See Upload File , on page 113 for information about using the Upload utility.

Step 5 Select the import file using the Select File to Import pull-down menu.

Step 6 Click **Import**.

Emergency Responder imports the file and shows you the import results. The ERL-to-port mappings and the location information for manually configured phones in the import file overwrite any existing data in the Emergency Responder configuration.

Step 7 Click **Close** to close the Import Manually Configured Phone page.

Related Topics

Switch Port Details, on page 438
Export Switch Ports, on page 440
Set Up Individual Switch Ports , on page 159
Export Switch Port Information , on page 162
Work with Emergency Responder Locations , on page 135

Export Manually Configured Phone Information

You can export your Emergency Responder manually configured phone configuration. By exporting this information, you can back up your data or create a file that you can use to update a large number of manually configured phone mappings in Emergency Responder. You can edit the export file, make your changes, then reimport the file and overwrite the information in Emergency Responder.

Before you begin

You must have system administrator or ERL administrator authority to export switch port definitions.

Procedure

Step 1 Select **ERL Membership** > **Manually Configured Phones**.

Emergency Responder opens the Find and List Manually Configured Phones page.

Step 2 Click **Export**.

Emergency Responder opens the Export Manual Phones page.

Step 3 Select the export format (csv) from the Select Export Format pulldown menu.

Step 4 Enter the desired file name in the Enter Export File Name field and click **Export**.

Emergency Responder exports the file to the export location.

Step 5 To download the exported file to your local system, select the file name from the Select file to download pulldown menu and click **Download**.

Step 6 Click **Close** to close the Export Manual Phones page.

Related Topics

Manually Define Phones , on page 168
Assign Large Number of Manually Configured Phones to ERLs , on page 170
Work with Emergency Responder Locations , on page 135
Synthetic Phones , on page 172

Synthetic Phones

With Emergency Responder, you can use Cisco Unified Operations Manager to monitor the health and functionality of Cisco Emergency Responder. To use Cisco Unified Operations Manager with Cisco Emergency Responder, you configure a synthetic phone in Emergency Responder and associate the synthetic phone to an ERL that is used as a test ERL. When a synthetic phone makes an emergency call, Emergency Responder uses the associated test ERL to route the call.

Note You can only configure test ERLs for conventional ERLs. You cannot configure test ERLs for off-premise ERLs and National E911 Service Provider ERLs.

For more information, see Set Up Test ERLs , on page 144.

View Emergency Call History

You can view the history of emergency calls made in your network that are handled by Emergency Responder. Emergency Responder sends emergency call notifications to the onsite alert personnel that you identify in your ERLs, and these people respond to the notifications. From the administrator interface, you can view the same call history that your onsite alert personnel can view, and see comments they make about the calls. You might need to review the call history to report on usage or to troubleshoot call routing problems.

Tip From the Call History page, you can view detailed information about the 10,000 most recent calls. You can find records of older calls in Emergency Responder raw call log files. See Call History Logs , on page 353 for more information.

Procedure

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

Emergency Responder opens the Call History page.

Step 2 Click **Find**.

All call summary information appears.

Step 3 Enter the search criteria that you want to use to create a list of emergency calls.

To view a list of all calls, click **Find** without entering any search criteria.

To narrow your search, select the item you on which you want to search, and click **Find**. For example, you can view calls that were made in a specific ERL, or calls that were made from a specific phone extension. If you want to search on more than one criteria, click **More** to add additional search fields. Select **All** at the top of the list to perform an AND search (a call only matches the search if each of the criteria is met), or **Any** for an OR search (a call matches the search if it matches one or more of the criteria).

Step 4 From the list of calls that Emergency Responder shows you in response to your search criteria, you can:

- View the call characteristics.
- Click the ERL name to view the ERL details. From the ERL details, you can also view the ALI for the call.
- Click **edit** in the comment field to change the comment. Emergency Responder opens a separate window where you make your editorial changes.

Tip If a large number of calls match your search criteria, Emergency Responder uses additional pages to list the calls. Use the links at the bottom of the list to move through these additional pages.

Related Topics

Call History Logs , on page 353

SAML Single Sign-On Overview

Use SAML Single Sign-On (SSO) to access a defined set of Cisco applications after signing into one of those applications. SAML describes the exchange of security-related information between trusted business partners. It is an authentication protocol used by service providers (such as Cisco Emergency Responder) to authenticate a user. With SAML, security authentication information is exchanged between an identity provider (IdP) and a service provider. The feature provides secure mechanisms to use common credentials and relevant information across various applications.

SAML Single Sign-On establishes a circle of trust (CoT) by exchanging metadata and certificates as part of the provisioning process between the IdP and the service provider. The service provider trusts user information of the IdP to provide access to the various services or applications.

Note During upgrade, SAML SSO login does not respond.

The client authenticates against the IdP, and the IdP grants an Assertion to the client. The client presents the assertion to the service provider. Because a CoT established, the service provider trusts the assertion and grants access to the client.

Note SSO is not supported for Cisco Unified OS Administration or Disaster Recovery System. If you log in to Cisco Unified OS Administration or Disaster Recovery System when SSO is enabled, and try to access Cisco ER Administration or Cisco ER Serviceability or Cisco ER User or Cisco ER Admin Utility, then Cisco Emergency Responder authorizes the user but not authenticate through IdP. To authenticate the user through IdP, close the web browser and access the Cisco Emergency Responder again. SSO is not supported for Cisco Emergency Responder Off-Premises User page.

SAML Single Sign-On Prerequisites

- DNS configured for the Cisco Emergency Responder cluster
- An identity provider (IdP) server
- Add the same users present in IdP to Cisco Emergency Responder.
- To configure the trust relationship between IdP and Cisco Emergency Responder servers, obtain the trust metadata file from your IdP and import it to all your servers.
- Export metadata from Cisco Emergency Responder and upload it on to the IdP server.

The following IdPs using SAML 2.0 are tested for the SAML Single Sign-On feature:

- OpenAM 10.0.1
- Microsoft® Active Directory® Federation Services 2.0, 3.0, and 4.0
- PingFederate® 6.10.0.4
- F5 BIP-IP 11.6.0

The third-party applications must meet the following configuration requirements:

- The mandatory attribute “uid” must be configured on the IdP. This attribute must match the attribute that is used for the user ID in Cisco Emergency Responder.

Note Cisco Emergency Responder currently supports only the sAMAccountName option as the LDAP attribute for user ID settings.

For information about configuring mandatory attribute mapping, see the IdP product documentation.

NTP Setup

In SAML SSO, Network Time Protocol (NTP) enables clock synchronization between the Cisco Emergency Responder and IdP. SAML is a time sensitive protocol and the IdP determines the time-based validity of a SAML assertion. If the IdP and Cisco Emergency Responder clocks are not synchronized, the assertion becomes invalid and stops the SAML SSO feature. The maximum allowed time difference between the IdP and Cisco Emergency Responder is 3 seconds.

Note For SAML SSO to work, you must install the correct NTP setup and make sure that the time difference between the IdP and Cisco Emergency Responder does not exceed 3 seconds.

For information about synchronizing clocks, see NTP Server List, on page 535.

Domain Name Server (DNS) Setup

Cisco Emergency Responder can use DNS to resolve Fully Qualified Domain Names (FQDNs) to IP addresses. The Service Providers and the IdP must be resolvable by the browser.

SAML Single Sign-On Task Flow

Follow these tasks to activate SAML Single Sign-On in Cisco Emergency Responder.

Procedure

	Command or Action	Purpose
Step 1	Add An IdP User, on page 175	Use this procedure to add an IdP user.
Step 2	Enable SAML Single Sign-On, on page 175	Use this procedure to enable SAML Single Sign-On.
Step 3	Disable SAML Single Sign-On, on page 177	Use this procedure to disable SAML Single Sign-On.

Add An IdP User

Procedure

Step 1 From Cisco ER Administration, choose **User Management** > **User**.
The **Find And List Users** page appears.

Step 2 Click **Add New User**.
The **Add User** page appears.

Step 3 Enter the username in the **User Name** field.

Step 4 From the **Authentication Mode** drop-down list, choose “IdP”.

Step 5 From the **CUCM Cluster** drop-down list, choose the Cisco Unified Communications Manager cluster IP address.

Note The users can login into the recovery url by using the password set in Cisco Unified Communications Manager through AXL, if the same user name exists in Cisco Unified Communications Manager.

Local credential policy is applicable only for the local users. IdP users have the same credential policy as remote users have in Cisco Emergency Responder.

Step 6 Click **Insert**.

What to do next

Enable SAML Single Sign-On, on page 175

Enable SAML Single Sign-On

Perform the following steps to enable SAML Single Sign-On:

Before you begin

Ensure that the following prerequisites are met before proceeding with the steps:

- Add An IdP User, on page 175—Ensure to manually add at least one IdP user in Cisco Emergency Responder.

Procedure

Step 1 From Cisco ER Administration, choose **System** > **SAML Single Sign-On**.

Step 2 Click **Enable SAML SSO**.

A warning message is displayed to notify that the change made takes a few minutes to reflect on the user interface.

Step 3 Click **Continue**.

A dialog box that allows you to import IdP metadata displays. To configure the trust relationship between the IdP and your servers, you must obtain the trust metadata file from your IdP and import it to all your servers.

Step 4 Click **Browse** to locate and upload the IdP metadata file.

Step 5 Click **Import IdP Metadata**.

Step 6 Click **Next**.

Note The **Next** button is enabled only if the IdP metadata file is successfully imported on at least one node in the cluster.

A new status message is added in the **SAML Single Sign-On Configuration** window. It provides optional information to either skip or continue further with steps to upload the server metadata to the IdP.

Step 7 Click **Download Trust Metadata Fileset** to download server metadata to your system.

Step 8 Upload the server metadata on the IdP server.

After you install the server metadata on the IdP server, run a Single Sign-On test to ensure that the metadata files are correctly configured.

Step 9 Click **Next** to continue.

Step 10 Select an ldP user with administrator rights from the list of valid administrator IDs.

Step 11 Click **Run Test**.

The IdP sign-in window displays.

Note You cannot enable SAML Single Sign-On until the Run Test succeeds.

Step 12 Enter a valid username and password.

After successful authentication, the following message is displayed:

```
SSO Test Succeeded
```

Close the browser window after you see this message.

If the authentication fails or takes more than 60 seconds to authenticate, a "sign-in Failed" message is displayed on the IdP sign-in window. The following message is displayed on the SAML Single Sign-On window:

```
SSO Metadata Test Timed Out
```

To attempt signing in to the IdP again, repeat Steps 11 and 12.

Step 13 Click **Finish** to complete the SAML Single Sign-On setup.

SAML Single Sign-On is enabled and it may take one to two minutes for the changes to take effect.

Disable SAML Single Sign-On

Perform the following steps to disable SAML Single Sign-On:

Procedure

Step 1 From Cisco ER Administration, choose **System** > **SAML Single Sign-On**.

Step 2 Click **Disable SAML SSO**.

A warning message is displayed to notify that the changes made take a few minutes to reflect on the user interface.

Access the Recovery URL

Use the recovery URL to bypass SAML Single Sign-On and log in to the Cisco Emergency Responder interface for troubleshooting. For example, enable the recovery URL before you change the domain or hostname of a server. Logging in to the recovery URL facilitates an update of the server metadata.

Before you begin

- Only application users with administrative privileges can access the recovery URL.
- If SAML Single Sign-On is enabled, the recovery URL is enabled by default. You can enable and disable the recovery URL from the CLI. For more information about the CLI commands to enable and disable the recovery URL, see *Cisco Emergency Responder Command Line Interface Guide*.

Procedure

In your browser, enter `https://<hostname/hostip>/ceradmin/servlet/showRecovery`.

Update Server Metadata After a Domain or Hostname Change

After a domain or hostname change either in IdP or Cisco Emergency Responder, update the server metadata and clear the browser cache, to ensure that SAML Single Sign-On is functional.

Before you begin

If the recovery URL is disabled, it does not appear for you to bypass the Single Sign-On link. To enable the recovery URL, log in to the CLI and execute the following command: **utils sso recovery-url enable**.

Procedure

Step 1 In the address bar of your web browser, enter the following URL:

`https://<CER-server-name>` where `< <CER-server-name>` is the hostname or IP address of the server.

Step 2 Click **Recovery URL to bypass Single Sign-On (SSO)**.

Step 3 Enter the credentials of an application user with an administrator role and click **Login**.

Step 4 From Cisco ER Administration, choose **System** > **SAML Single Sign-On**.

Step 5 Click **Export Metadata** to download the server metadata.

Step 6 Upload the server metadata file to the IdP.

Step 7 Click **Run SSO Test**.

Step 8 Enter a valid User ID and password.

Step 9 After you see the success message, close the browser window.

Manually Provision Server Metadata

To provision a single connection in your IdP for multiple UC applications, you must manually provision the server metadata while configuring the Circle of Trust between the Identity Provider and the Service Provider. For more information about configuring the Circle of Trust, see the IdP product documentation.

The general URL syntax is as follows:

```
https://<SP FQDN>:8443/ssosp/saml/SSO/alias/<SP FQDN>
```

Procedure

To provision the server metadata manually, use the Assertion Customer Service (ACS) URL.

Example:

Sample ACS URL:
```
<md:AssertionConsumerService
Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://cucm.ucsso.cisco.com:8443/ssosp/saml/SSO/alias/cucm.ucsso.cisco.com"
index="0"/>
```

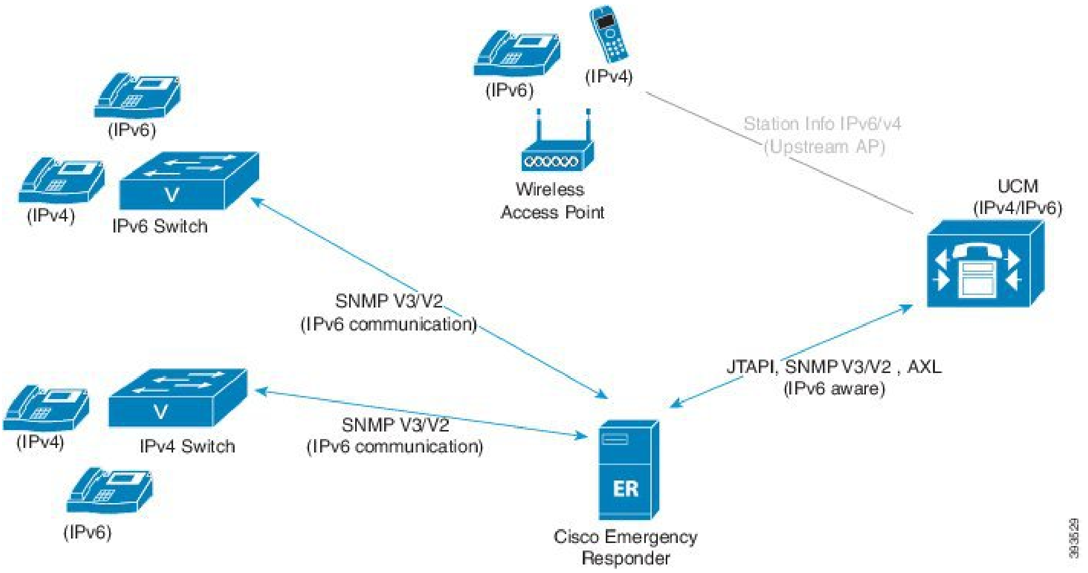
The remaining services are accessible only after providing valid local, IdP or Remote user credentials. In case of testing the SAML SSO Rest APIs using any rest client, valid credentials is necessary. The client validates the local, IdP or Remote(CER Users) authentication is same as Recovery URL, and the authentication grants an Assertion to the client. After successful authentication, the client presents the Assertion to the Service Provider. Since there is a CoT established, the Service Provider validates the Assertion and grants access to the client.

Note When you try to EnableSSO through the rest client, the server restarts. During this period, when 911 call is made, it may fetch the default ERL and the server also takes some time to publish all node information under **Cisco Emergency Responder Administration** > **System** > **SAML Single Sign-On**.

IPv6 Endpoints Support

Cisco Emergency Responder can track the IPv6-only phone through the switch port based tracking or access point based tracking or as manually configured phone. For the switch port based tracking, Cisco Emergency Responder can talk to Cisco switches configured as the IPv4 address or IPv6 address through the SNMP protocol. Access point based tracking requires the IPv6-only phone to communicate its upstream infrastructure information to Cisco Unified Communications Manager. For more information on Access Point Configuration and Discovery, see Access Point Configuration and Discovery, on page 164.

Figure 20: IPv6 Endpoints



For more details about IPv6 deployment, see the *IPv6 Deployment Guide for Cisco Collaboration Systems Release 12.0* at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-system/products-implementation-design-guides-list.html.

IPv6 Endpoints Task Flow

Complete these tasks to track the IPv6 phones at the IPv4 switch and IPv6 switch, and also to discover an IPv6 switch ports in Cisco Emergency Responder.

Procedure

Step 1 Prerequisites for Cisco Unified Communications Manager to Track IPv6 Endpoints , on page 180.

Step 2 Prerequisites for Cisco Emergency Responder to Discover IPv6 Switch , on page 181.

Step 3 Set Up SNMPv6 , on page 181.

Step 4 Add IPv6 Switch, on page 182.

Step 5 Add IPv6 as Manually Configured Phones, on page 182.

Prerequisites for Cisco Unified Communications Manager to Track IPv6 Endpoints

To track all IPv6 phones in Cisco Emergency Responder, enable IPv6 in Cisco Unified Communications Manager.

Procedure

Step 1 Select **Cisco Unified OS Administration** > **Settings** > **IP** > **Ethernet IPv6**.
The **Ethernet IPv6 Configuration** page appears.

Step 2 Check the **Enable IPv6** check box.
The **Router Advertisement** options are enabled.

Step 3 Click **Manual Entry** radio button to enter the IPv6 address manually.
The **IPv6 Address**, **Prefix Length**, and **Default Gateway** fields are enabled.

Step 4 Enter the values in the following fields:

- Enter an **IPv6 Address**. For example, `fd62:6:96:21e:bff:fecc:2e3a`.
- Enter the **Prefix Length**. For example, `64`.
- Enter the **Default Gateway**. For example, `fe80::3ece:73ff:fea9:c641`.

Step 5 Check the **Update with Reboot** check box to ensure that the system reboots after you save.

Step 6 Click **Save**.

Step 7 Select **Cisco Unified CM Administration** > **System** > **Server**.
The **Find and List Servers** page appears.

Step 8 Click **Find** and then select the added server from the displayed list.

Step 9 Enter **IPv6 Address**.

Step 10 Click **Save**.

Step 11 Select **Cisco Unified CM Administration** > **System** > **Enterprise Parameters**.
The **Enterprise Parameters Configuration** page appears.

Step 12 Set the value of the **Enable IPv6** enterprise parameter to **True** under **IPv6** section.

Step 13 Click **Save**.

Step 14 Select **Cisco Unified CM Administration** > **Device** > **Device Settings** > **Common Device Configuration**.
The **Find and List Common Device Configurations** page appears.

Step 15 Click **Add New**.

Step 16 Configure the fields in the **Common Device Configuration** window. For help with the fields and their settings, refer to the Cisco Unified Communications Manager online help.

Step 17 Select the **IP Addressing Mode** as **IPv4 and IPv6**.

Step 18 Click **Save**.

What to do next

Prerequisites for Cisco Emergency Responder to Discover IPv6 Switch , on page 181.

Prerequisites for Cisco Emergency Responder to Discover IPv6 Switch

To discover an IPv6 switch, enable IPv6 in **Cisco Emergency Responder**.

Before you begin

Prerequisites for Cisco Unified Communications Manager to Track IPv6 Endpoints , on page 180.

Procedure

Step 1 Select **Cisco Unified OS Administration** > **Settings** > **IP** > **Ethernet IPv6**.
The **Ethernet IPv6 Configuration** page appears.

Step 2 Check the **Enable IPv6** check box.
The **Router Advertisement** options are enabled.

Step 3 Click **Manual Entry** radio button to enter the IPv6 address manually.
The **IPv6 Address**, **Prefix Length**, and **Default Gateway** fields are enabled.

Step 4 Enter the values in the following fields:

- Enter an **IPv6 Address**. For example, `fd62:6:96:21e:bff:fecc:2e3a`.
- Enter the **Prefix Length**. For example, `64`.
- Enter the **Default Gateway**. For example, `fe80::3ece:73ff:fea9:c641`.

Step 5 Check the **Update with Reboot** check box to ensure that the system reboots after you save.

Step 6 Click **Save**.

What to do next

Set Up SNMPv6 , on page 181.

Set Up SNMPv6

Before you begin

Prerequisites for Cisco Emergency Responder to Discover IPv6 Switch , on page 181.

Procedure

Step 1 Select **Phone Tracking** > **SNMPv2 Settings** or **Phone Tracking** > **SNMPv3 Settings**.

Emergency Responder opens the **SNMP Settings** page.

Step 2 In the **IP Address/Host Name** field, enter an IPv6 address pattern to which you want to associate an SNMP read community string.

Note Wildcard characters are not supported for the IPv6 address.

Step 3 Based on the SNMP selection in step 1, complete the task as stated in the Set Up SNMPv2, on page 149 or Set Up SNMPv3 , on page 151.

What to do next

Add IPv6 Switch, on page 182.

Add IPv6 Switch

Before you begin

Set Up SNMPv6 , on page 181.

Procedure

Step 1 Select **Phone Tracking** > **LAN Switch Details**.

Emergency Responder opens the **LAN Switch Details** page.

Step 2 In the **Switch Host Name/IP Address** field, enter IPv6 address or hostname of the switch.

Step 3 Complete the task as stated in the Identify LAN Switches One at a Time , on page 153.

Add IPv6 as Manually Configured Phones

Procedure

Step 1 Select **ERL Membership** > **Manually Configured Phones**.

Emergency Responder opens the **Find and List Manually Configured Phones** page.

Step 2 Click the **Add New Manual Phone** button.

Step 3 If the phone is an IP phone, enter the IPv6 address and MAC address for the phone in the **IPv6 Address** and **MAC Address** fields respectively.

Step 4 Complete the task as stated in the Manually Define Phones , on page 168.

IPv6 Endpoint Restrictions

- Cisco Emergency Responder communications for email alerts and the file transfer is through IPv4 address only.
- IP subnet based tracking is for IPv4 endpoints (IP phones). Analog phones can be tracked through the IPv4 address gateway.
- Teleworkers and the off-premises features are supported with IPv4 only.

CHAPTER 6

Configure Emergency Responder and National E911 Service Provider Enterprise Services

Emergency Responder and National E911 Service Provider Enterprise Services Overview

Cisco Emergency Responder (Emergency Responder) supports National E911 Service Provider for Enterprise Service in the Cisco Unified Communications environment as an alternative to direct connection with the Local Exchange Carrier (LEC). The National E911 Service Provider for Enterprise Service provides local routing and emergency service response for National E911 Service Provider customers. Emergency Responder works in conjunction with National E911 Service Provider to provide emergency services to phones that are on the corporate network (on-premise) and phones that are located away from the corporate network (off-premise).

For more information about configuring Emergency Responder, managing Emergency Responder users, working with ERLs, and other related topics, see the "Add Scheduled National E911 Service Provider Updates" section.

These topics provide an overview of how Emergency Responder operates with National E911 Service Provider for Enterprise Service and how to configure and use Emergency Responder to support National E911 Service Provider Enterprise users.

National E911 Service Provider for Enterprise Service

If you are a subscriber to National E911 Service Provider for Enterprise Service, you can use Emergency Responder to simplify emergency call management. Emergency Responder provides an interface that allows you to enter and synchronize location information directly to the National E911 Service Provider database. Emergency Responder provides location information for emergency calls for both on-premise phones and off-premise phones and works with National E911 Service Provider and Unified CM to complete emergency calls.

Emergency Responder tracks IP phones by the IP subnet or when someone manually configures and assigns the MAC address. Emergency Responder maintains the status of the phones (on-premise, off-premise, unlocated), and passes on any ALI or ELIN information to National E911 Service Provider. Users with on-premise phones rely on Cisco Unified Communications to route their emergency calls to National E911 Service Provider and the designated emergency provider.

Users with off-premise phones cannot make emergency calls until the users enter in their location and associate this information with their directory number. After the location information has been verified, emergency calls placed from off-premise phones can be completed.

Note Users can only configure one off-premise location for each DID (DN + External Mask). This configuration also applies to shared lines. If two off-premise phones share a DID, the user can only associate one location to the DID.

The following figure shows the interactions between users, Emergency Responder, and National E911 Service Provider.

Figure 21: Understanding the Interactions Between Users, Emergency Responder, and National E911 Service Provider

Emergency Call Flow

When a user makes an emergency call:

1. Unified CM routes the call to Emergency Responder.
2. Emergency Responder routes the call to National E911 Service Provider.
3. National E911 Service Provider receives the 10-digit ELIN for the calling party and obtains the ALI data for the caller from this calling party number.
4. National E911 Service Provider completes the call.

Set Up Support for National E911 Service Provider for Enterprise Service

After you have confirmed your emergency service support with National E911 Service Provider, you must configure Emergency Responder to support National E911 Service Provider for Enterprise Service.

You must complete the tasks described in the following procedure before creating National E911 Service Provider ERLs.

Note You must configure the IP address of the DNS server to resolve the URLs provided by National E911 Service Provider before completing these tasks. See *Cisco Unified Operating System Administration Web Interface For Cisco Emergency Responder*.

Procedure

Step 1 Configure the following items in the Validation and Update Interface (VUI):

a) Upload the certificate provided by National E911 Service Provider.
b) Validate the certificate.
c) Configure National E911 Service Provider Account Information.

Step 2 Configure Route Patterns for routing calls to National E911 Service Provider on the Emergency Responder server.

Step 3 Configure Route Patterns and gateway for routing calls to National E911 Service Provider on Unified CM server.

See Understanding Route Plans chapter in *Cisco Unified Communications Manager System Guide*, and the “Gateway Configuration” chapter in the *Cisco Unified Communications Manager Administration Guide*.

Step 4 Create National E911 Service Provider ERL and verify the validity and consistency of the ALI data for the National E911 Service Provider ERL against the National E911 Service Provider TN database.

Step 5 Assign National E911 Service Provider ERLs to switch ports, IP subnets, and unlocated phones.

Related Topics

Set Up Emergency Responder to Support Off-Premise Users
Set Up National E911 Service Provider VUI Settings , on page 187
Set Up National E911 Service Provider Patterns on Emergency Responder , on page 188
Reconcile ALI Discrepancies , on page 190
Switch Port Configuration , on page 159
Identify Unlocated Phones , on page 167

Set Up National E911 Service Provider VUI Settings

Before you can configure National E911 Service Provider VUI settings, you must have your account information and a certificate from National E911 Service Provider.

Note To continue emergency service support when there is a failover to the Emergency Responder subscriber, you must upload the certificate file to the Emergency Responder subscriber separately.

Note After upgrading the Cisco Emergency Responder, upload the certificate again to continue using the National E911 Service Provider Service.

Procedure

Step 1 From Emergency Responder, choose **System > National E911 Service Provider VUI Settings.**

The National E911 Service Provider VUI Settings page displays.

Step 2 Click **Upload Certificate**.
An Upload Certificate window opens.

Step 3 Use the **Browse** button to locate the National E911 Service Provider certificate file, highlight the file, and click the **Upload** button.

Step 4 Enter the **Certificate Password** and the **VUI URL** in the adjacent text boxes. Click **Test and Validate**.

Step 5 Check the **Enable HTTP Proxy** check box if you want to use a proxy server for requests between Emergency Responder and National E911 Service Provider.

Step 6 Enter the **Proxy Host Name/IP Address** of the proxy server, along with the port.

Step 7 Check the **Authentication needed on HTTP Proxy** check box if you want to communicate with the National E911 Service Provider using authentication based proxy server. If you enable this check box, only then the **Proxy User Name** and **Proxy Password** fields are enabled.

Step 8 Enter the configured user name for proxy server in the **Proxy User Name** field and the **Proxy Password** associated to the username.

Step 9 Click the **Test and Validate Certificate** button to test the validity of your certificate.

Step 10 Enter the Account Information.

- VUI Schema URL

- National E911 Service Provider Account ID
- Max VUI Connections
- Set MyE911 for location Updates: **True**

Note In case the remote users are not updating their locations using MyE911 or Remote Location Manager when Off-premises, set the **MyE911 for Location Updates** flag to **False**.

Step 11 Click **Update**.

Note To replace the National E911 Service Provider VUI certificate, you must delete the existing National E911 Service Provider account and then proceed from Step 1. Else, the **Upload Certificate** option will be grayed out.

For more information about the National E911 Service Provider VUI settings, see National E911 Service Provider VUI Settings, on page 386.

Step 12 Click **Test Connectivity** to verify whether Emergency Responder can successfully connect to the customer specific account through the National E911 Service Provider VUI.

Related Topics

Set Up National E911 Service Provider Patterns on Emergency Responder , on page 188
Set Up National E911 Service Provider ERLs, on page 188
Reconcile ALI Discrepancies , on page 190

Set Up National E911 Service Provider Patterns on Emergency Responder

Before any emergency calls can be completed by National E911 Service Provider for Enterprise Service, you must configure the route patterns for routing the call to National E911 Service Provider.

Procedure

Step 1 From Emergency Responder, Choose **System** >**Telephony Settings.**

The Telephony Settings page is displayed.

Step 2 Under National E911 Service Provider Route Pattern Settings, enter the National E911 Service Provider Route/ Translation Pattern and click the **Add** button.

Set Up National E911 Service Provider ERLs

Before you begin

You must first configure National E911 Service Provider route patterns before you can add any National E911 Service Provider ERLs.

Note National E911 Service Provider ERLs differ from conventional ERLs in the following ways:

- You can only select route patterns from a preconfigured list in the Telephony Settings web page.
- You can query and validate ALI data from National E911 Service Provider by using National E911 Service Provider VUI (Validation & Update interface).
- You must submit ALI data (TN Update) to National E911 Service Provider by using National E911 Service Provider VUI before an emergency call can be successfully routed.

Procedure

Step 1 From Emergency Responder, choose **ERL**>**National E911 Service Provider ERL** > **National E911 Service Provider ERL(Search and List)**.

The Find National E911 Service Provider ERL Data page displays.

Step 2 Click the **Add New ERL** button.

Emergency Responder opens the Add New ERL window. See Find National E911 Service Provider ERL, on page 411 for a detail explanation of each field.

Step 3 Fill in the ERL Information.

Step 4 Click **ALI Details**

Emergency Responder opens the ALI Information window.

Step 5 Enter the ALI Information. The "ALI Information section", *Cisco Emergency Responder Administration Web Interface Appendix A*, contains detailed explanations of each field. To look up an address in the National E911 Service Provider MSAG database, click **Query from National E911 Service Provider**.

Step 6 After entering the ALI Information, click **Pre-validate from National E911 Service Provider**.

Step 7 Make the Add New ERL window the active window if it is not, and click **Insert**.

Emergency Responder saves the ERL and its ALI.

National E911 Service Provider ERL Imports

If you have multiple ERLs, and you want to add them all at once, you can create a file that contains more than one ERL definition, and import all the ERLs at the same time into your Emergency Responder configuration. For more information about importing ERLs, see Import Several ERLs , on page 141.

National E911 Service Provider ERL Information Export

Use the Export ERL page to create ERL export files for our own use, for example, to back up or move an ERL configuration. For more information about importing ERLs, see Export ERL Information , on page 146.

Related Topics

Set Up National E911 Service Provider VUI Settings , on page 187

Set Up National E911 Service Provider Patterns on Emergency Responder , on page 188
Reconcile ALI Discrepancies , on page 190

Reconcile ALI Discrepancies

You can use Emergency Responder to compare the records from National E911 Service Provider VUI with the records in the database and displays ALI records that have discrepancies. You can examine each record and choose to update the local record with information from National E911 Service Provider or update National E911 Service Provider's record.

Procedure

Step 1 In Emergency Responder Administration, choose **ERL** > National E911 Service Provider **ERL** > **View ALI Discrepancies**.

The View National E911 Service Provider ALI Discrepancies page appears.

Step 2 Enter search criteria to find any specific ELINS and click **Find**, or click **Find** without any search criteria to display all National E911 Service Provider ALI discrepancies. The search results appear.

Step 3 Click on the radio button next to the ELIN that you want to view or click **View ALI Discrepancies** to launch the View National E911 Service Provider ALI discrepancies for a particular ELIN.

The View National E911 Service Provider ALI Discrepancies for a particular ELIN window appears.

Step 4 Choose the correct data from either the local Emergency Responder database or from National E911 Service Provider.

Step 5 Click **Save** to save changes to the local Emergency Responder database. Click **Save** National E911 Service Provider **ALI Info** to save changes to the National E911 Service Provider VUI.

Step 6 Click **Close** to close this window.

Related Topics

Set Up National E911 Service Provider VUI Settings , on page 187
Set Up National E911 Service Provider Patterns on Emergency Responder , on page 188
Set Up National E911 Service Provider ERLs, on page 188

ERL Data Migration

Emergency Responder supports migrating existing conventional ERLs to National E911 Service Provider ERLs and vice versa.

Migrate Conventional ERL Data to National E911 Service Provider ERL Data

Procedure

Step 1 In Emergency Responder Administration, choose **ERL** > **ERL Migration Tool**.

The ERL Migration Tool page appears.

Step 2 Choose **Conventional ERL** in the search parameter drop-down list, enter the search criteria, and click **Find**.

Step 3 Select the ERLs that you want to migrate by checking the check box next to the ERL name.

The Enter Route Patterns for ERL Migration window appears.

Step 4 Choose an updated route pattern from the drop-down list.

Step 5 Click **Migrate to** National E911 Service Provider **ERL**.

Related Topics

Set Up Support for National E911 Service Provider for Enterprise Service , on page 186
Migrate National E911 Service Provider ERL Data to Conventional ERL Data , on page 191

Migrate National E911 Service Provider ERL Data to Conventional ERL Data

Procedure

Step 1 In Emergency Responder Administration, choose **ERL** > **ERL Migration Tool**.
The ERL Migration Tool page appears.

Step 2 Choose National E911 Service Provider ERL in the search parameter drop-down list, enter the search criteria, and click **Find**.

Step 3 Select the ERLs that you wish to migrate by checking the check box next to the ERL name.
The Enter Route Patterns for ERL Migration window appears.

Step 4 Enter an updated route/pattern translation pattern in the adjacent text box.

Step 5 Click **Migrate to Conventional ERL**.

Related Topics

Migrate Conventional ERL Data to National E911 Service Provider ERL Data , on page 190
ERLs, on page 135

Add Scheduled National E911 Service Provider Updates

You can create ALI and Secondary Status update schedules between Emergency Responder and National E911 Service Provider. A scheduled ALI update sends newly created TN records to National E911 Service Provider. A scheduled Secondary Status update sends queries to National E911 Service Provider requesting information about records with errors that have been corrected.

Procedure

Step 1 Choose **ERL** > National E911 Service Provider **ERL** > National E911 Service Provider **Schedule** from Emergency Responder.
The National E911 Service Provider Schedule page appears.

Step 2 Choose the days of the week and the time of day that you want to schedule an update.

Step 3 Check the **Enable Schedule** check box if you want to activate this schedule.

Step 4 Choose either **ALI Update Schedule** or **Secondary Status Update Schedule**.

Step 5 Click **Add** to add the schedule to the list of schedules.

Related Topics

Emergency Responder User Management , on page 117
Emergency Responder Role Management , on page 121
Emergency Responder User Group Management , on page 123
Log In to Emergency Responder , on page 126
Server and Server Group Configuration , on page 128
Set Up Emergency Responder Cluster and Cluster DB Host , on page 134
Cisco Unified Communications Manager Cluster Changes , on page 134
Work with Emergency Responder Locations , on page 135
Emergency Responder Switch Configuration , on page 148
Phone Management , on page 159
National E911 Service Provider ERL - Secondary Status, on page 413
National E911 Service Provider Schedule, on page 414

Update Scheduled National E911 Service Provider Update

Procedure

Step 1 From Emergency Responder, choose **ERL**National E911 Service Provider **ERL**National E911 Service Provider **Schedule**.
The National E911 Service Provider **Schedule** page appears.

Step 2 Click the **Edit** link adjacent to the schedule that you want to update.

Step 3 Choose the days of the week and the time of day.

Step 4 Check the **Enable Schedule** check box to activate this schedule.

Step 5 Click **Update** to change the schedule on the list of schedules.

Related Topics

Emergency Responder User Management , on page 117
Emergency Responder Role Management , on page 121
Emergency Responder User Group Management , on page 123
Log In to Emergency Responder , on page 126
Server and Server Group Configuration , on page 128
Set Up Emergency Responder Cluster and Cluster DB Host , on page 134
Cisco Unified Communications Manager Cluster Changes , on page 134
Work with Emergency Responder Locations , on page 135
Emergency Responder Switch Configuration , on page 148
Phone Management , on page 159
National E911 Service Provider ERL - Secondary Status, on page 413

National E911 Service Provider Schedule, on page 414

CHAPTER 7

Configure Cisco Emergency Responder Serviceability

Cisco Emergency Responder Serviceability Configuration Overview

Note The following information addresses SNMP Management. For information about SNMP setting for phone tracking , refer to Set Up SNMP Connection, on page 149.

Emergency Responder supports SNMP V1/V2C and V3. You can use the Serviceability web interface to configure SNMP V1/V2C (Community String and Notification Destination) and SNMP V3 (User and Notification Destination).

Each SNMP version has security models and security levels. Users are assigned to groups that are defined by a security model and specified security levels. Each group also has a defined security access level to a set of MIB objects for reading and writing, which are known as views. The switch has a default view (all MIB objects) and defaults groups defined for SNMP V1 and V2C security models. SNMP V3 provides additional security features that cover message integrity, authentication, and encryption. In addition, SNMP V3 controls user access to specific areas of the MIB tree.

The following sections describe how to configure SNMP V1/V2C and V3.

Serviceability Tools

The following sections describe the Emergency Responder Serviceability tools.

Use Control Center

The Control Center allows you to perform actions on the services running on the selected Emergency Responder system.

Procedure

Step 1 From the Emergency Responder Serviceability web interface, select **Tools** > **Control Center**.
The Control Center page appears.

Step 2 To change the status of a service, click the radio button to the left of the Service Name and click the button corresponding to the desired action. Available actions are:

- Start
- Stop
- Restart

Note Cisco Tomcat and Cisco IDS services cannot be started, stopped, or restarted from the Emergency Responder Serviceability website. These services can only be started, stopped, or restarted using the CLI.

Step 3 Click **Refresh** to refresh the page.

Related Topics

Control Center, on page 509

Use Event Viewer

The Event Viewer allows you to view events for the prior six months.

Procedure

Step 1 From the Emergency Responder Serviceability web interface, select **Tools** > **Event Viewer**.
The Event Viewer page appears.

Step 2 Click **Find** without entering any search criteria to find all events that occurred over the prior six months

To find events that match specific criteria, enter search criteria:

- Select a specific month to view events from the month only.
- If you select Type, you can then select the type on which to search from the pull-down menu to the right.

If you select Module, you can then select the module on which to search from the pull-down menu to the right.

Note For a list of available Types and Modules, see Event Viewer, on page 510.

When you have entered your search criteria, click **Find**.

Step 3 Perform an ascending or descending sort of the results. To perform a sort, click the up arrow or down arrow next to the Time, Type, or Module column headings.

Related Topics

Event Viewer, on page 510

SNMP Configuration

Note The following SNMP configuration information is for SNMP management. For information on SNMP setting for phone tracking, see Set Up SNMP Connection, on page 149.

Emergency Responder supports SNMP V1/V2C and V3. You can use the Serviceability web interface to configure SNMP V1/V2C (Community String and Notification Destination) and SNMP V3 (User and Notification Destination).

Each SNMP version has security models and security levels. Users are assigned to groups that are defined by a security model and specified security levels. Each group also has a defined security access level to a set of MIB objects for reading and writing, which are known as views. The switch has a default view (all MIB objects) and defaults groups defined for SNMP V1 and V2C security models. SNMP V3 provides additional security features that cover message integrity, authentication, and encryption. In addition, SNMP V3 controls user access to specific areas of the MIB tree.

The following sections describe how to configure SNMP V1/V2C and V3.

Set Up SNMP Community String

By configuring SNMP, you can control SNMP access to the Emergency Responder SNMP agent. A management station must first submit a valid community string for authentication.

You configure a community string by entering the Community String Name, the IP addresses of host that can be authenticated using the community string, and the access privileges allowed. The available access privileges are as follows:

- ReadOnly
- ReadWrite
- ReadWriteNotify
- NotifyOnly
- None

Procedure

Step 1 From the Emergency Responder Serviceability web interface, select **SNMP** > **V1/V2C Configuration** > **Community String**.
The SNMP Community String Configuration page appears.

Step 2 Enter the name of the community string in the Community String Name text box.

Step 3 Click **Accept SNMP Packets only from these hosts** to specify specific hosts whose SNMP packets will be accepted, enter the IP addresses in the text box, and click **Insert**.

To accept SNMP packets from any host, click the **Accept SNMP Packets from any host** radio button.

Step 4 Select the host IP address and click **Remove** to remove an existing host, .

Step 5 Select the access privilege for the host from the Access Privileges pull-down menu then click **Insert**.

Related Topics

SNMP Community String Configuration, on page 514

Set Up SNMP Users

SNMP V3 provides additional security features that include message integrity, authentication, and encryption. In addition, SNMP V3 controls user access to specific areas of the MIB tree.

Note FIPS Mode and Enhanced Security Mode do not support MD5 or DES encryption methods. If SNMPv3 setting is enabled using MD5 or DES, then enabling FIPS Mode or Enhanced Security Mode changes these encryption methods to SHA-1 or AES-128 respectively.

Before Emergency Responder (in FIPS Mode) upgrade, ensure that there are no MD5 or DES encryption methods in the FIPS Mode. If the MD5 or DES encryption methods were not updated to SHA-1 or AES-128 respectively in the FIPS Mode before upgrade, they will get updated automatically after the upgrade.

Procedure

Step 1 From the Emergency Responder Serviceability web interface, choose **SNMP** > **V3 Configuration** > **User**.

Step 2 Click **Add New** to add a new SNMP User.

Step 3 Enter the new SNMP user name in the **User Name** text box.

Step 4 Check the **Authentication Required** check box to require authentication. Enter a password in the **Password** text box, reenter the password in the **Reenter Password** textbox, and choose either **MD5** or **SHA** to select an authentication protocol. Click **Insert** to add the user.

Step 5 Check the **Privacy Required** check box to require information privacy. Enter a password in the **Password** textbox, reenter the password in the **Reenter Password** textbox, and choose either **DES** or **AES** to select a privacy protocol.

Note A message appears to restart the SNMP master agent for the changes to take effect. Click **OK** to restart the SNMP master agent or **Cancel** to continue without restarting the master agent.

The new user is added to the list of users on the SNMP User Configuration page.

Step 6 Repeat Step 2 through to Step 4 to add additional users.

Related Topics

SNMP User Configuration, on page 516

Set Up MIB2

The SNMP MIB2 tool allows you to specify a contact person for a MIB2 managed node and the physical location of the managed node.

Procedure

Step 1 From the Emergency Responder Serviceability web interface, select **SNMP** > **System Group Configuration** > **MIB2 System Group Configuration**.

Step 2 In the **System Contact** text box, enter the name of the contact.

Step 3 In the **Location** text box, enter the location of the managed node.

Step 4 Click **Update** in the upper left corner of the page.

Step 5 Click **Clear** in the upper left corner of the page to modify the information, enter the new information in the **System Contact** and **Location** text boxes, and click **Update**.

Related Topics

MIB2 System Group Configuration, on page 517

System Monitor Tools

The following sections describe how to use the System Monitor tools.

Use CPU and Memory Usage Tool

You can use the CPU and Memory Usage tool to monitor and log this information. By default, the information is refreshed every 30 seconds. You change how often the information refreshes, or you can disable the auto-refresh feature.

Procedure

Step 1 From the Emergency Responder Serviceability web interface, select **System Monitor** > **CPU & Memory Usage**.

The CPU and Memory Usage page appears.

The page is divided into two sections **Processors** and **Memory**. For details about the information that is displayed, see Table 125: CPU and Memory Usage Page , on page 518.

Step 2 Enter a value (in seconds) in the **Set the screen refresh value** text box to change the rate at which the page refreshes, and click **Set**. The minimum value you can enter is 5 seconds.

Step 3 Check the **Disable Auto-Refresh** check box in the upper left corner to disable the auto-refresh feature.

Step 4 Click the **Start Log** button in the Processors section of the page to create a log file of the CPU usage.

Click **Start Log** in the Memory section of the page to create a log file of the Memory usage.

You can create up to 25 log files.

The default interval for logging is 10 seconds. To change the logging interval, follow these steps:

a) To change the CPU logging interval, enter a value between 5 seconds and 600 seconds in the **Set CPU Logging Interval** text box and click **Set**.
b) To change the Memory logging interval, enter a value between 5 seconds and 600 seconds in the **Set Memory Logging Interval** text box and click **Set**.

Step 5 Click **Download CPU Log File** or **Download Memory Log File** to download the log files.

The system displays a Log Files page that shows all the current log files. Thereafter, log files are recycled; when a new log file is added, the oldest log file is deleted.

Step 6 To download individual files, click the check box to the left of the log file names that you want to download. To download all log files, check the check box to the left of the File Name column heading. When you have selected the files, click **Download**. If you select multiple files for download, the system creates and downloads a zipped folder called CPULogs (for Processor log files) and MemoryLogs (for Memory log files).

Step 7 To view the log files online without downloading them, click the file name. The system displays the contents of the log file.

Related Topics

CPU and Memory Usage, on page 518

Use Processes Tool

You can use the Processes tool to monitor and log process information. By default, the information is refreshed every 30 seconds; the minimum refresh value is 5 seconds. You can change how often the information refreshes, or you can disable the auto-refresh feature.

Procedure

Step 1 From the Emergency Responder Serviceability web interface, select **System Monitor** > **Processes**.

The Processes page appears. For details about the information that is displayed, see Table 126: CPU Log Files Page , on page 520.

You can perform an ascending or descending sort of the results. To perform a sort, click the up arrow or down arrow next to the column heading that you want to sort by. For example, to perform a descending sort based on the process, click the down arrow next to the Process column heading. Similarly, to perform an ascending sort based on the process ID, click the up arrow next to the PID column heading.

Step 2 Enter a value in the **Set the screen refresh value** text box in the upper right corner and click **Set** to change the rate at which the page refreshes. The minimum value you can enter is 5 seconds.

Step 3 Select the **Disable Auto-Refresh** check box in the upper left corner to disable the auto-refresh feature.

Step 4 Select the check box to the left of the process name and click **View Selected Processes** to view the details of a process. You can select a maximum of ten processes.

The Selected Processes displays the details of the process. On this page you can also set the refresh rate and disable the auto-refresh feature. To start a log of the process, click **Start Log**. To stop a log, click **Stop Log**.

To change the Process logging interval, enter a value between 5 seconds and 600 seconds in the **Set Process Logging Interval** text box and click **Set**.

Step 5 Click **Download Process Logs** from the Process Log Files page to download the log files. To download log files click **Download Log File** from the Processes page.

Step 6 Select the check box to the left of the log file names to download individual files. To download all log files, click the check box to the left of the File Name column heading. When you have selected the files, click **Download**. If you select multiple files for download, the system creates and downloads a zipped folder called ProcessLogs.

Step 7 You can also view the log files online without downloading them. To do so, click the file name. The system displays the contents of the log file in a separate window.

Related Topics

Processes, on page 521

Use Disk Usage Tool

The Disk Usage tool displays the percentage of available disk space used by the different partitions in the system.

Procedure

Step 1 From the Emergency Responder Serviceability web interface, select **System Monitor** > **Disk Usage**.

The Disk Usage page appears. For details about the Disk Usage page, see Table 130: Disk Usage Page , on page 523.

Step 2 Perform an ascending or descending sort. Click the up arrow or down arrow next to the column heading that you want to sort by. For example, to perform a descending sort based on the partition, click the down arrow next to the Partition column heading. Similarly, to perform an ascending sort based on the available disk space, click the up arrow next to the Available Space column heading.

Related Topics

Disk Usage, on page 522

Use Emergency Responder Logs

Emergency Responder provides an interface to collect system and application logs. These logs share the same user interface and log files can be viewed and downloaded in the same manner. The following procedure applies to all of the Emergency Responder logs.

Emergency Responder logs are organized into three types. The three types, and the logs within these types, are as follows:

- CER Logs
  - CER Admin
  - CER Server
  - CER Phone Tracking

  - CER Audit
  - CER API Services
  - JTAPI
  - Tomcat
  - Event Viewer
  - Audio Driver
  - Detailed Logs
- Platform Logs
  - CLI
  - CLM
  - Certificate Management/IPSec
  - DRS
  - Install/Upgrade
  - Remote Support
  - Syslog
  - Servm
- DB Logs
  - Cerdbmon
  - Install DB
- CLI Output Files
  - Platform
  - DB
- SLM Logs
  - SLM
  - GCH
  - TP

Procedure

Step 1 From the Emergency Responder Serviceability web interface, select **System Logs** > **Log Type** > **Log Name**.

The selected Log Files page appears. See Use Emergency Responder Logs , on page 201 for details about each of these pages.

You can perform an ascending or descending sort of the results. To perform a sort, click the up arrow or down arrow next to the column heading that you want to sort by.

Step 2 Download the log files to your local system using the **Download** button.

To select individual files, click the check box to the left of the log file name you want to download. To select all log files, click the check box to the left of the File Name column heading. When you have selected the files, click **Download**. If you select multiple files for download, the system creates and downloads a zipped folder called CPULogs. The names of the zipped folders are based on the type of logs that they contain, as follows:

- CER Admin
- CER Server
- CER Phone Tracking
- Syslog
- CER API Services
- JTAPI
- Tomcat
- Detailed Logs
- Install
- DRS
- CLILogs
- CMILogs
- ServmLogs
- RemoteSupportLogs
- InstallDBLogs
- CertificateManagement&IPSecLogs
- CerdbmonLogs
- CLIOutputPlatform
- CLIOutputDB
- SLMLogs
- GCHLogs
- TPLogs

Step 3 Click the file name to view the log files online without downloading them.
The system displays the contents of the log file in a separate window.

Step 4 Click **Reload Log File** to refresh the log file you are viewing.

Step 5 Click **Download Log** to download the log file you are viewing.

Related Topics

System Logs Menu, on page 523

CHAPTER 8

Configure Cisco Unified Operating System

Access Cisco Unified Communications Operating System Administration

Note Do not use the browser controls (for example, the Back button) while you are using Cisco Unified Communications Operating System Administration.

Procedure

Step 1 Log in to Emergency Responder.

Step 2 From the Navigation menu in the upper right corner of the Emergency Responder Administration page, choose **Cisco Unified OS Administration** and click **Go**.

The Cisco Unified Communications Operating System Administration Logon window appears.

Note You can also access Cisco Unified Communications Operating System Administration directly at **http://**"server-name"**/cmplatform**.

Step 3 Enter your Administrator username and password.

Note The Administrator username and password are established during installation or created by using the CLI.

Step 4 Click **Submit.**

The Cisco Unified Communications Operating System Administration window appears.

Recover Administrator and Security Passwords

If you lose the administrator password or security password, use the following procedure to reset these passwords.

To perform the password recovery process, you must be connected to the system through the system console, that is, you must have a keyboard and monitor connected to the server. You cannot recover a password when connected to the system through a secure shell session.

Caution The security password on all servers in the server group must match. Change the security password on all machines, or the servers will not communicate with one another.

Caution You must reset each server in a server group after you change its security password. Failure to reboot the servers causes system service problems and problems with the Emergency Responder Administration page on the subscriber server.

Note During this procedure, you must remove and then insert a valid CD or DVD in the disk drive to prove that you have physical access to the system.

Procedure

Step 1 Log in to the system with the following username and password:

- Username: **pwrecovery**
- Password: **pwreset**

The Welcome to platform password reset window displays.

Step 2 Press any key to continue.

Step 3 If you have a CD or DVD in the disk drive, remove it now.

Step 4 Press any key to continue.

The system tests to ensure that you have removed the CD or DVD from the disk drive.

Step 5 Insert a valid CD or DVD into the disk drive.

Note For this test, you must use a data CD, not a music CD.

The system tests to ensure that you have inserted the disk.

Step 6 After the system verifies that you have inserted the disk, you get prompted to enter one of the following options to continue:

- Enter **a** to reset the administrator password.
- Enter **s** to reset the security password.
- Enter **q** to quit.

Step 7 Enter a new password of the type that you chose.

Step 8 Reenter the new password.

The password must contain at least 6 characters. The system checks the new password for strength. If the password does not pass the strength check, you get prompted to enter a new password.

Step 9 After the system verifies the strength of the new password, the password gets reset, and you get prompted to press any key to exit the password reset utility.

View Cisco Unified OS Information

Using the CiscoUnifiedOS Administration web pages, you can view the status of the operating system, platform hardware, or the network. The following sections describe how to display this information.

View ServerGroup Information

Procedure

Step 1 From the main CiscoUnified Operating System Administration web page, select **Show** > **ServerGroup**. The ServerGroup page appears.

Step 2 For descriptions of the fields on the ServerGroup page, see Table 133: ServerGroup Page , on page 528.

View Hardware Status

Procedure

Step 1 From the main CiscoUnifiedOperating System Administration web page, select **Show** > **Hardware**. The Hardware Status page appears.

Step 2 For descriptions of the fields on the Hardware Status page, see Table 134: Hardware Status Page , on page 528.

View Network Status

The network status information that appears depends on whether Network Fault Tolerance is enabled. When Network Fault Tolerance is enabled, Ethernet port 1 automatically takes over network communications if Ethernet port 0 fails. If Network Fault Tolerance is enabled, network status information appears for the network ports Ethernet 0, Ethernet 1, and Bond 0. If Network Fault Tolerance is not enabled, status information appears only for Ethernet 0.

Procedure

Step 1 From the CiscoUnifiedOperating System Administration web page, select **Show** > **Network**.
The Network Settings page appears.

Step 2 See Table 135: Network Configuration Page , on page 529 for descriptions of the fields on the Network Settings page.

View Installed Software

Procedure

Step 1 From the CiscoUnifiedOperating System Administration web page, select **Show** > **Software**.

The Software Packages page appears.

Step 2 For a description of the fields on the Software Packages page, see Table 136: Software Packages Page , on page 530.

View System Status

Procedure

Step 1 From the CiscoUnifiedOperating System Administration web page, select **Show** > **System**.
The System Status page appears.

Step 2 See Table 137: System Status Page , on page 531 for descriptions of the fields on the System Status page.

View IP Preferences

Procedure

Step 1 From the CiscoUnifiedOperating System Administration web page, select **Show** > **IP Preference**.
The IP Preferences page appears.

Step 2 To find all records in the database, ensure the dialog box is empty; go to Step 3, on page 209.

To filter or search records:

- From the first drop-down list box, select a search parameter.
- From the second drop-down list box, select a search pattern.
- Specify the appropriate search text, if applicable.

Note To add additional search criteria, click the + button. When you add criteria, the system searches for a record that matches all criteria that you specify. To remove criteria, click the – button to remove the last added criterion or click **Clear Filter** to remove all added search criteria.

Step 3 Click **Find**.

All matching records display. You can change the number of items that display on each page by choosing a different value from the Rows per Page drop-down list box.

Display and Modify Cisco Unified OS Settings

Use the Settings options to display and modify IP settings, host settings, and Network Time Protocol (NTP) settings. The following sections describe how to display and modify CiscoUnifiedOS settings.

Set Up Ethernet Settings

The Ethernet Settings options allow you to view and change Dynamic Host Configuration Protocol (DHCP), port, and gateway information.

The Ethernet Configuration page allows you to enable or disable DHCP, to specify the Ethernet port IP address and subnet mask, and to specify the IP address for the network gateway.

Note All Ethernet settings apply only to Eth0. You cannot configure any settings for Eth1. The maximum transmission unit (MTU) on Eth0 defaults to 1500.

Procedure

Step 1 From the CiscoUnifiedOS Administration web page, select **Settings** > **IP** > **Ethernet**.
The Ethernet Configuration page appears.

Step 2 Modify the Ethernet settings by entering the new values in the appropriate fields. For a description of the fields on the Ethernet Configuration page, see Table 139: Ethernet Configuration Page , on page 533.

Note If you enable DHCP, then the Port Information and Gateway Information settings are disabled and cannot be changed.

Step 3 Click **Save** to preserve your changes.

Set Up NTP Servers

Ensure that external NTP server is stratum 9 or higher (1–9). To add, delete, or modify an external NTP server, follow these steps.

Note You can only configure the NTP server settings on the Publisher.

Procedure

Step 1 From the **CiscoUnifiedOS Administration** web page, select **Settings** > **NTP Servers**.

The **NTP Server List** page appears. For details about the **NTP Server List** page, see NTP Server List, on page 535.

Step 2 You can add, delete, or modify an NTP server:

- To delete an NTP server, check the check box in front of the appropriate server and click **Delete Selected**.
- To add an NTP server, click **Add**. The **NTP Server Configuration** page appears. Enter the hostname or IP address, and then click **Save**.
- To modify an NTP server, click the IP address. The **NTP Server Configuration** page appears. Modify the hostname or IP address and then click **Save**.

Note Any change you make to the NTP servers can take up to five minutes to complete. Whenever you make any change to the NTP servers, you must refresh the page to display the correct status.

Step 3 To refresh the **NTP Server Settings** page and display the correct status, choose **Settings** > **NTP Servers**.

Note After deleting, modifying, or adding NTP server, you must restart all both the Publisher and Subscriber for the changes to take affect.

Set Up SMTP Settings

The SMTP Settings window allows you to view or set the SMTP hostname and indicates whether the SMTP host is active.

Tip If you want the system to send you e-mail, you must configure an SMTP host.

Procedure

Step 1 From the CiscoUnifiedOS Administration web page, select **Settings** > **SMTP**.

The SMTP Settings page appears. For details about the SMTP Settings page, see SMTP Settings, on page 537.

Step 2 Enter the hostname or IP address of the SMTP host.

Step 3 Click **Save**.

Set Up Time Settings

Before you begin

Note Before you can manually configure the server time, you must delete any NTP servers that you have configured. See Set Up NTP Servers , on page 210 for information about deleting NTP servers.

Procedure

Step 1 From the **CiscoUnifiedOS Administration** web page, select **Settings** > **Time**. The **Time Settings** page appears. For details about the **Time Settings** page, see Time Settings, on page 537.

Step 2 Enter the date and time for the system.

Step 3 Click **Save**.

Manage Software Versions

You can use this option both when you are upgrading to a newer software version or when you must fall back to an earlier software version.

Caution This procedure causes the system to restart and become temporarily out of service.

Procedure

Step 1 From the CiscoUnifiedOS Administration web page, select **Settings** > **Version**.

The **Version Settings** page appears. For details about the Version Settings page, see Version Settings, on page 538.

Step 2 Click **Restart** to restart the version running on the active partition.

The system restarts on the current partition without switching versions.

Step 3 Click **Shutdown** to shut down the system.

The system halts all processes and shuts down.

Note The hardware does not power down automatically.

Caution If you press the power button on the server, the system immediately shuts down.

Step 4 Click **Switch Versions** to shut down the system that is running on the active disk partition and then automatically restart the system using the software version on the inactive partition.

The system restarts and the partition that is currently inactive becomes active.

Note The **Switch Version** button only appears if there is software installed on the inactive partition.

Note You can use this option when you are upgrading to a newer software version or when you must fall back to an earlier software version.

Note If the vRAM size on Release 15 is greater than 6GB and if you are planning to switch to any previous releases, you should reduce the vRAM size to lesser than 6GB as all the Pre-15 sources do not support vRAMs greater than 6GB.

Change IP Addresses for Emergency Responder Servers

You can change the IP address of either the Emergency Responder Publisher, Emergency Responder Subscriber, or both the Emergency Responder Publisher and Subscriber.

The following sections provide information on changing IP addresses on the Emergency Responder servers.

Change IP Address of Emergency Responder Publisher or Standalone Server

Before you begin

Note Update the IP address information about your DNS server before you begin changing the IP address on the server.

Procedure

Step 1 Change the IP address on the Emergency Responder Publisher by using one of the following options:

- In Cisco Unified Operating System Administration, enter the new IP address in **Settings** > **IP** > **Ethernet**.

- On the CLI, configure the new IP address with the **set network ip** command.

Step 2 Reboot the Emergency Responder Publisher or Standalone server and wait until it is fully operational. For a Standalone server, go to Step 7 once the server is operational.

Step 3 When the Emergency Responder Publisher is fully operational, login to Cisco Unified Operating System Administration on the Emergency Responder Subscriber.

Step 4 Choose **Settings** > **IP** > **Publisher**. Cisco Unified Operating System Administration displays the old IP address of the Publisher. Enter the new IP address of the Publisher in the Edit box and click **Save**.

Step 5 Reboot the Emergency Responder Subscriber immediately, so that the Emergency Responder Publisher maintains communication with the Emergency Responder Subscriber.

Step 6 Verify the replication using the **utils dbreplication status** CLI command. The value on each server should equal two.

Step 7 Verify that the CTI ports are registered on the Emergency Responder Publisher server. If the CTI ports are not registered, you must recreate the CTI ports by deleting the ports and adding them back in again.

Related Topics

Ethernet Configuration, on page 532

Create Required CTI Ports, on page 90

Change IP Address of Emergency Responder Subscriber

Before you begin

Update the IP address information about your DNS server before you begin changing the IP address on the server.

Procedure

Step 1 Change the IP address on the Emergency Responder Subscriber by using one of the following options:

- In Cisco Unified Operating System Administration, enter the new IP address in **Settings** > **IP** > **Ethernet**.
- On the CLI, configure the new IP address with the **set network ip** command.

Step 2 Reboot the Emergency Responder Subscriber.

Step 3 After the Emergency Responder Subscriber is fully operational, reboot the Emergency Responder Publisher.

Step 4 Verify that the replication using the **utils dbreplication status** CLI command. The local server will have a value of 2 and the remote server will have a value of 3 with the status as Local and Connected on Publisher and Subscriber.

Related Topics

Ethernet Configuration, on page 532

Change IP Address of Emergency Responder Publisher and Subscriber

If you are planning to change the IP address of both the Publisher and Subscriber, you must change the IP addresses on the servers sequentially, starting with the subscriber first.

⚠

Caution Do not begin to change the IP address of the publisher server until you have completed the task of changing the IP address on the subscriber.

For information about changing the IP address of the Emergency Responder Subscriber server, see Change IP Address of Emergency Responder Subscriber , on page 213.

For information about changing the IP address of the Emergency Responder Publisher server, see Change IP Address of Emergency Responder Publisher or Standalone Server , on page 212.

Security Management

The information in the following sections describes how to perform security and IPsec management tasks.

Set Internet Explorer Security Options

You need to ensure that your Internet Explorer security settings are configured correctly so that you can download certificates from the server.

Procedure

Step 1 Start Internet Explorer.

Step 2 Navigate to **Tools** > **Internet Options**.

Step 3 Click **Advanced**.

Step 4 Scroll down to the Security section on the **Advanced** tab.

Step 5 If necessary, clear the **Do not save encrypted pages to disk** check box.

Step 6 Click **OK**.

Certificate Management

The following sections describe the functions you can perform using the Certificate Management menu options.

Display Certificates

Procedure

Step 1 Select **Security** > **Certificate Management** from the **CiscoUnifiedOS Administration** web page.
The **Certificate List** page appears. For details about the Certificate List page, see Certificate Management, on page 539.

Step 2 Use the Find controls to filter the certificate list.

Step 3 Click the file name to view details of a certificate or trust store.

The **Certificate Configuration** page displays information about the certificate.

Step 4 Select **Back To Find/List** in the Related Links list to return to the **Certificate List** page then click **Go**.

Download Certificate or CTL to Your Local System

Procedure

Step 1 From the **CiscoUnifiedOS Administration** web page, select **Security > Certificate Management**.
The **Certificate List** page appears. Click the filename of the certificate or CTL.

Step 2 Use the **Find** controls to filter the certificate list.

Step 3 Click the filename of the certificate or CTL.
The **Certificate Configuration** page appears.

Step 4 Click **Download**.

Step 5 In the **File Download** dialog box, click **Save**.

Certificate Deletion or Regeneration

The following sections describe deleting and regenerating a certificate.

Delete Certificate

⚠ **Caution** Deleting a certificate can affect your system operations. Any existing CSR for the certificate that you choose from the Certificate list gets deleted from the system, and you must generate a new CSR. For more information, see Generate Certificate Signing Request, on page 218.

Procedure

Step 1 From the **CiscoUnifiedOS Administration** web page, select **Security > Certificate Management**.
The **Certificate List** page appears.

Step 2 Use the Find controls to filter the certificate list.

Step 3 Click the file name of the certificate or CTL.

The **Certificate Configuration** page appears.

Step 4 Click **Delete**.

Regenerate Certificate

Caution Regenerating a certificate can affect your system operations.

Procedure

Step 1 From the **CiscoUnifiedOS Administration** web page, select **Security > Certificate Management**.
The **Certificate List** page appears.

Step 2 Click **Generate New**.
The **Generate Certificate** dialog box opens.

Step 3 Choose a certificate name from the Certificate Name list. For a description of the certificate names that display, see the following table.

Table 15: Certificate Names and Descriptions

Name	Description
tomcat	This self-signed root certificate gets generated during installation for the HTTPS server.
ipsec	This self-signed root certificate gets generated during installation for IPsec connections with MGCP and H.323 gateways.

Step 4 Click **Generate New**.

Certificate or Certificate Trust List Uploads

Caution Uploading a new certificate or Certificate Trust List (CTL) file can affect your system operations. After you upload a new tomcat certificate or certificate trust list, you must restart the Cisco Tomcat service by entering the CLI command **utils service restart Cisco Tomcat**.

Note The system does not distribute trust certificates to other cluster servers automatically. If you must have the same certificate on more than one server, you must upload the certificate to each server individually.

The following sections describe how upload a CA root certificate, application certificate, or CTL file to the server.

Upload Certificate or CTL File

Procedure

Step 1 Select **Security > Certificate Management** from the CiscoUnifiedOS Administration web page.
The **Certificate List** page appears.

Step 2 Click **Upload Certificate**.
The Upload Certificate dialog box opens.

Step 3 Select the certificate name from the **Certificate Name** list.

Step 4 If you are uploading an application certificate that was issued by a third party CA, enter the name of the CA root certificate in the **Root Certificate** text box. If you are uploading a CA root certificate, leave this text box empty.

Step 5 Select the file to upload by doing one of the following steps:

- Enter the path to the file in the **Upload File** text box.
- Click the **Browse** button and navigate to the file, then click **Open**.

Step 6 Click **Upload File** to upload the file to the server.

Upload Trusted Certificate

Procedure

Step 1 From the **CiscoUnifiedOS Administration** web page, select **Security > Certificate Management**.
The **Certificate List** page appears.

Step 2 Click **Upload CTL**.
The **Upload Certificate Trust List** dialog box opens.

Step 3 Select the certificate name from the **Certificate Name** list.

Step 4 If you are uploading an application certificate that was issued by a third-party CA, enter the name of the CA root certificate in the **Root Certificate** text box. If you are uploading a CA root certificate, leave this text box empty.

Step 5 Select the file to upload by doing one of the following steps:

- In the **Upload File** text box, enter the path to the file.
- Click **Browse** and navigate to the file, then click **Open**.

Step 6 Click **Upload File** to upload the file to the server.

Use Third-Party CA Certificates

Cisco Unified OS supports certificates that a third-party Certificate Authority (CA) issues with PKCS # 10 Certificate Signing Request (CSR). The following procedure outlines this process, with references to additional documentation.

Procedure

Step 1 Generate a CSR on the server.

Step 2 Download the CSR to your PC.

Step 3 Use the CSR to obtain an application certificate from a CA.

Get information about obtaining application certificates from your CA.

Step 4 Obtain the CA root certificate.

Get information about obtaining a root certificate from your CA.

Step 5 Upload the CA root certificate to the server.

Step 6 Upload the application certificate to the server.

Step 7 Restart the services that are affected by the new certificate.

For all certificate types, restart the corresponding service (for example, restart the Tomcat service if you updated the Tomcat certificate). In addition, if you updated the certificate for CAPF or Unified CM, restart the TFTP service.

Related Topics

Generate Certificate Signing Request, on page 218

Download Certificate or CTL to Your Local System , on page 215

Third-Party CA Certificates , on page 219

Certificate or Certificate Trust List Uploads , on page 216

Use Control Center, on page 196

Generate Certificate Signing Request

Procedure

Step 1 From the **CiscoUnifiedOS Administration** web page, select **Security** > **Certificate Management**.
The Certificate List page appears.

Step 2 Click **Generate CSR**.
The **Generate Certificate Signing Request** dialog box opens.

Step 3 Select the certificate name from the **Certificate Name** list.

Step 4 Click **Generate CSR**.

Download Certificate Signing Request

Procedure

Step 1 From the **CiscoUnifiedOS Administration** web page, select **Security** > **Certificate Management**.
The **Certificate Lis**t page appears.

Step 2 Click **Download CSR**.
The **Download Certificate Signing Request** dialog box opens.

Step 3 Select the certificate name from the **Certificate Name** list.

Step 4 Click **Download CSR**.

Step 5 Click **Save** in the File Download dialog box.

Third-Party CA Certificates

To use an application certificate that a third-party CA issue, you must obtain from the CA both the signed application certificate and the CA root certificate. You can get information about obtaining these certificates from your CA. The process varies among CAs.

CAPF and Emergency Responder CSRs include extensions that you must include in your request for an application certificate from the CA. If your CA does not support the Extension Request method, you must enable the X.509 extensions that are listed on the final page of the CSR generation process.

Cisco Unified OS generates certificates in DER and PEM encoding formats and generates the CSRs in PEM encoding format. It accepts certificates in DER and DER encoding formats.

Set Up Certificate Expiration Monitor

The system can automatically send you an e-mail when a certificate is close to its expiration date.

Before you begin

To update information about the C**ertificate Expiration Monitor** page, the Cisco Certificate Expiry Monitor service must be running.

Procedure

Step 1 Select **Security** > **Certificate Monitor** from the **CiscoUnifiedOS Administration** web page.
The **Certificate Monitor** page appears.

Step 2 Enter the required configuration information. See Table 155: Certificate Monitor Page , on page 546 for a description of the Certificate Monitor Expiration fields.

Step 3 Click **Save** to save your changes,.

IPsec Management

The following topics describe how to manage IPsec.

Note IPsec does not get automatically set up between servers in the server group during installation.

Display or Change Existing IPsec Policy

Note Because any changes that you make to an IPsec policy during a system upgrade are lost, do not modify or create IPsec policies during an upgrade.

Caution IPsec, especially with encryption, affects the performance of you system.

Procedure

Step 1 Select **Security** > **IPsec Configuration** from the **CiscoUnifiedOS Administration** web page.

Caution Any changes that you make to the existing IPsec policies can impact your normal system operations.

The **IPsec Policy Configuration** page appears.

Step 2 Click the **Display Detail** link. The **Association Details** page appears. For an explanation of the fields in this page, see Table 157: IPSec Policy Configuration Page, on page 547.

Set Up IPsec Policy

Note Because any changes you make to an IPsec policy during a system upgrade are lost, do not modify or create IPsec policies during an upgrade.

Caution IPsec, especially with encryption, affects the performance of you system.

Procedure

Step 1 Select **Security** > **IPsec Configuration** from the **CiscoUnifiedOS Administration** web page.
The **IPsec Policy List** page appears.

Step 2 Click **Add New**.
The **IPsec Policy Configuration** page appears.

Step 3 Click **Next**.
The **Setup IPsec Policy and Association** page appears.

Step 4 Enter the appropriate information about the **IPsec Policy Configuration** page. For a description of the fields on this page, see Table 157: IPSec Policy Configuration Page, on page 547.

Step 5 Click **Save** to set up the new IPsec policy.

Manage Existing IPsec Policies

To display, enable or disable, or delete an existing IPsec policy, follow this procedure:

Note Because any changes that you make to an IPsec policy during a system upgrade are lost, do not modify or create IPsec policies during an upgrade.

Caution IPsec, especially with encryption, affects the performance of your system.

Caution Any changes that you make to the existing IPsec policies can impact your normal system operations.

Procedure

Step 1 Navigate to **Security > IPsec Configuration**.

Note To access the Security menu items, you must log in to Cisco Unified Communications Operating System Administration again by using your Administrator password.

The IPsec Policy List window displays.

Step 2 Follow these steps to display, enable, or disable a policy :

a) Click the policy name.
The **IPsec Policy Configuration** window displays.
b) To enable or disable the policy, check or uncheck the **Enable Policy** check box.
c) Click **Save**.
d) If you disable the policy, you must run the **utils ipsec restart** command for the disable changes to take effect.

Step 3 Follow these steps to delete one or more policies:

a) Select the check box next to the policies that you want to delete.

Select **Select All** to select all policies or **Clear All** to clear all the check boxes.

b) Click **Delete Selected**.

Software Upgrades

The information in the following sections describes how to perform software upgrades.

Software Upgrade Overview

The Software Upgrade pages enable you to upgrade Emergency Responder software from a DVD (local source) or from a network location (remote source) that the Emergency Responder server can access. The Emergency Responder Publisher must be upgraded first, followed by the Subscriber.

Note Direct Refresh Upgrades from Pre-12.5.x source to Release 15 is not supported. You should first upgrade your source to Release 12.5.x or 14 and SUs and then upgrade your source to Release 15.

Note Emergency Responder 15 does not support Install with Data Import.

Note If your Emergency Responder publisher node is on Release 15 and the subscribers nodes are in Release 12.5.x or 14 and SUs, the nodes in the cluster will not be authenticated. Only when the subscribers nodes are upgraded to Release 15, all the nodes will be in the authenticated state.

With Emergency Responder 10.0 and later, you cannot install upgrade software on your server while the system continues to operate. A Refresh Upgrade is required for all upgrades from Emergency Responder 10.0, 11.x, 12.0, or earlier to the most recent version of Emergency Responder. A Refresh Upgrade is a fresh install on the inactive partition, with embedded data migration. A Refresh Upgrade requires server downtime. This is less critical in a redundant system with both Emergency Responder Publisher and Subscriber.

Before you begin the upgrade, back up your system.

When you install the upgrade software, there will be a temporary server outage while the Emergency Responder software is installed. After you begin the upgrade, using either the command line or graphical user interface, the data will be migrated, and the system will automatically reboot, at which point the server outage begins. The duration of this outage depends on your configuration and amount of data. A notification email is sent at the start and end of Refresh Upgrade.

If an administrator makes changes during the upgrade process such as exporting data, then that data could be lost after the upgrade.

The previous software remains in the inactive partition until the next upgrade.

A manual switch back can revert to the old version. If the upgrade fails, the system automatically reverts to the previous version. Your configuration information migrates automatically to the upgraded version in the active partition.

If for any reason you decide to back out of the upgrade, you can restart the system to the inactive partition that contains the older version of the software using the switch-version option.

However, any configuration changes that you made since you upgraded the software will be lost, because the database on the inactive partition does not get updated. If you make changes to the database after an upgrade, you must repeat those changes after switching back to the inactive partition.

When you upgrade Emergency Responder from any older release versions to Release 14SU2 and if the Unified CM is running on an older version lesser than Release 14SU2, use the following steps to prevent the CTI Route points from getting unregistered:

1. From the Cisco Unified CM Administration, navigate to **User Management > User Setting > Application User CAPF Profile**, and choose the **application user for the CAPF operation**.
2. Select the **Instance Id** registered for CAPF.
3. Select **Install/Upgrade** option from the **Certificate Operation** drop-down list. And, provide the **Authentication String** as configured under **Phone Tracking > Cisco Unified Communications Manager > Secure Authentication String for Publisher** in the Cisco Emergency Responder Administration Web Interface.
4. Ensure that the **Operation Completes By field** shouldn't have a past due date and save the changes.
5. Verify that all the route points (911/912/913) get registered.

Supported Upgrades

For supported upgrades, see the Cisco Emergency Responder Release Notes.

Upgrade Cisco Unified Operating System

Note You must complete the items mentioned in the procedure before you perform any configuration tasks. You also must not make any configuration changes to Cisco Emergency Responder during an upgrade. Configuration changes include any changes that you make in Emergency Responder Administration or Serviceability pages. Any configuration changes that you make during an upgrade could be lost after the upgrade completes, and some configuration changes can cause the upgrade to fail.

Note Do not perform configuration tasks until the upgrade completes on both Emergency Responder publisher and subscriber until you have:

- switched the servers over to the upgraded partition.
- verified that database replication is functioning.

Procedure

Step 1 Stop all configuration tasks, including all configuration tasks in the various Emergency Responder-related GUIs or the CLI.

Step 2 Apply the required Upgrade Readiness COP Files (pre-upgrade). For example, `ciscocm.cer_preUpgradeCheck-X.k4.cop.sha512.`

Step 3 Upgrade the Emergency Responder publisher.

Note The upgraded system *will not* automatically reboot to the upgraded partition. Instead you are presented with two options: **Reboot to new partition** and **Do not reboot to new partition**. The latter is the default option and is considered the best practice. If you choose to reboot to a new partition, then steps 5 and 6 are not required.

Step 4 Upgrade the Emergency Responder subscriber.

Step 5 Switch over the Emergency Responder publisher to the upgraded partition.

Step 6 Switch over the Emergency Responder subscriber to the upgraded partition.

Step 7 Ensure that database replication is functioning between the Emergency Responder publisher and the Emergency Responder subscriber.

Step 8 Apply the required Upgrade Readiness COP Files (post-upgrade). For example, `ciscocm.cer_postUpgradeCheck-X.k4.cop.sha512.`

Step 9 When all other upgrade tasks are complete, you can perform any needed configuration tasks as required.

Upgrade File

Before you begin the upgrade process, you must obtain the appropriate upgrade file by placing an order for Cisco Emergency Responder software. You must also download the appropriate cop file as needed from https://www.cisco.com/.

Note Do not rename the patch file before you install it because the system will not recognize it as a valid file.

Note Do not unzip or untar the upgrade file. If you do, the system cannot read the upgrade files.

You can access the upgrade file during the installation process from either a local DVD or from a remote FTP or SFTP server. Be aware that directory names and filenames that you enter to access the upgrade file are case-sensitive.

Install or Upgrade Software From DVD

You can install software from a DVD that is in the local disk drive and then start the upgrade process.

Note Be sure to back up your system data before starting the software upgrade process. For more information, see Configure Cisco Emergency Responder Disaster Recovery System, on page 237 chapter.

Procedure

Step 1 Order the appropriate upgrade file. You may choose to receive a physical DVD or download an disk image file through electronic software delivery.

Note If you download a disk image file, create the DVD by using the .iso file to burn a DVD. The .iso file contains the complete image of the original DVD disk. You *must not* copy the .iso file to the DVD. You must use your burner software to extract the files that are in the image and burn them on the DVD. This creates an exact replica of the DVD disk.

Step 2 Insert the DVD into the disk drive on the local server that is to be upgraded.

Step 3 From the CiscoUnifiedOS Administration web page, select **Software Upgrades** > **Install/Upgrade**. The Software Installation/Upgrade page appears.

Step 4 Choose **DVD/CD** from the Source list.

Step 5 Enter the path to the patch file on the DVD in the Directory field.

If the file is in the root directory, enter a slash (/).

Step 6 Click **Next** to continue the upgrade process.

Step 7 Choose the upgrade version that you want to install and click **Next**.

Step 8 On the next page, monitor the progress of the download, which includes the filename and the number of megabytes that are being transferred.

Step 9 Choose **Switch to new version after upgrade** to install the upgrade and automatically reboot to the upgraded partition. The system restarts on the upgraded software.

Install Software From Network Drive or Remote Server

Note Do not use your browser controls, such as Refresh/Reload, while accessing Cisco Unified Operating System Administration. Instead, you should use use the navigation controls on the interface.

Before you begin

Be sure to back up your system data before starting the software upgrade process. For more information, see Configure Cisco Emergency Responder Disaster Recovery System, on page 237 chapter.

Procedure

Step 1 From the **CiscoUnifiedOS Administration** web page, select **Software Upgrades** > **Install/Upgrade**. The **Software Installation/Upgrade** page appears.

Step 2 Choose **Remote Filesystem** from the **Source** list.

Step 3 Enter the path to the patch file on the remote system in the **Directory** field.

If the upgrade file is on a Linux or UNIX server, you must enter a forward slash at the beginning of the directory path you want to specify. For example, if the upgrade file is in the patches directory, you must enter **`/patches`**.

If the upgrade file is on a Windows server, remember that you are connecting to an FTP or SFTP server so use the appropriate syntax, including:

- Begin the path with a forward slash (/) and use forward slashes throughout the path.
- The path must start from the FTP or SFTP root directory on the server, so you cannot enter a Windows absolute path, which starts with a drive letter (for example, C:).

Step 4 Enter the server name in the **Server** field.

Step 5 Enter your user name in the **User Name** field.

Step 6 Enter your password in the **User Password** field.

Step 7 Select the transfer protocol from the **Transfer Protocol** field.

Step 8 Click **Next** to continue the upgrade process.

Step 9 Choose the upgrade version that you want to install and click **Next**.

Step 10 On the next page, monitor the progress of the download, which includes the filename and the number of megabytes that are getting transferred.

Step 11 When the download completes, verify the checksum value against the checksum for the file you that downloaded that is shown on Cisco.com.

Caution The two checksum values must match to ensure the authenticity and integrity of the upgrade file. If the checksum values do not match, download a fresh version of the file from Cisco.com and try the upgrade again.

Note If you lose your connection with the server or close your browser during the upgrade process, you may see following message when you try to access the **Software Upgrades** menu again:

```
Warning: Another session is installing software, click Assume
      Control to take over the installation.
```

Click **Assume Control** if you are sure you want to take over the session.

If Assume Control is not displayed, you can also monitor the upgrade with the Real Time Monitoring Tool.

Step 12 Choose **Reboot to upgraded partition** to install the upgrade and automatically reboot to the upgraded partition. The system restarts and runs the upgraded software.

Step 13 To install the upgrade and then manually reboot to the upgraded partition at a later time, do the following steps:

a) Choose **Do not reboot after upgrade**.

b) Click **Next**.
The **Upgrade Status** window displays the **Upgrade log**.

c) Click **Finish** when the installation completes, .

d) Choose **Settings > Version** to restart the system and activate the upgrade, then click **Switch Version**.
The system restarts running the upgraded software.

Troubleshoot Stalled Upgrades

During a software upgrade, the software installation may stall. Check the upgrade log for new messages. If the upgrade log does not have any new log messages, then the installation may have stalled.

You must cancel the upgrade, disable I/O throttling, and restart the upgrade procedure. When you successfully complete the upgrade, you do not need to enable I/O throttling again.

- To disable I/O throttling, enter the CLI command **utils iothrottle disable**.
- To display the status of I/O throttling, enter the CLI command **utils iothrottle status**.

- To enable I/O throttling, enter the CLI command **utils iothrottle enable**. By default, I/O throttle remains enabled.

If the system does not respond to the cancellation, you must reboot the server, disable I/O throttling, and restart the upgrade process procedure.

If the software upgrade shows stalled at /partb rpm deletion in the logs, then stop the rpm -e process using the root to proceed further.

```
[root@<Hostname>]# ps -eaf | grep rpm

root      4925  4913  0 18:21 ?        00:00:00 rpm -e --nodeps master

root      7264     1  0 14:02 ?        00:00:00 /usr/local/os-services/sbin/arpmond

root     24359 24188  0 18:37 pts/3    00:00:00 grep
[root@<Hostname>]# kill -9 4925

[root@<Hostname>]# ps -eaf | grep rpm

root      7264     1  0 14:02 ?        00:00:00 /usr/local/os-services/sbin/arpmond

root     24652 24188  0 18:37 pts/3    00:00:00 grep rpm
```

What to do next

If the software upgrade continues to stall, then contact Cisco TAC for assistance.

Revert to Previous Version

After upgrading, you can revert to the software version that was running before the upgrade, by restarting your system and switching to the software version on the inactive partition.

Procedure

Step 1 Revert the publisher node.

For more information, see Revert Publisher Server to Previous Version , on page 227.

Step 2 Revert all backup subscriber nodes.

For more information, see Revert Subscriber Server to Previous Version , on page 228.

Revert Publisher Server to Previous Version

Procedure

Step 1 Open Cisco Unified Communications Operating System Administration directly by entering the following URL:

https://"server-name"/**cmplatform**

Server-name is the host name or IP address of the Emergency Responder server.

Step 2 Enter your Administrator username and password.

Step 3 Choose **Settings>Version**.
The Version Settings window displays.

Step 4 Click **Switch Versions**.

After you verify that you want to restart the system, the system restarts, which might take up to 15 minutes.

Step 5 Verify that the version switch was successful:

a) Log into Open Cisco Unified Communications Operating System Administration again.
b) Choose **Settings>Version**.
The **Version Settings** window displays.
c) Verify that the correct product version is now running on the active partition.
d) Verify that all activated services are running.
e) Log into Emergency Responder by entering the following URL and entering your user name and password:

https://"server-name"**/ccmadmin**

f) Verify that you can log in and that your configuration data exists.

Revert Subscriber Server to Previous Version

Procedure

Step 1 Open Cisco Unified Communications Operating System Administration directly by entering the following URL:

https://"server-name"/**cmplatform**

"server-name" is the host name or IP address of the Emergency Responder server.

Step 2 Enter your Administrator user name and password.

Step 3 Choose **Settings>Version**.
The Version Settings window displays.

Step 4 Click **Switch Versions**.

After you verify that you want to restart the system, the system restarts, which might take up to 15 minutes.

Step 5 Verify that the version switch was successful:

a) Log into Open Cisco Unified Communications Operating System Administration again.
b) Choose **Settings>Version**.
The Version Settings window displays.
c) Verify that the correct product version is now running on the active partition.
d) Verify that all activated services are running.

Upload Customized Logon Message

You can upload a text file that contains a customized logon message that appears in Cisco Unified Communications Operating System Administration, Unified CM Administration, and the CLI.

Procedure

Step 1 From the Cisco Unified Communications Operating System Administration window, navigate to **Software Upgrades** > **Customized Logon Message**.

The Customized Logon Message window displays.

Step 2 Click **Browse** to choose the text file that you want to upload.

Step 3 Click **Upload File**.

Note You cannot upload a file that is larger than 10 KB.

The system displays the customized logon message.

Step 4 Click **Delete** to revert to the default logon message.

Your customized logon message is deleted, and the system displays the default logon message.

Cisco Unified OS Services

The following sections describe how to use CiscoUnifiedOS services.

Ping Another System

The Ping Configuration page enables you to send ping requests to test if other systems are reachable over the network.

Procedure

Step 1 From the **CiscoUnifiedOS Administration** web page, select **Services** > **Ping**.

The **Ping Configuration** page appears. For details about the **Ping Configuration** page, see Ping Configuration, on page 558.

Step 2 Enter the IP address or network name for the system that you want to ping.

Step 3 Enter the ping interval in seconds.

Step 4 Enter the packet size.

Step 5 Enter the ping count, which is the number of times that you want to ping the system.

Note When you specify multiple pings, the **ping** command does not display the ping date and time in real time. The **ping** command displays the date and time once the ping count is completed.

Step 6 Choose if you want to validate IPsec or not.

Step 7 Click **Ping**.

The **Ping Results** text box displays the ping statistics.

Set Up Remote Support

From the **Remote Support** page, you can set up a remote account that Cisco support personnel can use to access the Emergency Responder system for a specified period of time.

1. The customer sets up a remote support account. This account includes a configurable time limit on how long Cisco personnel can access it.
2. When the remote support account is set up, a pass phrase gets generated.
3. The customer calls Cisco support and provides the remote support account name and pass phrase.
4. Cisco support enters the pass phrase into a decoder program that generates a password from the pass phrase.
5. Cisco support logs into the remote support account on the customer system by using the decoded password.
6. When the account time limit expires, Cisco support can no longer access the remote support account.

To set up remote support, follow these steps:

Procedure

Step 1 From the **CiscoUnifiedOS Administration** web page, select **Services > Remote Support**.
The **Remote Access Configuration** page appears.

Step 2 If no remote support account is configured, click **Add**.

Step 3 Enter an account name for the remote account and the account life in days.

Note Ensure the account name at least six-characters long and all lowercase, alphabetic characters.

Step 4 Click **Save**.
The **Remote Access Configuration** page redisplays. For descriptions of fields on the **Remote Access Configuration** page, see Table 165: Remote Access Configuration Page , on page 560.

Step 5 To access the system by using the generated pass phrase, contact your Cisco TAC.

Branding Customizations Overview

The Branding feature lets you upload customized branding for Cisco Emergency Responder. Branding gets applied to the Cisco ER Administration login and configuration windows. Among the items that you can modify include:

- Company logos

- Background colors
- Border colors
- Font colors

Once **Branding** is enabled, it is applicable only on that particular Cisco Emergency Responder node. Follow the same process to enable branding on each of the other Cisco Emergency Responder nodes.

Branding Prerequisites

You must create a branding zip file with the prescribed folder structure and files. For details, see Branding File Requirements, on page 232.

Branding Task Flow

Complete these tasks to apply branding in Cisco Emergency Responder.

Procedure

	Command or Action	Purpose
Step 1	Configure your branding settings using one of these procedures: • Enable Branding, on page 231 • Disable Branding, on page 232	Apply branding across the Cisco Emergency Responder cluster.

Enable Branding

Use this procedure to upload branding images for Cisco Emergency Responder. Branding updates appear even if the system is enabled for SAML Single Sign-On.

Note To enable branding, you must use the master administrator account with privilege level 4 access. This is the main administrator account that is created during installation.

Before you begin

Prepare your branding images folder `branding.zip` according to the requirements in Branding File Requirements, on page 232 and save it in a location that Cisco Emergency Responder can access.

Procedure

Step 1 Log in to Cisco Unified OS Administration, choose **Software Upgrades** > **Branding**.

Step 2 **Browse** to your remote server and select the `Branding.zip` file.

Step 3 Click **Upload File**.

Step 4 Click **Enable Branding** to enable the branding page.

Refresh the page for the changes to take effect.

Note You can also enable branding by running the **utils Branding enable** CLI command.

Related Topics

Branding, on page 558

Disable Branding

Use this procedure to disable branding in your Cisco Emergency Responder cluster.

Note To disable branding, you must use the master administrator account with privilege level 4 access. This is the main administrator account that is created during installation.

Procedure

Step 1 Log in to Cisco Unified OS Administration, choose **Software Upgrades** > **Branding**.

Step 2 Click **Disable Branding** to disable the branding page.

Note You can also disable branding by running the **utils Branding disable** CLI command.

Step 3 Refresh your browser.

Step 4 Repeat this procedure on all Cisco Emergency Responder cluster nodes.

Branding File Requirements

Before you apply customized branding to your system, create your `Branding.zip` file according to the prescribed specifications. On a remote server, create a `CER` folder and fill the folder with the specified contents. Once you have added all the image files and subfolders, zip the entire folder and save the file as `Branding.zip`.

Your branding folder must contain the following subfolders and image files:

```
Branding (folder)
   ccmadmin (folder)
      BrandingProperties.properties (properties file)
      brandingHeader.gif (652*1 pixel image)
      ciscoLogo12pxMargin.gif (44*44 pixel image)
```

User Interface Branding Options

The following images display the customization options for the Cisco ER Administration user interface:

Figure 22: Branding Options for Cisco ER Administration Login Screen

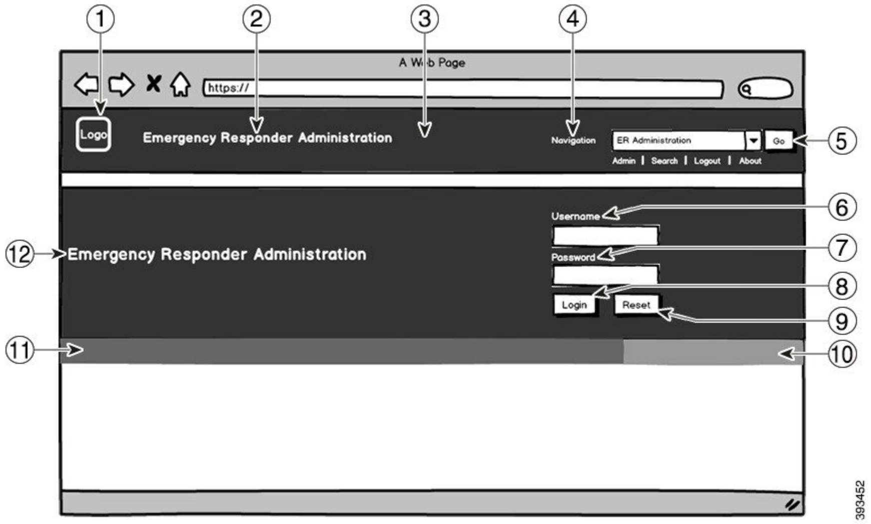
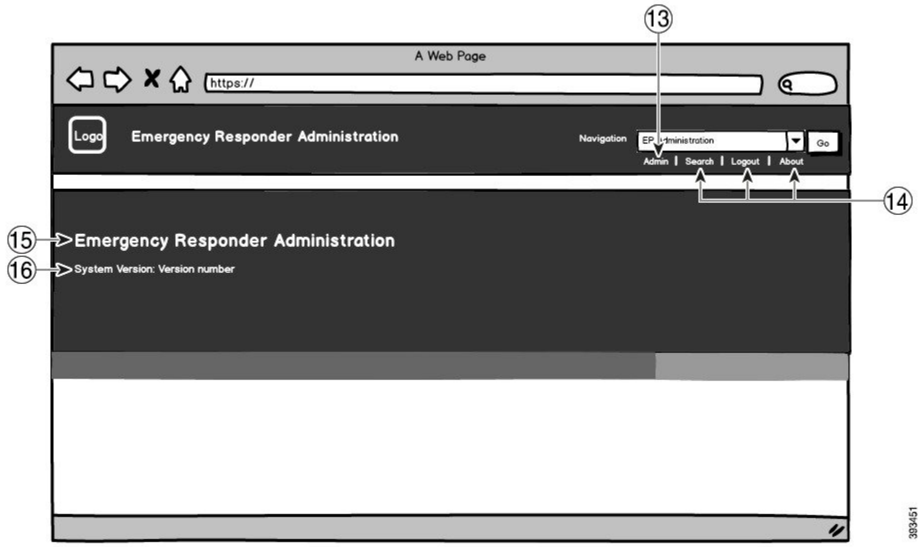

1
2
3
4
A Web Page
https://
Logo
Emergency Responder Administration
Navigation
ER Administration
Go
5
Admin | Search | Logout | About
Username
6
12
Emergency Responder Administration
Password
7
8
Login
Reset
9
11
10
393452

Figure 23: Branding Options for Cisco ER Administration Logged In Screen


13
A Web Page
https://
Logo
Emergency Responder Administration
Navigation
ER Administration
Go
Admin | Search | Logout | About
14
15
Emergency Responder Administration
16
System Version: Version number
393451

The following table describes the callout options.

Table 16: User Interface Branding Options

Item	Description	Image or Property Details
Login Screen		

Item	Description	Image or Property Details
1	Company Logo	To add your logo to Cisco Emergency Responder, save your company logo as a 44x44 pixel image with the following filename: `ciscoLogo12pxMargin.gif` (44*44 pixels)
2	Cisco ER Administration header font color	header.heading.color
3	Header Background	Save your header background as a single image: • brandingHeader.gif (2048*1 pixel)
4	Navigation text	header.navigation.color
5	Go button	header.go.font.color header.go.background.color header.go.border.color
6	Username text	splash.username.color
7	Password text	splash.password.color
8	Login button	splash.login.text.color splash.login.back.ground.color
9	Reset button	splash.reset.text.color splash.reset.back.ground.color
10	Bottom background color– right	splash.hex.code.3
11	Bottom background color– left	splash.hex.code.2
12	Banner	splash.hex.code.1
Logged In Screen		
13	User text (for example, 'admin')	header.admin.color
14	Search, About and Login text	header.hover.link.color
15	Emergency Responder Administration text heading	splash.header.color
16	System Version	splash.version.color

Branding Properties Editing Example

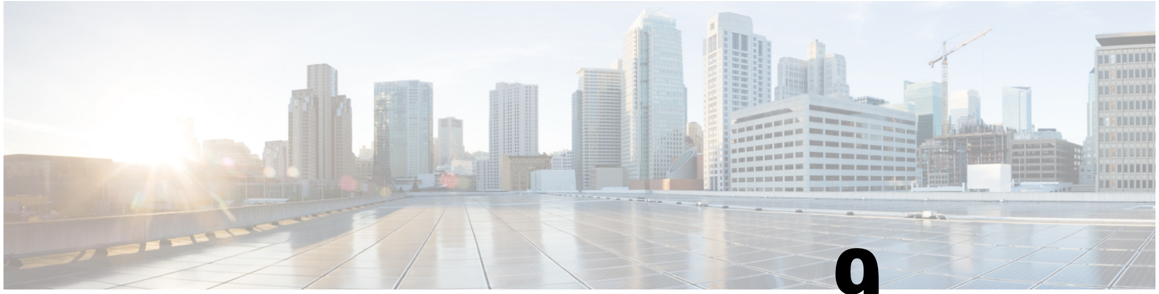
Branding properties can be edited by adding the hex code in the properties file (`BrandingProperties.properties`). The properties file uses HTML-based hex code. For example, if you want to change the color of the Cisco ER Administration header font color (callout item #2) to red, add the following code to your properties file:

```
heading.heading.color="#FF0000"
```

In this code, `heading.heading.color` is the branding property that you want to edit, and `"#FF0000"` is the new setting (red).

Related Topics

Branding, on page 558



CHAPTER 9

Configure Cisco Emergency Responder Disaster Recovery System

Disaster Recovery System Overview

The Disaster Recovery System (DRS), which can be invoked from the main Cisco Emergency Responder web interface, provides full data backup and restore capabilities for all servers in an Emergency Responder server group. The Disaster Recovery System allows you to perform a regularly scheduled automatic or user-invoked data backup. DRS supports multiple backup schedules.

The Cisco Disaster Recovery System performs a server group-level backup, which means that it collects backups for all servers in an Emergency Responder server group to a central location and archives the backup data to physical storage device.

Cisco Emergency Responder provides DRS Email Alerts to System Administrators with status and description of any successes or failures.

DRS restores its own settings (backup device settings and schedule settings) as part of the platform backup/restore. DRS backs up and restores drfDevice.xml and drfSchedule.xml files. When the server is restored with these files, you do not need to reconfigure DRS backup device and schedule.

When performing a system data restoration, you can choose which servers in the server group that you want to restore.

The Disaster Recovery System includes the following capabilities:

- A user interface for performing backup and restore tasks
- A distributed system architecture for performing backup and restore functions
- Scheduled backups
- Archive backups to a physical tape drive or remote SFTP server

Note The tape device must be attached to the Publisher.

The Disaster Recovery System contains two key functions, Master Agent (MA) and Local Agent (LA). The Master Agent coordinates backup and restore activity with all the Local Agents.

The system automatically activates both the Master Agent and the Local Agent on all servers in the server group.

Note The Disaster Recovery System does not migrate data from Windows to Linux or from Linux to Linux. A restore must run on the same product version as the backup. For information about data migration from a Windows-based platform to a Linux-based platform, see the Data Migration Assistant User Guide before performing the following the steps.

Note From Release 14SU2 onwards,

- The tomcat and tomcat-ecdsa certificates should be exchanged between the publisher and subscriber nodes before taking the DRS backup.
- After DRS backup/restore, if the subscriber-administrative interface is loading up as publisher, then ensure that the tomcat and tomcat-ecdsa certificates is exchanged between the publisher and subscriber nodes.

Backup and Restore Procedures

The following sections provide a quick reference for the backup and restore procedures.

Note Smart License Manager is not backed-up or restored as part of DRS backup/restore.

After successfully restoring the Cisco Emergency Responder server components, Cisco Emergency Responder will be in the Unregistered State. Then, register Cisco Emergency Responder with Cisco Smart Software Manager or Cisco Smart Software Manager satellite.

If the product is already registered before taking the backup, then re-register the product for updating the license information.

If Product is already Authorized for Export Restricted License before taking backup, and product instance is present in Cisco Smart Software Manager or Cisco Smart Software Manager satellite, contact Cisco to remove the product from CSSM and Cisco Smart Software Manager satellite and then register from the product while using Satellite deployment. For direct deployment, re-register the product and request for the export restricted license.

For more information on how to register the product with Cisco Smart Software Manager or Cisco Smart Software Manager satellite, see Cisco Smart Software Licensing , on page 10.

Perform Backup Procedure

The following procedure provides a quick, high-level reference to the major steps, in chronological order, that you must perform to do a backup procedure using the Disaster Recovery System.

Procedure

Step 1 Create backup devices on which to back up data.

For more information, see Add Backup Devices , on page 242.

Step 2 Create and edit backup schedules to back up data on a schedule.

Note Either a manual or a scheduled backup backs up the server group.

For more information, see Create and Edit Backup Schedules , on page 243.

Step 3 Enable and disable backup schedules to back up data.

For more information, see Manage Backup Schedules , on page 244.

Step 4 (Optional) Run a manual backup.

For more information, see Start Manual Backup , on page 245.

Step 5 Check the status of the backup.

While a backup is running, you can check the status of the current backup job. For more information, see Check Backup Status , on page 245.

Perform Restore Procedure

The following procedure provides a quick, high-level reference to the major steps, in chronological order, that you must follow to perform a restore procedure using the Disaster Recovery System.

Procedure

Step 1 Choose storage location.

You must first choose the storage location from which you want to restore a backup file.

Step 2 Choose the backup file.

From a list of available files, choose the backup file that you want to restore.

Step 3 Choose features.

From the list of available features, choose the features that you want to restore.

Step 4 Choose server.

If the feature was backed up from multiple servers, you must choose the servers that you want to restore.

Step 5 Check the status of the restore.

While the restore process is running, you can check the status of the current restore job.

Related Topics

Restore Backup File , on page 245
View Restore Status, on page 249

Supported Features and Components

For your Emergency Responder release, you can back up and restore Emergency Responder.

When you choose a feature for backup, the system backs up all of its subcomponents automatically.

System Requirements

Make sure that the current version of Emergency Responder is running on all servers in the server group.

To back up data to a remote device on the network, you must have an SFTP server that is configured. For internal testing, Cisco uses the SFTP Server on Cisco Prime Collaboration Deployment (PCD) which is provided by Cisco, and which is supported by Cisco TAC. Refer to the following table for a summary of the SFTP server options:

Table 17: SFTP Server Information

SFTP Server	Information
SFTP Server on Cisco Prime Collaboration Deployment	This server is the only SFTP server that is provided and tested by Cisco, and fully supported by Cisco TAC. Version compatibility depends on your version of Emergency Responder and Cisco Prime Collaboration Deployment. See the Cisco Prime Collaboration Deployment Administration Guide before you upgrade its version (SFTP) or Emergency Responder to ensure that the versions are compatible.
SFTP Server from a Technology Partner	These servers are third party provided and third party tested. Version compatibility depends on the third party test. See the Technology Partner page if you upgrade their SFTP product and/or upgrade Emergency Responder for which versions are compatible.
SFTP Server from another Third Party	These servers are third party provided and are not officially supported by Cisco TAC. Version compatibility is on a best effort basis to establish compatible SFTP versions and Emergency Responder versions. **Note** These products have not been tested by Cisco and we cannot guarantee functionality. Cisco TAC does not support these products. For a fully tested and supported SFTP solution, use Cisco Prime Collaboration Deployment or a Technology Partner.

Note While a backup or restore is running you cannot perform any OS Administration tasks because Disaster Recovery System blocks all OS Administration requests by locking the platform API. However, a backup or restore does not block most CLI commands because only the CLI-based upgrade commands use the Platform API locking package.

Access Disaster Recovery System

To access the Disaster Recovery System, select **Disaster Recover System** from the pull-down **Navigation** menu on the main Emergency Responder web interface. Log in to the Disaster Recovery System by using the same Administrator username and password that you use for the CiscoUnifiedOS Administration web interface.

Note You set the Administrator username and password during Emergency Responder installation, and you can change the Administrator password or set up a new Administrator account by using the CLI.

Master Agent Duties and Activation

The system automatically activates the Master Agent on all servers in the server group, but only the Master Agent running on the publisher server is fully active.

The Master Agent (MA) performs the following duties:

- The MA stores systemwide component registration information.
- The MA maintains a complete set of scheduled tasks in the Emergency Responder database. When it receives updates from the user interface, the MA sends executable tasks to the applicable Local Agents, as scheduled. (Local Agents execute immediate-backup tasks without delay.)
- You access the MA through the Disaster Recovery System user interface to perform activities such as scheduling backups, adding a new backup task for a specific server or a defined server group, updating or reviewing an existing entry, displaying status of executed tasks, and performing system restoration.
- The MA stores backup sets on a locally attached tape drive or a remote network location.

Local Agents

Each server in an Emergency Responder server group, including the server that contains the Master Agent, must have its own Local Agent to perform backup and restore functions for its server.

Note By default, a Local Agent automatically gets activated on each server in the server group.

The Local Agent runs backup and restore scripts on each server in the server group.

Add Backup Devices

Before using the Disaster Recover System, you must configure the locations where you want the backup files to be stored. You can configure up to 10 backup devices.

Procedure

Step 1 Select **Backup** > **Backup Device** from the main **Disaster Recovery System** web page.
The **Backup Device List** page appears.

Step 2 Click **Add New** to configure a new backup device. To edit a backup device, select it in the **Backup Device** list and click **Edit Selected**.
The **Backup Device** window appears.

Step 3 In the **Backup device name** field, enter the backup device name.

Note The backup device name may contain only alphanumeric characters, spaces ( ), dashes (-), and underscores (_). No other characters are allowed.

Step 4 Choose one of the following backup devices and enter the appropriate field values in the Select Destination area:

- **Tape Device**—Stores the backup file on a locally attached tape drive. Choose the appropriate tape device from the list.

  Note You cannot span tapes or store more than one backup per tape.

- **Network Directory**—Stores the backup file on a networked drive that is accessed through an SFTP connection. Enter the following required information:
  - **Server name:** Name or IP address of the network server.
  - **Path name:** Path name for the directory where you want to store the backup file.
  - **User name:** Valid username for an account on the remote system.
  - **Password:** Valid password for the account on the remote system.
  - **Number of backups to store on Network Directory:** The number of backups to store on this network directory.

Note You must have access to an SFTP server to configure a network storage location. The SFTP path must exist before the backup. The account that is used to access the SFTP server must have write permission for the selected path.

Step 5 Click **Save** to update these settings, .

Note For network directory backups, after you click the Save button, the DRS Master Agent validates the selected SFTP server. If the user name, password, server name, or directory path is invalid, the save fails.

Step 6 To delete a backup device, select it in the Backup Device list and **Delete Selected**.

Note You cannot delete a backup device that is configured as the backup device in a backup schedule.

Create and Edit Backup Schedules

You can create up to 10 backup schedules. Each backup schedule has its own set of properties, including a schedule for automatic backups, the set of features to back up, and a storage location.

Procedure

Step 1 Select **Backup** > **Scheduler** from the main Disaster Recovery System web page.

The Schedule List window appears.

Step 2 Do one of the following steps to add a new schedule or edit an existing schedule:

- Click **Add New** to create a new schedule.
- Click a name in the **Schedule List** column to configure an existing schedule.

The scheduler window appears.

Step 3 Enter a schedule name in the **Schedule Name** field.

Note You cannot change the name of the default schedule.

Step 4 Select the backup device in the **Select Backup Device** area.

Step 5 Select the features to back up in the **Select Feature**s area. You must choose at least one feature.

Step 6 Choose the date and time when you want the backup to begin in the **Start Backup at** area.

Step 7 Choose the frequency at which you want the backup to occur in the **Frequency** area: Once, Daily, Weekly, or Monthly. If you choose Weekly, you can also choose the days of the week when the backup occurs.

Tip To set the backup frequency to Weekly, occurring Tuesday through Saturday, click **Set Default**.

Step 8 Click **Save** to update these settings.

Step 9 Click **Enable Schedule** to enable the schedule.

The next backup occurs automatically at the time that you set.

Note Ensure that all servers in the server group are running the same version of Emergency Responder and are reachable through the network. Servers that are not running at the time of the scheduled backup are not backed up.

Step 10 Click **Disable Schedule** to disable the schedule.

Manage Backup Schedules

Procedure

Step 1 Select **Backup** > **Scheduler** from the main **Disaster Recovery System** web page.
The **Schedule List** window appears.

Step 2 Select the check boxes next to the schedules that you want to modify:

- Click **Select All** to select all schedules.
- Click **Clear All** To uncheck all check boxes.

Step 3 Click **Enable Selected Schedules** to enable the selected schedules.

Step 4 Click **Disable Selected Schedules** to disable the selected schedules.

Step 5 Click **Delete Selected** to delete the selected schedules.

Start Manual Backup

Procedure

Step 1 Select **Backup** > **Manual Backup** from the main **Disaster Recovery System** web page.
The **Manual Backup** page appears.

Step 2 Select a backup device in the **Select Backup Device** area.

Step 3 Select the features to back up in the **Select Features** area.

Step 4 Click **Start Backup** to start the manual backup.

Check Backup Status

You can check the status of the current backup job and cancel the current backup job. To view the backup history, see Backup and Restore History , on page 249.

Procedure

Step 1 Select **Backup** > **Current Status** from the main **Disaster Recovery System** web page.
The **Backup Status** page appears.

Step 2 Click the log filename link to view the backup log file.

Step 3 Click **Cancel Backup** to cancel the current backup.
The backup is cancelled after the current component has completed its backup operation.

Restore Backup File

Disaster Recovery System adheres to strict version checking and allows restore only for matching versions of Emergency Responder.

The Restore Wizard leads you through the steps that are required to restore a backup.

Tip To restore all servers in a server group, see Restore Entire Server Group , on page 246.

Caution Before you restore Emergency Responder, ensure that the Emergency Responder version that is installed on the server matches the version of the backup file that you want to restore. The Disaster Recovery System supports only matching versions of Emergency Responder for restore.

The product version needs to match, end-to-end, for the Disaster Recovery System to run a successful Emergency Responder database restore.

Procedure

Step 1 Select **Restore** > **Restore Wizard** from the main **Disaster Recovery System** web page.
The first page of the **Restore Wizard (Step1 Restore—Choose Backup Device)** appears.

Step 2 Choose the backup device to restore in the **Select Backup Device** area.

Step 3 Click **Next**.
The Step 2 Restore—Choose the Backup Tar File page appears.

Step 4 Choose the backup file that you want to restore.

Note The backup filename indicates the date and time that the system created the backup file.

Step 5 Click **Next**.
The **Step 3 Restore—Select the Type of Restore** page appears.

Step 6 Choose the features that you want to restore.

Note Only the features that were backed up to the chosen file are displayed.

Step 7 Click **Next**.
The Step 4 Restore—Final Warning for Restore page appears.

Step 8 Click **Restore** to start restoring the data, .
You are prompted to choose the server to restore.

Step 9 Choose the appropriate server.

Caution After you choose the server that you want restored, any existing data on that server will be overwritten.

Your data is restored on the server that you chose. To view the status of the restore, see View Restore Status, on page 249.

Step 10 Restart the server.

Note The system can require one hour or more to restore depending on the size of your database and the chosen components.

Restore Entire Server Group

If a major failure or a hardware upgrade occurs, you may need to restore all the servers in the server group.

Note Before you restore a server group, make sure that the subscriber server in the server group is up and communicating with the publisher server. You must carry out a fresh install for the subscriber server that is down or not communicating with publisher server at the time of the restore.

Procedure

Step 1 Restore both Emergency Responder Publisher and Subscriber at the same time by selecting both the servers using Restore wizard.

Step 2 Restart Publisher.

Step 3 Restart the Subscriber after the publisher is back online.

Note You must restore both the servers in the server group at the same time.

The following sections provide the procedures for restoring servers in a server group.

Restore Publisher Server

Caution Before you restore Emergency Responder, ensure that the Emergency Responder version that is installed on the server matches the version of the backup file that you want to restore. The Disaster Recovery System supports only matching versions of Emergency Responder for restore.

Procedure

Step 1 Perform a fresh installation of CiscoEmergency Responder on the Publisher server. See the Install Emergency Responder Publisher procedure for more information.

Step 2 From the main Disaster Recovery System web page, select **Restore** > **Restore Wizard**.
The first page of the **Restore Wizard (Step 1 Restore—Choose Backup Device)** appears.

Step 3 Choose the backup device from which to restore in the **Select Backup Device** area.

Step 4 Click **Next**.
The **Step 2 Restore—Choose the Backup Tar File** page appears.

Step 5 Choose the backup file that you want to restore.

Note The backup filename indicates the date and time that the backup file was created.

Step 6 Click **Next**.
The **Step 3 Restore—Select the Type of Restore** page appears.

Step 7 Choose the features that you want to restore.

Note Only the features that were backed up to the chosen file are displayed.

Step 8 Click **Next**.
The **Step 4 Restore—Final Warning for Restore** page appears.

Step 9 Click **Restore** to start restoring the data.

Step 10 Choose only the Publisher when you are prompted to choose the server to restore.

Step 11 Your data is restored on the publisher server. To view the status of the restore, see View Restore Status, on page 249.

Note During the restore process, do not perform any tasks with Emergency Responder Administration or User Pages.

Step 12 Restart the server.

Note Depending on the size of your database and the components that you choose to restore, the system can require one hour or more to restore.

Step 13 After the publisher server restarts, continue with the Restore Subscriber Server , on page 248.

Restore Subscriber Server

⚠ **Caution** When restoring a server group, you must restore the publisher server before you restore the subscriber server.

Before you begin

Before you restore Emergency Responder, ensure that the Emergency Responder version that is installed on the server matches the version of the backup file that you want to restore. The Disaster Recovery System supports only matching versions of Emergency Responder for restore.

Procedure

Step 1 Perform a fresh installation of Cisco Emergency Responder on the Subscriber server.

Step 2 Select **Restore** > **Restore Wizard** from the main **Disaster Recovery System** web page.
The first page of the **Restore Wizard (Step1 Restore—Choose Backup Device)** appears.

Step 3 Choose the backup device in the **Select Backup Device** area.

Step 4 Click **Next**.
The **Step 2 Restore—Choose the Backup Tar File** page appears.

Step 5 Choose the backup file that you want to restore.

Caution To restore the subscriber server in the server group, you must choose the same backup file that you used to restore the Publisher.

Step 6 Click **Next**.
The **Step 3 Restore—Select the Type of Restore** page appears.

Step 7 Choose the features that you want to restore.

Note Only the features that were backed up to the chosen file are displayed.

Step 8 Click **Next**.
The **Step 4 Restore—Final Warning for Restore** page appears.

Step 9 Click **Restore** to start restoring the data.

Step 10 Choose only the Subscriber when you are prompted to choose the servers to restore.

Step 11 Your data is restored on the subscriber server.

Step 12 Restart the server.

Note The system can require one hour or more to restore depending on the size of your database and the components that you choose to restore.

Step 13 When the subscriber has rebooted and is running the restored version of Emergency Responder, reboot the publisher.

Step 14 Check the Replication Status value on all nodes by using the **utils dbreplication status** CLI command. The value on each node should equal two.

Tip If replication does not set up properly, use the **utils dbreplication reset** CLI command.

View Restore Status

Procedure

Step 1 From the main **Disaster Recovery System** web page, select **Restore** > **Status**.
The **Restore Status** page appears. The Status column in the Restore Status window shows the status of the restoration in progress, including the percentage of completion of the restore procedure.

Step 2 Click the **log filename** link to view the restore log file.

Backup and Restore History

The following sections describe how you can see the last 20 backup and restore jobs.

View Backup History

Procedure

Step 1 Select **Backup** > **History** from the main **Disaster Recovery System** web page.
The Backup History page appears.

Step 2 From the **Backup History** page, you can view the backups that you have performed, including filename, backup device, completion date, result, and features that are backed up.

Note The **Backup History** page displays only the last 20 backup jobs.

View Restore History

Procedure

Step 1 Select **Restore** > **History** from the main **Disaster Recovery System** web page.
The **Restore History** page appears.

Step 2 From the **Restore History** page, you can view the restores that you have performed, including filename, backup device, completion date, result, and the features that were restored.

Note The **Restore History** page displays only the last 20 restore jobs.

Trace Files

Trace files for the Master Agent, the GUI, and each Local Agent are written to the following locations:

- For the Master Agent, the trace file is platform/drf/trace/drfMA0*
- For each Local Agent, the trace file is platform/drf/trace/drfLA0*
- For the GUI, the trace file is platform/drf/trace/drfConfLib0*

You can view trace files by using the CLI.

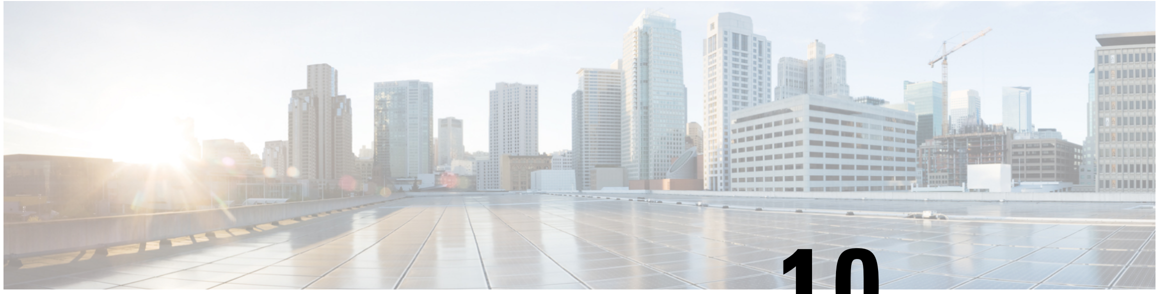
Use the CLI for Backup and Restore

The Disaster Recovery System also provides command-line access to a subset of backup and restore functions.

Table 18: Disaster Recovery System CLI

Command	Description
utils disaster_recovery backup	Starts a manual backup by using the features that are configured in the Disaster Recovery System interface.
utils disaster_recovery restore	Starts a restore and requires parameters for backup location, filename, features, and servers to restore.
utils disaster_recovery status	Displays the status of ongoing backup or restore job.
utils disaster_recovery show_backupfiles	Displays existing backup files.
utils disaster_recovery cancel_backup	Cancels an ongoing backup job.
utils disaster_recovery show_registration	Displays the currently configured registration.

Command	Description
utils disaster_recovery show_tapeid	Displays the tape identification information.



CHAPTER 10

Enhanced Location Tracking For Jabber Clients

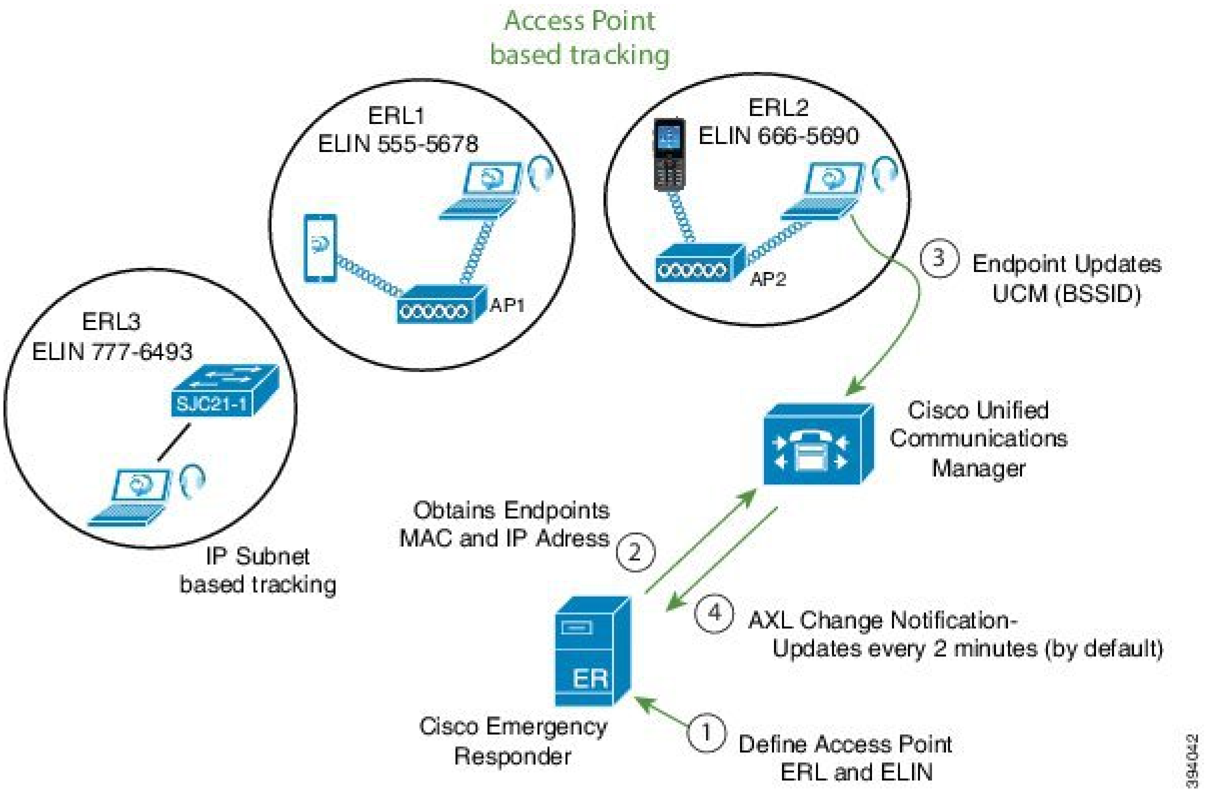
Enhanced Location Tracking for Jabber Clients

The Enhanced Location Tracking allows Unified Communications Manager along with Emergency Responder tracks the physical location of wireless Cisco Jabber clients. The location is tracked through a wireless access point which serves as the location identifier.

Unified Communications Manager can synchronize all the wireless access points deployed in the infrastructure through a Wireless LAN Controller (WLC) synchronization or through a manual import using Bulk Administration Tool (BAT). Using AXL discovery, the Emergency Responder administrators can learn about the various access points through the Unified Communications Manager. The Emergency Responder administrator defines emergency response locations (ERLs) for these access points and corresponding 911 call treatment. Cisco Jabber clients, if defined by the Policy in Unified Communications Manager, sends their upstream infrastructure information like BSSID and any subsequent changes to Emergency Responder. Emergency Responder provides ERL treatment to Cisco Jabber clients based on the associated access point.

Note Emergency Responder AXL discovery runs every 2 minutes (by default) to identify a location update (Access Point BSSID) and so can be identified within 2 to 4-min period. If the system is running large number of Jabber clients or load conditions, administrators can change the frequency accordingly. Any AXL communication error is reported through the Event Viewer and the administrator must take corrective actions immediately.

Figure 24: Basic Deployment of Enhanced Location Tracking



Enhanced Location Tracking feature is available for the following components:

- Unified Communications Manager Release 12.5.1SU1
- Emergency Responder 12.5.1SU1
- Cisco Jabber 12.6

Enhanced Location Tracking Recommendations Considerations

- Enhanced location tracking feature works only for the 12.5.1SU1 or above versions of Emergency Responder and Unified Communications Manager.
- If any Cisco Jabber or wireless device falls under non-defined Access Points, then the device is tracked using IP subnet (if IP subnet is configured) or Unlocated Phones page.

- Cisco Jabber devices should be tracked using the AXL discovery method. The MAC address of a Cisco Jabber device (wireless or wired) displays the same details as the Device Name.
- Off-Premise emergency response location (ERL) does not support Cisco Jabber AXL discovery tracking.
- Emergency Responder Clustering is not supported. Phones that are discovered using AXL discovered phones is not shared through an Emergency Responder cluster.
- If different Unified Communications Manager clusters are connected to Emergency Responder, you should not use the combination of different Unified Communications Manager versions. For example, you should not combine a Release 12.5.SU1 Unified Communications Manager with a version above or below. Similarly, if multiple clusters of Unified Communications Manager are connected to Emergency Responder, then all the Unified Communications Manager clusters should have release 12.5.1SU1 version or above.
- For enhanced location tracking, if the Unified Communications Manager version is over 12.5.1SU1 release and above, different discoveries take the following priority:
    - If Major discovery is running, AXL discovery and phone tracking cannot take place.
    - If Incremental discovery is running, AXL discovery can run in parallel.

Initial Configurations for Enhanced Location Tracking for Jabber Clients

The following sections describe the initial setup tasks that you must complete before you begin to configure the enhanced location tracking feature for Cisco Jabber devices.

- Unified Communications Manager Configurations Task Flow, on page 255
- Emergency Responder Configurations Task Flow, on page 256

Unified Communications Manager Configurations Task Flow

Perform the following tasks to set up your access points in Unified Communications Manager.

Procedure

	Command or Action	Purpose
Step 1	Configure Access Points in Unified Communications Manager, on page 256	Use the instructions in this task to synchronize the database with a Cisco Wireless Access Point Controller (WLC) use either of the following tasks: • Through a Wireless LAN Controller (WLC). • Inserting a CSV file into the Unified Communications Manager database.

	Command or Action	Purpose
Step 2	Configure Cisco Jabber on Unified Communications Manager, on page 258	Adds a Cisco Jabber device manually.
Step 3	Configure Cisco Jabber Configuration Files in Unified Communications Manager, on page 258	Creates Jabber Client Configuration (jabber-config.xml) files and associates them to end users.
Step 4	Configure AXL Application User, on page 259	Use this procedure to configure an AXL user that Emergency Responder uses to access the device configuration and database access.
Step 5	Enable Change Notifications, on page 260	Use this procedure to enable AXL change notifications in support for the Enhanced Location Tracking feature.

Emergency Responder Configurations Task Flow

Perform the following procedures to provision the access points and track Cisco Jabber devices (wired or wireless) that are configured in Unified Communications Manager and discovered by Emergency Responder.

Procedure

	Command or Action	Purpose
Step 1	Set Up SNMP Connection, on page 149	Emergency Responder uses SNMP to obtain information about Unified Communications Manager nodes in the cluster.
Step 2	Configure AXL Application User, on page 259	You must configure the AXL application user for Emergency Responder on Unified Communications Manager.
Step 3	Set Up Default ERL , on page 138	You can create emergency response locations (ERLs) for tracking devices under a single location.
Step 4	Configure AXL Phone Tracking, on page 264	Use this procedure to track wired or wireless Cisco Jabber devices from any location.

Configure Access Points in Unified Communications Manager

There are two types of deployment models for Access Points configuration:

- Configure Access Points Through Wireless LAN Controller Synchronization Service, on page 257
- Configure Access Points Using Bulk Administration Tool, on page 257

Configure Access Points Through Wireless LAN Controller Synchronization Service

To configure access points through WLAN Controller, use the following procedure:

Procedure

Step 1 In the Cisco Unified Serviceability interface, choose **Tools** > **Service Activation** and select the publisher node.

Step 2 From the Location based Tracking Services, check the **Cisco Wireless Controller Synchronization Service** option and save the configuration changes. This will activate the CWLCSS service.

Step 3 In Cisco Unified Serviceability interface, choose **Tools** > **Control Centre – Feature Services**.

Step 4 Select the publisher node to enable the **Cisco Wireless Controller Synchronization Service** option from the Location based Tracking Services section.

Step 5 In Cisco Unified CM Administration user interface, choose **Advanced Features** > **Device Location Tracking Services** > **Wireless Access Point Controllers**.

Step 6 Enter the required details in **Wireless Access Controller Details** and select an automatic synchronization schedule using the **Wireless Access Point Controller Synchronization Schedule**. Click **Save**.

Step 7 After synchronizing a WLC, in Cisco Unified CM Administration user interface, navigate to **Advanced Features** > **Device Location Tracking Services** > **Switches and Access Points** to view all the access points details.

Configure Access Points Using Bulk Administration Tool

An IPv4 address, IPv6 address, or BSSID may be associated with only one infrastructure device. Two devices cannot have the same IP address or BSSID. Also, all BSSIDs must end in 0.

Before you begin

Create a .csv file with the following delineated columns: ACCESS POINT or SWITCH NAME, IPV4 ADDRESS, IPV6 ADDRESS, BSSID, DESCRIPTION.

Procedure

Step 1 In Cisco Unified CM Administration user interface, navigate to **Bulk Administration** > **Upload/Download files** and upload the .csv file.

Step 2 Choose **Bulk Administration** > **Infrastructure Device** > **Insert Infrastructure**.

Step 3 In the **File Name** field, choose the CSV data file that you created for this transaction.

Step 4 In the **Job Information** area, enter the job description.

Step 5 Choose the .csv file and select the option **Run Immediately** or **Run Later** as per the requirement. If you choose to **Run Later**, ensure you use the Job Scheduler page to schedule and activate the job.

Step 6 Click **Submit**.

Step 7 To verify whether your device is added, navigate to **Advanced features > Device Location Tracking services > Switches and Access Points**.

You can view all the Access Points that were successfully added through the Bulk Import.

Configure Cisco Jabber on Unified Communications Manager

Note Ensure that you specify the name of the Jabber device configuration type (CSF, BOT, TCT, or TAB) in the **Device Name** of the Phone Configuration window.

To add a new Cisco Jabber device manually with a user, perform the following procedure:

Procedure

Step 1 From the Cisco Unified CM Administration, choose **Device > Phone > Add a New Phone**.

Step 2 From Find and List Phones page, click **Add New** to manually add a phone.

Step 3 Find and select the appropriate wireless or Jabber device which you want to add to your access point.

Step 4 Complete the fields in the **Phone Configuration** window.

Step 5 Click **Save**.

Step 6 If you want to add another Cisco Jabber device, repeat these steps.

Configure Cisco Jabber Configuration Files in Unified Communications Manager

The following are three new configuration parameters that must be set to have the Jabber client send location updates:

- EnableE911OnPremLocationPolicy
- EnableE911EdgeLocationPolicy
- 911EdgeLocationWhiteList

For more information on the parameters, see https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/jabber/12_5/Parameter_Guide/cjab_b_parameters-reference-guide-jabber_125.html.

If these three parameters are not properly configured, then by default, Jabber will not send the location updates. You can centrally manage Jabber client configuration parameters using the Cisco Unified CM Administration interface. You can create multiple Jabber Client Configuration templates for various deployment scenarios and assign them to end users. Jabber clients can now send their location information to Unified Communications Manager.

Procedure

Step 1 Open the **Cisco Unified CM Administration** interface on Unified Communications Manager.

Step 2 Select **User Management > User Settings > UC Service**.

Step 3 Using the **Jabber Client Configuration (jabber-config.xml)** service, you can create multiple Jabber Client Configuration templates as per your deployment needs.

Note Ensure that you configure the three new configuration parameters for Cisco Jabber device tacking.

Step 4 Navigate to **User Settings > Service Profiles** to associate them to Common, Desktop, and Mobile Jabber client types once the templates are created.

Step 5 Navigate to **User Management > End User** to add a new user.

Step 6 Select a **UC Service Profile** that you have created in Step 3 for this end user.

Configure AXL Application User

Note It is not mandatory that CallManager Service runs on all Unified Communications Manager nodes. Only the Unified Communications Manager that is configured in Emergency Responder and the Unified Communications Manager nodes that acts as the backup server (in case of connection failures) needs to run the CallManager Service.

To create a new AXL application user, perform the following procedure:

Procedure

Step 1 In Cisco Unified CM Administration, choose **User Management > Application User**.

Step 2 Click **Add New** to create a new application user and configure the fields in the Application User Configuration window.

Step 3 Click **Save**.

Step 4 In Cisco Unified CM Administration, choose **User Management > User Settings > Role**.

Step 5 Click **Add New** and select **Cisco CallManager AXL Database** and configure the remaining fields.

Step 6 Ensure that you check the **Allow to use API** check box and click **Save**.

Step 7 In Cisco Unified CM Administration, choose **User Management > User Settings > Access Control Group**.

Step 8 Click **Add New**, enter a name and click **Save**.

Step 9 Click **Add App User to Group**.

Step 10 Search for the user with the new application User ID, check the required check box to select the user and click **Add Selected**.

Step 11 Select **Assign Role to Access Control Group** from the drop-down list on the top right side.

Step 12 Click **Assign Role to Group** and select **Custom AXL Access** to select the role.

Step 13 Click **Add Selected** and save the configuration changes.

Enable Change Notifications

Procedure

Step 1 In Cisco Unified CM Administration user interface, navigate to **System** > **Service Parameter**.

Step 2 Select the publisher server and select **Cisco Database Layer Monitor (Active)**.

Step 3 Click **Advanced**.

Step 4 Under Clusterwide Parameters section, make sure that the parameter value of **AXL Change Notification** is set to On and click **Save**.

Configure Access Points in Cisco Emergency Responder

Perform the following procedures to provision the access points and track Cisco Jabber devices (wired or wireless) that are configured in Unified Communications Manager and discovered by Emergency Responder:

- Set Up SNMP Connection, on page 149
- Configure AXL Application User for Emergency Responder, on page 262
- Assign ERLs, on page 264
- Configure AXL Phone Tracking, on page 264

Set Up SNMP Connection

Emergency Responder uses SNMP to obtain information about the ports on a switch. Emergency Responder must obtain this port information so that you can assign the ports to ERLs, and so that Emergency Responder can identify phones that are attached to the ports and update their ERL assignments.

Emergency Responder only reads SNMP information, it does not write changes to the switch configuration, so you only have to configure the SNMP read community strings.

When you configure the SNMP strings for your switches, you must also configure the SNMP strings for your Unified CM servers. Emergency Responder must be able to make SNMP queries of all Unified CM servers in the cluster that it supports.

If your Cisco Emergency Responder servers, Unified CM servers, and Cisco IP Phones are in a different subnet than your switches, you must either configure both the subnets for the servers and phones as well as the subnet for the switches or use *.*.*.*.

Related Topics

SNMP Settings, on page 419

LAN Switch Identification , on page 153

Set Up SNMP Community String

By configuring SNMP, you can control SNMP access to the Emergency Responder SNMP agent. A management station must first submit a valid community string for authentication.

You configure a community string by entering the Community String Name, the IP addresses of host that can be authenticated using the community string, and the access privileges allowed. The available access privileges are as follows:

- ReadOnly
- ReadWrite
- ReadWriteNotify
- NotifyOnly
- None

Procedure

Step 1 From the Emergency Responder Serviceability web interface, select **SNMP** > **V1/V2C Configuration** > **Community String**.
The SNMP Community String Configuration page appears.

Step 2 Enter the name of the community string in the Community String Name text box.

Step 3 Click **Accept SNMP Packets only from these hosts** to specify specific hosts whose SNMP packets will be accepted, enter the IP addresses in the text box, and click **Insert**.

To accept SNMP packets from any host, click the **Accept SNMP Packets from any host** radio button.

Step 4 Select the host IP address and click **Remove** to remove an existing host, .

Step 5 Select the access privilege for the host from the Access Privileges pull-down menu then click **Insert**.

Related Topics

SNMP Community String Configuration, on page 514

Set Up SNMP Users

SNMP V3 provides additional security features that include message integrity, authentication, and encryption. In addition, SNMP V3 controls user access to specific areas of the MIB tree.

Note FIPS Mode and Enhanced Security Mode do not support MD5 or DES encryption methods. If SNMPv3 setting is enabled using MD5 or DES, then enabling FIPS Mode or Enhanced Security Mode changes these encryption methods to SHA-1 or AES-128 respectively.

Before Emergency Responder (in FIPS Mode) upgrade, ensure that there are no MD5 or DES encryption methods in the FIPS Mode. If the MD5 or DES encryption methods were not updated to SHA-1 or AES-128 respectively in the FIPS Mode before upgrade, they will get updated automatically after the upgrade.

Procedure

Step 1 From the Emergency Responder Serviceability web interface, choose **SNMP** > **V3 Configuration** > **User**.

Step 2 Click **Add New** to add a new SNMP User.

Step 3 Enter the new SNMP user name in the **User Name** text box.

Step 4 Check the **Authentication Required** check box to require authentication. Enter a password in the **Password** text box, reenter the password in the **Reenter Password** textbox, and choose either **MD5** or **SHA** to select an authentication protocol. Click **Insert** to add the user.

Step 5 Check the **Privacy Required** check box to require information privacy. Enter a password in the **Password** textbox, reenter the password in the **Reenter Password** textbox, and choose either **DES** or **AES** to select a privacy protocol.

Note A message appears to restart the SNMP master agent for the changes to take effect. Click **OK** to restart the SNMP master agent or **Cancel** to continue without restarting the master agent.

The new user is added to the list of users on the SNMP User Configuration page.

Step 6 Repeat Step 2 through to Step 4 to add additional users.

Related Topics

SNMP User Configuration, on page 516

Set Up MIB2

The SNMP MIB2 tool allows you to specify a contact person for a MIB2 managed node and the physical location of the managed node.

Procedure

Step 1 From the Emergency Responder Serviceability web interface, select **SNMP > System Group Configuration > MIB2 System Group Configuration**.

Step 2 In the **System Contact** text box, enter the name of the contact.

Step 3 In the **Location** text box, enter the location of the managed node.

Step 4 Click **Update** in the upper left corner of the page.

Step 5 Click **Clear** in the upper left corner of the page to modify the information, enter the new information in the **System Contact** and **Location** text boxes, and click **Update**.

Related Topics

MIB2 System Group Configuration, on page 517

Configure AXL Application User for Emergency Responder

You must configure the AXL application user for Emergency Responder on Unified Communications Manager, so that an off-premises user can log in to the Emergency Responder off-premises user website.

Note You should use the Unified Communications Manager release 12.51SU1 version to locate Cisco Jabber through AXL application.

Procedure

Step 1 In CiscoUnifiedCM Administration interface, choose **User Management** > **Application User**. Click **Add New**.

Step 2 Complete the following required fields:

- **User ID**—Use a descriptive name such as AXL Application User.
- **Password**—Enter a password for this user.
- **Confirm Password**—Reenter the password for this user.

Step 3 Click **Save**.

Step 4 Choose **User Management** > **User Group**.

Step 5 At search criterion, enter **standard** and click **Find**.

The list of user groups starting with the name standard appears.

Step 6 Click **Standard CCM Admin Users** to display the User Group configuration page.

Step 7 Click **Add App Users to Group**.
The Find and List Application Users pop-up window appears.

Step 8 Enter the User ID created in Step 2 as the search criterion and click **Find**.
The list of Applications users appears.

Step 9 Click the check box next to the user ID. Click **Add Selected**.

Unified Communications Manager adds the selected user to the **Standard CCM Admin Users** user group.

Step 10 Choose **User Management** > **User Group**.
The user group search page appears.

Step 11 Enter **standard** as the search criterion and click **Find**.
The list of user groups starting with the name Standard appears.

Step 12 Click the **Standard TabSync User** group.

Step 13 Repeat steps 7 through 9 to add the user to the Standard TabSync User group.

Step 14 Choose **User Management** > **User Group**.
The user group search page appears.

Step 15 Enter **standard** as the search criterion and click **Find**.
The list of user groups starting with the name Standard appears.

Step 16 Click the **Standard RealtimeAndTraceCollection** group.

Step 17 Repeat steps 7 through 9 to add the user to the Standard RealtimeAndTraceCollection group.

Assign ERLs

Emergency Responder does not automatically assign new switch ports and unlocated phones to the default emergency response location (ERL). New switch ports and unlocated phones are treated as ERLs that are not configured.

You must not configure the default ERL to any of the Switch Ports, Unlocated Phones, Manually Configured Phones or IP subnets. The default ERL is used internally by Emergency Responder only if no other ERL is configured for that phone.

Emergency Responder also uses the default ERL for all emergency calls when the Emergency Responder server is first started (or restarted when there is no standby Emergency Responder server) until the initial switch port update is finished. (This process is started immediately.)

Before you begin

You must log into Emergency Responder with system administrator or ERL administrator authority.

You must first configure the required ELINs in Unified Communications Manager.

Procedure

Step 1 Select **ERL > Conventional ERL**.

Step 2 Click **Configure Default ERL**.

Step 3 Fill in the ERL Information for Default window.

Step 4 Click **ALI Details**.

Step 5 Fill in the ALI Information window.

When finished filling in the ALI, click **Update ALI Info**. Emergency Responder saves your ALI. Click **Close** to close the window.

Step 6 Make the ERL Information for Default window the active window if it is not, and click **Update**.

Emergency Responder saves the ERL and its ALI.

Step 7 Click **Close** to close the window.

Tip You cannot delete the default ERL. In addition, you cannot configure other ERLs unless the default ERL is configured.

Configure AXL Phone Tracking

To track phones successfully, Emergency Responder must periodically contact Unified Communications Manager and switches to obtain the port and device information. Emergency Responder updates network information using two processes:

- Phone Tracking—A periodic comparison of the phones registered with Unified Communications Manager to the location information is obtained from the switches. If a phone moves, Emergency Responder updates the phone's ERL. Phones that cannot be located are classified as unlocated.

Note If you do not configure a switch port phone update schedule, the default schedule runs at midnight.

- Switch-Port and Phone Update—The phone tracking process plus a more extensive check of the network switches, which can identify new or changed switch modules (additional or removed ports). Any newly discovered ports are assigned to the Default ERL. Ensure that your ERL administrator updates the ERL assignment for new ports.

Before you begin

You must have system administrator or network administrator authority to define the schedule.

Procedure

Step 1 Select **Phone Tracking** > **Schedule**.

Step 2 Enter the incremental phone tracking schedule in minutes and click **Update**.

Emergency Responder runs the phone tracking process after this number of minutes from the start of previous phone tracking process.

Step 3 Enter the AXL incremental location phone tracking schedule in minutes and click **Update**.

Emergency Responder runs the enhanced location phone tracking for wireless devices after this number of minutes from the start of previous location tracking process.

Note By default, Emergency Responder actively queries the Cisco Jabber client every 2 minutes through AXL discovery on receipt of the device location.

Step 4 Enter the schedule for the switch port and phone update process. You should run this process at least once per day (but not more than four times per day).

Troubleshooting Enhanced Location Tracking For Jabber Clients

Unable to Discover Cisco Jabber or Access Points from Unified Communications Manager

Problem: If the AXL Change Notification queue has changed due to Unified Communications Manager reboot or upgrade, or Tomcat services restart, the server log displays the following error message: *500 internal error for the AXL request sent by CER*.

Solution: The **CER Service** needs to be restarted.

Emergency Responder Lost Connection with Unified Communications Manager

Problem: If Unified Communications Manager publisher node goes down, Emergency Responder loses connection due to queue identifier (QID) mismatch and tries to connect to another Unified Communications Manager node in the same cluster. Displays the following error message based on the AXL phone tracking schedule configured: AXL Phone Discovery failed to connect to axl url- *https://<ip address>*:8443.

Connectivity issues arise due to the following:

- AXL connection down
- AXL authentication credentials changed
- Unified Communications Manager server is rebooted
- Tomcat services restarted

Solution: Ensure that the AXL credentials are correct. If the credentials are correct, verify whether the AXL service is running on Unified Communications Manager and restart the **CER Service**.

Major Discovery Shows Message Incorrectly that Phone Tracking is in Progress

Problem: When a forced Major discovery is initiated for enhanced location tracking during ongoing AXL discovery, it displays an incorrect message stating “Phone tracking is in progress”.

Solution: Run the Major discovery after sometime.

CHAPTER 11

Configure Switch Refresh Utility

Switch Refresh Utility Overview

The Switch Refresh Utility feature helps ease migration of old switch models to newer switch models with minimal change in Cisco Emergency Responder. This feature allows you to save the old switch model configuration details which can be uploaded to your new switch configuration after discovery of the new switch.

As part of this feature, the following functionalities are introduced:

- **Save Switch Config**—The Save Switch Port Configuration page allows you to select and save the switch configuration details of an older switch in a CSV data file in your Cisco Emergency Responder system. You may download, review, and modify the csv file if needed.
- **Upload Switch Config**—The Upload Switch Configuration page allows you to upload the saved switch CSV file to the new switch after it is physically replaced and discovered in Cisco Emergency Responder.

The functionality of **Save Switch Config** or **Upload Switch Config** is mainly for scenario of switch refresh where the IP address of the old switch and the new switch is the same. If the IP address of the new switch is different, you should perform an export switch functionality on the Switch Port Page. The Save Switch Config data may include the assigned ERL Name, Switch IP Address, IfName, Location, Port Name, Switch HostName, Port Identifier, Port Description, and Index details.

For more information on **Save Switch Config** and **Upload Switch Config** configuration pages, see Save Switch Port Configuration, on page 442 and Upload Switch Port Configuration, on page 443. You can also view details of all the saved CSV data files in the **File Management Utility** page.

Note We recommend that you replace minimal number of switches at a time using the switch refresh utility method. If you have a large network, you can replace up to 50 switches at a time.

Save Switch Configuration

Use the Switch Port Details page to save the switch port configuration details.

Procedure

Step 1 From Cisco ER Administration, navigate to **ERL Membership > Switch Ports** to view the list of switches.

Step 2 In the Switch Port Search Parameters, click **Find**.

Step 3 Select the IP address of the switches which are going to be refreshed.

Step 4 Click **Save Switch Config**.

The Save Switch Port Configuration page displays.

Step 5 From the **Select Save Config Format** drop-down list, choose the CSV format.

Step 6 In the **Enter Save Config File name** option, enter the name of the file you want to save with.

Step 7 Click **Save Config** to create and save the file.

Step 8 Use the **Download** drop-down menu to select a file and download a copy to your local system.

Physical Refresh of Switch and Full Discovery in Emergency Responder

During the maintenance window, physically replace the older switch and replace it with a new switch. After the physical replacement with a new switch, perform full discovery on Cisco Emergency Responder.

Procedure

Step 1 To run full discovery (phone tracking), select **Phone Tracking > Run Switch-Port & Phone Update**.

Step 2 Navigate to **ERL Membership > Switch Ports**. Check for the timestamp mentioned in the Switch Port Details page which is updated once full discovery is complete.

Step 3 Verify the new switch details and then perform the **Upload Switch Config** functionality.

Upload Switch Configuration

After uploading the CSV file, the current configuration data will be overwritten and the saved ERL, Port, Location, and IP Address details will be added to the new switch.

Note The saved switch config details will be uploaded to the respective ports on the new switch. Any differential ports must be assigned manually by the administrator.

Before you begin

Ensure that you run full discovery so that the new switch information is updated in the system.

Procedure

Step 1 From Cisco ER Administration, navigate to **ERL Membership > Switch Ports** to view the list of new switches added.

Step 2 Click **Upload Switch Config**.

The Upload Switch Port Configuration page displays.

Step 3 From the **Select Upload config File Format** drop-down list, choose the CSV format.

Step 4 From the **Select File to Upload Config** drop-down list, select the file to be uploaded.

Step 5 Click **Upload**.

You can view the status of the upload in the **Status** box.

CHAPTER 12

Remote Teleworker and Off-Premises User—E911

Remote Teleworker and Off-Premises User—E911 Overview

Cisco Emergency Responder can be configured to provide E911 support to remote teleworker and off-premises users. These users, when registering over Virtual Private Network (VPN) or Mobile Remote Agent, can update their location through the phone display or through Cisco Emergency Responders Off-premises User Page. The Enterprise requires an arrangement with a National Emergency Service Provider to perform location updates, Master Street Address Guide (MSAG) address validation, and call completion.

Currently, Cisco Emergency Responder supports integrations with National E911 Service Provider as National Emergency Service Providers.

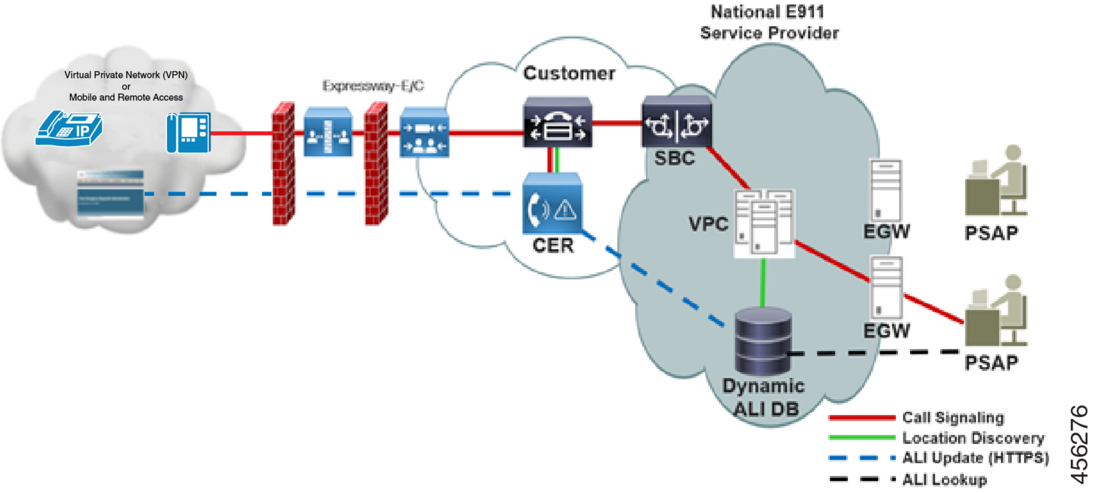
Cisco Unified Communications Manager (Unified Communications Manager) requires users with off-premises phones to set their current location before allowing any outbound call from the phone. Users that have an off-premises phone rely on Unified Communications Manager to route their emergency calls to a National Emergency Service Provider to deliver the emergency call to the appropriate Public Service Answering Point (PSAP) along with the current address.

A legal disclaimer notice is displayed on any phone device that is dynamically identified as an off-premises device (that is, connected remotely to the customer network). The disclaimer advises the users that their administrator has identified their device as outside the customer network and the user must select their current location before being able to place outbound calls. Users can confirm their current location or select another previously stored location from their device display.

If the user's current location has not been previously defined, the user is directed to the Cisco Emergency Responder Off-Premises User web page to create a new location. After the new location has been defined and the address has been validated in the MSAG, emergency calls placed from off-premises phones will then be completed through the National Provider.

Note Remote Teleworker or Off-premises user can have up to 8 preconfigured locations.

Note Extension Mobility is not supported for off-premises users.



Remote Teleworker Emergency Calling Prerequisites

- Configure National E911 Service Provider Enterprise Services. For more information, see chapter Configure Emergency Responder and National E911 Service Provider Enterprise Services , on page 183.
- Enhanced e911 feature is supported only on X/Open System Interface (XSI) capable phones. For more information on XSI, see Cisco Unified IP Phone Services Application Development Notes for Cisco Unified Communications Manager and Multiplatform Phones.
  - Cisco IP Phone 7800 Series
  - Cisco IP Phone 8800 Series
  - Cisco IP Phone 7941/7945
  - Cisco IP Phone 7961/7965
  - Cisco IP Phone 7970/7971/7975
  - Cisco IP Phone 8941/8945
  - Cisco IP Phone 8961
  - Cisco IP Phone 9951/9971
  - Cisco IP Communicator

- Cisco Virtual Desktop (VXCC)

Initial Configurations for Setting Up Remote Teleworker Emergency Calling

Unified Communications Manager Configurations Task Flow

Perform the following tasks to set up Emergency Responder Location Management feature in the Unified Communications Manager server before you can use it to enter the off-premises locations.

Procedure

	Command or Action	Purpose
Step 1	Set Up AXL Application User , on page 273	Allows you to configure the AXL application user for Emergency Responder on Unified CM.
Step 2	Set Up Application Server in Unified CM, on page 274	Allows you to add an application server in Unified CM to define the configuration details for the Emergency Responder (Phone Tracking Menu page in Emergency Responder).
Step 3	Associate End User to a Device, on page 275	Associates the end user to a phone or device.
Step 4	Configure Off-Premises Location Facility, on page 275	Configure this option for remote or mobile devices that change locations frequently.
Step 5	Configure a Directory Number, on page 275	You can configure the directory number configuration settings for the phone or device.

Set Up AXL Application User

When configuring the off-premises user feature, Emergency Responder uses an application user to perform AXL queries and device registration checks. This application user should be different than the CTI Manager User Name. The CTI Manger User Name is used to control the CTI Route Points and the CTI Ports. The AXL User is used to perform device and user queries in the Unified Communications Manager database and device registration status.

Procedure

Step 1 In Cisco Unified CM Administration user interface, choose **User Management > Application User** and click **Add New**.

Step 2 Complete the following required fields:

- **User ID**—Use a descriptive name such as AXL Application User.
- **Password**—Enter a password for this user.
- **Confirm Password**—Reenter the password for this user.

Step 3 Click **Save**.

Step 4 Choose **User Management > User Group** in the CiscoUnifiedCommunications Manager menu.

Step 5 At search criterion, enter **standard** and click **Find**.

Step 6 Click **Standard CCM Admin Users** to display the User Group configuration page.

Step 7 Click **Add App Users to Group**.

Step 8 Enter the User ID created in Step 2 as the search criterion and click **Find**.

Step 9 Click the check box next to the user ID. Click **Add Selected**.

Unified CM adds the selected user to the **Standard CCM Admin Users** user group.

Step 10 Choose **User Management > User Group**.

Step 11 Enter **standard** as the search criterion and click **Find**.

Step 12 Click the **Standard TabSync User** group.

Step 13 Repeat steps 7-9 to add the user to the Standard TabSync User group.

Step 14 Choose **User Management > User Group**.

Step 15 Enter **standard** as the search criterion and click **Find**.

Step 16 Click the **Standard RealtimeAndTraceCollection** group.

Step 17 Repeat steps 7-9 to add the user to the Standard RealtimeAndTraceCollection group.

Set Up Application Server in Unified CM

You must configure the Emergency Responder Location Management server on the Unified CM server before your users can use it to enter their off-premise locations.

Procedure

Step 1 From Cisco Unified CM Administration, choose **System > Application Server**.

Step 2 Click **Add New**.

Step 3 From the Application Server Type drop-down list, choose **CER Location Management** and click **Next**.

Step 4 Enter a name that identifies Emergency Responder Off-Premise application.

Step 5 Enter details for the following:

- **IP Address**—IP Address of the Emergency Responder to which Unified Communications Manager is connected.
- **Selected Application Users**—Select the AXL application user that was created in the previous step.

Step 6 Enter the End User URL for users to access the Emergency Responder Off-Premises page.

The URL takes the form of `http://cer_host/ofpuser` , where `cer_host` is the FQDN of the Emergency Responder server or the IP address of the Emergency Responder. The end user URL is the URL that is presented to the user when they select **Add New** on the device when the user wants to define a new location.

Step 7 Click **Save**.

Associate End User to a Device

Required devices should be associated with the user on the End User page as Controlled Devices (From Cisco Unified CM Administration user interface, navigate to **User Management > End User** and associate the device in the Controlled Devices section) and also on the Phones page in the **Owner User ID** field.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Phone**.

Step 2 Enter the device details.

Step 3 In Device Information, select the **Owner** as **User** and set the **Owner User ID** to the user that this device is assigned to.

Step 4 Click **Save**.

Configure Off-Premises Location Facility

To trigger the off-premises notification sequence, the administrator must configure the device to invoke the off-premise location check during the registration process. Perform the following:

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Phone**.

Step 2 In the Device Information section, check the **Require off-premises location** option if the device requires off-premises location check upon registration. Off-premises location update is required when the device's location is associated with an off-premises ERL (as defined in Emergency Responder).

Step 3 Click **Save**.

Configure a Directory Number

Configure the following in the Directory Number configuration page to ensure proper call routing for Remote Teleworkers:

Procedure

Step 1 In the Phone Configuration page, select the **DN** from the Association section on the left side of the page.

Step 2 In the Directory Number Configuration page, verify that the **External Phone Number Mask** will make the actual directory number into a 10-digit North American Numbering Plan (NANP) number.

If the DN on the phone is not a 10-digit NANP number, define the external phone number mask to create a 10-digit NANP number. If the **External Phone Number Mask** is used, the mask must include at least one X to be considered valid for the Remote Teleworker feature.

Step 3 Click **Save**.

Emergency Responder Configurations Task Flow

Perform the following tasks to set up Emergency Responder Location Management feature in the Emergency Responder server.

Procedure

	Command or Action	Purpose
Step 1	Set Up and Test National E911 Service Provider Connectivity, on page 276	Validate connectivity to National E911 Service Provider.
Step 2	Set Up an National E911 Service Provider Route Pattern, on page 277	Sets the route patterns for routing the call to National E911 Service Provider.
Step 3	Set Up AXL Authentication , on page 277	Allows you to configure the AXL credentials and port information.
Step 4	Set Up Off-Premises ERL , on page 278	Adds a new emergency response location (ERL) for Off-Premises phones.
Step 5	Configure Default ALI Values for National E911 Service Provider ERLs, on page 278	Adds the Default ALI Values for National E911 Service Provider URLs.
Step 6	Configure IP Subnet, on page 279	Defines the IP subnet and associated URL.

Set Up and Test National E911 Service Provider Connectivity

You can use the National E911 Service Provider VUI configuration page to enter the account information that is required for Emergency Responder to interoperate with National E911 Service Provider Validation and Update Interface (VUI). After entering the required information, you can test the connectivity to National E911 Service Provider from this page.

Contact your chosen National Emergency Service Provider (National E911 Service Provider) to obtain the required National E911 Service Provider configuration details. For more information on the National E911 Service Provider VUI configuration settings in Emergency Responder, see National E911 Service Provider VUI Settings, on page 386.

Before you begin

- DNS must be configured in Emergency Responder and Unified Communications Manager to reach the National Providers VUI services.

Note: To configure the Domain Name System (DNS) in both the Unified Communications Manager and Emergency Responder, execute the **set network dns primary** command.

Run the **set network domain** command to set the network domain.

Procedure

Step 1 From Cisco ER Administration, choose **System** > National E911 Service Provider **VUI Settings**.

Step 2 Upload the certificate from your local drive to the Emergency Responder server.

Step 3 Enter the **Certificate Password** and the **VUI URL** that was specified by the provider.

Step 4 Test and Validate the Certificate.

Step 5 After verifying the validity of the certificate, add the **VUI Schema URL** and **Account ID**.

Step 6 Click **Test Connectivity** to verify whether Emergency Responder can successfully connect to National E911 Service Provider VUI or not.

On the 'Test National E911 Service Provider Connectivity' pop-up window, the Test Results section should show status “200 OK” after pressing the **Connect** button. This response indicates that both the certificate and account information are valid.

Set Up an National E911 Service Provider Route Pattern

Before any emergency calls can be completed by National E911 Service Provider for Enterprise Service, you must configure the route patterns for routing the call to National E911 Service Provider.

Procedure

Step 1 From Cisco ER Administration, choose **System** > **Telephony Settings**.

Step 2 Under National E911 Service Provider Route Pattern Settings, enter the National E911 Service Provider **Route/Translation Pattern** and click the **Add** button.

What to do next

Verify that the lock icon next to the **ERL** > **Off Premise ERL** is removed and the page is accessible.

Set Up AXL Authentication

When setting up Emergency Responder for supporting Remote Teleworkers, Emergency Responder will use the AXL user to access information about device configuration and status through the AXL interface. You must define and test AXL connectivity to the Unified Communications Manager in Emergency Responder to ensure that the user has access to the AXL resources. This procedure verifies that the user information entered has connectivity to the required AXL resources.

Procedure

Step 1 From Emergency Responder, choose **Phone Tracking** > **Cisco Unified Communications Manager**.

Step 2 Select the Unified CM cluster for which you will be providing the off-premises user support.

You can find the previously defined Unified CM clusters at the bottom of the page.

Step 3 Under AXL Setting, enter the following information:

- AXL Username
- AXL Password
- AXL Port Number

Step 4 Click the **Text AXL Connectivity** URL.

Step 5 Click **Connect**.

If the AXL user is correctly defined, the result displays "Connection succeeded". If an error comes back, try reentering the user and password information and try the connection again.

Step 6 Click **Update** to save the information.

Set Up Off-Premises ERL

Use this procedure to create a new emergency response location (ERL) for Off-Premises phones. For most installations, users need only a single Off-Premise ERL to route Off-premises calls to the National Provider.

Procedure

Step 1 From Cisco ER Administration, choose **ERL** > **Off-Premises ERL** > **Off-Premises ERL (Search and List)** from Emergency Responder.

Step 2 Click **Add New ERL**.

Step 3 Enter an ERL name and description.

Step 4 Enter the National E911 Service Provider Route/Translation Pattern.

Step 5 Select the Off-Premises users who should be notified when an emergency call is made from this ERL.

Step 6 Click **Insert** to save the Off-Premises ERL information.

Configure Default ALI Values for National E911 Service Provider ERLs

Use the Default ALI Values page to set the default values that automatically populate the respective ALI fields when a user updates their National E911 Service Provider ERL settings.

Procedure

Step 1 From Cisco ER Administration, choose **ERL** > National E911 Service Provider **ERL** > **Default ALI Values**.

Step 2 Enter the **Company ID**.

Step 3 Enter the **Customer Name**.

Step 4 Click **Save**.

Configure IP Subnet

Use the Configure IP Subnet page to manually define an IP subnet and its ERL. The IP Subnet used to identify the off-premises devices will be the internal address of the Expressway E/C nodes or the VPN subnet/VPN concentrator.

Procedure

Step 1 From Cisco ER Administration, choose **ERL Membership > IP subnets** and click **Add new IP subnet**.

Step 2 Enter the Subnet ID and Mask details.

- For VPN connected devices, the IP Subnet should be a subnet/mask format.
- For Mobile Remote Agent connected devices, the IP Subnet may be subnet/mask or a specific IP address.

Step 3 Click **Search ERL** to select the ERL you want to assign to the subnet.

Step 4 In the ERL Search Parameters, set the find value to **Off-Premise ERL** and click **Find**.

Step 5 Click the radio button next to the Off-Premise ERL (defined previously) and click **Select ERL**.

Step 6 Click **Insert** to add the subnet on the Configure IP Subnet page.

Configure Remote Teleworker Emergency Calling For Off-Premises Locations

Add New Location

Before a user can associate a location to their phone or device, the user must first enter a location into Emergency Responder. All locations defined in Emergency Responder are user-specific. Each user must add their own locations. When a user has multiple locations, each location must have a unique name to identify that unique location.

Procedure

Step 1 Log in to the Cisco Emergency Responder Off-Premises User page at **https://<CER_FQDN>/ofpuser** using the end user credentials.

Note Emergency Responder Off-Premises User page does not support SSO logins.

Step 2 From the Cisco Emergency Responder Off-Premises User page, select **Locations** and click **Add New Locations**.

Enter a valid address. Use this location name to identify this address when you associate your phone with this address.

Step 3 Click **Validate** to verify the address with your National Provider.

Step 4 If the address validation fails, the user must correct the address before saving the location.

Step 5 Click **Save** to save the location information in Emergency Responder.

Note Saving the location does not immediately update the National Provider, but stores the location information in Emergency Responder. When a user selects the location from the device, the stored address information is sent to the National Provider to update the address for the user's E.164 number.

Associate Your Location to Your Phone

After a user defines a location in Emergency Responder, the user should associate and verify that the device is associated to the desired location.

Procedure

Step 1 From the Cisco Emergency Responder Off-Premises User page, choose **Phones**.

Step 2 To associate a location to a phone, click the corresponding **Assign** link.

Step 3 In the Associate Location page, select the desired location from the **Select New Location** drop-down list. The new location becomes active when you click the **Associate Location** button.

The Status field show displays that the "Location Association Is Successful." This indicates that the address is valid and has been updated with the National Provider.

Step 4 Once the location is associated, the device on the Phones page should display the device status as **Off Premises** and the Associated Location should match the one that was selected. Additionally, ensure that the Direct Inward Dial (DID) is a properly formatted 10-digit NANP number.

Verify the Remote Teleworker Off-Premises Locations in Emergency Responder

Note If the remote or off-premises user chooses not to update their current location, the Disclaimer prompts the user to acknowledge that calls may be restricted until the location is updated. 911 calls will not work until the user decides to associate their device to the desired location.

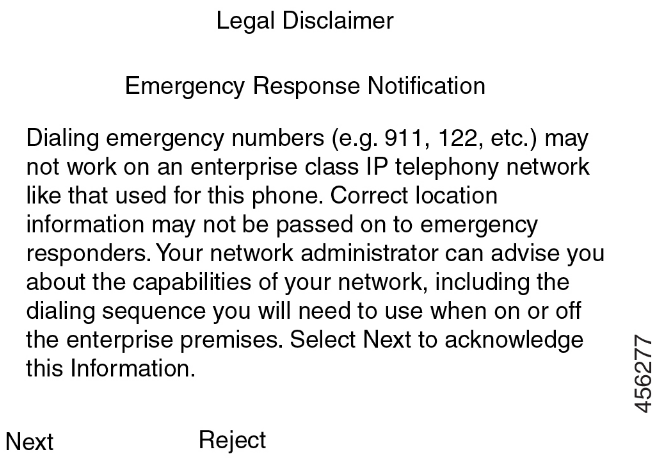
As the System Administrator, you can configure to select and mandate location update so that the device user has to acknowledge the disclaimer and provide current location information before the device is enabled for normal use. (From Cisco Unified CM Administration, choose **System** > **E911 Messages** to configure the mandatory location update disclaimer message.)

Procedure

Step 1 Reset the phone or device.

After the phone has rebooted and after 2-5 seconds after registering, the device should display the Remote Teleworker legal notification. At this point, the remote teleworker location selection process should start.

Step 2 Ensure that the following legal disclaimer message appears on the phone.



Legal Disclaimer

Emergency Response Notification

Dialing emergency numbers (e.g. 911, 122, etc.) may not work on an enterprise class IP telephony network like that used for this phone. Correct location information may not be passed on to emergency responders. Your network administrator can advise you about the capabilities of your network, including the dialing sequence you will need to use when on or off the enterprise premises. Select Next to acknowledge this Information.

Step 3 Click **Next**.

You will get the details of all the locations added through Cisco Emergency Responder Off-premises URL.

Step 4 Using the toggle buttons on the phone or device, choose a location and press the **Select** button.

A few seconds later, the phones user interface should indicate the successful settings of the off-premises user's location.

What to do next

Administrators should instruct the users on how to validate the accuracy of the E911 address based on the user-defined setting. This process should follow the company's procedure for emergency address validation. When a user dials 911 as per the company process for validating the emergency dispatch address, the call should be routed to public-safety answering point (PSAP) using the off-premises ERL and the address reported by the PSAP should be the address currently assigned to the device through the Cisco Emergency Responder Off-Premises User Page.

Configuring Mobile and Remote Access Connected Devices

Configuring devices connected over the Mobile and Remote Access Edge (Cisco Expressway-E/C) will occur in the same way as the VPN connected phones. The IP Subnet used to identify Mobile and Remote Access clients will be the Expressway-C's IP Address. All phones or devices registered to Unified Communications Manager using Mobile and Remote Access will have the same IP Address as the Unified CM.

The configuration procedures for Mobile and Remote Access clients are the same as for VPN clients except that the Mobile and Remote Access setup requires one additional configuration step on the Expressway-C to work. In order to allow the HTTP requests from the phones to the E911Proxy service to obtain the XSI messages, the external Cisco Expressway server must have an explicit HTTP service mapping. This mapping is required to map the external request to an internal resource.

The following configuration must be set up in the Cisco Expressway:

Procedure

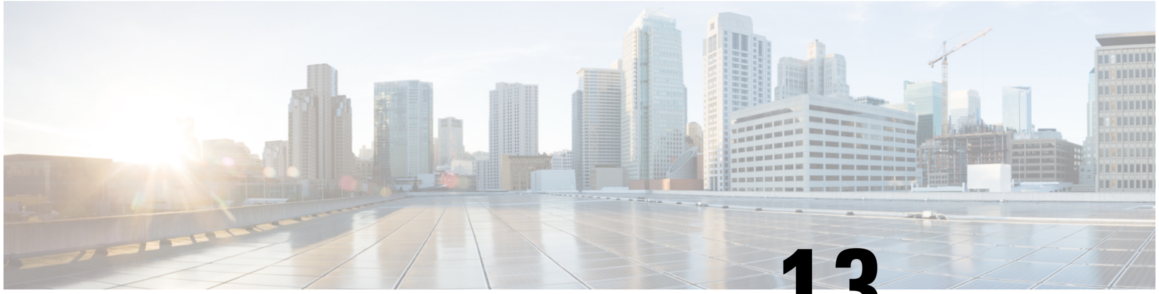
Step 1 From the Cisco TelePresence Video Communication Server Control, navigate to **Configuration > Unified Communications > HTTP allow list > Editable inbound rules**.

Step 2 Enter a description.

Step 3 Enter the **URL** to reach the E911Proxy service. The URL should be **https://cucmfqdn:8080/e911proxy** .

Step 4 Enter the **Allowed Methods** and **Match type**.

Note Because E911Proxy HTTP requests are node-specific, the Expressway administrator must add the ‘E911Proxy’ service for all call processing nodes in the cluster. Any node that has phone registrations must have an Expressway-C entry to allow the XSI messages to be retrieved to complete the remote teleworker location selection process.



CHAPTER 13

Configure Cisco Emergency Responder Onsite Alerts

Cisco Emergency Responder Onsite Alerts

In this feature, Emergency Responder provides information about the emergency call as Onsite Alerts or notifications.

When someone makes an emergency call (that is routed through Cisco Emergency Responder), Cisco Emergency Responder offers the ability route the emergency call to the public safety answering point (PSAP), and provides notification to onsite alert (security) personnel. Notifications to onsite alert personnel are made via IP Phone message, a web-based alert on the Emergency Responder end-user interface, and an email message or page if using email-based paging.

Depending on how your administrator sets up your system, you may receive an email alert that provides you with the caller's extension, the time and date of the emergency call, the extension of the caller, the caller's alerting name, the ERL name, and the phone location. You can choose to either view a specific emergency call alert (Web Alert) assigned to a particular personnel or all the alerts in that location using the Cisco Emergency Responder User interface.

Onsite Alerts Configuration Task Flow

Use the following task flow to guide you to configure the Cisco Emergency Responder Onsite Alert notifications.

Procedure

	Command or Action	Purpose
Step 1	Configure Users, on page 284	You can add users to the system and then assign them to user groups.
Step 2	Configure Users Groups, on page 285	You can add user groups to the system and assign users and roles to each new user group.

	Command or Action	Purpose
Step 3	Configure Onsite Security Personnel, on page 285	Identify your security or onsite alert personnel whom you can assign to your emergency response locations (ERLs).
Step 4	Configure Default ERL, on page 286	Create emergency response locations (ERLs) to receive onsite alert email notifications for your area.

Configure Users

You can add users to the system and then assign them to user groups. The security levels for new users are determined by which user groups you assign them to.

In Emergency Responder, you can add a user either as a local user or a remote user. Remote users must use their Unified CM credentials or Active Directory credentials for authentication.

You can add users to either the primary and standby servers within a single Emergency Responder group. As access is allowed based on the combination of the user groups defined on the two servers, a user that is defined only on the primary server can log into the backup server.

Before you begin

Develop a list of users for each security level. You must know the user names of all onsite alert personnel, and you should determine who should have access to each of the administration security levels.

Note You can use this procedure to add or remove users. However, you cannot remove the administrative user created at the time of Emergency Responder installation.

Procedure

Step 1 From the Cisco ER Administration web interface, select **User Management** > **User**.

Step 2 Click **Add New User** .

Step 3 Enter the required information in the User Name, Authentication Mode, Password, Confirm Password, and Unified CM Cluster fields.

Step 4 Click **Insert**.

Step 5 Repeat these steps to add additional users. For example, user1, user2.

Step 6 To assign security levels to the new users, you must add them to one or more user groups.

Step 7 Repeat this procedure on the other Emergency Responder server in the Emergency Responder server group.

Note To remove a user from a group, you must remove the user from both the groups in the primary and standby servers.

Configure Users Groups

You can add user groups to the system and assign users and roles to each new user group.

Before you begin

You should decide what additional user groups that you want to create and determine if any existing default user groups meet your needs.

Procedure

Step 1 From the Cisco ER Administration web interface, select **User Management** > **User Group**.

Step 2 Click **Add New User Group**.

Step 3 Enter the **User Group Name** (required) and **Description** (optional) in the text boxes.

Step 4 Click **Add Users**.

Step 5 Enter search criteria to find a specific user and click **Find**, or click **Find** without any search criteria to display all configured users. The search results appear.

Step 6 Check the check box to the left of the user names to be added and click **Add**.

The User Name page closes and the added names appears in the **Add Users to Group** text box in the Add User Group page.

Note To delete users from this list, select the user name and click **Remove Users**.

Step 7 Click **Add Roles**.

Step 8 Enter search criteria to find a specific role and click **Find**, or click **Find** without any search criteria to display all configured roles. The search results appear.

Step 9 Check the check box to the left of the roles to be added and click **Add**.

The Role Names page closes and the added roles appear in the **Add Roles to Group** text box in the Add User Group page.

Note To delete roles from this list, select the user name and click **Delete Roles**.

Step 10 Click **Insert** to add the new user group to the system.

Configure Onsite Security Personnel

You must identify your security, or onsite alert personnel so that you can assign them to your Emergency Response locations (ERLs). If an emergency call is made from an ERL, the associated onsite alert personnel receive the following:

- A web-based alert on the Cisco Emergency Responder end-user interface specific to emergency calls originating from the assigned ERL. They also can view all alerts in the system.
- An email message. If you use an email-based paging address, the message results in a page.
- A telephone call indicating that an emergency call was made.

In case an Onsite Security personnel is managing multiple sites (Emergency Response Locations); the Onsite Security personnel can configure Emergency Responder to get alerts from all the ERLs or only from specific ERL.

Before you begin

- You must log into Emergency Responder with system administrator or ERL administrator authority.
- Collect information about all of your onsite alert personnel, including names, telephone numbers, and email addresses. Also, develop a unique identification name for each, if you do not already have one readily available (such as badge number).

Procedure

Step 1 From the Cisco ER Administration web interface, select **ERL > Onsite Alert Settings**.

Step 2 Enter the unique ID, name, telephone number, email address, and pager address, and available User Group of a security or onsite alert person.

Unique ID might be a badge number, email name, or other site-specific unique name. You use this ID to assign the person to an ERL, so ensure that you use a naming strategy useful to you.

You can use an email-based paging address for the email address, so that onsite alert personnel receive a page rather than an email.

Step 3 Click **Insert**.

Emergency Responder adds the person to the list of onsite personnel. Repeat until you define all security or onsite personnel.

Tip

- To delete a person, first remove the person from all ERL definitions. Then, in the Available Onsite Alerts list on the Onsite Alerts Settings page, click the **Delete** icon corresponding to that person's record.
- To modify onsite alert settings, click on the person's Onsite Alert ID, Onsite Alert Name, Onsite Alert Number, Onsite Alert Email Address, or Onsite Alert Pager Address in the Available Onsite Alerts list. The information for that person displays in the 'Modify Onsite Alert Contact' section of the page. Modify the information as needed and then click **Update**. You cannot change a person's Onsite Alert ID: to change the Onsite Alert ID, delete the person's entry and create a new one.

Configure Default ERL

In addition to supporting switch port-based ERLs, Emergency Responder supports IP subnet-based (Layer 3) ERLs. You can configure IP subnets and assign ERLs to the configured IP subnets; Cisco Emergency Responder then routes the emergency calls based on the configured IP subnet and ERL associations.

This feature is useful in environments where strict IP addressing rules are followed and cubicle-level location is not required, such as configurations with wireless phones.

Note Subnet-based tracking is limited by the IP subnet addressing plan. It cannot distinguish location within a same IP Subnet.

Note From Release 15SU1 onwards, Emergency Responder also supports IPv6 Subnets. Any specific reference to IP Subnets should be understood to mean either IPv4 or IPv6 Subnets.

Before you begin

You must have a system administrator or ERL administrator authority to access this page.

Procedure

Step 1 From Cisco ER Administration web interface, select **ERL Membership** > **IP Subnets**.

Step 2 In the Find and List IPv4 and IPv6 Subnets page, click **Add New IPv4 Subnet or Add New IPv6 Subnet**.

Step 3 At the Subnet ID field, enter the IP address of the IPv4 or IPv6 subnet that you want to define. For example,the subnet ID for IPv4 is 10.76.35.0. For IPv6, subnet ID can be a normal IPv6 address or a wildcard IPv6 address like :: which is equivalent to 0:0:0:0:0:0:0:0.

Step 4 For IPv4 subnet, enter the mask of the subnet that you want to define, for example, 255.255.255.224 at the Subnet Mask field. For IPv6 subnet, enter a prefix length (mandatory, the range is 1 to 128) for the subnet.

Step 5 In the ERL Name, enter a name for the specific ERL site.

Step 6 To select the ERL you want to assign to the subnet, click the **Search ERL** button next to the ERL Name field. The Find ERL page appears.

Step 7 Enter the ERL Search Parameters and click **Find**. The search results appear.

Step 8 Click the radio button next to the ERL that you want to assign to the subnet and click **Select ERL**. The Find ERL page closes.

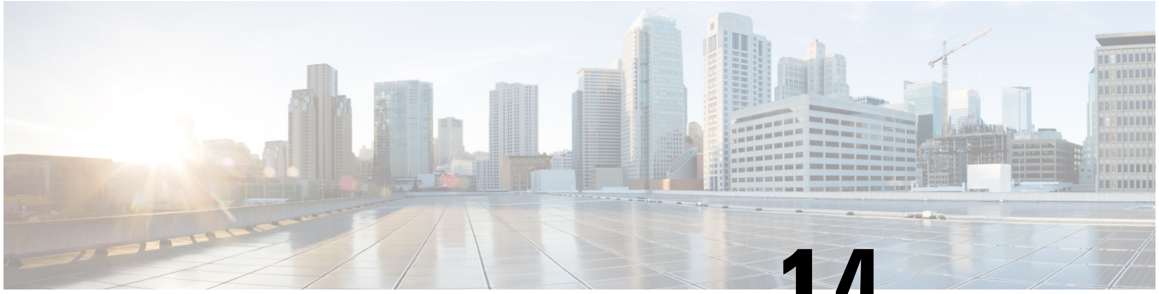
Step 9 Click **Insert** to add the subnet.

A pop-up message requests that you perform a switch port update. You can do this after all the IP subnets have been added.

Step 10 To revert back to the last saved settings, click **Cancel Changes**.

Onsite Alerts Email Example

```
EMERGENCY CALL DETAILS (Generated by CiscoER)
Caller Extension : 7975
Display Name : Test Phone
Zone/ERL : TestERL
Location :
Port Description :
Call Time : May 13, 2019 10:38:31 AM EDT
For detailed call information please refer to --  http://TestCERServer/ceruser
Emergency call Details Caller Extension:7975 Display Name :Test Phone Zone/ERL :TestERL
LOCATION : Port Description : Call Time : May 13, 2019 10:38:31 AM EDT
```



CHAPTER 14

Configure Emergency Responder and National E911 Service Provider

National E911 Service Provider Integration with Emergency Responder—Overview

Important Although Emergency Responder uses the name National E911 Service Provider for all configuration tasks, both the RedSky and Intrado National E911 Service Providers are approved 3rd party National Emergency Calling Service Provider with Emergency Responder. From Release 14SU2 onwards, any specific reference to National E911 Service Provider should be understood to mean either National E911 Service Provider, depending on your chosen provider. Also, PKCS12 format is no longer supported from 14SU2 release onwards.

E911 comprises of two parts: Location Conveyance and Call Completion. Cisco Emergency Responder (Emergency Responder) integrates with National E911 Service Provider like National E911 Service Provider for automated Location update, MSAG (Master Street Address Guide) for a User input location and Call Completion. For location with visibility on infrastructure (On-premises), Emergency Responder can send automated ERL-ELIN information or updates to National E911 Service Provider. For location where there is no visibility on associated infrastructure (Off-premises), Emergency Responder can help send user input location against User DID to National E911 Service Provider.

Emergency Responder automatically finds and tracks the dispatchable locations of all your devices as they move throughout the enterprise so you can comply with E911 regulations.

Emergency Responder tracks Cisco IP Phones through Switch Port or Access Point or IP Subnet or Manually configured. Emergency Responder maintains the status of the phones (On-premises, Off-premises, unlocated), and passes on any ALI or ELIN information to National E911 Service Provider. Phone users rely on Unified CM to route their emergency calls to National E911 Service Provider and the designated emergency provider.

For Off-premises phones, if the user's phones current location has not been previously defined, the user is directed to the Emergency Responder Off-Premises User web page to create a new location. After the new location has been defined and the address has been validated, emergency calls placed from off-premises phones will then be completed through the National E911 Service Provider.

Note RedSky/Intrado Integration is supported when Emergency Responder system is enabled in FIPS mode.

Set Up and Test National E911 Service Provider Connectivity

After you have received confirmation that your company's emergency service account has been created with National E911 Service Provider, you must configure Emergency Responder to communicate with the National E911 Service Provider service for On-premises or Off-premises phones.

You must complete the tasks described in the following procedure before creating National E911 Service Provider ERLs.

Important Although Emergency Responder uses the name National E911 Service Provider for all configuration tasks, both National E911 Service Provider are approved 3rd party National Emergency Calling Service Provider with Emergency Responder. Any specific reference to National E911 Service Provider should be understood to mean either National E911 Service Provider, depending on your chosen provider.

Note You must configure the IP address of the DNS server to resolve the URLs provided by National E911 Service Provider before completing these tasks. See Cisco Unified Operating System Administration Web Interface for Emergency Responder.

Procedure

Step 1 Configure the following items in the National E911 Service Provider VUI Settings page:

- Upload the certificate provided by National E911 Service Provider.
- Validate the certificate.
- Configure National E911 Service Provider Account Information.

Step 2 Configure Route Patterns for routing calls to National E911 Service Provider on the Emergency Responder server.

Step 3 Configure Route Patterns and gateway for routing calls to National E911 Service Provider on Unified CM server.

Step 4 Create National E911 Service Provider ERL and verify the validity and consistency of the ALI data in the National E911 Service Provider database.

Step 5 Assign National E911 Service Provider ERL to the phones discovered under IP subnet.

Configure Emergency Responder for National E911 Service Provider Integration

Use the following workflow to guide you through the setup of your National E911 Service Provider feature.

Procedure

	Command or Action	Purpose
Step 1	Set Up National E911 Service Provider VUI Settings, on page 291	Keep the account information and a certificate from National E911 Service Provider handy before you configure the National E911 Service Provider VUI Settings.
Step 2	Set Up a National E911 Service Provider Route Pattern, on page 292	Configures the route patterns for routing the call to National E911 Service Provider.

Set Up National E911 Service Provider VUI Settings

Before you can configure National E911 Service Provider VUI settings, you must have your account information and a certificate from National E911 Service Provider.

Note To continue emergency service support when there is a failover to the Emergency Responder subscriber, you must upload the same certificate file to the Emergency Responder subscriber separately.

Note From Release 14SU2 onwards, the only supported certificate extension is .bcfks. A new certificate must be obtained from your National E911 Service Provider and perform the following procedure to upload the new certificate.

Procedure

Step 1 From Emergency Responder, choose **System** > National E911 Service Provider **VUI Settings**.

Step 2 Click **Upload Certificate**.

Step 3 Use the **Browse** button to locate the National E911 Service Provider certificate file, highlight the file, and click the **Upload** button.

Step 4 Enter the **Certificate Password** and the **VUI URL** specified by the provider.

Step 5 Click **Test and Validate**.

A successful result means Emergency Responder was able to establish a secure connection to National E911 Service Provider's location update service.

Step 6 Check the **Enable HTTP Proxy** check box if you want to use a proxy server for requests between Emergency Responder and National E911 Service Provider.

Step 7 Enter the **Proxy Host Name/IP Address** of the proxy server, along with the port.

Step 8 Check the **Authentication needed on HTTP Proxy** check box if you want to communicate with the National E911 Service Provider using authentication based proxy server. If you enable this check box, only then the **Proxy User Name** and **Proxy Password** fields are enabled.

Step 9 Enter the configured user name for proxy server in the **Proxy User Name** field and the **Proxy Password** associated to the username.

Step 10 Click the **Test and Validate Certificate** button to test the validity of your certificate.

Step 11 Enter the Account Information.

- VUI Schema URL
- National E911 Service Provider Account ID
- Set MyE911 for location Updates: **True**

Note In case the remote users are not updating their locations using MyE911 or Remote Location Manager when Off-premises, set the **MyE911 for Location Updates** flag to **False**.

Step 12 Click **Test Connectivity** to verify whether Emergency Responder can successfully connect to the customer-specific account through the National E911 Service Provider VUI.

On the 'Test National E911 Service Provider Connectivity' pop-up window, the Test Results section should show status "200 OK" after pressing the **Connect** button. This response indicates that both the certificate and account information are valid. If the above steps are successful, then the National E911 Service Provider related features like National E911 Service Provider ERL and Off-Premise ERL are now unlocked.

For more information about the National E911 Service Provider VUI settings, see National E911 Service Provider VUI Settings, on page 386.

Set Up a National E911 Service Provider Route Pattern

Before any emergency calls can be completed by National E911 Service Provider, you must configure at least one route pattern for routing emergency calls to National E911 Service Provider. Since all emergency calls that are routed to a National Emergency Calling Service provider use the same path, only 1 National E911 Service Provider route pattern is needed. Connection redundancy is accomplished through Unified CM route list and route group configuration, so defining additional National E911 Service Provider route patterns is not required.

Procedure

Step 1 From Cisco ER Administration, choose **System** > **Telephony Settings**.

Step 2 Under National E911 Service Provider Route Pattern Settings, enter the National E911 Service Provider Route/Translation Pattern and click the **Add** button.

Configure Emergency Responder and Unified CM for National E911 Service Provider Integration for On-premises Phones

Use the following workflow to guide you through the setup of your National E911 Service Provider feature for On-premises devices after you have confirmed your emergency service support with National E911 Service Provider.

Procedure

	Command or Action	Purpose
Step 1	Set Up National E911 Service Provider ERLs, on page 293	Configures the ERLs for National E911 Service Provider.
Step 2	Add Scheduled National E911 Service Provider Updates, on page 294	Creates ALI and Secondary Status update schedules between Emergency Responder and National E911 Service Provider.
Step 3	Update Scheduled National E911 Service Provider Update, on page 295	In case, you want to update the schedules, peform this task.

Set Up National E911 Service Provider ERLs

Before you begin

You must first configure National E911 Service Provider route patterns before you can add any National E911 Service Provider ERLs.

Note National E911 Service Provider ERLs differ from conventional ERLs in the following ways:

- You can only select route patterns from a preconfigured list in the Telephony Settings web page.
- You can query and validate ALI data from National E911 Service Provider by using National E911 Service Provider VUI (Validation & Update interface).
- You must submit ALI data (TN Update) to National E911 Service Provider by using National E911 Service Provider VUI before an emergency call can be successfully routed.

Procedure

Step 1 From Emergency Responder, choose **ERL** > National E911 Service Provider **ERL** > National E911 Service Provider **ERL (Search and List)**.

Step 2 Click the **Add New ERL** button.
Emergency Responder opens the Add New ERL window. See Find National E911 Service Provider ERL for a detail explanation of each field.

Step 3 Fill in the ERL Information.

Step 4 Click **ALI Details**.
Emergency Responder opens the ALI Information window.

Step 5 Enter the ALI Information. The "ALI Information section", Cisco Emergency Responder Administration Web Interface Appendix A, contains detailed explanations of each field.

Note To help match Emergency Responder ERL names with the corresponding National E911 Service Provider Location entry, fill in the **Comments** field of the ALI record with the ERL Name.

Note The ALI Location field must be less than 20 characters to be accepted by National E911 Service Provider. All entries longer than 20 characters is rejected.

Note **Query from** National E911 Service Provider is not supported with RedSky.

Step 6 After entering the ALI Information, make the Add New ERL window the active window if it is not, and click **Insert**.

Emergency Responder saves the ERL and its ALI to the local database.

Note **Level of service** is not supported for RedSky.

What to do next

Important In case you have existing ERLs and need to migrate the existing conventional ERLs to National E911 Service Provider ERLs and vice versa, use the **ERL Migration Tool** page to migrate the ERLs.

Add Scheduled National E911 Service Provider Updates

To ensure consistency between Emergency Responder’s National E911 Service Provider ERL’s and the National Emergency Calling Service Provider, you can create ALI and Secondary Status update schedules between Emergency Responder and National E911 Service Provider. A scheduled ALI update sends newly created TN records to National E911 Service Provider. A scheduled Secondary Status update sends queries to National E911 Service Provider requesting information about records with errors that have been corrected.

Procedure

Step 1 Choose **ERL** > National E911 Service Provider **ERL** > National E911 Service Provider **Schedule** from Emergency Responder.

Step 2 Choose the days of the week and the time of day that you want to schedule an update.

Step 3 Check the **Enable Schedule** check box if you want to activate this schedule.

Step 4 Choose either **ALI Update Schedule** or **Secondary Status Update Schedule**.

Step 5 Click **Add** to add the schedule to the list of schedules.

Update Scheduled National E911 Service Provider Update

Procedure

Step 1 From Emergency Responder, choose **ERL**National E911 Service Provider **ERL**National E911 Service Provider **Schedule**.

Step 2 Click the **Edit** link adjacent to the schedule that you want to update.

Step 3 Choose the days of the week and the time of day.

Step 4 Check the **Enable Schedule** check box to activate this schedule.

Step 5 Click **Update** to change the schedule on the list of schedules.

Emergency Responder should be configured using traditional tracking methods and the ERL/ELIN will be delivered to National E911 Service Provider over the customer defined transport (SIP or PRI). Basically, by selecting the National E911 Service Provider, ERL sends the call to National E911 Service Provider.

Configure Emergency Responder and Unified CM for National E911 Service Provider Integration for Off-premises Users

Use the following workflow to guide you through the setup of your National E911 Service Provider feature for Off-premises users after you have confirmed your emergency service support with National E911 Service Provider.

Procedure

	Command or Action	Purpose
Step 1	Verify Off-Premises MyE911 Service Settings , on page 296	Ensure that the National E911 Service Provider VUI configuration settings has the **MyE911 for Location Updates** flag set to **True**.
Step 2	Set Up National E911 Service Provider Off-Premise ERLs, on page 296	Ensure to configure National E911 Service Provider route patterns before you can add the National E911 Service Provider Off-Premise ERLs.
Step 3	Configure a Phone, on page 297	Create or update a device in Unified CM for off-premise.

	Command or Action	Purpose
Step 4	Associate Devices to End User, on page 298	Associates the phone or device to an end user.
Step 5	Configure IP Subnet for Off-Premise Users in Emergency Responder, on page 298	Defines the IP subnet for off-premise phone and associated ERL.
Step 6	Instruct Users to Set and Configure Remote Teleworker Emergency Calling For Off-Premises Locations, on page 298	Off-premises phone users need to add locations and associate their devices to those locations.

Verify Off-Premises MyE911 Service Settings

When Emergency Responder is integrated with a National Emergency Calling Service Provider like National E911 Service Provider and remote users will be using an application to set their location, Cisco Emergency Responder must be then configured to pass the calls to the National Provider without the users configuring their location settings in the system. If the remote users are updating their locations using an application connecting National E911 Service Provider (Over the Top), Emergency Responder must be configured to pass the calls from those users directly to the National Service Provider by configuring the **MyE911 Location Updates** option. For example, applications that can set the off-premise location of a user are National E911 Service Provider MyE911, National E911 Service Provider Remote Location Manager, and Cisco Webex App.

Procedure

Step 1 From Cisco ER Administration page, navigate to **System** > National E911 Service Provider **VUI Settings**.

Step 2 Set the **MyE911 for Location Updates** drop-down to **True** if Cisco Jabber and Webex App are using MyE911 or Remote Location Manager to set the users location when Off-premises.

Note In case the remote users are not updating their locations using MyE911 or Remote Location Manager to set the users location when Off-premises, set the flag to **False**.

Set Up National E911 Service Provider Off-Premise ERLs

You must first configure National E911 Service Provider route patterns before you can add any National E911 Service Provider ERLs.

Procedure

Step 1 From Emergency Responder, choose **ERL** > National E911 Service Provider **ERL** > **Off-Premises ERL (Search and List)**.

Step 2 Click the **Add New ERL** button.

Emergency Responder opens the Add New ERL window. See Off-Premises ERL, on page 407 for a detail explanation of each field.

Step 3 Fill in the ERL **Name** and **Description** Information.

Step 4 Select the Route/Translation Pattern defined for reaching National E911 Service Provider and any user that should be notified when an Off-premises call has been placed.

Note When configuration the Off-Premises ERL, there is no option to set an ELIN. This is because the calling party number is the calling party's number. By passing the user's calling party, National E911 Service Provider can uniquely identify the caller and their specific location.

Note **Query from** National E911 Service Provider is not supported with RedSky.

Step 5 Click **Insert**.

Note **Level of service** is not supported for RedSky.

Configure a Phone

Perform these steps to update a phone to in Unified Communications Manager to send the location selection service to phones when they are Off-premise.

Note This setting is only applicable to Cisco IP Phones. Soft clients (like Cisco Jabber and Webex App) cannot use this procedure.

Procedure

Step 1 From Cisco Unified CM Administration interface, select the phone that is Off-premise.

Step 2 In the Device Information section, select the **Owner** as **User** and set the **Owner User ID** to the user that this device is assigned to.

Step 3 In the Phone Configuration window, check the **Require off-premise location** option to activate the device for off-premises location check upon registration. Off-premises location check is required to determine if the phone is off-premise and the user must select a location before allowing outbound calls.

Step 4 Click **Save**.

Step 5 In the Association area, click Line [1]-**Directory Number**.

Note Extensions may be longer than 10 digits, but a leading + is not currently supported by Emergency Responder.

Step 6 Configure the external phone number mask to ensure that the directory number defined on the line will be a fully qualified 10-digit E.164 number after the mask is applied.

Note The phone number mask must contain at least 1 X to be valid.

Step 7 Click **Save** and on the phone page, click **Apply Configuration**.

Note Ensure that the status of the configured phone is in the Registered state.

Associate Devices to End User

Any user with devices that will be using the Off-premises feature must be defined in Unified CM with the devices that are assigned to the user. All devices should be associated with the user on both the Owner ID field and in the End User page as Controlled Devices.

Procedure

Step 1 From Cisco Unified CM Administration, choose **User Management > End User** menu option to find the end user.

Step 2 In the Device Information pane, click **Device Association**.

Step 3 To find all records in the database, Click **Find**.

Step 4 From the Device association for (this user) pane, choose the devices that you want to associate with this end user by checking the box to the left of the device names.

Use the buttons at the bottom of the window to select and deselect devices to associate with the end user.

Step 5 Repeat the preceding steps for each device that you want to assign to the end user.

Step 6 To complete the association, click **Save Selected/Changes**.

Configure IP Subnet for Off-Premise Users in Emergency Responder

Use the Configure IP Subnet page to define an IP Subnet for devices that are Off-premise. The IP Subnet should be the IP Address of the Expressway-C inside address or the IP Subnet of a VPN concentrator for client VPN session or Hardware VPN solutions.

Procedure

Step 1 From Cisco ER Administration, choose **ERL Membership** > **IP subnets** and click **Add new IP subnet**.

Step 2 Enter the Subnet ID and Mask details.

Step 3 Click **Search ERL** to select the ERL you want to assign to the subnet.

Step 4 In the ERL Search Parameters, set the find value to **Off-Premise ERL** and click **Find**.

Step 5 Click the radio button next to the Off-Premises ERL (defined previously) and click **Select ERL**.

Step 6 Click **Insert** to add the subnet on the **Configure IP Subnet** page.

Instruct Users to Set and Configure Remote Teleworker Emergency Calling For Off-Premises Locations

Add New Location

Before a user can associate a location to their phone or device, the user must first enter a location into Emergency Responder’s Off-Premises User Page. All locations defined in Emergency Responder are user-specific. Each user must add their own locations. When a user has multiple locations, each location must have a unique name to identify that unique location.

Procedure

Step 1 Log in to the Cisco Emergency Responder Off-Premises User page at **https://<CER_FQDN>/ofpuser** using the end user credentials.

Note Emergency Responder Off-Premises User page does not support SSO logins.

Step 2 From the Cisco Emergency Responder Off-Premises User page, select **Locations** and click **Add New Locations**.

Enter a valid address. The location name will be used to identify this address when you associate your phone with this address.

Step 3 Click **Validate** to verify the address with your National Provider.

Step 4 If the address validation fails, the user must correct the address before saving the location.

Step 5 Click **Save** to save the location information in Emergency Responder.

Note Saving the location does not immediately update the National Emergency Calling Service Provider, but stores the location information in Emergency Responder. When a user selects the location from the device, the stored address information is sent to the National Provider to update the address for the user’s E.164 number.

Associate Your Location to Your Phone

After a user defines a location in Emergency Responder, the user should associate and verify that the device is associated to the desired location.

Procedure

Step 1 From the Cisco Emergency Responder Off-Premises User page, choose **Phones**.

Step 2 To associate a location to a phone, click the corresponding **Assign** link.

Note If there are multiple devices, it does not matter which assign link you select since all of them will associate the address to the DID number listed.

Step 3 In the Associate Location page, select the desired location from the **Select New Location** drop-down list. The new location becomes active when you click the **Associate Location** button.

The Status field show displays that the “Location Association Is Successful.” This indicates that the address is valid and has been updated with the National Emergency Calling Service Provider.

Step 4 Once the location is associated, the device on the Phones page should display devices that are registered with an IP address that is considered off-premise with a status as **Off Premises** and the Associated Location should match the one that was selected. Additionally, ensure that the Direct Inward Dial (DID) is a properly formatted 10-digit NANP number.

Verify the Remote Teleworker Off-Premises Locations in Emergency Responder

Note If the remote or Off-premises user chooses not to update their current location, the Disclaimer prompts the user to acknowledge that calls may be restricted until the location is updated. Outbound calls and 911 calls will not work until the user associates their device to a configured location.

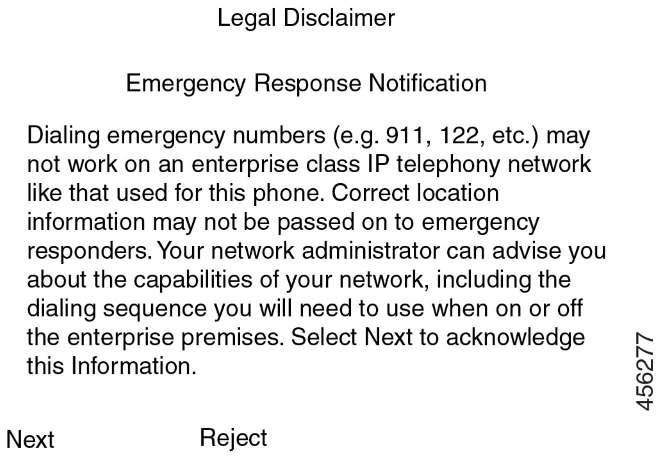
As the System Administrator, you can configure to select and mandate location update so that the device user has to acknowledge the disclaimer and provide current location information before the device is enabled for normal use. (From Cisco Unified CM Administration, choose **System** > **E911 Messages** to configure the mandatory location update disclaimer message.)

Procedure

Step 1 Reset the phone or device.

After the phone has rebooted and after 2-5 seconds after registering, the device should display the Remote Teleworker legal notification. At this point, the remote teleworker location selection process should start.

Step 2 Ensure that the following legal disclaimer message appears on the phone.



Legal Disclaimer

Emergency Response Notification

Dialing emergency numbers (e.g. 911, 122, etc.) may not work on an enterprise class IP telephony network like that used for this phone. Correct location information may not be passed on to emergency responders. Your network administrator can advise you about the capabilities of your network, including the dialing sequence you will need to use when on or off the enterprise premises. Select Next to acknowledge this Information.

Step 3 Click **Next**.

You will get the details of all the locations added through Cisco Emergency Responder Off-premises URL.

Step 4 Using the toggle buttons on the phone or device, choose a location and press the **Select** button.

A few seconds later, the phones user interface should indicate the successful settings of the off-premises user’s location.

Any error encountered during the setting of the location from the phone must be resolved through Emergency Responders Off-Premises User Page or working with the system administrator.

What to do next

Administrators should instruct the users on how to validate the accuracy of the E911 address based on the user-defined setting. This process should follow the company's procedure for emergency address validation. When a user dials 911 as per the company process for validating the emergency dispatch address, the call should be routed to public-safety answering point (PSAP) using the off-premises ERL and the address reported by the PSAP should be the address currently assigned to the device through the Cisco Emergency Responder Off-Premises User Page.

All calls originating from On-premise devices route the National Emergency Calling Service Provider using the National E911 Service Provider Route/Translation pattern. For On-Premise devices, Emergency Responder sends the ERL for the On-premise location to National E911 Service Provider to reach the correct PSAP for the calling party.

PART IV

Administration

CHAPTER 15

Cisco Emergency Responder Admin Utility

Cisco Emergency Responder Admin Utility Overview

In CiscoEmergencyResponder (Emergency Responder), the Admin Utility is integrated into the Emergency Responder itself. The Admin Utility has its own web interface that you can access from the main Emergency Responder web page. As with the other Emergency Responder administration web interfaces, the Admin Utility web interface is password protected.

Change Cisco Unified Communications Manager Version

Note When the Unified Communications Manager cluster is upgraded, the AXL queueID will change on the publisher node. To re-establish AXL connection after the Unified Communications Manager cluster upgrade, the Emergency Responder administrator must restart the CER Service. Failing to do so may result in the breaking of AXL change notifications between Unified Communications Manager and Emergency Responder.

Procedure

Step 1 Log in to the Emergency Responder Admin Utility web interface.

Step 2 From the main Emergency ResponderAdmin Utility page, select **Update** > **CCM Version**.
The **Upgrade CCM Version** page appears.

Step 3 Select the new version of Unified CM from the **Choose the CCM Version to Upgrade** pull-down menu and click **Go**.

Note You must change the Unified Communications Manager version separately for the Publisher and Subscriber nodes.

The Status area of the **Upgrade CCM Version** page displays the new version number after the system makes the change.

Update Emergency Responder Cluster Database Host Details

By default, each server in a cluster considers its own database to be the cluster database host. Because each cluster should have only one database host, you must update the cluster configuration accordingly.

For example, if you have two server groups (ServergroupA and ServergroupB), each containing a Publisher and a Subscriber, you would do the following to update the cluster database host details:

1. Update the cluster database host password for ServergroupA using ServergroupA's own host name.
2. Update the cluster database host password for ServergroupB by entering the IP address and cluster database password for ServergroupA.
3. Repeat Step2 for other server groups in the cluster.

Note If you use hostnames, then the hostname must be resolvable using DNS. If DNS is not configured or DNS is unavailable for any reason, hostname resolution fails and cluster functionality is impaired. It is recommended that the DNS configuration include redundant entries to prevent unavailability. Alternatively, the IP address of the cluster database host can be configured on this screen. The hostname can begin with a numeric value.

Note This procedure only updates the Emergency Responder Cluster DB host details for this server group. Other servers in this Emergency Responder cluster do not updated automatically.

Before you begin

You must reboot the server to update Emergency Responder Cluster DB host details. Only restarting Emergency Responder services does not work because the IP address is cached by other services.

Procedure

Step 1 Log in to the **Emergency Responder Admin Utility** web interface.

Step 2 Select **Update > Cluster DBHost** from the main **Emergency ResponderAdmin Utility** page.
The **Update Cluster DB Host** page appears.

Step 3 Enter the new Cluster DBHost name (if DNS is configured) or IP address in the text box. If the cluster is spread across domains, enter a fully qualified host name.

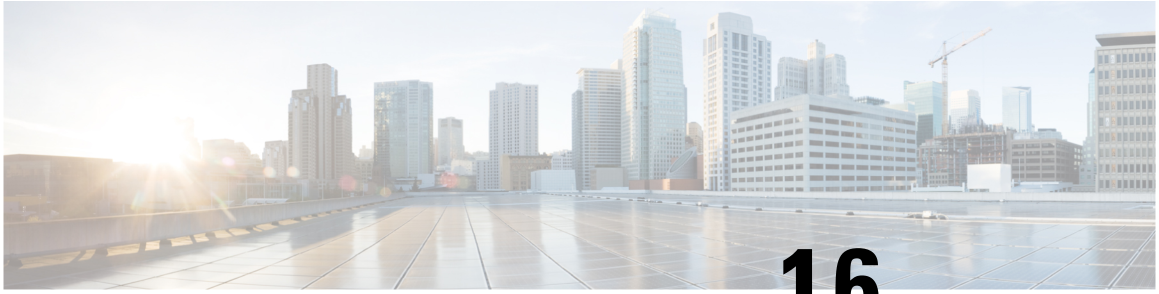
Step 4 Enter the password for the new Cluster DBHost in the **Password** text box.

Step 5 Reenter the password for the new Cluster DBHost in the **Confirm Password** text box.

Step 6 Click **Go**.

Related Topics

Update Cluster DB Host, on page 574



CHAPTER 16

Cisco Emergency Responder User Preparation

Cisco Emergency Responder User Preparation Overview

This chapter describes the various roles for CiscoEmergencyResponder (Emergency Responder) users. The topics describe not only the use of the software, but help you understand the larger policy and procedure decisions your organization must make to determine how Emergency Responder fits into your organization's emergency response needs.

Emergency Responder Onsite Alert Personnel Preparations

You probably already have emergency response policies and procedures in place. Consider how CiscoEmergency Responder (Emergency Responder) fits into these policies and procedures, and work with your emergency response teams (onsite alert or security personnel) to update these procedures if necessary.

Consider training these personnel on these aspects of Emergency Responder:

- How to use the Emergency Responder web interface. See the Emergency Responder user web interface online help for information about these topics. The online help includes a user's guide in PDF format that you can print out and distribute to your users. The information in the user's guide is the same as the information in the online help. Train users on these areas:
  - How to log into the user web interface.
  - How alerts show up on the screen and how to view specific (if set by the administrator) or all alerts in the system.
  - How to obtain more information about the location of the call. Summary information includes the actual extension of the caller; the ELIN, which is the phone number the PSAP gets as the number of the emergency caller; the phone location associated with the switch port; and the location field of the ALI. Users can also view the entire ALI.

  - How to acknowledge the call and add comments to it. Consider developing rules for these procedures to ensure consistent behavior from your emergency response teams.
  - How to look up emergency calls in the emergency call history.

- Explain how they receive notification of an emergency call.
  - A web alert appears for everyone logged into the Emergency Responder user web interface.
  - All personnel assigned to an ERL receive a telephone call when an emergency call is made from the ERL. The telephone call includes information about the extension of the caller.
  - If you configure email addresses for the personnel, they also receive an email, which includes more information than the phone call, including ERL name and phone location. If the email address is for an email-based pager, they are paged. Paging is the most efficient way of getting information to users who are not at their desks.

    If the standby CiscoEmergency Responder server handles an emergency call, all onsite alert personnel get notified of the call, and of the fact that the standby server handled the call. Decide how you want people to respond to these notifications.

- Explain the ERL naming and phone location you are using. This is the primary information the personnel have for identifying the location of the emergency caller.
- Explain the organization's policy for responding to emergency calls. Work with the emergency response teams to develop an acceptable policy if you do not already have one.

Related Topics

Preparing Your Staff for Emergency Responder , on page 38

Emergency Responder ERL Administrator Role

The following table lists the recurring tasks for which an ERL administrator is responsible. A system administrator can also perform these tasks.

Table 19: Cisco Emergency Responder ERL Administration Recurring Tasks

Recurring Task	Description	More Information
Assign ERLs to new or changed switch ports	If switches are added to the network, or if modules with additional ports are added to existing switches, assign the new ports ERLs.	Switch Port Configuration , on page 159
Create ERLs as required	As your business expands, create new ERLs as required. Work with the telephony administrators to obtain ELINs for the ERLs, and with the network administrator to get the new switches defined in Emergency Responder.	• ERL Creation , on page 138 • Switch Port Configuration , on page

Recurring Task	Description	More Information
Export ALI data and submit to your service provider	If you make changes to ALI data, add or remove ERLs, or change the ELINs assigned to an ERL (for example, by adding or removing them), export the ALI and resubmit it to your service provider.	• Export ERL Information , on pag • Export ALI Information for Subr Your Service Provider , on page • ERL Creation , on page 138 • ALI Submission and Service Pro Requirements , on page 37
Audit the manually defined phones	Regularly check your manual phone definitions to ensure each phone is still assigned to the correct ERL. Work with the telephony administrator to get notification of any adds, moves, or changes that involve these phones. Add phones as required.	• Manually Define Phones , on pag
Audit the unlocated phones list	Regularly audit the unlocated phones list, and work with the network administrator to determine why CiscoEmergency Responder cannot locate the phones and to resolve the problems.	• Identify Unlocated Phones , on p • Unlocated Phones , on page 324
Add new onsite personnel or remove old ones; update phone numbers	As onsite alert personnel are added, define them in CiscoEmergency Responder and assign them to the appropriate ERLs. Likewise, as personnel are removed, remove them from their ERLs and then from CiscoEmergency Responder. Update phone numbers, email address, and other contact information as they change.	• Add Onsite Security Personnel, o • ERL Creation , on page 138
Add IP subnet for the IP subnets to be tracked	If there is a new IP subnet that needs to be discovered by Emergency Responder, then perform the following tasks: • Configure an ERL spanning the new IP subnet's geographical location. • Configure this new IP subnet and the appropriate mask and assign this IP subnet to the created ERL.	• Set Up IP Subnet-based ERLs , o

Related Topics

Phone Management , on page 159

Emergency Responder Network Administrator Role

The following table lists the recurring tasks for which a network administrator is responsible. A system administrator can also perform these tasks.

Table 20: Cisco Emergency Responder Network Administration Recurring Tasks

Recurring Task	Description	More Information
Add new switches	Add any switches that you add to the network to the CiscoEmergency Responder configuration. A switch is considered new if it has an IP address not defined in CiscoEmergency Responder.	• LAN Switch Identification , o 153 • Manually Run the Switch-Por Phone Update Process , on pa
Remove old switches	Remove switches from the CiscoEmergency Responder configuration if you remove them from the network. Nonexistent switches in the CiscoEmergency Responder configuration do not create problems, but they do increase the time required to do phone tracking, because CiscoEmergency Responder attempts to connect to the switch must time out before moving on to the next switch.	• LAN Switch Identification , o 153
Update the SNMP read community if it changes	If you change the read community string on any defined switch, you must update the SNMP settings in CiscoEmergency Responder. Until the setting is updated, CiscoEmergency Responder cannot track phones attached to the switch.	• Set Up SNMPv2, on page 149
Update or remove Unified CM servers	If a Unified CM cluster is added to the network, or one is removed, update the configuration for the CiscoEmergency Responder group that supports the cluster. Although you have the authority to make these updates, your organization might assign the primary responsibility to the CiscoEmergency Responder system administrator.	• Identify Cisco Unified Commu Manager Clusters , on page 1
Check ERL assignments	Use the ERL Debug Tool to check that the correct and expected ERL is used for a selected phone.	• Emergency Responder Admin on page 345

Related Topics

Emergency Responder Switch Configuration , on page 148

Emergency Responder System Administrator Role

The following table lists the recurring tasks for which a system administrator is responsible. A system administrator might also be responsible for some or all of the ERL and network administrators' tasks, as explained in the Emergency Responder ERL Administrator Role , on page 310 and the Emergency Responder Network Administrator Role , on page 311.

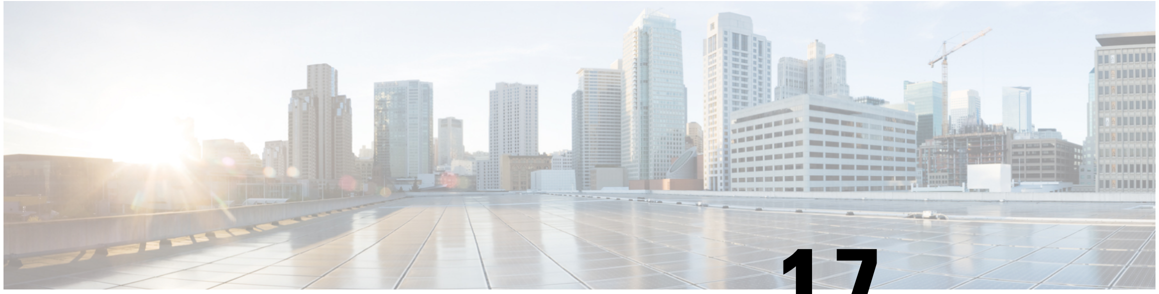
Table 21: Cisco Emergency Responder System Administration Recurring Tasks

Recurring Task	Description	More Information
Add additional CiscoEmergency Responder groups	As telephones are added to the network, you might need additional CiscoEmergency Responder groups. Install and define them and their telephony settings. Work with the telephony administrator to complete the required Unified CM configuration.	• Installation on a New Syste 63 • Set Up a Server Group, on • Set Up Group Telephony S Server , on page 129 • Configure Servers , on pag • Identify Cisco Unified Con Manager Clusters , on page
Monitor the system and troubleshoot any problems	Help resolve any problems that arise. Work with the network and ERL administrators, and the telephony administrator, as appropriate.	
Create new CiscoEmergency Responder users; remove old users	As onsite alert personnel change, or as CiscoEmergency Responder system, network, and ERL administrators change, add or remove them as required.	• Emergency Responder Use , on page 117
Add or remove Unified CM servers	If a Unified CM cluster is added to the network, or one is removed, update the configuration for the CiscoEmergency Responder group that supports the cluster. Although you have the authority to make these updates, your organization might assign the primary responsibility to the CiscoEmergency Responder network administrator.	• Identify Cisco Unified Con Manager Clusters , on page
Monitor the email alerts that CiscoEmergency Responder generates	If your email ID is configured in the server group settings, CiscoEmergency Responder sends email alerts about critical errors to you. You are expected to understand the error and take action to correct the problem. See Troubleshoot Email Alerts , on page 336 for information to help you understand the email alerts and resolve problems.	• Set Up a Server Group, on

Related Topics

Server and Server Group Configuration , on page 128

Troubleshoot Email Alerts , on page 336



CHAPTER 17

ALI Formatting Tool

ALI Formatting Tool Overview

Network engineers, system administrators, and telecommunications engineers should review these topics to learn the steps that are required to use and troubleshoot AFT. You should be familiar with CiscoEmergencyResponder (Emergency Responder) and with CiscoUnifiedCommunicationsManager (Unified CM) before deploying AFT.

Features

Emergency Responder helps you manage emergency calls in your telephony network. Emergency Responder tracks a system's phones and locations and exports this information in ALI records that conform to National Emergency Number Association (NENA) 2.0, 2.1, and 3.0 formats. However, many service providers do not use NENA standards. The AFT allows you to modify the ALI records that you create in Emergency Responder to a format that is compatible with the one used by your service provider. The service provider then uses the reformatted file to update their ALI database.

The AFT reads the ALI file generated by Emergency Responder and displays all the ELIN records on the AFT web page. You can use AFT to:

- Easily view the details of the ALI records. ALI files are difficult to read in the NENA fixed-length format. AFT reads the ALI files and presents the NENA fields in an interface that is easy to read.

- Select a record and update the value for ALI fields. AFT allows you to edit the ALI fields to customize them to meet the requirements of different service providers. Your service provider can then read the reformatted ALI files and use them to update their ELIN records.

- Perform bulk updates on multiple ALI records. Using the bulk update feature, you can apply common changes to all the records that you have selected, to one area code, or to one area code and one city code.

- Selectively export ALI records based on Area Code, City Code or a 4-digit Directory Number. By selecting to export all the ALI records in an Area Code, for example, you can quickly access all the ELIN records for each service provider allowing you to easily support multiple service providers.

File Generation

This section provides information about how to use the ALI Formatting Tool (AFT):

- Using the ALI Formatting Tool Interface
- Using AFT to Generate a Formatted ALI File

ALI Formatting Tool Interface Capabilities

You can edit the following fields using AFT:

- The header and trailer fields. The ALI Formatting Tool (AFT) displays all the ALI record data in the ALI tab. The ALI file consists of one header record and one trailer record only; there is not an individual header and trailer record for each ELIN record.
- The Function/Transaction Code field
- Any service provider-specific fields

You cannot edit the following fields using AFT:

- The ALI records fields that you configure and edit through Emergency Responder. They are disabled in AFT.
- The record count field. This trailer field cannot be edited in AFT because AFT calculates this number internally based on the number of records selected to export.

The following table shows how to use the AFT interface to perform the main AFT tasks.

Table 22: Using the AFT Interface to Perform Main Tasks

Task	Procedure	Notes
Open AFT for your service provider	Go to **Tools > ALI Formatting Tool**. Click the name of your service provider in the pull-down menu.	You must log in to the En Responder Administration with the proper privileges
Give a NENA files as input to AFT	Select an Input File for the AFT from the list of files provided in the pull-down menu.	If no NENA files are liste **Tools > Export PS-ALI** and export a NENA 2.0 f
Go to a specific ELIN number	All ELINs in the NENA file given as input for the AFT are displayed. To narrow down to a specific ELIN, perform an ELIN search.	
View ALI details for an ELIN/Select an ELIN to edit its ALI fields	Each ELIN is a link. Click on the specific ELIN link to see the specific record. The ELIN details appear in the right pane of the screen.	You can then edit the AL by entering new values in editable fields.
Perform a bulk update to the ALI files	Select the ELINs on which you want to perform a bulk update. Click the **Bulk Update** button above the list of ELINs.	

Task	Procedure	Notes
Review Changes	After you make some changes, click the **Review Changes/Generate File** button. A list of all the ELINs that have been changed appears.	Click the **ELIN** link o Changes/Generate File the changed informati
View/Edit Header Record	Select any ELIN on the ALI Record Details for ELIN page and click the **Header Record** link. You can now edit the editable fields of the header record.	Header record is comm ALI file and not per E
View/Edit Trailer Record	Select any ELIN on the ALI Record Details for ELIN page and click the **Trailer Record** link. You can now edit the editable fields of trailer record.	Trailer record is comm ALI file and not per E
Add More ELINs	On the Review Changes/Generate File page, click the **Add More ELIN(s)** button. A list of unchanged ELINs appears. Select the ELINs that you want to keep in the final generated file.	
Remove ELINs	On the Review Changes/Generate File page, select the ELIN to be removed and click the **Remove ELIN(s)** button.	The changes made on are lost and this ELIN the pool of unchanged
Generate Formatted File	On the Review Changes/Generate File page, follow these steps: **1.** Select the ELINs that you want to include in the formatted file. **2.** Enter a Name for the Formatted File to be generated. **3.** Click the **Generate File** Button.	You can download the file after it is successf generated. If you want to downlo later, follow these step **1.** Go to **Tools > Fil Management Uti** **2.** In the search param ALI Formatting T select the service Formatted files ar **3.** Select the formatt click **Download**.

Generate Formatted ALI File

Procedure

Step 1 Provide a NENA 2.0 file generated by Emergency Responder as input to AFT by following these steps:

a) From the Emergency Responder Administration web page, go to **Tools > ALI Formatting Tool**.

b) Click your service provider name in the menu.

c) Select an Input File for the ALI Formatting Tool from the list of files provided in the pull-down menu.

AFT displays all the ELINs from the NENA file.

Step 2 Click on an **ELIN** link to view details of the ALI files. The ALI Record Details for ELIN are populated in the right pane of the screen.

Step 3 Edit the ALI fields by entering new values in the editable fields.

Step 4 Select the ELINs that you want to export to the service provider by clicking in the corresponding check boxes in the left side of the screen.

Step 5 Update the service provider fields in AFT.

For details about the service provider-specific information required, see Using AFT for Specific Service Providers , on page 577

Step 6 At this point, if you want to edit some fields in many ELINs simultaneously, you can use the AFT Bulk Update feature. To do so, follow these steps:

a) Select the ELINs to edit using Bulk Update.
b) Click on the **Bulk Update** button. The Bulk Update form appears.
c) For details about the service provider-specific information required, see Using AFT for Specific Service Providers , on page 577

Step 7 Generate a formatted file by following these steps:

a) Click on the **Review Changes/Generate File** button.

The list of edited ELINs are displayed. You can add unchanged ELINs and remove edited ELINs from the list.

b) Select the ELINs that will be part of the final formatted file and enter the name for the formatted file.
c) Click **Generate File** to generate the file.

AFT generates an ALI file in a format specific to your service provider and prompts you to download the same.

Note Before generating the formatted file, verify the details entered.

Step 8 Using the service provider's preferred method of transmitting files, send the ALI file to your service provider so that they can update their E911 database with the ELINs from the AFT ALI file.

Note Be sure to keep a copy of the AFT ALI file for your records. This is helpful if the service provider reports errors; you can make any required changes to the file without having to re-do all of the AFT formatting changes.

Step 9 Your service provider returns the status of the ALI files.

If your service provider reports that there are no errors, you can continue using AFT to generate more formatted records or you can quit the program.

If your service provider reports that there are ALI errors, follow these steps:

a) Make corrections to the formatted file that you sent to the service provider. All the error codes for the service providers are defined in the ALI format documentation for that service provider. See their documentation to determine the errors in your file and correct the errors using AFT.

Note If an error occurs in fields that cannot be edited using AFT, you must use Emergency Responder to correct the fields. Then use AFT to regenerate the file.

b) Send the corrected file to your service provider. Be sure to keep a copy of your corrected file for your records.
c) Repeat this process until your service provider can read the formatted files and can use them to update their ELIN records.

Related Topics

Convert ALI Data , on page 142

ALI Formatting Tool, on page 484

PART V

Troubleshooting

CHAPTER 18

Troubleshoot Cisco Emergency Responder

Troubleshoot Phone-Related Problems

The following sections help you troubleshoot problems related to assigning phones to ERLs and managing the phones.

Check Unified CM SNMP Settings

If Cisco Emergency Responder (Emergency Responder) is not discovering the phones homing to Cisco Unified Communications Manager (Unified CM), check that all Unified CMs are SNMP-reachable and that the SNMP settings are correct. Emergency Responder logs an event if Unified CM is SNMP-unreachable.

Procedure

Step 1 Log in to the Emergency Responder Administration CLI and use the following command to ping the Unified CM server:

```
utils network ping <ipaddress of CUCM>
```

Step 2 If you successfully ping the Unified CM, verify that the SNMP settings are correct on Unified CM, as follows:

- If you are using a Linux-based version of Unified CM (version 6.0 or higher), log in to the Unified CM Serviceability web interface and use the SNMP web pages to check the SNMP community string settings.
- If you are using a Windows-based version of Unified CM, open the services on Unified CM and choose **Start** > **Settings** > **Control Panel** > **Administrative Tools** > **Services Properties** > **SNMP** > **Properties** > **Security Tab**.

Step 3 Check to see if Unified CM is SNMP reachable by running the following CLI command on the Emergency Responder server:

```
utils snmp get <ccm ip-address/host name> <snmp-read-community-string> 1.3.6.1.2.1.1.2.0
```

If the Unified CM is SNMP reachable, then the output of the preceding command should be similar to the following:

```
Variable = 1.3.6.1.2.1.1.2.0

value = OBJECT IDENTIFIER <sys-oid-of-ccm>
```

Unlocated Phones

Emergency Responder obtains a list of registered phones from Unified CM and tries to locate all phones. If Emergency Responder cannot locate a phone behind a switch port or in any configured IP subnets, and the phone is not a configured synthetic phone, the phone is placed in the list of unlocated phones.

If there are a lot of unlocated phones, first try running the switch port and phone update process to see if Emergency Responder can resolve some of the problems automatically. See Manually Run the Switch-Port and Phone Update Process , on page 157 for more information.

These are some of the situations that can prevent Emergency Responder from locating a phone:

- If more than one switch port reports the phone as a Cisco Discovery Protocol (CDP) neighbor, then the phone is placed in unlocated phones. This condition is corrected in the next phone tracking when only one switch port reports this phone as its CDP neighbor.
- The phone is attached to a switch that is not defined in Emergency Responder. See LAN Switch Identification , on page 153 for information about defining switches.
- The phone is connected to an unsupported device, such as a router port, a hub connected to a router, or an unsupported switch. See Network Hardware and Software Requirements , on page 10 for a list of supported switches. See Manually Define Phones , on page 168 for information about configuring these types of phones if you cannot connect them to a supported device.
- The phone is connected to a hub, which is connected to a supported switch port, but it does not support CDP. Emergency Responder can consistently discover CDP-enabled phones attached to hubs (which are

attached to supported switch ports), but cannot always track non-CDP phones attached in this manner. For non-CDP phones, ensure the phones are attached directly to supported switch ports.

- The switch to which the phone is connected is currently unreachable, for example, it does not respond to SNMP queries. This could be for several reasons:
    - The SNMP read community string on the switch does not match the string configured in Emergency Responder. Correct the Emergency Responder configuration. See Set Up SNMPv2, on page 149.
    - The phone requires CAM table access, but CAM tracking is not enabled for the switch in Emergency Responder. See LAN Switch Identification , on page 153.
    - There is a network outage preventing communication between the Emergency Responder server and the switch. Locate and resolve the network outage problem.

      Unreachable switches are not retried until Emergency Responder runs the next full switch port and phone update process, unless you run it against the individual switch.

- The phone has moved to a switch served by a different Emergency Responder group. If this is the case, the Emergency Responder group name is shown for the phone in the unlocated phones list. If the phone is not in the next incremental phone tracking process after it is moved, the phone remains unlocated in any Emergency Responder group until a full switch port and phone update process is run.
- The phone requires CAM-based tracking, but CAM-based tracking is not enabled on the switch to which the phone is connected. Cisco IP SoftPhone and some other phone models require CAM-based tracking. See LAN Switch Identification , on page 153 for information about enabling CAM-based tracking, and Network Hardware and Software Requirements , on page 10 for a list of phones that require CAM-based tracking.

After fixing the problems that are preventing Emergency Responder from locating phones, run the switch port and phone update process on the affected switches, or on all switches:

- To run the process on a specific switch—Select **Phone Tracking** > **LAN Switch Details** and select the switch in the left-hand column; then click **Locate Switch Ports**.
- To run the process on all switches—Select **Phone Tracking** > **Run Switch-Port & Phone Update**.

Related Topics

Identify Unlocated Phones , on page 167

IP Subnet Phones, on page 452

Cisco Unified OS CLI Commands

Phones Not Located with SMNPv3

Check if the SNMP V3 settings on the **SNMPv3** page match the Cisco Unified Communications Manager settings on the **Serviceability** page. Select **Phone Tracking** > **SNMP V3 Settings**. For more information, see Set Up SNMPv3 , on page 151.

Check if the **Use SNMP V3 for Discovery** check box is enabled on the **LAN Switch Details** page. Select **Phone Tracking** > **Cisco Unified Communications Manager** and **Phone Tracking** > **LAN Switch Details**
.

Check if the Unified Communications Manager and switch added in Emergency Responder are SNMP reachable by executing a **SNMP Walk** command. Use the CLI and follow one of these examples:

- `snmpwalk -v3 <CUCM IP Address> -u <USERNAME> -l AuthPriv -a <AUTH PROTOCOL> -A <AUTH PASSWORD> -x <PRIVACY PROTOCOL> -X <PRIVACY PWD> 1.3.6.1.4.1.9.9.156.1.1.2.1.7`
- `snmpwalk -v3 <CUCM IP Address> -u <USERNAME> -l AuthNoPriv -a <AUTH PROTOCOL> -A <AUTH PASSWORD> 1.3.6.1.4.1.9.9.156.1.1.2.1.7`
- `snmpwalk -v3 <CUCM IP Address> -u <USERNAME> -lNoAuthNoPriv 1.3.6.1.4.1.9.9.156.1.1.2.1.7`
- `snmpwalk -v3 <SWITCH IP Address> -u <USERNAME> -lAuthPriv-a <AUTH PROTOCOL> -A <AUTH PASSWORD> -x <PRIVACY PROTOCOL> -X <PRIVACY PWD> 1.3.6.1.4.1.9.9.23.1.2.1.1.3`
- `snmpwalk -v3 <SWITCH IP Address> -u <USERNAME> -lAuthNoPriv-a <AUTH PROTOCOL> -A <AUTH PASSWORD> 1.3.6.1.4.1.9.9.23.1.2.1.1.3`
- `snmpwalk -v3 <SWITCH IP Address> -u <USERNAME> -lNoAuthNoPriv1.3.6.1.4.1.9.9.23.1.2.1.1.3`

If you notice a SNMPReqTimeOut or SNMP Unreachable issue in the event logs or the phone tracking logs, then increase the Timeout and Maximum Retry Attempts value under **Phone Tracking > SNMP V3 Settings** page and run a Major Discovery.

If the issue continues, then try the following:

1. Log in to Cisco Emergency Responder from CLI and enter the **command utils network capture eth0 file** <"filename"> **count 10000 size ALL port 161**.
2. Navigate to **Phone Tracking > Run Switch-Port & Phone Update** and run a Major Discovery.
3. When the Major Discovery is completed, stop the CLI command by pressing **CTRL-C**.
4. Download the packet capture file. The packet capture files will be stored in `activelog platform/cli/` location on the server. You can transfer the files through CLI to an SFTP server using the command **file get activelog platform/cli/packets.cap**. Alternatively to collect all .cap files stored on the server, use ‘file get activelog platform/cli/*.cap’. See the Command Reference guide for more information.

   Open it and examine the file for the error codes; take the appropriate actions, if needed.

Table 23: Common Error Messages

SL No	Error message	Occurrence
1	usmStatsUnsupportedSecurityLevel (.1.3.6.1.6.3.15.1.1.1.0)	This is set when the security level (AuthPrivAuthNoPriv/NoAuthNoPriv) specified is not supported by the agent. This error is reported by the agent with its first varbind containing the OID .1.3.6.1.6.3.15.1.1.1.0".

SL No	Error message	Occurrence
2	usmStatsNotInTimeWindows (.1.3.6.1.6.3.15.1.1.2.0)	This is set when the engineTime specified is not within the timeWindow of agent. The engineTime is considered not within the timeWindow if any of the following is true: • If the agent's snmpEngineBoots value is equal to 2147483647. • If the request's snmpEngineBoots value differs from that of the agent. • If the difference between the SNMP request's snmpEngineTime and that of the agent is greater than 150.
3	usmStatsUnknownUserNames (.1.3.6.1.6.3.15.1.1.3.0)	This is set when the user name specified is not present in the agent. This error is reported by the agent with its first varbind containing the OID .1.3.6.1.6.3.15.1.1.3.0.
4	usmStatsWrongDigests (.1.3.6.1.6.3.15.1.1.5.0)	This is set when the password specified is not correct. So check if both Auth and Priv passwords are correct if configured. This error is reported by the agent with its first varbind containing the OID .1.3.6.1.6.3.15.1.1.5.0.
5	usmStatsDecryptionErrors (.1.3.6.1.6.3.15.1.1.6.0)	This is set when the packet is unable to decrypt on the agent side. This error occurs while querying an AuthPriv user. So check if the Auth and Priv Protocol specified are correct. This error is reported by the agent with it's first varbind containing the OID .1.3.6.1.6.3.15.1.1.6.0".

IP Subnet Marked as Non-trackable

The IP Subnet Phones page appears when you choose **ERL Membership> IP Subnets**. The Tracked column shows if the phones under the IP subnet are tracked or not. For IP subnets configured as non-trackable, the View Phones icon will show all phones that are not tracked.

- If a phone falls under both a tracked and non-tracked IP subnets, precedence is given to the more specific IP subnet.
- The phones under the IP subnet marked as non-trackable are not displayed on **Switch Ports** or **Unlocated Phones** page.
- If a phone moves between a trackable and non-trackable IP subnet, you must perform a Major Discovery to reflect the changes.
- Cisco Emergency Responder does not restrict a 911 call flow for the phones that are under a non-trackable IP subnet. If a call is made, the default ERL treatment is provided.

Phone Disappears in Emergency Responder

If Emergency Responder is in the middle of a phone tracking process, and a phone is in the middle of homing to a different Unified CM cluster, no Unified CM cluster has a record of the phone. Thus, Emergency Responder does not know the phone exists, and you cannot look up the phone in the Emergency Responder interface. However, assuming the phone successfully connects to a Unified CM cluster, Emergency Responder tracks the phone during the next incremental phone tracking process, and the phone should then appear in the Emergency Responder interface.

This problem can also occur if phones are reconnecting to a primary Unified CM server from a backup server during the Emergency Responder phone tracking process.

Wrong ERL Used for Shared Line

When two or more phones with a shared line appearance move from switches that are monitored by one Emergency Responder group to switches that are monitored by a different Emergency Responder group, then Emergency Responder may assign an incorrect ERL to these phones during an emergency call. This situation can occur when the phones move to a different campus that has a different Unified CM cluster (although the moved phones are still registered with the original Unified CM cluster), and it can also occur when the phones move within a single large campus that is served by multiple Unified CM clusters.

Because the moved phones are still registered to their original Unified CM cluster, emergency calls from these phones are routed to the original Emergency Responder group. In this case, the Emergency Responder group detects that the calling phone is connected to a switch that is monitored by a different Emergency Responder group, and the call is forwarded to the appropriate Emergency Responder group through an H.323 inter-cluster trunk. Because the inter-cluster trunk does not pass the MAC address of the calling phone, the receiving Emergency Responder group does not know the MAC address of the calling phone and must associate the phone to an ERL based on the calling party number.

In cases with a single phone connected to the switches monitored by the receiving Emergency Responder group, this is not a problem. However, when multiple phones with a shared line appearance connect to switches monitored by the receiving Emergency Responder group, then Emergency Responder must guess which phone has placed the emergency call. If all of the phones with a shared line appearance are in the same ERL, the guess is correct. If the phones span multiple ERLs, then the guess might be incorrect.

Related Topics

Two Main Site Deployments , on page 44

Wireless Endpoints Using Unexpected ERL

Wireless endpoints (such as CiscoWirelessIP7920Phones and CiscoIPSoftPhones) may be using switch port-based ERL instead of the configured subnet-based ERL.

CiscoEmergency Responder (Emergency Responder) give a higher priority to switch port association for call routing. If Emergency Responder finds a switch port mapping for any endpoint (including wireless endpoints), it uses the switch port mapping to route emergency calls. If the switch port mapping is not found or if the ERL is not configured for the corresponding switch port, Emergency Responder routes emergency calls using subnet-ERL configuration.

See the switch port screen or the ERL debug tool (see Check Emergency Responder Configuration Using ERL Debug Tool , on page 344) to check if the wireless endpoint is associated with a switch port.

It is recommended that you track wireless endpoints using subnet-based ERLs.

Related Topics

Set Up IP Subnet-based ERLs , on page 143

Troubleshoot Emergency Call Problems

The following sections describe how to troubleshoot emergency calls routing and how to use the information supplied with the calls.

Emergency Calls Not Intercepted by Emergency Responder

If Emergency Responder is not intercepting emergency calls, there is probably a mistake in your Unified CM configuration or its representation in the Emergency Responder configuration.

- The emergency call number (911) is in the Phones partition and uses the E911CSS calling search space. Ensure that this number was identified during Emergency Responder installation (see Installation on a New System , on page 63) to ensure that users can dial the emergency number. See Create Emergency Call Route Points, on page 87 for information about setting up the Unified CM configuration for this number.

- The standby Emergency Responder server route point (912) is in the E911 partition and uses the E911CSS calling search space. See Create Emergency Call Route Points, on page 87 for information about setting up the Unified CM configuration for this number. Ensure this number is defined as the standby server route point in the Emergency Responder configuration (see Set Up Group Telephony Settings for Server , on page 129).

- The PSAP callback route point pattern (913XXXXXXXXXX) is in the E911 partition and uses the E911CSS calling search space. See Create Emergency Call Route Points, on page 87 for information about setting up the Unified CM configuration for this number. Ensure this number is defined as the PSAP callback route point pattern in the Emergency Responder configuration, and that the strip prefix (913) is also identified (see Set Up Group Telephony Settings for Server , on page 129).

- All ELIN route patterns are in the E911 partition. See Create Route Patterns for ERLs, on page 94 for information about setting up the Unified CM configuration for these numbers.

- All phones and CTI ports (both device and line) are in the Phones partition and use the PhoneCSS calling search space. You can use additional partitions, but they must be set up with relationship to the Emergency Responder partitions and calling search spaces in the same manner as these partitions in the examples described in the Create Route Patterns for ERLs, on page 94.

- All gateways to the service provider's network use the E911CSS calling search space. See Set Up Calling Search Space for Gateway and PSAP Connection , on page 100 for more information.

- The Unified CM Version (JTAPI jar) being configured is proper. To check the Unified CM version, follow these steps:
  1. Log in to the Emergency Responder Admin Utility website.
  2. Select **Update** > **CCM Version**
  3. In the **Status** section, check the **Current Version of CCM**.

ELIN Not Transmitted to PSAP

If the ELIN is not transmitted to the PSAP, and you are using a PRI connection to route emergency calls to the PSAP, check the configuration of the gateway. The PRI must be configured to send the real calling party number (the ELIN) rather than a static number, such as the main site number. See CAMA and PRI Trunks , on page 36.

ELIN Default ERL Used for Calls From Other ERLs

If an emergency call is assigned an ELIN defined for the default ERL instead of an ELIN assigned to the ERL from where the call was made:

- Check the Unified CM configuration for the route pattern for the ELIN you expected to be used. See Create Route Patterns for ERLs, on page 94.
- Check the ERL definition in Emergency Responder to ensure that the ELIN is correctly configured for the ERL. See Set Up Individual ERL and Automatic Location Information (ALI) , on page 140.

If the route pattern for an ERL fails, Emergency Responder uses the route pattern defined for the default ERL.

Emergency Calls Not Routed to Correct PSAP

If an emergency call is not routed to any PSAP, check whether the route patterns used for the ERL from which the call was made and for the default ERL are configured and use the correct partitions and calling search spaces (see Create Route Patterns for ERLs, on page 94). Ensure that the partitions and calling search spaces for the gateways are correct (see Set Up Calling Search Space for Gateway and PSAP Connection , on page 100).

Note When a 911 call is made, the call does not route to an alternate PSAP when the primary PSAP call fails. The caller may hear a busy tone, but the Emergency Responder administrator will not receive an email alert that the emergency call could not be routed.

If an emergency call successfully leaves your network but does not get routed to the correct PSAP, look at these possible points of failure:

- Is Emergency Responder configured to assign the correct ELIN to the ERL assigned to the phone? Emergency calls are routed based on the ELIN, so if you assign the wrong ELIN, the call is not routed correctly. See ERL Creation , on page 138.
- No Calling Party Transformation masks are set at the Gateway or Trunk, which may transform the ELIN set by Emergency Responder.

- If the ELIN is correct, is the ELIN route pattern configured to use the correct gateway? If you select the wrong gateway, the call might be routed to a part of the service provider's network that cannot connect to the desired PSAP. Consult with your service provider to determine gateway requirements.

  See these topics:

  - ELIN Numbers Emergency Calls and PSAP Callbacks , on page 93
  - Deployment in Main Site with Two or More PSAPs, on page 40

- Does the service provider's ALI database contain the correct information for the ELIN? Emergency call routing outside your network is based on the information in the service provider's database, not on the information in your local network. See Export ERL Information , on page 146.

- Does the emergency caller's phone register with a Unified CM cluster supported by a different Emergency Responder group than the Emergency Responder group that supports the originating switch port? Then you might have a mis-configured Emergency Responder cluster. See these topics:

  - Installation on a new system
  - Create route patterns for Inter-Cisco Emergency Responder Group communications
  - Set up group telephony settings for server

Note If the call reaches the PSAP, but the PSAP cannot talk to the caller, ensure that the Unified CM for the remote Emergency Responder group has the Unified CM for the local Emergency Responder group defined as a gateway.

Emergency Calls Get Busy Signal and Not Routed

If callers hear a busy signal when calling the emergency call number, or if emergency calls sometimes do not get routed, there is probably a problem with the configuration of your standby Emergency Responder server:

- If you have only configured a primary Emergency Responder server, install and configure a standby Emergency Responder server. If CPU utilization on the primary server reaches 100 percent, Emergency Responder cannot handle emergency calls. In this case, the standby server handles the calls.

- Check the route point configuration for the standby server. Ensure the emergency call route point's call forward settings are configured to forward calls to this number. See Create Emergency Call Route Points, on page 87 for information about the Unified CM configuration, and the Set Up Group Telephony Settings for Server , on page 129 for the Emergency Responder configuration.

PSAP Call Back Errors

You might encounter a PSAP call back error if a PSAP operator tries to call back an emergency caller using the ELIN provided by caller ID. The following sections describe two such errors: if a PSAP cannot reach the original emergency call extension and if onsite security personnel get a call back from a PSAP.

PSAP Cannot Reach Original Emergency Call Extension

Problem PSAP could not reach the original emergency call extension.

Solution Emergency Responder caches a mapping between the caller's true extension and the ELIN you define for an ERL. If more calls get made than the number of ELINs you define for an ERL, Emergency Responder must reuse these numbers and thus overwrites the original caller's extension. You can view the call history to determine the extension of the original caller. See Emergency Call Process , on page 26.

If this is not the problem, check the configuration of the PSAP callback route point in Unified CM and Emergency Responder (see Create Emergency Call Route Points, on page 87 and Set Up Group Telephony Settings for Server , on page 129), and ELIN translation patterns in Unified CM (see Create Translation Patterns for ELINs, on page 95).

Onsite Alert Security Personnel Get Callbacks From PSAP

Problem Onsite alert (security) personnel get callbacks from the PSAP.

Solution Please check if Default ELIN Digit Translation is set in the Group Telephony Settings for Server. For more information, see Set Up Group Telephony Settings for Server , on page 129.

Onsite Alert Personnel Not Getting Telephone Alerts

If the onsite alert personnel are not getting telephone alerts when an emergency call is made in an ERL they are covering, ensure that all phones and CTI ports (both device and line) are in the Phones partition and use the PhoneCSS calling search space. You can use additional partitions, but they must be set up with relationship to the Emergency Responder partitions and calling search spaces.

Also, ensure that the Emergency Responder configuration for the Unified CM clusters is correct. The Emergency Responder configuration should show the correct beginning address for the telephony ports that you defined as CTI ports in Unified CM. The number of telephony ports should be the correct number, and the number must be greater than 0 for any calls to occur. Emergency Responder uses this CTI port to place the telephone calls to onsite alert personnel.

If the Event Viewer in the Emergency Responder Serviceability web interface displays the error message “No port to place call,” then there were not enough CTI ports defined to initiate all the calls to onsite alert personnel. Therefore, you must define additional ports. To access the Event Viewer, log in to the Emergency Responder Serviceability web interface and select **Tools > Event Viewer**.

Onsite Alert Phone Does Not Ring When Emergency Call Placed

You might encounter this problem if the onsite alert phone does not ring when an emergency call is placed.

Problem The onsite alert phone does not ring when an emergency call is placed.

> **Possible Cause** The onsite alert phone does not ring if the Do Not Disturb (DND) feature is enabled on the phone and if Emergency Responder is configured with Unified CM6.x.

Solution Do not enable DND on an onsite alert phone.

You might encounter this problem if the onsite alert does not work during an emergency call, when the Cisco Emergency Responder publisher database is not operational.

Problem The onsite alert does not work for an emergency call if the Cisco Emergency Responder publisher database is not operational.

Possible Cause The onsite alert will not work as the Cisco Emergency Responder publisher is still active even when the database is not operational and the Cisco Unified Communications Manager CTI ports get registered with the Cisco Emergency Responder publisher.

Solution Restart the Cisco Emergency Responder publisher.

Prompts for Phone Alerts Not Getting Played

You might encounter this problem if prompts for phone alerts are not getting played.

Problem Prompts do not get played at the onsite alert phone when the call is initiated from the CTI ports.

Possible Cause This problem can occur when a single CTI port is configured with multiple lines. Prompts may not get played from one or more of these lines when the onsite alert notifications call is initiated through them.

Solution To avoid this problem, configure only one line per CTI port in the Unified CM that is configured for Emergency Responder.

Onsite Alert Personnel Not Getting Email or Paging Notifications

If the onsite alert personnel are not getting email or email-based pages, even though you configure email addresses for them, check the Emergency Responder configurations SMTP settings. Ensure that the SMTP server address and source mail ID are correct, and that there is an account for the mail ID in the SMTP server.

Incorrect Location Information Sent to Onsite Alert Personnel

If your onsite alert (security) personnel are receiving incorrect location information for an emergency call, consider these potential problems:

- Is the ALI data for the ERL correct? See ERL Creation , on page 138.
- Is the phone location data for the switch port correct? See Switch Port Configuration , on page 159.
- Is the correct ERL assigned to the switch port to which the phone is connected? If not, there could be two problems:
  - Someone switched wires on the switch, so your previously correct configuration is no longer correct. Wires cannot be moved from port to port without potentially invalidating the ERL assignment. See Data Integrity and Reliability, on page 34.
  - The wiring closet is secure, but the ERL assignment is incorrect. See Switch Port Configuration , on page 159.
- Did the call come from the Default ERL (assuming you do not use the Default ERL for any permanent ERL)? This could indicate these problems:
  - The phone is connected to an unsupported port and is not defined as a manual phone. See Manually Define Phones , on page 168.
  - The phone is not supported and it is not defined as a manual phone. See Manually Define Phones , on page 168.
  - The phone is supported but Emergency Responder could not locate it. You might have to manually assign the phone to an ERL if you cannot resolve the problem. See Unlocated Phones , on page 324.

- Did the call come from a manually-defined phone extension? If so, it is likely the incorrect ERL is assigned, perhaps because the phone moved. See Manually Define Phones , on page 168.

Emergency Call History Problems

There are two issues you might encounter when viewing the emergency call history information:

- Emergency call information does not appear in call history.
- Call history does not show call ELIN and route pattern.

For additional information, see View Emergency Call History , on page 172.

Emergency Call Information Does Not Appear in Call History

Problem Emergency call information does not show up in call history right away.

Solution Emergency Responder writes call history information to the database every 15 seconds. You can view history information after 15 seconds.

Call History Does Not Show Call ELIN and Route Pattern

Problem The call history does not show the ELIN and route pattern used for a call.

Solution If the call could not be routed to the PSAP, you will not see an ELIN or route pattern. Check to determine why the call could not be routed. See Emergency Calls Not Routed to Correct PSAP , on page 330.

Onsite Audio Alert Not Sent From Emergency Responder For Encrypted Calls

Problem The onsite audio alerts are not sent from Emergency Responder.

- **Possible Cause** The **Enable SRTP for Audio Alerts** check box is not enabled on the Unified Communications Manager cluster setting in the Emergency Responder and the Unified Communications Manager service parameter **Block Unencrypted Calls** is set to TRUE in the Cisco Unified CM Administration user interface.

- **Solution** Ensure that you enable the **Enable SRTP for Audio Alerts** check box on the Unified Communications Manager cluster setting in the Emergency Responder.

- **Possible Cause** You encounter this issue even if the **Enable SRTP for Audio Alerts** check box is enabled on the Unified Communications Manager cluster setting in the Emergency Responder and the Unified Communications Manager service parameter **Block Unencrypted Calls** is set to TRUE in the Cisco Unified CM Administration user interface. This might be because the Onsite phones do not support encryption and Unified Communications Manager does not allow the routing of unencrypted calls.

- **Solution** Ensure that the Onsite phone supports encryption and is properly configured in the Unified Communications Manager.

Troubleshoot Licensing

Cisco Smart Software Licensing is a new way of thinking about licensing. It adds flexibility to your licensing and simplifies it across the enterprise. It also delivers visibility into your license ownership and consumption.

Cisco Smart Software Licensing helps you to procure, deploy, and manage licenses easily where devices self-register and report license consumption, removing the need for product activation keys (PAK). It pools license entitlements in a single account and allow you to move licenses freely through the network, wherever you need them. It is enabled across Cisco products and managed by a direct cloud-based or mediated deployment model.

This service registers the product instance, reports license usage, and obtains the necessary authorization from Cisco Smart Software Manager or Cisco Smart Software Manager satellite.

Cisco Smart Software Manager replaces Prime License Manager in Cisco Emergency Responder Release 12.0 and later versions.

Related Topics

E911 and Cisco Emergency Responder Terminology , on page 6

Cisco Smart Software Licensing , on page 10

License Manager Status Messages

The following table shows a list of all status messages as they appear on the **License Manager** page.

Table 24: Status Messages on the Landing Page

Device	State	Status or Warning Message	Description
Emergency Responder	Evaluation mode	Cisco Emergency Responder (CER) is currently unregistered with Smart Software Manager and running in Evaluation mode with 90 days remaining. Register with Smart Software Manager or Smart Software Manager satellite to avoid stopping of Cisco Phone Tracking Engine.	This message is displayed on Emergency Responder during the Evaluation Period.
Emergency Responder	Evaluation period expired	The system has passed the Evaluation Period. The Cisco Phone Tracking Engine has been stopped. Register with Smart Software Manager or Smart Software Manager satellite to restart the Cisco Phone Tracking Engine.	This message is displayed on Emergency Responder when the Evaluation Period expires.

Troubleshoot Email Alerts

The following sections describe how you troubleshoot problems related to the email alerts generated by Emergency Responder.

JTAPI Incompatibility Warning

As an administrator, you will be alerted if the Unified CM version configured on Emergency Responder differs from the version to which Emergency Responder route points are registered, so that you can take corrective action and assure that emergency calls are processed correctly. An email alert will be sent to the configured email address using SMTP mail server.

Ensure that email alerts for Emergency Call Routing Parameters are enabled under Email Alert Settings on the Emergency Responder administration pages.

The error is also displayed on the Event Viewer page. See the Related Links below.

Alert would be as follows:

```
Unified CM at <IP address> is version CUCM x which differs from CUCM version
setting CUCM y on Cisco Emergency Responder.
```

This warning could occur in the following cases:

- Unified CM version is no longer supported; for example, Unified CM 2.0 integrated with Cisco Emergency Responder 8.7 or 9.0
- Unified CM version is not yet supported; for example, Unified CM 9.5 integrated with Cisco Emergency Responder 8.7 or 9.0
- Unified CM version is supported, but Unified CM version setting on Emergency Responder is incorrect; for example, Unified CM 9.0 integrated with Cisco Emergency Responder 8.7 or 9.0, but Emergency Responder Unified CM version setting is Unified CM 7.1

Multiple Unified CM versions in the same Emergency Responder will always cause one of the above situations.

Related Topics

Event Viewer, on page 510

JTAPI Route Point Registration Failure Alarm

As an administrator, you will be alerted if Emergency Responder cannot register its JTAPI route points so that you can take corrective action and assure that emergency calls are processed correctly.

The following events can cause the route point to register or unregister:

- Cisco Emergency Responder or SNMP service restart.
- Cisco Emergency Responder failover or fallback.
- JTAPI version upgrade or downgrade.
- Incompatible JTAPI version.

- Emergency Responder or Unified CM upgrade.
- Application user's credential is incorrectly mentioned in Emergency Responder.
- Application user password expired.
- CTI telephony port begin number is wrongly mentioned in Emergency Responder (impacts only CTI ports).
- CTI telephony port count is wrongly mentioned in Emergency Responder (impacts only CTI ports).
- SNMP configuration is incorrect in either Emergency Responder or Unified CM.
- Route point DN numbers mismatch in Cisco Emergency Responder or Unified CM.

If Unified CM is SNMP unreachable or application user credentials to Unified CM are incorrect, then Emergency Responder will send an email alert to the configured email ID. Ensure that the email alert settings under the discovery parameters are enabled under Email Alert Settings on the Emergency Responder administration pages.

The email alert would be as follows:

<CERserver hostname> Cisco ER Phone Tracking could not get information [using SNMP] from 1 Cisco CallManager(s) Check EventViewer on CERServer for details.

This is a serious condition and may indicate that Emergency Responder will not receive and process emergency calls.

Emergency Call Alert

Whenever a user makes a 911(Emergency) call, Emergency Responder generates an email alert. Emergency Responder sends the email alert to all the onsite alert (security) personnel whose email IDs are configured for the ERL from which the call was made.

Security personnel are expected to respond to that user. For detailed call information, see the following URL:

```
http://<<CERServer HostName>>/ceruserreports
```

When a 911 call is made and the backup Emergency Responder server handles the call, an alert similar to the following is sent:

```
Subject: Emergency Call Alert -- Extn # 332101 (Generated by Backup CiscoER)
Message: EMERGENCY CALL DETAILS (Generated by Emergency Responder)
Caller Extension : 332101
Display Name     : Caller's Name
Zone/ERL         : Z1
Location         : ddd
System Call Time : March 13, 2018 11:07:54 AM IST
Local Call Time  : March 12, 2018 22:37:54 PM PDT (Note: In this example, Local Call Time
is for the America/Los_Angeles time zone.)
```

Transition Alert

When the standby Emergency Responder server takes control and becomes the active server, a Transition Alert is sent to the Emergency Responder administrator. This situation occurs under any of the following circumstances:

- If the primary Emergency Responder server is stopped.

- If the Emergency Responder service is stopped on that server.
- If the connectivity between primary and standby Emergency Responder servers is broken.

The administrator should diagnose the cause and fix the problem as soon as possible.

When the Emergency Responder backup server takes control, an alert similar to the following is sent:

```
Subject: Transition Alert: Cisco ER Backup is activeMessage:
Backup Cisco ER <<CER HostName>> has taken control as Active Cisco ER.
Transition Time  :June 2, 2003 3:57:12 PM IST
```

When the master Emergency Responder server takes control, an alert similar to the following is sent:

```
Subject: Transition Alert: Cisco ER Master is activeMessage:
Master Cisco ER <<Emergency Responder Server HostName>> has taken control
as Active Cisco ER. Transition Time  :June 2, 2003 3:57:12 PM IST
```

Tracking Failure

At the end of a switch port and phone tracking process, if there are any devices that could not be tracked, Emergency Responder sends a Tracking Failure email to the Emergency Responder administrator.

The administrator should look at the event log on the Emergency Responder server to find the list of devices that were not tracked. The administrator should check the following and make any required corrections:

1. Make sure that the correct SNMP Community String is configured in Emergency Responder.
2. Check that the device is connected.
3. Check that the host name for the Emergency Responder server is resolvable, that is, it can be found.
4. Check that the SNMP service is enabled on that particular device (Switch / Unified CM).

Here is an example of a tracking failure alert:

```
Subject: CER Phone Tracking failed to track some devicesMessage:
CER Phone Tracking could not get information [using SNMP] from 2
CiscoUnified CM(s) and 1 Switch(es)Check Event Viewer
on CER Server for details.
```

Failed to Get Provider Alert

Emergency Responder sends a Failed to Get Provider alert to the Emergency Responder administrator if Emergency Responder is not able to register to one of the configured Unified CM clusters. Emergency Responder continues trying the registration until it succeeds. Emergency Responder sends the Failed to Get Provider email after a few retries.

The message provides information about how to clear the problem, as shown in the following example:

```
Subject: Failed to get JTAPI Provider for Cisco Unified CM <<CCM IP/Host Name>>
(Generated by Backup Cisco ER)Message:
```

```
Please check the following:
1) Check if the Cisco Unified CM is connected to the CER server.
2) Check if the configured Call Manager is running a version
supported by the CER server.
3) Check if the given login credentials are correct:
CTI Manager Host Name:<<CCM IP/HostName>>
```

Failed to Establish Communication with Emergency Responder Phone Tracking Engine

Emergency Responder sends this email alert to the Emergency Responder administrator if the Emergency Responder server fails to establish communication with the Phone Tracking Engine for a period of time. This failure to communicate can occur if the Emergency Responder Phone Tracking Engine service is down. The administrator should perform the following steps:

1. If the Emergency Responder Phone Tracking Engine service is down, start the service.
2. Make sure that the Host Name of the Emergency Responder server does not contain any underscore (_) characters.

Here is an example of a tracking failure alert:

```
Subject: CER Server failed to establish communication
with CER Phone Tracking Engine.Message:
CER Server could not communicate with CER Phone Tracking Engine.
```

Lost Communication with Emergency Responder Phone Tracking Engine

Emergency Responder sends this email alert to the Emergency Responder administrator if the Emergency Responder server loses communication with the Emergency Responder Phone Tracking Engine. This situation is likely to occur if the Emergency Responder Phone Tracking Engine service goes down when the Emergency Responder server is running.

The administrator should restart the Emergency Responder Phone Tracking Engine service.

The following shows an example of a tracking failure alert:

```
Subject: CER Server lost communication with CER Phone Tracking EngineMessage:
CER Server could not communicate with CER Phone Tracking Engine.
```

Failed to Send Unlocated Phone Details to Remote Emergency Responder Server Group

If Emergency Responder fails to send unlocated entries to a server group because it is already in the process of sending entries to that server group, this alert is sent.

This alert occurs very rarely. It can occur when a Emergency Responder server is found in more than one Emergency Responder server group. To resolve this problem, check to see which server group is an old configuration and remove that server group.

```
Subject: CER Server failed to send Unlocated Phones details
to Remote CER Server Group.Message:
CER Server failed to send Unlocated Phones to Remote CER Server Group.
Please ensure that the CER servers are not found under more than one CER Server
Group.
CER Servers in Remote Server Group:<< CERServer HostNames >>
```

Emergency Call Could Not Be Routed

If the emergency call routing to some route patterns configured in the ERL fails, Emergency Responder sends an email to the system administrator.

Subject: Emergency call could not be routed using some route patterns (CERServer:<server hostname>)

Message Body: Emergency call from :<Caller Extn> could not be routed using some Route Patterns. Check Event Log.

The Event Log displays the following message:

```
Emergency call from <extn> could not be routed using the following route patterns
<RoutePattern1>
<RoutePattern2>
*****************
Call Routed to <RoutePattern-X>

Please check the availability of the above routes. Also, check for the following
 error conditions:

1. If FAC and/or CMC are configured on the route patterns used for Cisco ER,
please disable them.
2. If the "Calling Party Number Modification" flag on the CER user page in
the Cisco Unified CM is not enabled, please enable it.
```

Solution

- If you are running Unified CM 4.2 or4.3, make sure that the Calling Party Number check box on the Emergency Responder User page is checked.
- If you are running Unified CM 5.x or Unified CM 6.x, make sure that the routes are available.
- Add the Emergency Responder Application User to the “Standard CTI Allow Calling Number Modification” user group.

Calling Party Modification Failed

If the calling party modification was not successful, Emergency Responder sends the following email to the system administrator:

Subject: Emergency Calling Party Modification Failed (Emergency ResponderServer: <server>)

Message Body: Emergency call from :<Caller Extn> cannot be routed with calling party modification. Check Event Log.

The Event Log displays the following message:

```
Emergency Call from <Caller Extn> has been routed to default ERL because the
calling party modification failed. Please make sure that the check box "Enable
Calling
Party Number Modification: is checked on the Cisco Unified CM user page for the
CER user. PSAP callbacks MAY NOT work correctly. The CER service will need to
be restarted once the flag is checked on the Cisco Unified CM User page.
```

Solution

Check the box for the “Enable Calling Party Number Modification” in the Emergency Responder user page in Unified CM 4.2 or4.3 Administration. After you enable this flag, restart the Emergency Responder service for the changes to take effect.

Troubleshoot Web Alerts

You might encounter Web Alert Refreshes Every 30 Seconds , on page 341 when receiving web alerts.

Web Alert Refreshes Every 30 Seconds

Problem Web alert continues to refresh every 30 seconds. You can see this problem by checking the status in the browser. The status displays the seconds remaining before refresh if it is in this mode.

Solution Check if there are other web alert screens open on the same client machine. Only one browser from a client machine can operate in the real-time mode. Remove any extra browsers.

Troubleshoot Emergency Responder System and Administration Problems

The following sections describe how you can troubleshoot problems related to the Emergency Responder system and its administration, such as server and web server problems.

Cannot Validate Publisher

If the installation cannot validate the Publisher (Step 5 of the Install Emergency Responder Subscriber, on page 69), check the following:

1. Verify that the Publisher hostname is correct and that the Publisher is reachable by hostname.
2. Verify that the Publisher and Subscriber servers are running the same version of Emergency Responder.
3. Verify that the database password that you entered is correct. This password was specified on the Database Access Security Configuration page during installation.
4. Make sure that the Subscriber has been configured correctly on the Publisher.

Troubleshoot Login Problems

The following section shows some issues you might encounter while logging into Emergency Responder.

Cannot Access Emergency Responder Administration Website

Problem You cannot log in to the Emergency Responder Administration website.

Solution Log in to CLI and run the **utils service list** command. Check if the status “Cisco IDS” is STARTED. If not, start the service using the **utils service start service name** command.

HTTP Error 500

If the Emergency Responder Administration website displays a HTTP Error 500 after the installation or upgrade, try the following:

- Restart Cisco Emergency Responder and Cisco Tomcat service.
- Run a select query to cerremote table and check if the RMI objects have been created for both Publisher and Subscriber Nodes.
- If you have replication issues between Publisher and Subscriber:
  - Check the .rhosts file of the Publisher and confirm that it was entered with the correct values. If the correct values have not been entered, restart the Cisco Emergency Responder service.
  - Run the **utils dbreplication repair** and **utils dbreplication reset** commands to reset the Database replication.
- If these steps do not fix this issue, set the server to permissive mode using the **utils os secure permissive** command and reboot it.

Cisco Unified Operations Manager

Use Cisco Unified Operations Manager to continuously monitor the health of the Emergency Responder system.

For information about setting up Emergency Responder to use Cisco Unified Operations Manager, see Set Up Test ERLs , on page 144.

For information about installing and using Cisco Unified Operations Manager, go to this location:

http://www.cisco.com/en/US/partner/products/ps6535/index.html.

Troubleshoot Emergency Responder Switch and Port Configuration Problems

The following sections describe several common issues that you might encounter while configuring switches or switch ports in Emergency Responder.

Phones Do Not Get Discovered

Problem Emergency Responder is configured with Unified CM information, but no phones get discovered.

Solution Ensure that the Unified CM servers are reachable on the network. Then ensure that the SNMP read community strings are configured correctly for the switches and Unified CM servers (see Set Up SNMPv2, on page 149.) Manually run the switch port and phone update process (see Manually Run the Switch-Port and Phone Update Process , on page 157.) Use the CLI-based **utils snmp** command to determine if the Unified CM is SNMP reachable.

Emergency Responder Does Not Show Ports on Switch

Problem Emergency Responder does not show the ports on a switch configured in Emergency Responder.

Solution If you add a supported switch to Emergency Responder and run phone tracking on the switch after adding it, you can view the list of Ethernet ports on the switch. If Emergency Responder does not list the ports, check the SNMP settings in Emergency Responder for the switch (see Set Up SNMPv2, on page 149.) Also, verify that the switch is reachable over the network. Retry the selective phone tracking process on the switch (click **Locate Switch Ports** when viewing the switch details; see LAN Switch Details, on page 434.)

If the problem persists, ensure that the switch is supported (see Network Hardware and Software Requirements , on page 10.) Also, check the Event Viewer for error messages.

Some Phones Do Not Appear in Switch Port List

Problem Some phones do not appear in the switch port list.

Solution Check if the phone is found under configured IP subnets or in synthetic phones. If it is not found in either of those places, then they are placed as unlocated phones. See Unlocated Phones , on page 324 for a list of reasons that a phone could not be located.

Cannot Delete Switch From Emergency Responder Configuration

Problem Cannot delete a switch from the Emergency Responder configuration.

Solution You cannot delete a switch when a phone tracking process is in progress. Retry the deletion after the process has ended. If this is not the problem, the Emergency Responder server might not be running. Check the control center and restart the server (see Manage Emergency Responder Server , on page 349.)

Import or Export of Switch Port Details Fails

Problem Import or export of the switch port details fails.

Solution If a switch port import or export attempt fails, it might be due to these reasons: the first switch port and phone update process has not yet ended (wait for it to finish); the Emergency Responder server is not running (use the control center to restart it, see Manage Emergency Responder Server , on page 349); the Emergency Responder server is not completely initialized (wait for it to initialize).

Import of Some Switch Port Configurations Fail

Problem The import of some switch port configurations fail.

Solution To import switch port configurations, Emergency Responder must already be configured with the switch and Emergency Responder must first discover the ports on the switch using the switch port and phone update process. If you try to import a configuration for ports not yet discovered in Emergency Responder, the importation of those settings fails. See Manually Run the Switch-Port and Phone Update Process , on page 157 for information about the process. Run it on the switches whose port configurations you could not import, then retry the import.

Phones Moved To and From Various Emergency Responder Groups Incorrectly Display in Switch Port Details

Problem Phones moved from other Emergency Responder groups to this Emergency Responder group, and then moved back, are still showing up in the switch port details for the Emergency Responder group.

Solution These types of phones are not removed from the switch port details until the next full switch port and phone update process is run. If this is an issue for you, you can run the process on the switch (or on all switches) manually. See Manually Run the Switch-Port and Phone Update Process , on page 157.

Check Emergency Responder Configuration Using ERL Debug Tool

The ERL Debug Tool takes a phone extension as the search criteria and displays the ERLs currently being used for routing emergency calls for the phones.

Use this diagnostic tool to verify the Emergency Responder configuration during the ERL creation and the ERL assignment phase, and to troubleshoot calls directed to incorrect ERLs.

For example, you configured the phone in ERL_1 as a manually configured phone; however, a mis-configured IP subnet matches this phone's IP address, and associates it with ERL_2. Now that you have found the configuration problem using the Debug Tool, you can correct it.

Procedure

Step 1 Select **Tools** > **ERL Debug Tool**.

Emergency Responder displays the ERL Debug Tool page.

Step 2 In the Find Phones field, to list specific phones, select the search criteria and click **Find**.

Emergency Responder displays the ERL currently being used for routing emergency calls for the phone.

Step 3 If the configurations are not correct, make the required changes.

Note Emergency Responder displays a maximum of 1,000 records.

Publisher and Subscriber Server Replacement

The following sections describe how to replace a faulty Publisher server and how to replace a faulty Subscriber server.

Replace Faulty Subscriber

To replace a faulty Subscriber, go to Emergency Responder administration and delete the faulty Subscriber. Install a new Emergency Responder Subscriber for the Publisher (see Installation on a New System , on page 63).

Note If the same host name is not going to be used by the replacement Subscriber server, you must delete the faulty Subscriber using the Emergency Responder administration screen on the Publisher server.

Replace Faulty Publisher

You can restore the Publisher only if you have backed up the Publisher using the Disaster Recovery System available as part of the Emergency Responder.

Procedure

Step 1 Install the same version of the Emergency Responder Publisher on a server with the same host name as the one you used previously.

Step 2 Choose the same configuration options (such as the Unified CM version, and so on) during the installation.

Step 3 Restore the old configuration data using the Disaster Recovery System.

Emergency Responder Admin Utility

You can use the Emergency Responder Admin Utility tool to perform the following tasks:

- To update Emergency Responder cluster database host details
- To upgrade the CCM version

Use Emergency Responder Admin Utility Tool

Procedure

Step 1 Log in to the Emergency Responder Admin Utility web interface.

Step 2 Using the menu bar, choose a task to perform:

a) To change the Publisher that the Subscriber server points to, select **Update** > **Publisher**.
b) To update the Unified CM version, select **Update** > **CCM Version**.
c) To update the cluster settings on both the Publisher and Subscriber servers, select **Cluster** > **DBHost**.

Note This action updates the Emergency Responder cluster DB details for this server group only. Other servers in this Emergency Responder cluster will NOT be updated automatically.

Step 3 To save the changes that you have made, restart both the Publisher and the Subscriber servers.

Set Up Subscriber Database

To configure the Publisher-Subscriber setup again if you have an issue with the Subscriber (apart from DB replication), follow these steps:

Procedure

Step 1 Log in to the Emergency Responder Admin Utility web interface on the Subscriber server.

Step 2 Select **Update** > **Publisher**.

Step 3 Specify the same Publisher Host Name, IP address (already being pointed to) and database access security password.

Step 4 Click **Go**.

This step might a take a while to set up.

Database and Enterprise Replication Troubleshooting

Use the following CLI commands for troubleshooting the Informix Dynamic Server (IDS) database:

- **utils service list**—Checks whether the IDS service is running or not.
- **show tech dbstateinfo**—Provides the DB state information, which is helpful in debugging database issues.
- **show tech dbinuse**—Displays the currently used database.
- **show tech dbintegrity**—Shows database integrity information.
- **show tech database**—Creates a .csv file with contents of all the tables in the database.

Use the following CLI commands for troubleshooting Enterprise Replication:

- **utils dbreplication status**—Displays the status of the database replication.
- **utils dbreplication reset**—Resets and restarts the database replication between the Publisher and Subscriber.
- **utils dbreplication repair**—Compares the data on replication servers (Publisher and Subscriber) and creates a report listing data inconsistencies and repairs the data inconsistencies. This command also tries to repair replication by rebuilding the corrupted .rhosts file if it is corrupted for some reason.

For troubleshooting database problems using logs, download logs from the Emergency Responder Serviceability website or through the CLI.

The following logs provide information for debugging database-related issues:

- Install and Upgrade logs—/var/log/install/
- Install DB logs—/var/log/active/er/trace/dbl/sdi/
- CERDbMon logs—/var/log/active/er/trace/dbl/sdi/cerdbmon/
- CLI logs—/var/log/active/platform/log/

Replication Fails to Start After Subscriber and DNS Installation

Problem Replication fails to start after the Subscriber is installed with DNS and the CLI command **utils dbreplication status** indicates that replication is not working.

Possible Cause The .rhosts have the host name for the Subscriber instead of FQDN (Fully Qualified Domain Name) of the Subscriber.

Solution Use the CLI command **utils dbreplication repair** to repair the replication issue. This command tries to repair replication by rebuilding the corrupted .rhosts file.

Troubleshoot Emergency Responder System Problems

The following sections discuss some issues you might encounter with general operation of the Emergency Responder system and the configuration screens that involve the Emergency Responder server, group, and cluster.

Emergency Responder Intra-Cluster Call Routing Fails or Phones Not Discovered Correctly

Problem Emergency Responder intra-cluster call routing fails or Emergency Responder does not discover phones correctly.

Solution Ensure that all the Emergency Responder servers in an Emergency Responder cluster can be found by their host name, and ensure that all are reachable on the network by all the other Emergency Responder servers.

Solution Ensure that all the Emergency Responder servers can reach the Emergency Responder cluster DB host and that the cluster DB password is the same across all servers in the cluster.

Emergency Responder Exits After Starting

Problem Emergency Responder exits after starting.

Possible Cause

You have configured Emergency Responder to use a TCP port that is already in use.

Solution Check the Windows Event Viewer for the message "CER could not open socket at port peer-tcp-port, Exiting." If you see this message, change the Emergency Responder group configuration to use a different TCP port.

Emergency Responder Groups in Cluster Screen Does Not Load and Displays a Cannot Connect to Cluster DB Host Error

Problem The Emergency Responder Groups in Cluster screen does not load, and exhibits the error “Cannot connect to cluster DB host.”

Solution Ensure that the cluster DB host can be found by host name.

Ensure that the specified cluster DB host password is the same across all Emergency Responder server groups in the cluster.

For more information, see Set Up Emergency Responder Cluster and Cluster DB Host , on page 134.

Related Topics

Identify Emergency Responder Groups and Servers in Cluster , on page 349
Manage Emergency Responder Server , on page 349

Troubleshoot Cisco Unified Communications Manager Configuration Problems

These are some issues that you might encounter when the Emergency Responder communicates with Unified CM. Additional problems with symptoms that involve emergency call failures are discussed in the Troubleshoot Emergency Call Problems , on page 329.

Emergency Responder Does Not Register with Route Points and CTI Ports

Problem Emergency Responder does not register with the route points and CTI ports configured for its use.

Solution Ensure that the route points and CTI ports are associated with the Unified CM CiscoEmergency Responder user (see Create Emergency Responder Cisco Unified Communications Manager User, on page 104.) Ensure that the CTI Manager on the Unified CM server (or the DC Directory on a Windows-based Unified CM server) is running properly.

Cannot Delete Unified CM From Emergency Responder Configuration

Problem When trying to delete a Unified CM from the CiscoEmergency Responder configuration, Emergency Responder displays the message "Phone tracking in progress."

Solution You cannot delete a Unified CM server from the Emergency Responder configuration while a phone tracking process is in progress. Retry the deletion after the process has ended.

Updating Cisco EmergencyResponder After You Add Devices

You must create a Unified CM user for Emergency Responder use and CTI ports and route points that must be assigned to the user before Emergency Responder tries to create a provider with the Emergency Responder cluster. Emergency Responder only registers the CTI ports and route points that are associated with the user when the provider is created. Any devices that you add to the user after starting Emergency Responder is not registered by Emergency Responder.

If you add devices to the Emergency Responder user in Unified CM, you can force Emergency Responder to recreate the provider using any of these techniques:

- Restart the Emergency Responder server.
- Delete the Unified CM server from the Emergency Responder configuration and reenter it.
- Change the backup CTI Manager setting for the Unified CM server in the Emergency Responder configuration and click **Update** to force Emergency Responder to log off the provider and to recreate it.
- Change the name of the user in Unified CM, or create a new user, and associate all devices with it. Then update the Emergency Responder configuration to use the new user.

Phone Moves Between Clusters

For additional information, see Track Phone Movement Across a Cluster, on page 32.

Identify Emergency Responder Groups and Servers in Cluster

If you are connected to the administrator interface on a Emergency Responder server, you can view the details of the server and the Emergency Responder group's standby server by selecting **System** > **CiscoER Group Settings**.

You can also identify the Emergency Responder groups and their Emergency Responder servers that are in the same Emergency Responder cluster. To view the other Emergency Responder groups in the cluster, select **System** > **CiscoER Groups in Cluster**. From the Emergency Responder Groups in Cluster page, select the group that you want to view; and Emergency Responder displays the Emergency Responder servers that are in the group. To view the details for these servers, you must log into the Emergency Responder Administration interface running on one of the servers, select **System > CiscoER Groups in Cluster**, then select the group that you want to view from the list of groups.

If you must uninstall a Emergency Responder group, first delete the group from the Emergency Responder cluster using this page. You must log in as a system administrator to delete the group. Deleting the group from the cluster only removes the entries for the group from the Emergency Responder Cluster DB; it does not remove Emergency Responder from the group's servers.

Related Topics

Server Groups in Cluster , on page 362

Manage Emergency Responder Server

When you install Emergency Responder, the Emergency Responder server is set up to automatically start whenever the computer is powered up or rebooted. However, you can stop and then restart an Emergency Responder server through the Emergency Responder Serviceability web interface without powering down or rebooting the computer.

Procedure

Step 1 Log in to the Emergency Responder Serviceability web interface and select **Tools** > **Control Center**.
The Control Center Services page displays, showing all Emergency Responder services and the current status of each one.

Step 2 Click the radio button to the left of the service name, then click **Start**, **Stop**, or **Restart** to perform the desired action on the service. Click **Refresh** to refresh the screen with updated information.

Note The buttons only appear if the action is possible; for example, **Start** only appears if the service is currently stopped.

Note The Cisco Tomcat and Cisco IDS services cannot be started or stopped from the Control Center. These services can only be started or stopped using the **utils service** command.

The following table explains the meaning of the icons that you see on the Control Center Services page.

Table 25: Cisco Emergency Responder Control Center Icons

Icon	Meaning
▶	The Emergency Responder server or the Emergency Responder Phone Tracking Engine is started and functioning normally.
■	The Emergency Responder server Emergency Responder Phone Tracking Engine was stopped by the administrator.

Related Topics

Control Center, on page 509

Troubleshoot ALI Data Uploads

Periodically, you must export your ALI data and submit it to your service provider. The ALI data is used to route emergency calls from your network to the correct PSAP, and provide the PSAP with information about the location of the emergency call.

Emergency Responder lets you export the ALI data in a variety of NENA formats. Ask your service provider which format you should use.

During the upload process, you might find that some ALI data records did not upload correctly. Your service provider can provide you with a list of errors, or you can see these when using your service provider's data upload software. You must fix any mistaken records and resubmit the ALI data export file. To fix the records, you need to manually edit the records in error.

The following sections describe the general procedure for fixing ALI data records, and explain how to edit the various types of NENA formatted files.

Fix ALI Data Records

To correct data errors that you might receive when uploading ALI records to your service provider, follow these steps.

Before you begin

Obtain NENA Doc 02-010, refer the appropriate Exhibit for NENA version for the Recommended Formats and Protocols for Data Exchange, from NENA or your service provider. Service Provider may have additional requirements.

Procedure

Step 1 Check the error reports to determine the problems you encountered.

Step 2 In the Emergency Responder web interface, change the fields that were in error for the ERL or ALI records that failed. For example, if the Street Suffix was an unacceptable abbreviation, change it to an acceptable one. Save all of your changes.

Step 3 Export the ALI data again (see the online help).

Step 4 If any of the records in error were new, you must change the database function for the records. Because Emergency Responder has already exported these records, Emergency Responder labels them as updates instead of new insertions. However, because these records failed on upload, the service provider's database views them as new.

Open the ALI export file in a text editor and change the function code for the records that you are fixing. Use an editor that will not add formatting or other extra characters. See these sections for details about editing the files:

- NENA 2.0 and 2.1 File Formats , on page 351
- NENA 3.0 File Formats , on page 352

Step 5 Submit the edited file to your service provider.

NENA 2.0 and 2.1 File Formats

The NENA 2.0 and 2.1 file formats have these characteristics:

- Fixed-length records.
- Fields are in a specific order.
- Unused fields are filled with blanks.
- End of record is indicated by an asterisk (*).

Use NENA Doc 02-010 (Exhibit 5.5 for Version 2.0 and Exhibit 5.9 for Version 2.1), Recommended Formats and Protocols for Data Exchange, to determine the byte location and length of each field. When you edit the file, ensure that you are not lengthening the records. Delete any extra spaces that get added. If the length of an item is less than the length of a field, pad the field with blanks. Depending on the field, padding might be on the right or the left.

The file contains one header and one trailer record. The ALI data records are contained between these records.

The following table describes the fields you are most likely to edit. You should use the Emergency Responder web interface to change the other fields.

Table 26: NENA 2.0 and 2.1 Common Fields

Field	Description
Function Code	**Location:** Byte 1. **Length:** 1 character. **Description:** The database function for the record. One of: • **I**—Insert new ALI record • **C**—Change existing record. You must have successfully uploaded the record once before you can use C. If you are correcting a record that has never been successfully uploaded, change the C to an I. • **D**—Delete the record. Emergency Responder only generates a deletion record once, in the export file created after you deleted the ALI from the Emergency Responder configuration. If you must regenerate the record, cut and paste it from the previous export file (and adjust the record count), or recreate the ALI in Emergency Responder, save it, export the data, then delete the ALI and export the data again.
Cycle Counter (sequence number)	**Location:** Byte 62 to 67. **Length:** 6 characters. **Description:** The sequence number of the file you are submitting to the service provider (for example, 1 or 2.) The number is right-aligned with leading spaces. Your service provider might ignore this field.
Record count	**Location:** Byte 62 to 70 in the trailer record. **Length:** 9 characters. **Description:** The total number of records in the file you are submitting to the service provider (for example, 1 or 2.) The number is right-aligned with leading spaces.

NENA 3.0 File Formats

The NENA 3.0 file format has these characteristics:

- Variable-length records.
- Fields are a tag and data combination, and can be in any order.
- Unused fields are not included. The presence or absence of a tag has this effect:
  - If the tag is not included, the previous value of the element, if any, is left unchanged.
  - If the tag is included with a blank value, any previous value for the element is removed.
  - If the tag is included with a non-blank value, the value of the element is changed to the new value.
- Tags are separated by a verticalbar(|).
- End of record is indicated by a predefined character.

Use NENA Doc 02-010 (Exhibit 5.13 for Version 3.1), Recommended Formats and Protocols for Data Exchange, to determine tag name and values for each field. Ensure that your values do not exceed the maximum length for the field. You do not need to pad fields with extra blanks.

The file contains one header and one trailer record. The ALI data records are contained between these records.

The following table describes the fields that you are most likely to edit. You should use the Emergency Responder web interface to change the other fields.

Table 27: NENA 3.0 Common Fields

Field	Description
Function Code	**Tag:** FOC. **Description:** The database function for the record. One of: • **I**—Insert new ALI record (FOCI) • **C**—Change existing record (FOCC). You must have successfully uploaded the record once before you can use C. If you are correcting a record that has never been successfully uploaded, change the C to an I. • **D**—Delete the record (FOCD). Emergency Responder only generates a deletion record once, in the export file created after you deleted the ALI from the Emergency Responder configuration. If you must regenerate the record, cut the version number and paste it from the previous export file (and adjust the record count); or recreate the ALI in Emergency Responder, save it, export the data, then delete the ALI and export the data again.
Cycle Counter (sequence number)	**Tag:** CYC. **Description:** The sequence number of the file you are submitting to the service provider (for example, CYC1 or CYC2.) Your service provider might ignore this field.
Record count	**Tag:** REC in the header and trailer records. **Description:** The total number of records in the file that you are submitting to the service provider (for example REC1 or REC2.)

Call History Logs

Emergency Responder maintains extensive call history logs, which include entries for each emergency call handled. You can view call history information from the administration and user interfaces.

Emergency Responder maintains in its database a history of the emergency calls that have been placed. When the primary Emergency Responder server (Publisher) is not active, emergency calls are handled by the backup Emergency Responder server (Subscriber). Through replication, the call history records on both these servers are synchronized when they are active. For this reason, the call history can be viewed on either of the Emergency Responder servers.

To download these records, click the **Download** button at the top of the table displaying the call history. These records are downloadable in Excel (.xls) format.

Trace and Debug Information

When you contact Cisco Technical Support for help with a problem that you are having with Emergency Responder, Cisco might request that you collect trace and debug information.

Because collecting trace and debug information affects Emergency Responder performance, you should only turn on tracing and debugging at Cisco's request. The generated information is for Cisco's use in resolving product problems.

Enable Emergency Responder Trace and Debug Information

Procedure

Step 1 From the Emergency Responder web interface, select **Cisco ER Group > Server Settings For CERServerGroup**.

Step 2 From the left column, select the server from which you must collect debug or trace information.

Step 3 Scroll down to the debug package and trace package sections and select the packages that Cisco Technical Support has requested.

The lists in each section are identical; make sure that you select the package in the list that Cisco requested. Packages selected in the Debug list generate trace information plus extra debug data. If Cisco requests that you select all packages, click **Select All** for the appropriate list.

The available packages include:

- CER_DATABASE—The database subsystem, covers the log information generated by the database access code.
- CER_REMOTEUPDATE—The remote update subsystem, which manages updates between servers.
- CER_PHONETRACKINGENGINE—The phone tracking subsystem, which runs the phone tracking and switch port and phone update processes.
- ER_ONSITEALERT—The onsite alert subsystem for notifying onsite alert personnel.
- CER_CALLENGINE—The call engine subsystem, which routes and processes calls.
- CER_PROVIDER—The local service provider.
- CER_AUDIT—The Audit trials provide change history for ERL configurations.
- CER_APPSERVICES—The API services subsystem which administers the traces of all the services belonging to it.
- CER_SYSADMIN—The system administration web interface subsystem.
- CER_TELEPHONY—The telephony subsystem, used for interactions with Unified CM.
- CER_AGGREGATOR—The aggregator module covers all Emergency Responder server communication and data handling with the phone tracking engine. The module includes the search and lookup of tracked data for the subsystems such as cluster, Administration, CiscoIPSoftPhone, and call routing.
- CER_GROUP—The Emergency Responder server group subsystem used for communicating between servers within a group.
- CER_CLUSTER—The server cluster subsystem used for communicating between Emergency Responder groups in a cluster.
- CER_ACCESSPOINT—The access point details all the devices configured in Unified CM.
- CER_CREDENTIALPOLICY—The credential policy defined for all the local and remote user accounts.

Step 4 Click **Update** to save and activate your changes.

Emergency Responder begins generating the requested trace and debug information.

Note The traces for Emergency Responder can be collected from either Emergency Responder Serviceability web interface or by using the CLI.

Step 5 When you have finished generating debug and trace information, click **Clear All** for each section in which you have made a selection to turn off debug and trace. Click **Update** to complete the change.

Related Topics

Server Settings for Emergency ResponderServerGroup , on page 370
Cisco Emergency Responder Serviceability Web Interface , on page 509

Syslog Enablement

To collect trace and debug information, you must enable syslog for Emergency Responder.

To enable syslog for Emergency Responder, see Collect Information From Syslog , on page 356.

Event Messages

You can view Emergency Responder event messages to help diagnose problems with the software by using the Emergency Responder Serviceability web interface.

For information about viewing Emergency Responder events, see Use Event Viewer, on page 196.

For details about the Find and List Events page, see Event Viewer, on page 510.

Performance Management

See the latest version of the Release Notes for Cisco Emergency Responder for supported platforms and their Emergency Responder scalability.

Emergency Responder performance can be affected if Emergency Responder is managing switches across a WAN link. Emergency Responder must send SNMP requests to the managed switches, and WAN delays can lead to SNMP timeouts and increase the time needed to track phone and switch changes. You might need to tune the SNMP parameters. See Set Up SNMPv2, on page 149 for more information.

Network Management Systems Integration

You can manage the status of the Emergency Responder server remotely using any SNMP-based network management system.

The following sections provide information to assist you in integrating Emergency Responder with network management systems.

Cisco Discovery Protocol Support

CiscoEmergency Responder uses the Cisco Discovery Protocol (CDP) to periodically send out CDP messages on the active interface to a designated multicast address. These messages contain information such as device identification, interface name, system capabilities, SNMP agent address, and time-to-live. Any Cisco device with CDP support can locate a CiscoEmergency Responder server by listening to these periodic messages.

Using information provided through CDP, the SNMP-based network management server can detect the CiscoEmergency Responder server and build topology maps displaying the CiscoEmergency Responder server.

In addition to sending out CDP messages, the CiscoEmergency Responder server uses CDP to locate phones that support CDP. You must ensure CDP is enabled on your switches so that CiscoEmergency Responder can obtain this information through SNMP queries to the switches.

Emergency Responder Components

CiscoEmergency Responder supports the SYSAPPL-MIB that allows you to use any SNMP-based browser to remotely access information about the following Emergency Responder components:

- CiscoEmergency Responder Server
    - CERServer.exe
- Cisco PhoneTrackingEngine
    - CERPhoneTracking.exe
- MSQL Server-related Services

The SYSAPPL-MIB uses SNMP. Emergency Responder supports the following SYSAPPL-MIB tables:

- SysApplInstallPkgTable—Provides installed application information such as Manufacturer, Product Name, Version installed, Date installed, and Location, which is a partial URL for accessing the associated Application Administration web page (when applicable).
- SysApplRunTable—Describes the application starting time and run-time status.
- SysApplInstallElmtTable—Describes the individual application elements, or associated executables, which comprise the applications defined in the SysApplInstallPkgTable.
- SysApplElmtRunTable—Describes the processes, or executables, that are currently running on the host system.

Collect Information From Syslog

You can configure Emergency Responder to use Syslog output from Emergency Responder for use with other network management systems.

Procedure

Step 1 Select **System** > **CiscoER Group Settings**.

Emergency Responder opens the Emergency Responder Group Settings page.

Step 2 Select enable in **Enable Syslog**.

Step 3 Enter the fully qualified DNS name of the server in the **Syslog Server** field, for example, server.domain.com.

Step 4 Click **Update Settings** to save your changes.

Emergency Responder immediately begins writing messages to syslog.

Related Topics

Group Settings, on page 363

Data Backup and Recovery

Emergency Responder uses the Disaster Recovery System to backup and restore system data.

For information about using the Disaster Recovery System, see Configure Cisco Emergency Responder Disaster Recovery System, on page 237

During a backup and restore procedure, you might encounter one of the following errors:

- Unable to send network request to master agent. This may be due to Master or Local Agent being down.
- Local Agent is not responding. This may be due to Master or Local Agent being down.

Check your Publisher and Subscriber services and confirm that your DRS Local and Master services are active and running.

Check your IPSEC certificates via the Cisco Emergency Responder OS Administration UI. Make sure these IPSEC-Trust certificates are not expired or corrupted. If they are expired or corrupted, regenerate these IPSEC certificates on all nodes and restart the Master and local agents.

Troubleshooting Data Migration Assistant

The Data Migration Assistant (DMA) operates in two phases. In the first phase, Database, the following folders are backed up to a tar file:

- export
- import
- etc
- nena_msag_records

In the second phase, the contents of the backed-up Emergency Responder database are verified against the Emergency Responder database schema.

DMA Backup and Validation Failed

Problem DMA backup and validation failed.

Solution Go through the following check list:

- Check if MSDE is running. If the database is not running, the backup fails.
- Verify that the node being backed up is a Publisher node, not a Subscriber node. DMA backup cannot be performed on a Subscriber node.
- Verify that CSA is not running. If CSA is running, stop it before starting the backup.

DMA Backup Is Successful but Validation Failed

Problem DMA backup is successful but the validation failed.

Solution Go through the following check list:

- Verify that CSA is not running. If CSA is running, stop it before starting the backup. CSA interferes with DMA operation.
- Collect the data validation logs for further analysis. In this case, some changes may need to be made to the data in the database before a migration to Emergency Responder can succeed.

Solution The DMA Logs are in the following locations:

- exportdb.log and migratecCERCSV.log are in C:\CiscoWebs\DMA\Bin
- installdbw1.log, installdbw1.log.err, installdbccm.log, installdbccm.log.err, and dbl_INSTALLDBxxxxxx.txt are located under C:\Program Files\Cisco\Trace\DBL
- Log Files are located under C:\Program Files\Cisco\Trace\DMA

Solution The validation log files are as follows:

- **Solution** exportdb.log
- **Solution** installdbw1.log
- **Solution** installdbw1.log.err
- **Solution** dbl_INSTALLEDBxxxxxx.txt

Troubleshoot Linux Upgrades

You might encounter certain problems when upgrading to future versions of Emergency Responder from your current version of Emergency Responder. This section explains what could cause these problems and the provides recommended actions.

No Valid Upgrade Options Found Error Appears on the First Page of Install/Upgrade Menu

Problem On the first page of the Install / Upgrade menu, after you enter the details for an upgrade patch, the error message “No valid upgrade options found” appears.

Solution Verify that you are not trying to upgrade the Subscriber before upgrading the Publisher. When upgrading an Emergency Responder server group, you must always upgrade the Publisher first.

Solution Verify that the local or remote path that you have specified actually contains a valid, signed ISO image, having the extension .sgn.iso.

Incorrect User Name/Password Error Appears on the First Page of the Install/Upgrade Menu

Problem On the first page of the Install / Upgrade menu, after you enter the details for an upgrade patch at a remote location, the error message “Incorrect user name/password” appears.

Solution Verify that the username and password entered for the remote SFTP or FTP location are correct.

Checksum Values Do Not Match After Downloading ISO Image on Emergency Responder Server

Problem After downloading the ISO image onto the Emergency Responder server, the checksum values do not match.

Solution Download a fresh ISO image from Cisco.com and try the upgrade again.

Upgrade Cancelled and Warning Message Appears Prompting You to Reboot System

Problem The upgrade was cancelled, but a warning message appears prompting you to reboot the system.

Solution During the upgrade, certain services on the Emergency Responder server could have been stopped, depending on when the upgrade was cancelled. In this case, it is highly recommended that you reboot the server.

Troubleshoot SAML Single Sign-On

Problem—The User Interface page does not come up when SAML Single Sign-On is Enabled or Disabled.

Solution—Check the status of the Cisco Tomcat service and restart the service manually on both publisher and the subscriber nodes if the status is not active.

Troubleshoot IOS Switch Upgrades

Assigned ERLs Turns to Null After IOS Switch Upgrade in Emergency Responder Server

Problem—After upgrading the IOS software on the switch in the Emergency Responder, it changes the port index value of the switch. And, the Emergency Responder treats the existing port as a new port and turns the assigned ERL to Blank (no ERL).

Solution—If the snmp-server ifindex persist configuration is present on the switch before the upgrade, then port information stays correct. By executing the "snmp-serverifindex persist" command on the switch, port information remains same after the upgrade.

Note Execute the **show run| inc snmp ifmib** command to check whether the snmp-server ifindex persist configuration is present in the Switch. If the ifIndex persist configuration exists, the output is displayed as:

```
Snmp ifmib ifindex persist
```

APPENDIX A

Cisco Emergency Responder Administration Web Interface

Server Groups in Cluster

The Emergency Responder Server Groups in Cluster page appears when you choose **System > CiscoEmergency Responder Groups in Cluster**.

Authorization Requirements

You must have system administrator, ERL administrator, or network administrator authority to access this page.

Description

Use the Emergency Responder Server Groups in Cluster page to view the Emergency Responder groups that form an Emergency Responder cluster. You can view which Emergency Responder servers belong to each Emergency Responder group within the cluster. You can click on the link for the remote server groups in an Emergency Responder cluster (select either the primary server or the backup server) to go directly to the Emergency Responder interface for these servers.

The following table describes the Emergency Responder Server Groups in Cluster page.

Table 28: Cisco Emergency Responder Server Groups in Cluster Page

Field	Description	Notes
Emergency Responder Groups		
Emergency Responder Groups list	A list of the Emergency Responder server groups that are pointing to the same cluster database host. Click a group name to view the servers in the group.	The Emergency Responder cluster consis set of Emergency Responder groups. You the cluster when installing Emergency Re servers. See Installation on a New System 63.
Servergroup Details		
Emergency Responder Group Name	The name of the server group.	Click the server group name to display th in that group in the Servergroup Details s page.

Field	Description	Notes
Primary Host Name	The DNS host name or IP address of the primary server in the group.	Click this host name (except for the lo group) to open the Emergency Respor administration page for that server in window.
Standby Host Name	The DNS host name or IP address of the standby, or backup server in the group.	Click this host name (except for the lo Group) to open the Emergency Respo administration page for that server in window.
Delete button	Click **Delete** to remove the Emergency Responder group you are viewing from the Emergency Responder cluster.	Only system administrators can delete Responder group from the cluster. Delete a group from the cluster before a Emergency Responder group.

Related Topics

Identify Emergency Responder Groups and Servers in Cluster , on page 349

E911 and Cisco Emergency Responder Terminology , on page 6

Group Settings

The Emergency Responder Group Settings page appears when you choose **System > Cisco ER Group Settings**.

Authorization Requirements

You must have a system administrator authority to access this page.

Description

Use the Emergency Responder Group Settings page to define the operational characteristics of an Emergency Responder server group.

The following table describes the Emergency Responder Server Group Settings page.

Table 29: Cisco Emergency Responder Group Settings Page

Field	Description	Notes
Emergency Responder Group Name	The name of the server group. This name is used for your information only, so create a name you find useful.	
Peer TCP Port	The TCP port used for communications between Emergency Responder servers within the server group. If you don't want to use the default port, ensure you select an unused port.	The range is 1024 to 65535.

Field	Description	Notes
Heartbeat Count	The number of counts an Emergency Responder server should wait before declaring an unresponsive Emergency Responder server unavailable.	The default number of counts is 3. The rang is 3 to 10. The time between counts is defined in Heartbeat Interval.
Heartbeat Interval (in sec)	The number of seconds between sending heartbeat messages to the other Emergency Responder server in the server group.	The default is 30 seconds. The range is 30 300 seconds.
Active Call Timeout (in min)	How long to maintain a call route mapping so the PSAP can call back the emergency caller.	The default is 180 minutes (3 hours). The range is 30 to 1440 minutes.
SMTP Mail Server	The IP address or fully qualified name of the mail server (for example, email.domain.com). Check the **Enable Secured connection** check box to send mails from the SMTP Mail Server in a secure mode.	Configure an email server if you want Emergency Responder to send email or email-based pages to security officers whe an emergency call is made. Ensure to configure the SMTP Mail Server a secure mode and the SMTP server certifica is added to the Tomcat trust store of the Cis Emergency Responder before enabling the check box. Failing to do so may result in em alert delivery failure. The Port number for enabling Secure SMT connection is 587. To set up a Secure SMT connection, perform the following: **1.** Exchange Cisco Emergency Responde Tomcat certificate chain to SMTP serve root certificate directory. **2.** Upload SMTP server certificate chain tomcat-trust certificates on Cisco Emergency Responder. **3.** Restart Cisco Tomcat service on Cisco Emergency Responder servers using th CLI command **utils service restart Cis Tomcat**.
Source Mail ID	If you configure a mail server, you must enter an email account on that server that can be used for sending email.	Emails or pages sent to security come from this email account.
System Administrator Mail ID	Mail account where Emergency Responder sends critical information about the system.	Emails or pages sent to the system administrator by Emergency Responder co to this email account.

Field	Description	Notes
Calling Party Modification	Dynamic modification of the calling party number. Allows you to reduce the number of route patterns by configuring multiple ELIN numbers for a single route pattern. ELIN numbers must still be unique.	You must set this flag if you enabled Ca Party Modification when you created Emergency Responder as a Unified CM
Syslog	Select from the drop-down list that enables and disables the writing of log messages.	
Syslog Server	The name of the server that has the log messages. Enter the fully qualified DNS name of the server, for example, cw2k.domain.com.	Enter the hostname or IP address of the s server to accept syslog messages. This s handles the logging of all the Cisco Emergency Responder application event-related information. 514 is the default port used to commun **Note** You can only enter a serve name if you choose **Enabl Syslog**.
Notes	Any notes you want to enter to help you understand the use of the server group.	
Dynamic Tracking of Switch IP Address	Dynamically updates a LAN switch's IP address if it is configured with hostname in Emergency Responder.	This action is not applicable to LAN sw that are added to Emergency Responder an IP address.
Security end user web interface language	Pulldown menu allows you to select the language that is displayed on the users web page—English (US), French (Canada), or Spanish (Spain).	After you change the language, you mu complete the following before the langu is displayed on the users web page: • Restart Emergency Responder Ser in Emergency Responder Servicea by choosing **Tools > Control Cen** • Restart Cisco Tomcat service usin CLI command **utils service restar Cisco Tomcat**. • Refresh the current Emergency Responder User webpage.
Limit Concurrent Sessions	Limits the number of concurrent sessions per user.	Selecting or deselecting this check box en or disables the Max. number of concurr sessions drop-down list.

Field	Description	Notes
Max. number of concurrent sessions	If Limit Concurrent Sessions is enabled, this limit is applicable for all the users.	The limit is imposed separately for each Emergency Responder website: • Emergency Responder Administratio • Emergency Responder Serviceability • Emergency Responder User • Emergency Responder Admin Utility
Enable AXL & Cluster Secured connection	AXL communication with other products and cluster communication is secured.	Ensure the Cisco Unified Communications Manager tomcat-trust certificate and the Cis Emergency Responder server group certifica is added to the Tomcat trust store of the Cis Emergency Responder (in both publisher an subscriber). Failing to do so may result in breaking of AXL communication between Cisco Unified Communications Manager an Cisco Emergency Responder, along with th cluster communication within the Cisco Emergency Responder group.
Discovery Threshold Time (in hrs)	Set the threshold time after which the Emergency Responder sends you an email alert when the discovery of Cisco IP Phones or devices is stalled. Emergency Responder should be able track the devices anytime from 6 to 24 hours. Check the **Enable Discovery Mail Alert** check box to enable the Discovery mail alert option.	The default is 0 hours if you do not enable t **Enable Discovery Mail Alert** check box. T threshold range is 6 to 24 hours.
IPv6 Subnet Configurations have precedence over IPv4	Check the check box if you want the E911 calls to take precendence of IPv6 subnet over the IPv4 subnet. If you uncheck this option, IPv4 subnet is given precedence, and the calls are routed via the IPv4 subnet. For more information on the various IPv6/IPv4 precedence scenarios using both dual-stack and single stack devices, see Table 30: IPv6 Subnet Precedence over IPv4 Scenarios, on page 367.	**Note** Cisco Jabber devices will not work with IPv6 subnets in Emergency Responder.
Update Settings button	Click **Update Settings** to save and activate your changes.	
Cancel Changes button	Click **Cancel Changes** to change the fields on this page back to the last saved settings.	

Table 30: IPv6 Subnet Precedence over IPv4 Scenarios

Scenario	IPv6 Subnet Added	IPv4 Subnet Added	IPv6 Precedence Disabled	IPv6 Precedence Enabled
New call from IPv6 + IPv4 Dual stack phone	Yes	Yes	Calls are routed via the ERL assigned to the IPv4 subnet	Calls are routed via the ERL assigned to the IPv6 subnet
New call from IPv6 + IPv4 Dual stack phone	Yes	No	Calls are routed via the ERL assigned to the IPv6 subnet	Calls are routed via the ERL assigned to the IPv6 subnet
New call from IPv6 + IPv4 Dual stack phone	No	Yes	Calls are routed via the ERL assigned to the IPv4 subnet	Calls are routed via the ERL assigned to the IPv4 subnet
New call from IPv6 + IPv4 Dual stack phone	No	No	Call is routed using the routing pattern configured for the caller's ERL. If none of the call routing criteria is used to determine the phone location using the Call Routing Order , the default ERL treatment is provided.	Call is routed using the routing pattern configured for the caller's ERL. If none of the call routing criteria is used to determine the phone location using the Call Routing Order , the default ERL treatment is provided.
New call from IPv6 single stack phone	Yes	Not a valid scenario since the phone has only the IPv6 subnet configured	Calls are routed via the ERL assigned to the IPv6 subnet	Calls are routed via the ERL assigned to the IPv6 subnet
New call from IPv6 single stack phone	No	Not a valid scenario since the phone has only the IPv6 subnet configured	Call is routed using the routing pattern configured for the caller's ERL. If none of the call routing criteria is used to determine the phone location using the Call Routing Order , the default ERL treatment is provided.	Call is routed using the routing pattern configured for the caller's ERL. If none of the call routing criteria is used to determine the phone location using the Call Routing Order , the default ERL treatment is provided.
New call from IPv4 single stack phone	Not a valid scenario since the phone has only the IPv4 subnet configured	Yes	Calls are routed via the ERL assigned to the IPv4 subnet	Calls are routed via the ERL assigned to the IPv4 subnet

Scenario	IPv6 Subnet Added	IPv4 Subnet Added	IPv6 Precedence Disabled	IPv6 Precedence Enabled
New call from IPv4 single stack phone	Not a valid scenario since the phone has only the IPv4 subnet configured	No	Call is routed using the routing pattern configured for the caller's ERL. If none of the call routing criteria is used to determine the phone location using the Call Routing Order , the default ERL treatment is provided.	Call is routed using the routing pattern configured for the caller's ERL. If none of the call routing criteria is used to determine the phone location using the Call Routing Order , the default ERL treatment is provided.

Related Topics

Set Up a Server Group, on page 128

Collect Information From Syslog , on page 356

Restrict Maximum Number of Concurrent Sessions , on page 127

Track Change of Switch IP Address Dynamically , on page 158

E911 and Cisco Emergency Responder Terminology , on page 6

Telephony Settings

The Telephony Settings page appears when you choose **System** > **Telephony Settings**.

Authorization Requirements

You must have system administrator authority to access this page.

Description

Use the Telephony Settings page to define the telephone numbers and telephony ports used by the Emergency Responder group.

The following table describes the Telephony Settings page.

Table 31: Telephony Settings Page

Field	Description	Notes
Specify telephony attributes		
Route Point for Primary Emergency Responder Server	The CTI route point that the primary server should use, such as 911.	See Create Emergency Call Route page 87 for more information.
Route Point for Standby Emergency Responder Server	The CTI route point that the standby server should use, such as 912. Configure this number as the call forward number for the primary emergency number.	See Create Emergency Call Route page 87 for more information.

Field	Description	Notes
PSAP Callback Route Point Pattern	CTI route point that you defined to receive calls from the public safety answering point (PSAP). For example, 913XXXXXXXXXX (913 plus ten Xs). The number can only consist of numbers and Xs.	For more information, see Crea Call Route Points, on page 87.
ELIN Digit Strip Pattern	Digits to strip from the beginning of the PSAP Callback Route Point Pattern, for example, 913. The number that results from stripping the pattern should be the ELIN numbers that the PSAP can use to call into your network.	This string must be part of the P Route Point Pattern.
Default ELIN Digit Translation	ELIN number obtained after stripping 913 is matched to a callers extension. If the mapping is not found, Emergency Responder will translate ELIN to Default ELIN Digit Translation number and complete the PSAP Call-back.	The number could be a dialabl number or a route pattern. If the reachable the PSAP Call-back reorder tone.
UDP Port Begin	Port numbers that are used by CTI ports during their registration.	The range is 1024 to 65535.
Inter-Emergency Responder Group Route Pattern	Route pattern that other Emergency Responder groups use to route emergency calls to this group, for example, 1000.911. The pattern can only consist of numbers and dots.	For a more detailed explanatio number, see "Create route patte Inter-Cisco Emergency Respon Communications".
IP Type of service (00-FF)	Value of the type of service (ToS) byte in the IP header. The default 0xB8 implies a ToS class of Priority Queue. It is recommended that this default value be used for Emergency Responder.	The ToS value entered here on the RTP packets sent by Emerg Responder for the onsite audio
Onsite Alert Prompt Repeat Count	Number of times the prompt is played on the onsite alert phone.	
Use IP Address from call signaling	If this parameter is enabled, Emergency Responder obtains the IP address of the phone from JTAPI. This parameter is used to route the call. If an IP subnet is configured for the phone, this parameter setting takes precedence over any other manual configuration. If this parameter is disabled, Emergency Responder uses the manual configuration of the phone to route the call. **Note** The feature is mainly for Analog Phones (which are manually defined). This option can be tracked behind IP Gateways and receive IP Subnet treatment.	This field is applicable only if Responder is configured with C Communications Manager 6.x
Update Settings button	Click **Update Settings** to save and activate your changes.	
Cancel Changes button	Click **Cancel Changes** to change the fields on this page back to the last saved settings.	
National E911 Service Provider Route Pattern Settings		

Field	Description	Notes
National E911 Service Provider Route/Translation Pattern	Enter the route patterns or translation pattern for an National E911 Service Provider emergency response location (ERL). An National E911 Service Provider ERL is an ERL that is serviced byNational E911 Service Provider. National E911 Service Provider ERL only lists the route patterns that have been configured on this page. You can add new route patterns or translation patterns, or you can update or remove existing route patterns or translation patterns. National E911 Service Provider Route Pattern Settings supports a maximum of 3000 characters in total.	To add a new route or translation pa on the text box, enter the route pat including numbers and wildcard (c spaces), and click **Add**. To update an existing route patterr the appropriate route pattern, modi pattern, and click **Update**. To remove an existing route patter the appropriate route pattern and c **Remove**. To cancel your existing changes ar to the last saved settings, click **Ca Changes.**

Related Topics

Set Up Group Telephony Settings for Server , on page 129

E911 and Cisco Emergency Responder Terminology , on page 6

Server Settings for Emergency ResponderServerGroup

The Server Settings for Emergency ResponderServerGroup page appears when you choose **System > Server Settings**.

Authorization Requirements

You must have system administrator authority to access this page.

Description

Emergency Responder servers are inserted in the Emergency Responder group when the Emergency Responder services are started. (See Installation on a New System , on page 63.)

Use the Server Settings for Emergency ResponderServerGroup page to update server settings, for example, to change the server name or to change the trace and debug settings, or to delete servers.

Note You cannot modify the host name of the server.

The following table describes the Server Settings Emergency ResponderServerGroup page.

Table 32: Server Settings for the Emergency ResponderServerGroup Page

Field	Description	Notes
Status	Displays the status of the Server Settings Emergency ResponderServerGroup page.	

Field	Description	Notes
Select Server		
Server	List of servers you have already created. Click on a server name to see the settings for that server.	You can configure a maximu servers per server group.
Modify Server Settings		
Server Name	The name of the server.	Change this server name fiel desired value.
Host Name	The DNS name of the Emergency Responder server.	This field cannot be modifie
Debug Package List	A selection of subsystems for which you must collect detailed debug information. Debug information includes trace messages as well as more detailed messages. Only select subsystems at the request of Cisco Technical Support; the debug information is for Cisco's use to help resolve problems that you cannot solve yourself.	See Trace and Debug Inform page 354 for an explanation
Select All button	Selects all subsystems in the Debug Package List.	
Clear All button	Clears all selected subsystems in the Debug Package List.	
Trace Package List	A selection of subsystems for which you must collect brief trace information. Only select subsystems at the request of Cisco Technical Support; the trace information is for Cisco's use to help resolve problems that you cannot solve yourself. If you select a subsystem for debug, you do not have to select it for trace.	See Trace and Debug Inform page 354 for an explanation
Select All button	Selects all subsystems in the Trace Package List.	
Clear All button	Clears all selected subsystems in the Trace Package List.	
Update Settings button	Click **Update** when viewing an existing server's settings to save changes you make to the settings.	Only available when viewin of an existing server.
Cancel Changes button	Click **Cancel Changes** to change the fields on this page back to the last saved settings.	

Related Topics

Configure Servers , on page 131

Trace and Debug Information , on page 354

E911 and Cisco Emergency Responder Terminology , on page 6

License Manager

The **License Manager** page appears when you choose **System** > **License Manager**.

Authorization Requirements

You must have the system administrator authority to access the **License Manager** page.

Description

The **License Manager** page provides the summary and detailed information on the system license usage, as it is reported to the Cisco Smart Software Manager or Cisco Smart Software Manager satellite. Licenses are assigned to the company Smart Account and are not node locked to a device.

Table 33: License Manager Page

Field	Description
Status	Displays the steps to register with Cisco Smart Software Manager or Cisco Smart Software Manager satellite and the current license registration mode. For information on alarms or licensing alerts and compliance, see License Manager Status Messages, on page 335 and License Compliance, on page 11. **Note** For Specific License Reservation status message displays current license status. **Note** For Permanent License Reservation, status message displays the number of licenses that the administrator specified for this system to operate within. License count does not affect compliance status and it is for administrator reference only. Admin can set the license count through Command Line Interface.
Smart Software Licensing Status	

Field	Description
Registration Status	Displays the current registration status of the product. The different statuses are: • Registered—For the product which is registered. • Unregistered or Unidentified—For the product which is unregistered. • Unregistered-Registration Expired—For the product whose registration has expired. • Registered-Specific License Reservation/Universal License Reservation—For product which is registered in SLR/PLR mode. **Note** Smart Agent may reflect status as Universal License Reservation but is for Permanent Licenses Reservation feature. • Reservation In Progress—For product whose License Reservation is in progress.

Field	Description
License Authorization Status	Displays the overall authorization status of the product. The different statuses are: • Authorized—Product in authorized or in compliance state. • Authorization Expired—Authorization is expired for the product. This usually happens when the product has not communicated with Cisco for 90 continuous days. • Out of Compliance—Product is in out of compliance state because of insufficient licenses. • No Licenses in Use—Product does not consume any licenses. • Evaluation Mode—Product is in evaluation mode and not yet registered with Cisco. • Evaluation Period Expired—Evaluation period has expired. • Not Applicable—Unable to determine current registration status. • Authorized-Reserved—Product in authorized or in compliance status for the reserved licenses. • Not Authorized-Reserved—Product is not in authorized state because of insufficient licenses reserved. • Export Control Not Allowed—Product in eval mode.

Field	Description
Transport Settings **Note** This section will not be available when Specific License Reservation or Permanent License Reservation is enabled.	

Field	Description
	The different settings through which Cisco Emergency Responder can connect to Cisco Smart Software Manager or Smart Software Manager satellite are: • Direct—Cisco Emergency Responder sends usage information directly over the internet. No additional components are needed. • Cisco Smart Software Manager satellite—Cisco Emergency Responder sends license usage information to an on-premises collector called Cisco Smart Software Manager Satellite which requires a periodic exchange of information with Cisco Smart Software Manager cloud service. • If you are using HTTP, go to the URL: http://Satellite-ip/Transportgateway. • If you are using HTTPS, go to the URL: https://SatelliteFQDN-OR-IP-address/TransportGateway. For more information on how to register your devices using Cisco Smart Software Manager satellite, see https://community.cisco.com/t5/cisco-software-documents/how-to-register-your-device-using-https-to-satellite-smart/ta-p/3747976. For more information on installation or configuration of the Smart Software Manager satellite, go to this URL: https://www.cisco.com/c/en/us/buy/smart-accounts/software-manager-satellite.html. • Proxy Server—Cisco Emergency Responder sends usage information over the internet through a proxy server. Check the **Authentication needed on HTTP or HTTPS proxy** check box if want to register to Cisco Smart Software Manager using authentication based proxy server. If you enable this check box, only then the **Proxy User** and **Proxy Password** fields are enabled. Enter the details in the following fields: • Host Name/IP Address • Port • Proxy User **Note** Administrators should ensure

Field	Description
	that they enter the configured user name for proxy in the **Proxy User** field. • Proxy Password • Check the **Do not share my hostname or IP address with Cisco** check box to allow the administrator to restrict the exchange of IP Address and hostname of the Cisco Emergency Responder during the registration and synchronization to Cisco Smart Software Manager or Cisco Smart Software Manager Satellite. **Note** When the check box is selected, Cisco Emergency Responder will not share the IP Address or hostname information from being sent through registration and regular license compliance synchronization activities. A unique identifier is generated for the Cisco Emergency Responder Product Instance and must be used for cross-referencing in Cisco Smart Software Manager. **Note** If you choose to use direct connection, then you must configure Domain Name System (DNS) on Cisco Emergency Responder that can resolve tools.cisco.com. **Note** If you choose not to configure the domain and Domain Name System (DNS) on Cisco Emergency Responder, then you can select the transport gateway or proxy server. In such case, DNS that can resolve tools.cisco.com has to be configured on either on the proxy server. **Note** If you choose not to use the DNS server in your deployment and not connect to the internet, then you can select the Cisco Smart Software Manager satellite with manual synchronization in disconnected mode.

Field	Description
Smart Account Name **Note** This section will not be available when Specific License Reservation or Permanent License Reservation is enabled.	Displays information of the customer Smart Account. It is created from the **Request a Smart Account** option under Administration section of the https://software.cisco.com/. It is the primary account created to represent the customer and all licenses for a company that are assigned to this Smart Account. It also manages licenses for all Cisco products.
Virtual Account **Note** This section will not be available when Specific License Reservation or Permanent License Reservation is enabled.	A self-defined construct to reflect the company organization. Licenses and Product instances can be distributed across virtual accounts. Created and maintained by the administrator on the Cisco Smart Software Manager or Cisco Smart Software Manager satellite with full visibility to company assets.
Licensing Mode	Displays the licensing mode of the product. The default mode is Enterprise.
Export-Controlled Functionality	Specifies if the Export-Controlled functionality was enabled in the token with which the product was registered. **Note** The **Allow export-controlled functionality on the products registered with this token** check box is not displayed for the Smart Accounts that are not permitted to use the Export-Controlled functionality. Displays one of the following status information: • Allowed—The token registered with has Allow export-controlled functionality selected. • Not Allowed—The token registered with do not have Allow export-controlled functionality selected or Cisco Emergency Responder not registered. **Note** In Specific License Reservation or Permanent License Reservation, Export-Controlled functionality of product depends on the configuration of Smart Account to which it is registered.

Field	Description
Actions **Note** This section will not be available when Specific License Reservation or Permanent License Reservation is enabled.	The **Actions** drop-down list box gets activated only after a successful registration. It lists the following type of actions which can be performed: • Renew Authorization Now • Renew Registration Now • Reregister • Deregister
Register **Note** This section will not be available when Specific License Reservation or Permanent License Reservation is enabled.	Use the **Register** button to register Cisco Emergency Responder with Cisco Smart Software Manager or Cisco Smart Software Manager satellite. **Note** The **Register** button gets disabled after a successful registration with Cisco Smart Software Manager or Cisco Smart Software Manager satellite.
Request Entitlement Now	
Synchronize Now **Note** This section will not be available when Specific License Reservation is enabled.	Click the **Synchronize Now** button to send a synchronization (entitlement) request to Cisco Smart License Manager.
Last Synchronization **Note** This section will not be available when Specific License Reservation is enabled.	This is a static field that displays the last authorization attempt time and its success or failure status. For example, Jan 19 23:31:00 2017 IST (Succeeded). **Note** This field gets displayed only after a successful registration with the Cisco Smart Software Manager or Cisco Smart Software Manager satellite.
License Requirement by Type	
License Type	Displays the Cisco Emergency Responder (CER) license type. The only available license type is CER_USER.
Description	Displays the description for the license type which is, CER User License.

Field	Description
Status	Displays the current license status based on the license type (CER_USER).The different statuses are: • Authorization Expired—The authorized period has expired. • Evaluation—The agent is using the evaluation period for this entitlement. • Evaluation Period Expired—Evaluation period has expired. • Authorized—In compliance (authorized). • No Licenses in Use—There are no licenses being consumed by the product instance. • Out of Compliance—Out of compliance. • Waiting—The initial state after an entitlement request while waiting for the authorization request response.
Count	Displays the total number of users currently tracked.
Details of Cisco ER Licenses	
Number of phones discovered	Displays the number of discovered phones tracked in an IP Subnet and the Switch port.
Number of phones manually configured	Displays the number of manually configured phones. For example, analog phones.
Total number of users being tracked currently	Displays the number of phones tracked by Cisco Emergency Responder, which requires a User License. When you click the displayed hyperlinked number, the **Tracked Phones List** window is displayed, which lists the tracked phones.
Total number of users configured not to be tracked	Displays a list of phones configured with an IP Subnet and Cisco Emergency Responder does not track it. **Note** In a scenario where a Dual-stack phone has both the IPv4 and IPv6 addresses configured, and the phone falls under both the IPv4 and IPv6 subnets having the same priority, and one of the subnet is trackable and the other one is non-trackable, the phone is considered to be trackable.
Smart Licensing Product Registration	

Field	Description
The Smart Software Manager or Cisco Smart Software Manager satellite manages the product license. It also provides a link to the **Smart Software Manager** page.	

Related Topics

E911 and Cisco Emergency Responder Terminology , on page 6

Cisco Smart Software Licensing , on page 10

Smart Software Licensing Product Registration

The **Smart Software Licensing Product Registration** window is displayed when you click the **Register** button on the **License Manager** page. See License Manager, on page 371 page for more information on the system license usage.

Table 34: Smart Software Licensing Product Registration Page

Field	Description
Status	Displays the product registration status.
Product Instance Registration Token	Displays a text area where you can enter the product registration token generated from the Cisco Smart Software Manager or Cisco Smart Software Manager satellite.
Reregister this product instance if it is already registered	Check the **Reregister this product instance if it is already registered** check box to enable a force registration of the product with Cisco Smart Software Manager or Cisco Smart Software Manager satellite.
Register	Click the **Register** button to register Cisco Emergency Responder with Cisco Smart Software Manager or Cisco Smart Software Manager satellite.

Note The **Register** button gets disabled after a successful registration with Cisco Smart Software Manager or Cisco Smart Software Manager satellite.

Transport Setting

The **Transport Setting** window is displayed when you click **View/Edit** link from the **License Manager** page. For more information on system license usage, see License Manager, on page 371 page.

In **Transport Setting** window, you can configure how the product communicates with Cisco Smart Software Manager or Cisco Smart Software Manager satellite. You can click the radio button to select one of the options. The available Transport Setting options are tabulated.

Table 35: Transport Setting Window

Field	Description
Status	Displays the current configuration status of the Smart Call Home.
Transport Settings	
Direct	Product sends usage information directly over the internet. No additional components are needed. This is the default communication mode.
Transport Gateway or Smart Software Manager satellite	Cisco Emergency Responder sends license usage information to an on-premises collector called Cisco Smart Software Manager Satellite which requires a periodic exchange of information with Cisco Smart Software Manager cloud service. • If you are using HTTP, go to the URL: http://Satellite-ip/Transportgateway. • If you are using HTTPS, go to the URL: https://SatelliteFQDN-OR-IP-address/TransportGateway. For more information on how to register your devices using Cisco Smart Software Manager satellite, see https://community.cisco.com/t5/cisco-software-documents/how-to-register-your-device-using-https-to-satellite-smart/ta-p/3747976.
HTTP or HTTPS Proxy Server	Product sends usage information over the internet through a proxy server (such as Cisco Transport Gateway or Apache). Check the **Authentication needed on HTTP or HTTPS proxy** check box if want to register to Cisco Smart Software Manager using authentication based proxy server. If you enable this check box, only then the **Proxy User** and **Proxy Password** fields are enabled. Enter the details in the following fields: • Host Name/IP Address • Port • Proxy User **Note** Administrators should ensure that they enter the configured user name for proxy in the **Proxy User** field. • Proxy Password
Do not share my hostname or IP address with Cisco	Check the check box to allow the administrator to restrict the exchange of IP Address and hostname of the Cisco Emergency Responder during the registration and synchronization to Cisco Smart Software Manager or Cisco Smart Software Manager Satellite. **Note** When the check box is selected, Cisco Emergency Responder will not share the IP Address or hostname information from being sent through registration and regular license compliance synchronization activities. A unique identifier is generated for the Cisco Emergency Responder Product Instance and will need to be used for cross-referencing in Cisco Smart Software Manager.

Note Transport settings are shared with **Smart Call Home**, so any changes made in the **Transport Setting** window applies to other features using this service.

Smart Software Licensing Product Re-registration

The **Smart Software Licensing Product Re-registration** window is displayed when you select the **Reregister** option from the **Actions** drop-down list box on the **License Manager** page. See License Manager, on page 371 page for more information on the system license usage.

Table 36: Smart Software Licensing Product Re-registration Page

Field	Description
Status	Displays the product re-registration status.
Product Instance Registration Token	Displays a text area where you can enter the product registration token generated from the Cisco Smart Software Manager or Cisco Smart Software Manager satellite.
Re-register	Click the **Re-register** button to re-register the product with Cisco Smart Software Manager or Cisco Smart Software Manager satellite.

Email Alert Settings

The Email Alert Settings page appears when you choose **System** > **Mail Alert Configurations**.

Authorization Requirements

You must have system administrator or ERL administrator authority to access this page.

Description

Use the Email Alert Settings page to specify the parameters under which Emergency Responder sends email alerts. Use the check box to the right of each parameter to enable (check) or disable (uncheck) email alerts for that parameter. Check the Include event viewer contents in mail check box if you want to include the details from the event viewer in the email message.

The following table describes the Email Alert Settings page.

Table 37: Email Alert Settings Page

Field	An email alert is sent when:
Discovery Parameters	
Discovery Engine Registration Failed	The Discovery Engine fails to register

Field	An email alert is sent when:
Discovery Engine goes out of connection	The Discovery Engine loses connection
For unreachable devices during recovery	Devices such as switches and CiscoUnified CommunicationsManagers become unreachable
Emergency Call Routing Parameters	
Call information	A 911 call is placed
Call routing session ended due to problems	Call routing is stopped due to any of these reasons: • Invalid CMC • Invalid FAC • FAC and CMC needed • CMC needed • FAC needed • RESOURCE_BUSY
Rerouting of call	An emergency call is rerouted
Routing failure	Call routing fails
Route Point out of Service	The route point goes out of service
Cluster Parameters	
Cluster DB Failure	The server cannot communicate with the cluster database host
Intra Cluster Failure	The intra-cluster communication to a server group in the cluster fails
Misc Parameters	
Subscriber becomes active	The Subscriber becomes active
Publisher comes back online	The Publisher comes back online
Not able to get the JTAPI Provider	When Emergency Responder cannot get the JTAPI provider
Available user licenses get exhausted during phone tracking	When the number of user licenses are exhausted during phone tracking
Switch Port location change reporting	When you enable switch port change reporting for phones
Suppress IP Communicator location change reporting	When you filter CiscoUnifiedIP Communicator from the location change reporting email alerts
DRF Alert	Enable or Disable DRF backup or restore mail alerts
Update Settings button	Updates the email alert settings

Field	An email alert is sent when:
Cancel Changes button	Cancels changes made to the email alert settings

Related Topics

Onsite Alert Settings, on page 388
Set Up a Server Group, on page 128

Add Subscriber

The Add Subscriber page appears when you choose **System** > **Add Subscriber**.

Authorization Requirements

You must have system administrator or ERL administrator authority to access this page.

Description

Use the Add Subscriber page to add a subscriber server to an Emergency Responder server group. After adding the subscriber information, you must enter the correct publisher server information when prompted during installation.

Before You Begin

You must first configure a publisher server before configuring a subscriber server.

The following table describes the Add Subscriber page.

Table 38: Add Subscriber Page

Field	Description
Add Subscriber	
HostName	Host name of the subscriber server.
Insert button	Click **Insert** to add the new subscriber server.
Cancel Changes button	Removes input from the Add Subscriber page.
Configured Servers	A list of all currently configured servers, showing the host name and IP address of each server.

Related Topics

Install Emergency Responder Publisher, on page 64
Install Emergency Responder Subscriber, on page 69

National E911 Service Provider VUI Settings

The National E911 Service Provider VUI Settings page appears when you choose **System** > **National E911 Service Provider VUI Settings**.

Authorization Requirements

You must have system administrator or ERL administrator authority to access this page.

Description

Use the National E911 Service Provider VUI Settings page to enter the account information that is required for Emergency Responder to interoperate with National E911 Service Provider Validation and Update Interface. After entering the required information, you can test the connectivity to National E911 Service Provider from this page.

The following table describes the National E911 Service Provider VUI Settings page.

Table 39: National E911 Service Provider VUI Settings

Field	Description
Status	Displays status messages.
National E911 Service Provider VUI Settings	
Upload Certificate	Uploads the certificate from your local drive to the Emergency Responder server. To upload a certificate, follow these steps: **1.** Click **Upload Certificate** An Upload Certificate window appears. **2.** Click the **Browse** button to locate the certificate file on your local machine. **3.** Click the **Upload** button to upload the certificate file.
Validate Certificate	
National E911 Service Provider Certificate Password	The password that was generated with this certificate.
VUI URL	VUI URL is provided by National E911 Service Provider.
Enable HTTP Proxy	Check this check box if you want to use a proxy server for requests between Emergency Responder and National E911 Service Provider.

Field	Description
Proxy Host Name/IP Address	Enter the IP address or hostname of the proxy server, along with the port. For example, http://<ip_address_or_hostname>:port.
Authentication needed on HTTP Proxy	Check this check box if you want to communicate with the National E911 Service Provider using authentication based proxy server. If you enable this check box, only then the Proxy User Name and Proxy Password fields are enabled.
Proxy User Name	Enter the configured user name for proxy server in the **Proxy User Name** field.
Proxy Password	Enter the password that is associated to the username.
Test and Validate Certificate	Use this button to test the validity of your certificate.
Configure Account Details	
VUI Schema URL	The VUI Schema URL provided by National E911 Service Provider.
National E911 Service Provider Account ID	Your National E911 Service Provider Account ID provided by National E911 Service Provider.
Max VUI Connections	The maximum number of simultaneous VUI connections that Emergency Responder allows across the Server group.
MyE911 for Location Updates	Set this drop-down to **True** if Cisco Jabber and Webex App are using MyE911 or Remote Location Manager to set the users location when Off-premises. Setting this drop-down to **False** requires users to update their location through Cisco's Off-Premise User Page. By default, this option is set to **True**.
Test Connectivity	Use this link to verify whether Emergency Responder can successfully connect to National E911 Service Provider VUI.
Delete Account	Deletes an existing National E911 Service Provider account from the Emergency Responder database.
Update	Click **Update** to save the changes you made on this page.
Cancel	Click **Cancel** to change the fields on this page back to the last saved settings.

Related Topics

Configure Emergency Responder and National E911 Service Provider Enterprise Services , on page 183

Onsite Alert Settings

The **Onsite Alert Settings** page appears when you choose **ERL > Onsite Alert Settings**.

Authorization Requirements

You must have system administrator or ERL administrator authority to access this page.

Description

Use the Onsite Alert Settings page to add information about your onsite alert personnel. When you configure ERLs, you assign these personnel to them. Emergency Responder alerts the assigned personnel when an emergency call is made within the zone.

Note Sometimes the prompts do not get played at the onsite alert phone when the call is initiated from the CTI ports. To avoid this problem, configure only one line per CTI port in the Unified CM that is configured for Emergency Responder.

Note In case a user configures an onsite alert for a call (not for email), the calling party displays as the Emergency Responder CTI port.

The following table describes the Onsite Alert Settings page.

Table 40: Onsite Alert Settings Page

Field	Description	Notes
Add New Onsite Alert Contact		
Onsite Alert ID	The identifier for the onsite alert contact. The identifiers you use should be based on your site identification strategy (for example, security ID or badge number). This field is used throughout Emergency Responder to identify the contact; for example, you select from Onsite Alert IDs when assigning contacts to zones. The Onsite Alert ID cannot be modified after you have saved it.	Use a naming strategy meaningful to you organization, but which is also useful wh configuring zones in Emergency Respon
Onsite Alert Name	The name of the onsite alert contact.	
Onsite Alert Number	The telephone number for the onsite alert contact. This number must be a voice telephone number; do not enter the number of a voice-mail system or an automated attendant.	When Emergency Responder gets an eme call from an ERL, it calls the onsite alert of the contact for the ERL and plays a pre message that includes the phone number fr the emergency call was placed.

Field	Description	Notes
Onsite Alert Email Address	The email address for the onsite alert contact, for example, email@domain.com.	When Emergency Responder gets an call from an ERL, it emails the onsite associated with the ERL. If the email email paging system, the contact rece instead of an email. The email or page phone number from which the emerge placed. **Note** You can add multiple ema by separating each addres comma (,). Avoid extra s between the email addres
Onsite Alert Pager Address	The pager email address for the onsite alert contact, for example, <pager_number>@domain.com.	You can limit the size of the message to the pager by configuring the fields Alert Setting Page. See Pager Alert S
Available User Group	The User Group which will receive the specific web alert from the associated ERL. By default Emergency Responder User Group is selected, which has all users.	The users can view all alerts in the sy selecting **ALL** on the Web Alert page
Insert	Click the **Insert** button to add the contact to the list of contacts. The contact is then listed in the **Available Onsite Alerts** section of the page.	
Cancel Changes	Click the **Cancel Changes** button to cancel any changes made to this page.	
Available Onsite Alerts	Section of the page that displays onsite alert contacts that have already been configured. For configured onsite alert contacts, the following information is displayed: • Onsite Alert ID • Onsite Alert Name • Onsite Alert Number • Onsite Alert Email Address • Onsite User Group To change an entry, click the entry or click the **Edit** icon; the person's contact information is loaded in the edit boxes. Make your changes and click **Update**. To delete an entry, click the **Delete** icon on the same line as the entry.	If no contacts have previously been co section is blank. You cannot modify a contact's Onsite Before you can delete the entry, you r the ERLs to which the person is assign the person from the ERL.
Add New	Click the **Add New** button to add another contact.	

Field	Description	Notes
Update	Click the **Update** button when viewing an existing contact's information to save changes you make to the information.	Only available when viewing the informa an existing contact.
Export	Click the **Export** button to export the onsite alert settings to another file. For more information, see Export OnsiteAlert Data, on page 390.	
Import	Click the **Import** button to import the onsite alert settings to your Cisco Emergency Responder configuration. For more information, see Import OnsiteAlert Data , on page 391.	

Related Topics

Add Onsite Security Personnel, on page 137

ERL Creation , on page 138

Emergency Responder Onsite Alert Personnel Preparations, on page 309

E911 and Cisco Emergency Responder Terminology , on page 6

Export OnsiteAlert Data

The **Export OnsiteAlert Data** window appears when you click **Export** on the **Onsite Alert Settings** page (opened when you choose **ERL** > **Onsite Alert Settings**).

Authorization Requirements

You must have the system administrator or ERL administrator authority to access this window.

Description

Use the **Export OnsiteAlert Data** window to perform the following:

- Create a file containing the Emergency Responder Export OnsiteAlert Data.
- Use the **Download** option to download a file containing the Emergency Responder Export OnsiteAlert Data. For more information, see Download File , on page 113.

The following table describes the fields found on the **Export OnsiteAlert Data** window.

Table 41: Export OnsiteAlert Data Window

Field	Description
Export OnsiteAlert Data	
Select Export Format	Select the file format from the drop-down list that matches the file being imported.
Enter Export File Name	Enter the name of the file that you want to create. Do not include the file extension.

Field	Description
Export	Click the **Export** button to add data from the import file to your Cisco Emergency Responder configuration.
Close	Click the **Close** button to close the window.
Export Status	This text box displays status information.
Download	
Select a File to Download	Select a file from the drop-down list and click the **Download** button to download the file to your machine.

Related Topics

Download File , on page 113

Import OnsiteAlert Data

The **Import OnsiteAlert Data** window appears when you click **Import** on the **Onsite Alert Settings** page (opened when you choose **ERL** > **Onsite Alert Settings**).

Authorization Requirements

You must have the system administrator or ERL administrator authority to access this window.

Description

Use the **Import OnsiteAlert Data** window to create or update several OnsiteAlert Data details at once from the file in which you have defined their data. You can create this file using a spreadsheet and save the information in the required formats. The **View sample file** link provides the sample information to create or update your import file.

You can import a previously exported file or you can upload a file that you created on your local system using the **Upload** option. For more information, see Upload File , on page 113.

Note Ensure that you restart the Cisco Emergency Responder service after using the Import feature to update the Emergency Responder onsite alerts in bulk, for the changes to take effect.

The following table describes the fields found on the **Import OnsiteAlert Data** window.

Table 42: Import OnsiteAlert Data Window

Field	Description
Import OnsiteAlert Data	

Field	Description
Select Import Format	Select the file format from the drop-down list that matches the file being imported. Click **View sample file** link to view an example of the expected format and sequence of values. Use this sample information to create your import file in a spreadsheet.
Select File to Import	Select the file from the drop-down list from which you want to import data.
Import	Click the **Import** button to add data from the import file to your Cisco Emergency Responder configuration.
Upload	Click the **Upload** button to upload the file from your machine. For more information, see Upload File , on page 113.
Close	Click the **Close** button to close the window.
Import Status	This text box displays status information.

Related Topics

Upload File , on page 113

Pager and Email Alert Configurations

The Pager Alert Settings and Email Alert Settings page appears when you choose **ERL** > **Pager Alert and Email Alert Configurations**.

Authorization Requirements

You must have system administrator or ERL administrator authority to access this page.

Description

Use the Pager Alert and Email Alert Configurations page to limit the size of system-wide pager and email messages by selecting the fields that are sent to the pager and by editing the labels for those fields.

Note If you are upgrading Emergency Responder from any source version prior to Release 12.5.1, ensure that you check the Local Call Time check box to receive the local call time via emails and pager alerts in the upgraded version.

The following table describes the Pager Alert Settings and Email Alert Settings page.

Table 43: Pager Alert and Email Alert Configuration Settings

Field	Descriptions
Pager Alert Settings	
	You can limit the size of the pager message that is sent by selecting the following fields and editing the labels are associated with those fields: • Extension • ERL • Location • System Time • Server • Local Time Check the check box to select the fields that you want to display on the pager. Click the text box to edit the label that you want to send to the pager.
Update Pager Settings	Click **Update Settings** to save changes that you made.
Restore Pager Defaults	Click **Restore Defaults** to restore the default pager and label settings.
Send Sample Message to a pager	Enter a pager address in the text box and click **Send Test Message** to send a test message to your pager.
Email Alert Settings	

Field	Descriptions
	You can customize email messages sent to the configured onsite security person by choosing the required fields. You can also add additional notes or mask digits on Caller DN to reflect the local dialing pattern. • Caller Extension • Display Name • Zone • Location • System Call Time • Local Call Time • Server Details—Enter the URL details for the Emergency Responder User page in which you can check the 911 call details. • Additional Notes—Enables you to provide any additional information as Admin Notes and the information is available in the email alerts. • Discard DN digits—You can enter the count of digits to be masked from the beginning on Caller DN to reflect local dialing pattern. Check the check box to select the fields that you want to display on the email message. Click the editable label text boxes to modify the label that you want to send to the email message.
Update Email Settings	Click **Update Email Settings** to save the changes made.
Restore Email Defaults	Click **Restore Email Defaults** to restore the default email message and label settings.
Sample Email Message Preview	Select the required email alert field settings and click **Update Email Settings** to preview the sample email message.

Conventional ERL

The Conventional ERL page appears when you choose **ERL >Conventional ERL**.

Authorization Requirements

You must have system administrator or ERL administrator authority to access this page.

Description

Use the Conventional ERL Data page to define the emergency response locations (ERLs) for your company. An ERL might be a whole building (if it is small), the floor of a building, or an area on a floor. Each community can have different laws concerning the size of an ERL, so consult your local ordinances and with your service provider before deciding on your ERLs. The ERLs you create are used by emergency response teams to locate the emergency, so the ERL should be small enough that these teams can locate the caller within a reasonable time.

The following table describes the Find and List ERLs page.

Table 44: Find and List ERLs Page

Field	Description	Notes
ERL Search Parameters		
Find Conventional ERL where...	Select search criteria and click Find to list existing ERLs. To list all ERLs, click **Find** without entering any criteria. From the drop-down menu, you can select the number of records that display per page for each search. From the search results list, you can: • Click an entry to view and update its characteristics. • Click the **Copy** icon to create a new ERL with the same ALI data. • Click the **Delete** icon to remove the ERL. • Click **view...** in the Audit Trail column to view a history of changes made to that ERL. See ERL Audit Trail, on page 478 for more information.	When copying an ERL, inform must be unique in an ERL is no See Add New ERL , on page 3 information.
Configure Default ERL	You must configure the Default ERL before configuring any other ERLs. The default ERL is the system-defined ERL that is used to route calls if no other ERL configuration is found. **Note** During the migration of data in an upgrade scenario, if any manually configured phone is assigned to the Default ERL, it remains there until it is modified.	See Add New ERL , on page 3 information.
Add New ERL	Click **Add New ERL** to create a new ERL.	See Add New ERL , on page 3 information.
Configure Default ERL	Click **Configure Default ERL** to configure a default ERL	
Export	Click the **Export** link to create a file containing your ERL configuration.	See Export ERL Data, on page information about exporting E
Import	Click the **Import** link to create or update ERLs using information stored in a separate file. By importing ERL data, you can create or update many ERLs at one time.	See Import ERL Data, on page information about importing E

Related Topics

Export PS-ALI Records, on page 479

ERL Creation , on page 138

ERLs, on page 135

ERL Management , on page 136
E911 and Cisco Emergency Responder Terminology , on page 6

Add New ERL

Note On the **ERL Information for** ERL Name page, the ERL Name variable is replaced with the name of the ERL associated with the page. For example, if you click the Default ERL, the page that appears is titled **ERL Information for Default**. If the ERL name is First Floor, the page that appears is titled **ERL Information for First Floor**.

The Add New ERL and ERL Information for ERL Name pages are essentially the same, as follows:

- The Add New ERL page appears when you select **Add New ERL** on the Find ERL Data page (opened when you choose **ERL** > **Conventional ERL**). The page also appears if you click **Copy** for an existing ERL.
- The ERL Information for Default page opens when you click **Configure Default ERL** on the Find ERL Data page. The ERL Information for ERL Name page also appears when you click any of the links associated with an existing ERL in the list on the Find ERL Data page (opened when you choose **ERL** > **Conventional ERL**).

Note You cannot use default ERLs as a Test ERL. The Test ERL check box is not available on the ERL Information for Default page.

Authorization Requirements

You must have system administrator or ERL administrator authority to access this page.

Description

Use the Add New ERL page to create a new emergency response location (ERL). Alternatively, you can create or update many ERLs at once by importing predefined ERL information from a separate file.

Emergency Responder allows you to select the ERL as a Test ERL.

Use the Find ERL Data page to view or update an existing ERL.

See ELIN Numbers Emergency Calls and PSAP Callbacks , on page 93 for information about configuring the ELIN numbers in Cisco Unified Communications Manager.

If you want to route emergency calls to onsite security instead of the PSAP, see Set Up ERLs for Non-PSAP Deployment , on page 139 for the Route and Translation Pattern and ELIN settings.

Note If you are upgrading Emergency Responder from any source version prior to Release 12.5.1, ensure that you check the Local Call Time check box to receive the local call time via emails and pager alerts in the upgraded version.

The following table describes the Add New ERL and ERL Information pages.

Table 45: Add New ERL and ERL Information Pages

Field	Description	Notes
ERL Settings		
ERL Name	The name of the ERL. The naming strategy you use is critical. The ERL name is one of the primary pieces of information your security team sees when alerted to an emergency call. If the name is easy to understand and descriptive, it can help your team respond quickly to a call. For example, if you are creating an ERL for each floor in a three story building called Building J, your ERL names might be BldgJ-Floor1, BldgJ-Floor2, BldgJ-Floor3. Work with your security team to develop an ERL naming strategy.	You cannot change the name o ERL. To change an ERL name, ERL, then delete the old ERL. Any leading and trailing spaces
Description	Enter a description of the new ERL (optional).	
Test ERL (Used for Synthetic Testing)	Check this check box if this ERL is used for testing. See Set Up Test ERLs , on page 144.	This setting is not available on Information for Default; defaul not be used as test ERLs.

Field	Description	Notes
ELIN Settings	The combination of a route pattern and a phone number that jointly route the emergency call to the PSAP and provide the PSAP with a callback number if the PSAP needs to call the emergency caller after disconnecting the call.	Each ERL must have unique ELIN number of ELINs that you define de how many callbacks you can suppo are used in order as emergency cal made, and recycled as needed. For if you define two ELINs for an ER three emergency calls are made, th cannot recontact the first emergenc However, concurrent emergency c not limited by the number of ELIN could have ten active emergency c if you only have two ELINs. The n ELINs only controls PSAP callbac capability. **Note** Emergency Responder the association of an E with an ERL if the EL been configured as a D Number for an Off-Pr Emergency Responde Emergency Responder impose this restriction DID Number belongs who has never associa off-premises location Emergency Responde
Route/Translation Pattern	The phone number, defined as a route pattern in Cisco Unified Communications Manager, that is configured to use the gateway that the call should be routed through to get to the correct PSAP. This number must include the external emergency number, such as 911 in the USA. For example, 10.911 or 10911. The pattern can only contain numbers and dots.	

Field	Description	Notes
ELIN Number	The unique phone number which the PSAP can use to locate a caller an emergency caller if the call is hung up. This number must be a DID (direct inward dial) number provided by your service provider; that is, it must be routeable on the PSTN. Enter the entire number, including area code, for the North American Numbering Plan, such as 4085551212, or an E.164 Number including country code such as +14085551212. The number can only contain numbers, a plus sign (+), single hyphens, dots, or parentheses. The National E911 Service Provider ERL allows maximum of 10 characters and the data type should only be numbers.	An ELIN when being sent as A through outgoing Gateway mu (direct inward dial) number prov service provider. If an ELIN number has a numer then add a “.” between the “+” number in *Cisco Unified Comm Manager* ,PSAP Call Back tran pattern. The '+' can be removed digit “Predot”. For example, if E.164 number country code such as +140855 in the *Cisco Unified Communi Manager* ,PSAP Call Back trans you should enter '\+.XXXXXX not '\+1.XXXXXXXXXX'. Th should be 913 followed by 11X 10X.
Add button	To add a route point and ELIN combination, enter the information and click **Add**.	
Update button	To change an existing combination, select it in the list, change the information in the edit boxes, and click **Update**.	
Remove button	To remove a combination, select it in the list and click **Remove**.	
Onsite Alert Settings		
Available Onsite Alert IDs	Text box that displays the IDs of all available onsite alert personnel. **Note** The onsite alert IDs list displays in a numerical order.	You must first add the contact onsite alert personnel.
Add button	Select the onsite alert (security) contacts to be assigned to the ERL. These contacts are notified when an emergency call is made from the ERL. To add a contact, select an Onsite Alert ID from the Available Onsite Alert IDs list and click **Add**. The contact's ID then appears in the Onsite Alert IDs for the ERL text box.	
Remove button	To remove a contact for the ERL, select the appropriate ID in the Onsite Alert IDs for the ERL text box and click **Remove**.	
ERL Address		

Field	Description	Notes
ALI Details button	Click **ALI Details** to view or change the automatic location information (ALI) of an ERL. The ALI provides detailed information about the location of the ERL, such as street address and phone number.	
Time Zone	Select a time zone for the ERL. The time zone provides the list of all available time zones.	When you dial 911, the selected ti is set as the local call time in Page Emergency alert. If a time zone is selected, then the local call time is the system call time.
Insert button	Click **Insert** to save your changes to the new ERL.	The Insert button is only available creating a new ERL.
Cancel Changes button	Click **Cancel Changes** to change the fields on this page back to the last saved settings.	
Update button	Click **Update** to save your changes to the ERL.	The Update button is only availabl changing an existing ERL.
Close button	Click **Close** to close the window. You must click **Update** or **Insert** to save your changes before you click **Close**.	

Related Topics

ERLs, on page 135
ERL Management , on page 136
Set Up Default ERL , on page 138
Set Up Individual ERL and Automatic Location Information (ALI) , on page 140
Set Up Test ERLs , on page 144
E911 and Cisco Emergency Responder Terminology , on page 6

ALI Information

Note On the **ALI Information** (**for** ERL Name) page, the ERL Name variable is replaced with the appropriate ERL name. For example, if you click on ALI Details on the ERL Information for Default page, the page that appears is titled **ALI Information for Default**. If the ERL name is First Floor, the page that appears is titled **ALI Information for First Floor**.

The ALI Information (for ERL Name) page appears when you do one of these:

- Click **Add/Edit ALI** in the ERL Address section on the Add New ERL page.

  Note The Add New ERL page appears when you choose **Add New ERL** on the Find ERL Data page (opened when you choose **ERL** > **Conventional ERL**).

- Click **Add/Edit ALI** on the ERL Information for ERL Name page. The ERL Information for ERL Name page appears when you click on an existing ERL name or on **Configure Default ERL** on the Find ERL Data page (opened when you choose **ERL > Details**).

Authorization Requirements

You must have system administrator or ERL administrator authority to access this page.

Description

Use the Enter ALI Information page to enter the automatic location information (ALI) for an emergency response location (ERL). Send this information to your service provider, who will ensure it gets into the required database so that calls from your ELINs are routed to the local PSAP and public safety answering points (PSAPs) can locate an emergency caller.

The data requirements for these fields might differ from service provider to service provider. Contact your service provider to determine their requirements. The descriptions of the fields in are based on the National Emergency Number Association (NENA) Version 2 standards (USA).

Caution The quality of the information you enter here is critical. This information is displayed to emergency call operators and to your local response team. They use this information to locate emergency callers. If the data is incorrect or difficult to understand, emergency response can be delayed, which might result in casualties that could have been prevented.

Table 46: Enter ALI Information Page

Field	Description	Notes
Find all prevalidated fields from validation file by selecting a tag		
Select a Tag	Select the tag whose associated ALI data you want to load into the window. You can then edit the information for this specific ALI.	You can simplify the entry of ALI da up tags in a file called validate.txt. explains where to place the file, and the samplevalidate.txt file, which ex format of the file. When you create a tag, you enter info is common between several ALIs, s company name, city, state, and so fo example, if you have a 25-story build are creating an ERL for each floor, create a tag called "25story." Then, retyping the information for the build you select a tag and the ALI data is the data you defined for the tag.

Field	Description	Value Type (A = Alphabets, N = Numeric, S = Sp Characters [# @ & * ( ) - _ + , . : ; " ' /
ALI Data		

Field	Description	Value Type (A = Alphabets, N = Numeric, S = Spec Characters [# @ & * ( ) - _ + , . : ; " ' /])
House Number	The number from the postal street address for the building. Example: 170 in 170 West Tasman Dr.	AN, dash "-", and @ sign "@" The number can be up to 10 characters, service provider might only support 8 c numbers.
House Number Suffix	The number extension (such as /2) for the house number, if any.	ANS
Street Name	The street name from the postal address for the building.	ANS You are limited to 60 characters.
Prefix Directional	The type of street. Select the type from the drop-down list, and the field is filled with one of the abbreviations accepted by the U.S. Postal Service Publication 28, for example, AVE for Avenue.	Can be one of these directions: • N • S • E • W • NE • NW • SE • SW
Street Suffix	The type of street. Select the type from the drop-down list, and the field is filled with one of the abbreviations accepted by the U.S. Postal Service Publication 28, for example, AVE for Avenue.	A You can also type in the suffix. You are to 4 characters.
Post Directional	A trailing directional indicator if the street name contains one, for example, N for North.	Can be one of these directions: • N • S • E • W • NE • NW • SE • SW

Field	**Description**	**Value Type** **(A = Alphabets, N = Numeric, S = S** **Characters [# @ & * ( ) - _ + , . : ; " '**
Community Name	The community name for the address, for example, a city, town, or district name.	ANS You are limited to 32 characters.
State	The 2-digit state abbreviation.	A You are limited to 2 characters.
Main NPA	The 3-digit area code of the main number associated with the ERL.	N
Main Telephone No.	The main phone number associated with the ERL. This might be the number of the security office for the ERL.	N
Class of Service	Select the class of service for the ERL.	If you do not know your class of serv service provider.
Type of Service	Select the type of service for the ERL.	If you do not know your class of serv service provider.
Exchange	The Local Exchange Carrier (LEC) exchange identifier for the serving telephone office for the phone.	ANS You are limited to 4 characters. Ask provider for this identifier
Customer Name	The subscriber name associated with the ERL, and typically your company name.	ANS You are limited to 32 characters.
Order Number	The service order number of the activity of establishing or updating this record.	ANS You are limited to 10 characters. Wo service provider to determine a vali number, if one is needed.
Extract Date	The date on which the record was created.	Date [mmddyy]
County ID	The county identification code for the zone. In the USA, use the FIPS code assigned to the county by the U.S. Census Bureau.	AN You are limited to 4 characters.
Zip Code	The postal zip code for the address.	AN, hyphen "-" Indicates a U.S. zip code on a U.S. record or a Canadian postal code or service order record. U.S. Format: NNNNN-NNNN; Canadian Format or ANA[space] NAN
Zip Code Extension	The postal zip code "plus four" number.	AN, hyphen "-" You are limited to 4 digits.

Field	Description	Value Type (A = Alphabets, N = Numeric, S = Spec Characters [# @ & * ( ) - _ + , . : ; " ' /])
Customer Code	Your customer code. Ask your service provider if you do not know your code.	ANS You are limited to 3 characters. If you change this field, Emergency Re generates two records: a Delete record t the ALI with the old code, and an Inser to add the ALI with the new code. This and Insert sequence is only generated t time you export ALI: you must ensure submit this export file to the service pr
Comments	Optional comments. These commentsmight be displayed at the PSAP if an emergency call is made from this ERL.	You are limited to 30 characters.
Longitude	The longitude of the ERL.	N, dot ".", plus "+", minus "-" You are limited to 9 digits.
Latitude	The latitude of the ERL.	N, dot ".", plus "+", minus "-" You are limited to 9 digits.
Elevation	The elevation of the ERL.	AN dot ".", plus "+",minus "-" You are limited to 5 digits.
TAR Code	The taxing area rate code.	ANS You are limited to 6 characters.
Location	Additional location information, in free form, to help identify the exact location of the phone. This information is displayed to your security personnel along with the ERL name when an emergency call is made, so use this field to help locate the caller. For example, you might repeat the street address that is defined in several separate fields elsewhere on this page.	ANS You are limited to 60 characters.

Field	Description	Value Type (A = Alphabets, N = Numeric, S = Sp Characters [# @ & * ( ) - _ + , . : ; " ' /
Reserved	Information your service provider might require to create a valid ALI file.	AN Ask your service provider if you m enter anything in the reserved area. Be aware that NENA and CSV requi be different. For example, ERL Imp require that you enter anything in th field. You can give an empty string i ERL records and Emergency Respo this file for importing. However, yo delete the field itself from the file. T be there in the record; it can be an e delimited with a comma.

Related Topics

- Set Up Default ERL , on page 138
- Set Up Individual ERL and Automatic Location Information (ALI) , on page 140
- Import Several ERLs , on page 141
- Export PS-ALI Records, on page 479
- ERLs, on page 135
- ERL Management , on page 136
- E911 and Cisco Emergency Responder Terminology , on page 6

Export ERL Data

The Export ERL Data page appears when you click the **Export** link on the Find ERL Data page (opened when you choose **ERL** > **Conventional ERL**).

Authorization Requirements

You must have system administrator or ERL administrator authority to access this page.

Description

Use the Export ERL Data page to create ERL export files for your own use only; do not submit ERL export files to your service provider. For example, use an ERL export file to back up your configuration or to move it to another Emergency Responder server.

To create a file to send to your service provider to update their ALI data, see Export PS-ALI Records, on page 479.

The following table describes the Export ERL Data page.

Table 47: Export ERL Data Page

Field	Description
Select Export Format	The file format to be used in the export file. For ERL data, either csv (comma-separated value
Enter Export File Name	The name of the file you want to create. Do not include a file extension.
Export button	Click **Export** to create the export file.
Close button	Click **Close** to close the window.

Related Topics

ALI Submission and Service Provider Requirements , on page 37

Export ERL Information , on page 146

ERLs, on page 135

ERL Management , on page 136

E911 and Cisco Emergency Responder Terminology , on page 6

Import ERL Data

The Import ERL Data page appears when you click the **Import** link on the Find ERL Data page (opened when you choose **ERL** > **Conventional ERL**).

Authorization Requirements

You must have system administrator or ERL administrator authority to access this page.

Description

Use the Import ERL Data page to create or update many ERLs at once from a file in which you have defined the ERL data. Create this file using a spreadsheet that can save the information in one of the required formats (CSV or XML). View the samples from this page before attempting to create an import file.

Note Import ERL Data does not support configuring E.164 number with a leading plus sign (+). Ensure that you remove the leading plus sign before importing onsite alert details.

If you must update many ERLs, you can export the ERL data, update the export file, and reimport the file.

You can also use the Upload utility to upload a file containing ERL data from your local system; you can then import the ERL data. See Upload File , on page 113 for more information.

The following table describes the Import ERL Data page.

Table 48: Import ERL Data Page

Field	Description
Select Import Format	Select the format used in the file you are importing. After you select the format, click **View sample file** to see an example of the expected format and sequence of values. Use this sample information to create your import file in a spreadsheet.
Select File to Import	Select the file from which you want to import ERL data.
Upload button	Click Upload to upload a file from your local system. See Upload File , on page 113 for more information.
Import button	Click **Import** to add ERL data from the import file to the Emergency Responder database. **Note** The imported ERL data overwrites conflicting data in the Emergency Responder database.
Close button	Click **Close** to close the window.

Related Topics

Import Several ERLs , on page 141
Export ERL Information , on page 146
Upload File , on page 113
ERLs, on page 135
ERL Management , on page 136
E911 and Cisco Emergency Responder Terminology , on page 6
Export PS-ALI Records, on page 479

Off-Premises ERL

The Find Off-Premises ERL Data page appears when you choose **ERL** > **Off-Premise ERL** > **Search And List**.

Authorization Requirements

You must have system administrator or ERL administrator authority to access this page.

Description

Use the Off-Premise ERL Data page to define the emergency response locations (ERLs) for individuals with phones that are located outside of the corporate network.

The following table describes the Find and List Off-Premise ERLs page.

Table 49: Find National E911 Service Provider ERL Data (Off-Premise)

Field	Description	Notes
ERL Search Parameters		
Find Off-Premises ERL where...	Select search criteria and click **Find** to list existing Off-Premise ERLs. To list all ERLs, click **Find** without entering any criteria. From the drop-down list, you can select the number of records that display per page for each search. From the search results list, you can: • Click an entry to view and update its characteristics. • Click the **Copy** icon to create a new ERL with the same ALI data. • Click the **Delete** icon to remove the ERL. • Click **view...** in the Audit Trail column to view a history of changes made to that ERL. See ERL Audit Trail, on page 478 for more information.	When copying a information that unique in an ER copied.
Add New ERL	Click **Add New ERL** to create a new ERL.	

Related Topics

Add New ERL , on page 408

Off-Premise ERL - Secondary Status, on page 410

Set Up Emergency Responder to Support Off-Premise Users

Add New ERL

The Add New ERL (Off-Premise phones) page appears when you choose **Add New ERL** on the Find National E911 Service Provider ERL Data page (opened when you choose **ERL** > **Off-Premise ERL** > **Search and List**).

Authorization Requirements

You must have system administrator or ERL administrator authority to access this page.

Description

Use the Add New ERL page to create a new emergency response location (ERL) for Off-Premise phones. Alternatively, you can create or update many ERLs at once by importing predefined ERL information from a separate file.

Use the Find ERL Data page to view or update an existing ERL.

The following table describes the Add New ERL (Off-Premise Phones) page.

Table 50: Add New ERL (Off-Premise Phones)

Field	Description	Note
ERL Settings		

Field	Description	Note
ERL Name	The name of the ERL. The naming strategy you use is critical. The ERL name is one of the primary pieces of information your security team sees when alerted to an emergency call. If the name is easy to understand and very descriptive, it can help your team respond quickly to a call. Work with your security team to develop an ERL naming strategy.	You cannot change the name o ERL. To change an ERL name, ERL, then delete the old ERL. Any leading and trailing space
Description	Enter a description of the new ERL (optional).	
Route/Translation Pattern Settings		
Route/Translation Pattern	The phone number, defined as a route pattern in Cisco Unified Communications Manager, that is configured to use the gateway the call should be routed through to get to the correct PSAP. This number must include the external emergency number, such as 911 in the USA. For example, 10.911 or 10911. The pattern can only contain numbers and dots.	
Add button	To add a route point, choose a route point from the drop-down list and click **Add**.	
Remove button	To remove a combination, select it in the list and click **Remove**.	
Onsite Alert Settings		
Available Onsite Alert IDs	Text box that displays the IDs of all available onsite alert personnel.	You must first add the contact t onsite alert personnel.
Add button	Select the onsite alert (security) contacts to be assigned to the ERL. These contacts are notified when an emergency call is made from the ERL. To add a contact, select an Onsite Alert ID from the Available Onsite Alert IDs list and click **Add**. The contact ID then appears in the Onsite Alert IDs for the ERL text box.	
Remove button	To remove a contact for the ERL, select the appropriate ID in the Onsite Alert IDs for the ERL text box and click **Remove**.	
ERL Address		
ALI Details button	Click ALI Details to view or change the automatic location information (ALI) of an ERL. The ALI provides detailed information about the location of the ERL, such as street address and phone number.	

Field	Description	Note
Time Zone	Select a time zone for the ERL. The time zone provides the list of all available time zones.	When you dial 911, the selected ti is set as the local call time in Page Emergency alert. If a time zone is selected, then the local call time is the system call time.
Insert button	Click **Insert** to save your changes to the new ERL.	The Insert button is only available creating a new ERL.
Cancel Changes button	Click **Cancel Changes** to change the fields on this page back to the last saved settings.	
Update button	Click **Update** to save your changes to the ERL.	The Update button is only availabl changing an existing ERL.
Close button	Click **Close** to close the window. You must click **Update** or **Insert** to save your changes before you click **Close**.	

Related Topics

Off-Premises ERL, on page 407
Off-Premise ERL - Secondary Status, on page 410
Set Up Emergency Responder to Support Off-Premise Users

Off-Premise ERL - Secondary Status

The Secondary Status page appears when you choose **ERL** > **Off-Premise ERL** > **Secondary Status**.

Authorization Requirements

You must have system administrator or ERL administrator authority to access this page.

Description

Use the Secondary Status page to query the National E911 Service Provider Secondary Status database for information about off-premise telephone number record update transactions that were flagged with errors. These records may include the following:

- Corrected records that are now in the National E911 Service Provider database.
- Error records that are referred back to customers for correction.
- Deleted error records from the National E911 Service Provider database.

You can query the National E911 Service Provider Secondary status database for off-premise telephone number records with errors.

The following table describes the Secondary Status for Off-Premise phones.

Table 51: Secondary Status (Off-Premise Phones)

Field	Description
Find DIDs where...	Select search criteria and click **Find** to list the result of a query on the National E911 Service Provider secondary status server.

Related Topics

Off-Premises ERL, on page 407
Add New ERL , on page 408
Set Up Emergency Responder to Support Off-Premise Users

Find National E911 Service Provider ERL

The Find National E911 Service Provider ERL page appears when you choose **ERL** > **National E911 Service Provider ERL** > **National E911 Service Provider ERL (Search and List)**.

Authorization Requirements

You must have system administrator or ERL administrator authority to access this page.

Description

When you use National E911 Service Provider V91-1-1 services, you can use the National E911 Service Provider ERL Data page to define the emergency response locations (ERLs) for your company.

The following table describes the Find and List National E911 Service Provider ERLs page.

Table 52: Find National E911 Service Provider ERL Data

Field	Description	Notes
ERL Search Parameters		
Find National E911 Service Provider ERL where...	Select search criteria and click **Find** to list existing National E911 Service Provider ERLs. To list all ERLs, click **Find** without entering any criteria. From the drop-down list, you can select the number of records that display per page for each search. From the search results list, you can: • Click an entry to view and update its characteristics. • Click the **Copy** icon to create a new ERL with the same ALI data. • Click the **Delete** icon to remove the ERL. • Click **view...** in the Audit Trail column to view a history of changes made to that ERL. See ERL Audit Trail, on page 478 for more information.	When copyin information t unique in an copied. See Add Nev page 396 for information.

Field	Description	Notes
Add New ERL	Click **Add New ERL** to create a new ERL.	See Add New El page 396 for mo information.
Level of service button	Click **Level of service** to display the level of service that National E911 Service Provider designates for the specific address that is configured in the ALI details. National E911 Service Provider supports the following level of service: • No Coverage—National E911 Service Provider does not have access to the selective router and cannot provide the callback number and address to the PSAP that services that address. • Basic—The PSAP that provides service currently can not provide emergency support for wire line services or VoIP service providers. • Enhanced—Calls can be routed to the PSAP with the existing E9-1-1 selective router network, and National E911 Service Provider can provide the callback number and address to the PSAP.	
Bulk TN Update button	Select multiple ERLs and click **Bulk TN Update** to update the ELIN for the selected ERL.	
Export	Click the **Export** link to create a file containing your ERL configuration.	See Export ERL page 405 for inf about exporting
Import	Click the **Import** link to create or update ERLs using information stored in a separate file. By importing ERL data, you can create or update many ERLs at one time.	See Import ERL page 406 for inf about importing

Related Topics

Default ALI Values, on page 412
National E911 Service Provider ERL - Secondary Status, on page 413
National E911 Service Provider Schedule, on page 414
View ALI Discrepancies, on page 415
National E911 Service Provider for Enterprise Service, on page 183

Default ALI Values

The Default ALI Values page appears when you choose **ERL** > **National E911 Service Provider ERL** > **Default ALI Values**.

Authorization Requirements

You must have system administrator or ERL administrator authority to access this page.

Description

Use the Default ALI Values page to set the default values that automatically populate the respective ALI fields when a new National E911 Service Provider ERL is created.

The following table describes the Default ALI Information page.

Table 53: Default ALI Values

Field	Description
Default ALI Values for National E911 Service Provider ERLs	
Type of Service	Defines the type of service for the calling party number, such as FX in 911 area or Non-Pub. **Note** National E911 Service Provider recommends setting the default to Non-Pub.
Class of Service	Defines the class of service for the calling party number, such as residential, business, VoIP. **Note** National E911 Service Provider recommends setting the default to VoIP.
Company ID	Specified by National E911 Service Provider.
Customer Name	Specified by National E911 Service Provider.
Update button	Click **Update** to save your changes.
Cancel Changes button	Click **Cancel Changes** to change the fields on this page back to the last saved settings.

Related Topics

- Find National E911 Service Provider ERL, on page 411
- National E911 Service Provider ERL - Secondary Status, on page 413
- National E911 Service Provider Schedule, on page 414
- View ALI Discrepancies, on page 415
- Configure Emergency Responder and National E911 Service Provider Enterprise Services , on page 183

National E911 Service Provider ERL - Secondary Status

The Secondary Status page appears when you choose **ERL > National E911 Service Provider ERL > Secondary Status**.

Authorization Requirements

You must have system administrator or ERL administrator authority to access this page.

Description

Use the Secondary Status page to query the National E911 Service Provider Secondary Status database for information about telephone number record update transactions that were previously flagged with errors. These records may include the following:

- Corrected records that are now in the National E911 Service Provider database.
- Error records that are referred back to customers for correction.
- Deleted error records from the National E911 Service Provider database.

You can query the National E911 Service Provider Secondary status database for telephone number records with errors that have been corrected.

The following table describes the Secondary Status for phones that are serviced by National E911 Service Provider.

Table 54: Secondary Status (National E911 Service Provider Phones)

Field	Description
Find ELINS where...	Select search criteria and click **Find** to list the result of a query on the National E911 Service Provider secondary status server.

Related Topics

Find National E911 Service Provider ERL, on page 411
Default ALI Values, on page 412
National E911 Service Provider Schedule, on page 414
View ALI Discrepancies, on page 415
Configure Emergency Responder and National E911 Service Provider Enterprise Services , on page 183

National E911 Service Provider Schedule

The National E911 Service Provider Schedule page appears when you choose **ERL** > **National E911 Service Provider ERL** > **National E911 Service Provider Schedule**.

Authorization Requirements

You must have system administrator or ERL administrator authority to access this page.

Description

Use the National E911 Service Provider Schedule page to specify the day of the week and time when ALI update requests and secondary status update requests are sent to National E911 Service Provider. ALI update requests sends newly created TN records to National E911 Service Provider. Secondary Status update requests sends queries to National E911 Service Provider requesting information about records with errors that have been corrected.

The following table describes the National E911 Service Provider Schedule page.

Table 55: National E911 Service Provider Schedule

Field	Description	Notes
Add new schedule	Specify the day of the week and time of the day when you want to schedule an update: 1. Select the days of the week when you want to run the switch port and phone update process. 2. Select the time of day when you want the process to run. 00 hour and 00 min is midnight. Time is based on the 24-hour clock. 3. Check the **Enable Schedule** check box if you want to activate this schedule. 4. Choose either **ALI Update Schedule** or **Secondary Status Update Schedule**.	We recommend that you run th E911 Service Provider update pr once per day. Because of the ad traffic, it is best to run the proc normal business hours.
Add button	Click **Add** to add the schedule to the list of schedules.	
Cancel Changes button	Click **Cancel Changes** to change the fields on this page back to the last saved settings.	
Update button	Click **Update** when viewing an existing schedule to save changes you make to the schedule.	Only available when viewing a schedule.

Related Topics

Find National E911 Service Provider ERL, on page 411

Default ALI Values, on page 412

National E911 Service Provider ERL - Secondary Status, on page 413

View ALI Discrepancies, on page 415

Configure Emergency Responder and National E911 Service Provider Enterprise Services , on page 183

View ALI Discrepancies

The View ALI Discrepancies page appears when you choose **ERL** > **National E911 Service Provider ERL** > **View ALI Discrepancies**.

Authorization Requirements

You must have system administrator or ERL administrator authority to access this page.

Description

Use the View ALI Discrepancies page to view discrepancies in the records between the ALI data that is stored in the local Emergency Responder database and the ALI data for this ELIN in the National E911 Service Provider database.

The following table describes the Find ALI Discrepancies page.

Table 56: ALI Discrepancies

Field	Description
Find ELIN where...	Enter search criteria to select the ELIN that you want to find. To find all ELIN, click **Find** without entering any criteria. To narrow your search, select the field that you want to search on from the drop-down list, select the search relationship (is contains, begins with, and so on), and enter the search string. Click **Find**.

Related Topics

Find National E911 Service Provider ERL, on page 411

Default ALI Values, on page 412

National E911 Service Provider ERL - Secondary Status, on page 413

National E911 Service Provider Schedule, on page 414

Configure Emergency Responder and National E911 Service Provider Enterprise Services , on page 183

View ALI Discrepancies for a Specific ELIN

Choose **ERL** > **National E911 Service Provider ERL** > **View ALI Discrepancies** and search for discrepancies. The View ALI Discrepancies for a specific ELIN page appears when you select a specific ELIN from the results.

Authorization Requirements

You must have system administrator or ERL administrator authority to access this page.

Description

Use the View ALI Discrepancies for a Specific ELIN page to view discrepancies in the records between the ALI data that is stored in the local Emergency Responder database and the ALI data for this ELIN in the National E911 Service Provider database.

The following table describes the Find ALI Discrepancies for a specific ELIN page.

Table 57: ALI Discrepancies for Specific ELIN

Field	Description
View National E911 Service Provider ALI Discrepancies	

Field	Description
ALI Fields	List of ALI field information from the local Emergency Responder database and from National E911 Service Provider database: • House Number • House Suffix • Street Name • Prefix Directional • Street Suffix • Post Directional • Community Name • State • Main NPA • Class of Service • Type of Service • Exchange • Customer Name • Order Number • Extract Date • County ID • Company ID • Zip Code • Zip Code Extension • Customer Code • Comments • Longitude • Latitude • Elevation • TAR Code • Location • Reserved
Save button	Click **Save** to save your changes in the local Emergency Responder database.

Field	Description
Save National E911 Service Provider ALI Info button	Click **Save National E911 Service Provider ALI Info** to update the National E911 Service Provider VUI database.
Cancel Changes button	Click **Cancel Changes** to change the fields on this page back to the last saved settings.
Close button	Click **Close** to close the window.

Related Topics

- Find National E911 Service Provider ERL, on page 411
- Default ALI Values, on page 412
- National E911 Service Provider ERL - Secondary Status, on page 413
- National E911 Service Provider Schedule, on page 414
- Configure Emergency Responder and National E911 Service Provider Enterprise Services , on page 183

ERL Migration Tool

The ERL Migration Tool page appears when you choose **ERL** > **ERL Migration Tool**.

Authorization Requirements

You must have system administrator or ERL administrator authority to access this page.

Description

Use the ERL Migration Tool page to migrate ERLs from conventional ERL data to National E911 Service Provider ERL data and vice versa.

The following table describes the ERL Migration Tool page.

Table 58: ERL Migration Tool

Field	Description
Status	Displays status messages
ERL Search Parameter	
Find	Select search criteria and click **Find** to list either existing Conventional ERLs or National E911 Service Provider ERLs. From the search results list, you can select the ERLs that you want to migrate
Migrate to National E911 Service ProviderERL Button	When you search for Conventional ERLs, you can select the ERLs that you want to migrate to National E911 Service Provider. When you click the **Migrate to** National E911 Service Provider **ERL** button, you can select an National E911 Service Provider route point for all the selected ERL.

Field	Description
Migrate to Regular ERL	When you search for National E911 Service Provider ERLs, you can select the ERLs that you want to migrate to a conventional ERL data. When you click the **Migrate to Regular ERL** button, you can enter a route point, and specify whether the ERL is a test ERL and test the ERL.

Related Topics

Find National E911 Service Provider ERL, on page 411

Default ALI Values, on page 412

National E911 Service Provider ERL - Secondary Status, on page 413

National E911 Service Provider Schedule, on page 414

View ALI Discrepancies, on page 415

Configure Emergency Responder and National E911 Service Provider Enterprise Services , on page 183

ERL Data Migration , on page 190

SNMP Settings

The SNMP Settings page appears when you choose **Phone Tracking** > **SNMPv2 Settings** or **Phone Tracking** > **SNMPv3 Settings**.

Authorization Requirements

You must have system administrator or network administrator authority to access this page.

Description

Use the SNMPv2 Settings page or the SNMPv3 Settings page to define the SNMP read community string used by your switches.

Related Topics

Set Up SNMPv2, on page 149

Set Up SNMPv3 , on page 151

E911 and Cisco Emergency Responder Terminology , on page 6

SNMP v2 Settings Page

Use the information in the following table to configure the SNMPv2 Settings.

Table 59: SNMP v2 Settings Page

Field	Description	Notes
Add SNMPv2 Community Setting		

Field	Description	Notes
IP Address/Host Name	The IP address or hostname of a switch whose SNMP read community string you are defining. If you use the same read community string for all switches, you only need to define one entry: *.*.*.*. If you use different read community strings for sets of switches, you can define each set, using variables and ranges. For example, if you have 10 switches from 10.1.115.0 to 10.1.125.0, you can use 10.1.115-125.0 as the IP address. You can also mix ranges and variables, such as *.*.115-125.*. **Note** If you are using IPv6 address, then wildcard characters are not supported. Enter the details for each switch.	You are not defining your switches page, you are only associating IP ad patterns to read community strings. Emergency Responder only tries to string with the specific switches you on the LAN Switch Details page. Se Switch Details, on page 434 for mor information. If two or more patterns match an IP Emergency Responder uses the SNM associated with the most closely ma pattern.
Timeout	The time, in seconds, in which Emergency Responder should consider an attempted SNMP connection to a switch to have failed. See the explanation of Retries for more information.	Default is 10 seconds. The optimal v to 15 seconds.
Maximum Retry Attempts	The number of times Emergency Responder should attempt to contact a switch. With each retry, the previous timeout is multiplied by 2, to ensure that the switch has enough time to respond. For example, if you specify 10 for timeout, the first attempt times out in 10 seconds, the second attempt times out in 20 seconds, the third attempt times out in 40 seconds, and so forth.	Default is 2 retries. This number do include the initial attempt; that is, if 2, Emergency Responder attempts t a switch up to 3 times (the initial att 2 retries). The optimal value is 2 to 3 retries.
Read Community	The SNMPv2 read community string for the switch. **Note** Community string does not support special characters like angle brackets (< >), backslash (\\), colon (:), quotation marks (“ “), and tilde (~).	Default is public for any IP address n in the SNMPv2 settings list.
Insert	Click the **Insert** button to add the entry to the list of SNMP settings.	
Cancel Changes	Click the **Cancel Changes** button to change the fields on this page back to the last saved settings.	
SNMPv2 Settings	A list of SNMPv2 settings that you have already defined. To change an entry, click any of the links associated with the entry to load the details into the edit boxes at the top of the page. Then make your changes and click **Update**. To delete an entry, click the **Delete** icon for the entry.	

Field	Description	Notes
Add New	Click the **Add New** button to add another SNMPv2 setting.	
Update	Click the **Update** button to save changes you make to an existing SNMPv2 setting.	Only available when viewing an setting.
Export	Click the **Export** button to export the SNMPv2 data settings to another file. For more information, see Export SNMPv2 Data, on page 421.	
Import	Click the **Import** button to import the SNMPv2 data settings to your Cisco Emergency Responder configuration. For more information, see Import SNMPv2 Data, on page 422.	

Export SNMPv2 Data

The **Export SNMPv2 Data** window appears when you click **Export** on the **SNMPv2 Settings** page (opened when you choose **Phone Tracking** > **SNMPv2 Settings**).

Authorization Requirements

You must have the system administrator or ERL administrator authority to access this window.

Description

Use the **Export SNMPv2 Data** window to perform the following:

- Create a file containing the Emergency Responder Export SNMPv2 Data.
- Use the **Download** option to download a file containing the Emergency Responder Export SNMPv2 Data. For more information, see Download File , on page 113.

The following table describes the fields found on the **Export SNMPv2 Data** window.

Table 60: Export SNMPv2 Data Window

Field	Description
Export SNMPv2 Data	
Select Export Format	Select the file format from the drop-down list that matches the file being imported.
Enter Export File Name	Enter the name of the file that you want to create. Do not include the file extension.
Export	Click the **Export** button to add data from the import file to your Cisco Emergency Responder configuration.
Close	Click the **Close** button to close the window.

Field	Description
Export Status	This text box displays status information.
Download	
Select a File to Download	Select a file from the drop-down list and click the **Download** button to download the file to your machine.

Related Topics

Download File , on page 113

Import SNMPv2 Data

The **Import SNMPv2 Data** window appears when you click **Import** on the **SNMPv2 Settings** page (opened when you choose **Phone Tracking** > **SNMPv2 Settings**).

Authorization Requirements

You must have the system administrator or ERL administrator authority to access this window.

Description

Use the **Import SNMPv2 Data** window to create or update several SNMPv2 settings details at once from the file in which you have defined their data. You can create this file using a spreadsheet and save the information in the required formats. The **View sample file** link provides the sample information to create or update your import file.

You can import a previously exported file or you can upload a file that you created on your local system using the **Upload** option. For more information, see Upload File , on page 113.

The following table describes the fields found on the **Import SNMPv2 Data** window.

Table 61: Import SNMPv2 Data Window

Field	Description
Import SNMPv2 Data	
Select Import Format	Select the file format from the drop-down list that matches the file being imported. Click **View sample file** link to view an example of the expected format and sequence of values. Use this sample information to create your import file in a spreadsheet.
Select File to Import	Select the file from the drop-down list from which you want to import data.
Import	Click the **Import** button to add data from the import file to your Cisco Emergency Responder configuration.

Field	Description
Upload	Click the **Upload** button to upload the file from your machine. For more information, see Upload File , on page 113.
Close	Click the **Close** button to close the window.
Import Status	This text box displays status information.

Related Topics

Upload File , on page 113

SNMP v3 Settings Page

Use the information in the following table to configure the SNMP v3 Settings.

Table 62: SNMP v3 Settings Page

Field	Description	Notes
Add SNMPv3 User Details		
User Information		
IP Address/Host Name	Enter the IP address or hostname of the Cisco Unified Communications Manager or LAN switch.	For IPv4 address, you can use ar as a wildcard character. **Note** For IPv6 address, w characters are not su You can also use a range of num such as 15 to 30.
User Name	Enter the username configured on Cisco Unified Communications Manager or LAN switch.	The name can contain up to 32 c can contain any combination of characters, hyphens (-), and und characters (_).
Authentication Information		
Password	To enable authentication, check the **Authentication Required** check box; in the Password and the Reenter Password fields, enter the password for the user configured on the Cisco Unified Communications Manager or LAN switch.	
Protocol	Choose the appropriate protocol as configured for the user on Cisco Unified Communications Manager or LAN switch.	
Privacy Information		

Field	Description	Notes
Password	If you selected the Authentication Required check box, you can specify the privacy information. To require privacy, select the check box, enter the password in both the Password, and the Reenter Password fields for the user configured on the Cisco Unified Communications Manager or LAN switch.	
Protocol	Choose the appropriate protocol as configured for the user on Cisco Unified Communications Manager or LAN switch.	
Other Information		
Timeout (in seconds)	The length of time that an attempted SNMP connection remains idle before it is considered to have failed. For more information, see the explanation for Maximum Retry Attempts.	The default value is 10 seconds. Th value is 10 to 15 seconds.
Maximum Retry Attempts	The number of times Emergency Responder attempts to contact a Cisco Unified Communications Manager or a switch. With each retry, the previous timeout is multiplied by two to ensure that the switch has time to respond. For example, if you specify a Timeout value of 10 seconds, the first attempt times out in 10 seconds, the second attempt times out in 20 seconds, and the third attempt times out in 40 seconds.	The default value is two. But the opti is two to three retries. The Maximum Retry Attempts does n the initial attempt. For example, if M Retry Attempts is set to two, Emerg Responder attempts to contact a swi times - the initial attempt plus two r
Insert	Click the **Insert** button to add the entry to the list of SNMP settings.	
Cancel Changes	Click the **Cancel Changes** button to change the fields on this page back to the last saved settings.	
SNMPv3 Settings	A list of SNMPv3 settings that you have already defined. To change an entry, click any of the links associated with the entry to load the details into the edit boxes at the top of the page. Then make your changes and click **Update**. To delete an entry, click the **Delete** icon for the entry.	
Add New	Click the **Add New** button to add another SNMPv3 setting.	
Update	Click the **Update** button to save changes you make to an existing SNMPv3 setting.	Only available when viewing an exi setting.

Field	Description	Notes
Import	Click the **Import** button to import the SNMPv3 data settings to your Cisco Emergency Responder configuration. For more information, see Import SNMPv3 Data, on page 425.	

Import SNMPv3 Data

The **Import SNMPv3 Data** window appears when you click **Import** on the **SNMPv3 Settings** page (opened when you choose **Phone Tracking** > **SNMPv3 Settings**).

Authorization Requirements

You must have the system administrator or ERL administrator authority to access this window.

Description

Use the **Import SNMPv3 Data** window to create or update several SNMPv3 settings details at once from the file in which you have defined their data. You can create this file using a spreadsheet and save the information in the required formats. The **View sample file** link provides the sample information to create or update your import file.

You can import a previously exported file or you can upload a file that you created on your local system using the **Upload** option. For more information, see Upload File , on page 113.

The following table describes the fields found on the **Import SNMPv3 Data** window.

Table 63: Import SNMPv3 Data Window

Field	Description
Import SNMPv3 Data	
Select Import Format	Select the file format from the drop-down list that matches the file being imported. Click **View sample file** link to view an example of the expected format and sequence of values. Use this sample information to create your import file in a spreadsheet.
Select File to Import	Select the file from the drop-down list from which you want to import data.
Import	Click the **Import** button to add data from the import file to your Cisco Emergency Responder configuration.
Upload	Click the **Upload** button to upload the file from your machine. For more information, see Upload File , on page 113.
Close	Click the **Close** button to close the window.

Field	Description
Import Status	This text box displays status information.

Related Topics

Upload File , on page 113

Phone Tracking Schedule

The Phone Tracking Schedule page appears when you choose **Phone Tracking > Schedule**.

Authorization Requirements

You must have system administrator or network administrator authority to access this page.

Description

Use the Phone Tracking Schedule page to define the CiscoEmergencyResponder (Emergency Responder) schedule for updating phone and switch information from the network. Emergency Responder updates network information using two processes:

- Phone Tracking—A periodic comparison of the phones registered with CiscoUnifiedCommunicationsManager to the location information obtained from the switches. If a phone moves, Emergency Responder updates the phone ERL.
- Switch Port and Phone Update—The phone tracking process plus a more extensive check of the network switches, which can identify new or changed switch modules (additional or removed ports). Ensure that your ERL administrator updates the ERL assignment for new ports.

The following table describes the Phone Tracking Schedule page.

Table 64: Phone Tracking Schedule Page

Field	Description	Notes
Incremental Phone Tracking		
Incremental Phone Tracking Interval	The time, in minutes, between making updates to the known phone locations. This periodic update ensures that phones that have moved are located and assigned to the correct ERL. Click **Update** to save your changes to this field.	The default is 30 minutes. The range of the interval that can b is 5 to 300 minutes.
Enhanced Location Phone Tracking	The time, in minutes, between making updates to the unknown phone locations. This periodic update ensures that devices that have moved are located and assigned to the correct ERL. Click Update to save your changes to this field.	The default is 2 minutes. The range of the interval that can b is 1 to 180 minutes. **Note** By default, AXL Incr Phone tracking shoulc greater than Increment tracking.

Field	Description	Notes
Add New Schedule	Enter the schedule that you want to add: 1. Select the days of the week when you want to run the switch port and phone update process. 2. Select the time of day when you want the process to run. 00 hour and 00 min is midnight. Time is based on the 24-hour clock.	We recommend that you run th and phone update process at le day. Because of the added netw it is best to run the process outs business hours.
Insert button	Click **Insert** to add the schedule to the list of schedules.	
Cancel Changes button	Click **Cancel Changes** to change the fields on this page back to the last saved settings.	
Update button	Click **Update** when viewing an existing schedule to save changes that you make to the schedule.	Only available when viewing a schedule.
Switch-Port and Phone Update Schedule	The list of schedules you have defined. To change a schedule, click the Hour link, the Minute link, or the Edit icon to load it into the Modify Schedule area above the list. Then, make your changes and click **Update**. To remove a schedule, click the **Delete** icon for the schedule.	If any schedules overlap, only is run.
Add New button	Click **Add New** to add another schedule.	

Related Topics

Define Phone Tracking and Switch Update Schedules, on page 152
Manually Run the Switch-Port and Phone Update Process , on page 157
E911 and Cisco Emergency Responder Terminology , on page 6

Cisco Unified Communications Manager Clusters

The Cisco Unified Communications Manager Clusters page appears when you choose **Phone Tracking > Cisco Unified Communications Manager**.

Authorization Requirements

You must have system administrator or network administrator authority to access this page.

Description

Use the Cisco Unified Communications Manager Clusters page to identify the Cisco Unified Communications Manager clusters whose emergency calls this Emergency Responder group handles. Only assign a Cisco Unified Communications Manager cluster to a single Emergency Responder group. Emergency Responder gets the list of phones registered with these Cisco Unified Communications Manager servers and tracks the movements of these phones.

The following table describes the Cisco Unified Communications Manager Clusters page.

Table 65: Cisco Unified Communications Manager Clusters Page

Field	Description	Notes
Add New Cisco Unified Communications Manager Cluster		
Cisco Unified Communications Manager	The IP address or DNS name of a Cisco Unified Communications Manager server that is running Cisco Unified Communications Manager and SNMP services. Only add one server per Cisco Unified Communications Manager cluster—Emergency Responder can identify the other servers in the cluster. The Cisco Unified Communications Manager server you specify represents the cluster in which it is a member.	When viewing a previously defined Cisco Unified Communications Manager server, Emergency Responder displays a **CCM List** link. Click **CCM List** to view a list of the Cisco Unified Communications Manager servers that belong to the same cluster as the selected server. **Note** The Cisco Unified Communications Manager servers should have run the CCM service at least once. After the IP address or DNS name has been configured, it cannot be modified.
CTI Manager	The IP address or DNS name of the CTI Manager used by the specified Cisco Unified Communications Manager server.	
CTI Manager User Name	The name of the user created in the Cisco Unified Communications Manager server for Emergency Responder use.	This user must have specific characteristics and device assignments. See Create Emergency Responder Cisco Unified Communications Manager User, on page 104 for specific information.
CTI Manager Password	The password for the user.	

Field	Description	Notes
Backup CTI Manager 1	The IP address or DNS name of the backup CTI Manager used by the specified Cisco Unified Communications Manager server.	
Backup CTI Manager 2	The IP address or DNS name of the backup CTI Manager used by the specified Cisco Unified Communications Manager server.	
Telephony Port Begin Address	The number of the first CTI port to use for calling onsite alert (security) personnel. When an emergency call is made, Emergency Responder calls the onsite alert personnel for the originating ERL using the telephony ports you configure here.	You must first create this port in Cisco Unified Communications Manager. See Create Required CTI Ports, on page 90 for more information.
Number of Telephony Ports	The number of CTI ports. Enter the number of CTI ports you created in Cisco Unified Communications Manager. The number of ports is the number of concurrent calls Emergency Responder can make to onsite alert personnel.	The ports used are in sequence from the beginning port. For example, if you enter 3000 for the begin port, and 4 for number of ports, Emergency Responder uses 3000, 3001, 3002, and 3003.
Enable Secure Connection		
Enable Secure Connection check box	Check this check box to enable a secure connection. You can enter data in the other fields of this section only if you have enabled Secure Connection.	
TFTP Server IP Address	The IP address of the TFTP server.	

Field	Description	Notes
TFTP Server Port	The port of the TFTP server.	
Backup TFTP Server IP Address	The IP address of the backup TFTP server, for the Unified CM node being added.	
CAPF Server IP Address	The IP address of the CAPF server.	
CAPF Server Port	The port of the CAPF server.	
Instance ID for Publisher	The instance ID for the Publisher node.	
Secure Authentication String for Publisher	The secure authentication string for the Publisher node.	
Instance ID for Subscriber	The instance ID for the Subscriber node.	
Secure Authentication String for Subscriber	The secure authentication string for the Subscriber node.	

Field	Description	Notes
Enable SRTP for Audio Alerts	Check this check box if you want Emergency Responder to send Secure Real-Time Transport Protocol (SRTP) enabled Onsite Phone alert to Onsite Security Users during an Emergency Call. With this option enabled for each Unified Communication Manager cluster, the Emergency Responder Onsite personnel receive secured onsite audio alerts. The default value for this check box leaves it unchecked. **Note** Ensure that the onsite phone supports encrypted audio calls and is properly configured in the Unified Communications Manager to get the onsite audio alerts.	The value of this field gets determined by the setting of the Unified Communications Manager service parameter **Block Unencrypted Calls**. This parameter specifies whether Unified Communications Manager allows calls from Emergency Responder without data encryption. When the **Block Unencrypted Calls** parameter is set to TRUE, only calls with media encryption support are allowed and unencrypted calls are blocked. When the **Block Unencrypted Calls** parameter is set to FALSE, calls are allowed whether or not their media is encrypted.
AXL Settings		

Field	Description	Notes
AXL Username	The username for the application user on Cisco Unified Communications Manager with privileges to perform AXL queries.	**Note** The selected user in the Cisco Emergency Responder Location Management application server in Unified CM should match the user in the Cisco Emergency Responder page: **Phone Tracking > CUCM > AXL Username**. Though, the Emergency Responder AXL username and CTI username have the required permissions, the username selected in the application server must match the AXL username. After updating the application server username, you must also restart the CUCM Cisco E911 network service on all the nodes in the cluster. This service restart causes the Unified CM 911 to use the new userID and establish the connection between the two servers.

Field	Description	Notes
AXL Password	The password for the application user on Cisco Unified Communications Manager with privileges to perform AXL queries.	
AXL Port Number	The port number that is used by the application on Cisco Unified Communications Manger. The default value is 8443.	
SNMP Settings		
Use SNMPv3 for discovery	Check this check box if the Cisco Unified Communications Manager has SNMPv3 enabled and you want Emergency Responder to use SNMPv3 for discovery.	
Insert button	Click **Insert** to add the new CiscoUnifiedCommunicationsManager server to the list of servers.	
Cancel Changes button	Click **Cancel Changes** to change the fields on this page back to the last saved settings.	
Update button	Click **Update** when viewing an existing server to save changes you make to the server.	Only available when viewing an existing server. Replaces the **Insert** button when viewing an existing server.
Cisco Unified Communications Manager Clusters		
Add New button	Click **Add New** to add another Cisco Unified Communications Manager server.	

Field	Description	Notes
Cisco Unified Communications Manager list	A list of Cisco Unified Communications Manager servers defined for this Emergency Responder group. Click a server link or the **Edit** icon to view and modify the Emergency Responder configuration for the server. Click the **Delete** icon to delete the server. Click **Number of Users associated** link to find the list of remote users associated with the Cisco Unified Communications Manager Server node.	

Related Topics

Identify Cisco Unified Communications Manager Clusters , on page 132
Create Emergency Responder Cisco Unified Communications Manager User, on page 104
Create Required CTI Ports, on page 90
E911 and Cisco Emergency Responder Terminology , on page 6

LAN Switch Details

The LAN Switch Details page appears when you choose **Phone Tracking > LAN Switch Details**.

Note Cisco Emergency Responder supports SNMP Version 1, Version 2 , Version 2C, and Version 3 of a LAN switch.

Authorization Requirements

You must have system administrator or network administrator authority to access this page.

Description

Use the LAN Switch Details page to add, remove, or change the switches that Emergency Responder manages. Ensure that you identify all switches that might have phones attached to them. You can only assign switch ports to ERLs if you enter the switches on this page. Any phones attached to unidentified switches or ports are listed as unlocated phones in Emergency Responder, and are assigned to the Default ERL.

Note Switches should not be configured with Static Engine ID.

The following table describes the LAN Switch Details page.

Table 66: LAN Switch Details Page

Field	Description
LAN Switch Details	
Switch Host Name/IP Address	The IP address or DNS name of the switch. For more information on standardized valid IPv4 or IPv6 address formats, see the following: • https://docs.oracle.com/javame/config/cdc/ref-impl/pbp1.1.2/jsr217/java/net/Inet4Address.html • https://docs.oracle.com/javame/config/cdc/ref-impl/pbp1.1.2/jsr217/java/net/Inet6Address.html
Description	Description of this switch.
Enable CAM-based Phone Tracking	Check this check box if there might be phones attached to this switch that do not use the Cisco Discovery Protocol (CDP) to announce themselves to the network. For non-CDP phones, Emergency Responder must use the Content Addressable Memory (CAM) information about the switch to identify phones.
Use port description as port location	Check this check box if you want to display the switch port description that is configured on the switch in the Location Field.
Use SNMPv3 for Discovery	Select this check box if the switch has SNMPv3 enabled and Emergency Responder should discover it using SNMPv3.
Insert button	Check **Insert** to add the switch to the list of switches. When you click Insert, Emergency Responder asks if you want to run the switch port and phone update process on the switch right away. Click **OK** to run the process now, or click **Cancel** to add the switch to the configuration without running the process right away. **Note** See Manually Run the Switch-Port and Phone Update Process , on page 157 for information about running the process if you select not to run it immediately.
Update button	Click **Update** when viewing an existing switch to save changes that you make to the switch.
Cancel Changes button	Click **Cancel Changes** to change the fields on this page back to the last saved settings.
LAN Switches	

Field	Description
LAN Switch list	A list of the switches you have already defined. Click the IP address/DNS name of the switch or click the **Edit** icon to view and modify settings for the switch. Click the **Delete** icon to delete the switch.
Add LAN Switch button	Click **Add LAN Switch** to add another switch.
Export	Click the **Export** link to export the switch definitions to another file. See Export LAN Switch , on page 436 for more information.
Import	Click the **Import** link to import a list of switches into the Emergency Responder configuration. This list might be exported from your network management software. See Import LAN Switch, on page 437 for more information.

Related Topics

LAN Switch Identification , on page 153
Manually Run the Switch-Port and Phone Update Process , on page 157
Identify Unlocated Phones , on page 167
E911 and Cisco Emergency Responder Terminology , on page 6

Export LAN Switch

The Export LAN Switch page appears when you click Export in the LAN Switch Details page (opened when you choose **Phone Tracking > LAN Switch Details**).

Authorization Requirements

You must have system administrator or network administrator authority to access this page.

Description

Use the Export LAN Switch page to create a file containing the Emergency Responder switch configuration.

If you must update several switch entries in Emergency Responder, you can export the switch information, make your changes in the export file using a spreadsheet, then reimport the file.

You can also download a file to your local system using the Download utility. See Download File , on page 113 for more information.

The following table describes the Export LAN Switch page.

Table 67: Export LAN Switch Page

Field	Description
Select Export Format	The format to use for the file, such as CSV (comma- separated values).
Enter Export File Name	The name of the file you want to create. Do not include the file extension.
Export button	Click **Export** to create the file. The Status box shows the status of the exportation.
Close button	Click **Close** to close the window.

Field	Description
Download	
Select a File to Download	Use the pull-down menu to select a LAN switches configuration file and click **Download** to download the file to your local system.

Related Topics

- Export Switch Information , on page 156
- Download File , on page 113
- Import a Group of Switches , on page 155
- LAN Switch Details, on page 434
- E911 and Cisco Emergency Responder Terminology , on page 6

Import LAN Switch

The Import LAN Switch page appears when you click **Import** in the LAN Switch Details page (opened when you choose **Phone Tracking > LAN Switch Details**).

Authorization Requirements

You must have system administrator or network administrator authority to access this page.

Description

Use the Import LAN Switch page to add several switches at once to the Emergency Responder configuration. You can import a previously exported file or a file that you created on your local system and uploaded using the Upload utility. See Upload File , on page 113 for more information.

The following table describes the Import LAN Switch page.

Table 68: Import LAN Switch Page

Field	Description
Select Import Format	Select the format used in the file you are importing. After you select the format, click **view sample file** to see an example of the expected format a of values. Use this sample information to create your import file in a spreadsheet, or to de your network management software can create the required format.
Select File to Import	Select the file from which you want to import data. Before you can import a file, you must place it in the folder mentioned on this page.
Upload button	Click **Upload** to upload a file from your local system. See Upload File , on page 113 for more

Field	Description
Import button	Click **Import** to add data from the information in the import file to your Emergency Respond configuration. Emergency Responder asks you whether you want to run phone tracking on the imported swi must run phone tracking before you can configure the switch ports, so normally you should cho If you choose **Cancel**, Emergency Responder imports the switches but does not run the phone process. **Note** If you elect not to run the phone-tracking process, after importing the file, run th port and phone update process. See Manually Run the Switch-Port and Phone Up Process , on page 157.
Close button	Click **Close** to close the window.
Import Status	Text box that displays status information.

Related Topics

Import a Group of Switches , on page 155

Export Switch Information , on page 156

Upload File , on page 113

LAN Switch Details, on page 434

E911 and Cisco Emergency Responder Terminology , on page 6

Run Switch-Port and Phone Update

When you choose **Phone Tracking/Run Switch-Port & Phone Update**, a dialog box appears that prompts you to “Press Okay to run Switch-Port and Phone update process on Emergency Responder.”

Authorization Requirements

You must have system administrator or ERL administrator authority to access this page.

Description

Use the Run Switch-Port and Phone Update page to run manually the switch port and phone update process.

Related Topics

Manually Run the Switch-Port and Phone Update Process , on page 157

Define Phone Tracking and Switch Update Schedules, on page 152

Identify Unlocated Phones , on page 167

Switch Port Details

The Switch Port Details page appears when you choose **ERL Membership** > **Switch Ports**.

Authorization Requirements

You must have system administrator or ERL administrator authority to access this page.

Description

Use the Switch Port Details page to assign switch ports to ERLs. This assignment allows Emergency Responder to assign the correct ERL to phones that connect to the network through the configured ports.

Note If the IOS software on the switch needs to be upgraded to the latest version, execute the **snmp-server ifindex persist** command before the upgrade. Failure in executing this command leads to change of port indexes. In that scenario, Emergency Responder treats the existing port as a new port and turns the assigned ERL to Blank (no ERL).

To support switches such as the CiscoCatalyst 3750 switch, which has ports that can be uniquely identified by Switch ID, Module ID and Port ID combination, Emergency Responder uses the following port-naming convention:

- IfName—New field display name for port as given for the switch CLI (for example, Fa1/5 or Gi2/0/1).
  - Port Identifier—Replaces the Module ID/Port ID.
  - It contains {optional} <<Switch ID (for stackable switches like the CiscoCatalyst3750)>>/ {optional} <<relative position of the module in switch>> / <<relative position of port in the module>> .
- Search on Port IfName replaces the Module ID/Port ID search.

The following table describes the Switch Port Details page.

Table 69: Switch Port Details Page

Field	Description	Notes
Switch Port Search Parameters		
Find ports where	Enter search criteria to select the ports that you want to view or configure. To view all ports, click **Find** without entering any criteria. To narrow your search: • Select **All** to indicate that only calls that match every criteria be selected (an AND search); select **Any** to indicate that calls that match any search criteria be selected (an OR search). From the pull-down menu, select the field that you want to search on (ERL Name, Phone MAC Address, and so on), select the search relationship (contains, starts with, and so on), enter the search string, and select how many results on page are displayed. • To search on a combination of fields, click the **Plus** icon **(+)** to add more search parameters. (Click the **Minus** icon (–) to remove search parameters.) • Click **Find** when you have entered all the search parameters.	If you are co ports, genera ports using t button.

Field	Description	Notes
	The list of switch ports that match your search criteria, one line per port. To assign ERLs to selected ports, check the check box to the left of the switch details, enter the ERL name in the text box, or click **Search ERL** to find and select the ERL, then click **Assign ERL**. To view and update the phone location for a port, click the **View** link in the port's Location column. **Note** Location name or switch port description cannot include special characters, such as the colon (:), semicolon (;), backslash (\\), brackets (( )), pound sign (#), or ampersand (&). Location details should not start with the special character, less than (<). To change the fields shown in the list and to change their order, click **Edit View**. This action opens a separate Edit View page: • To add a field, select it in the Available Fields list and click > (right arrow). • To remove a field, select it in the Selected Fields list and click < (left arrow). **Note** You cannot remove the ERL Name from the table view. Click **Apply** to save your changes on the Edit Table View page. Click **Close** to close the window.	Emergency Resp displays a maxin number of 1,000 port records at a the search result than 1,000 switc error message to search is display If many ports ma search criteria, E Responder uses pages to display the First, Previou and Last links at bottom of the pag between pages. Y also enter a spec number on the P and press Enter t that page.
Export	Click **Export** to export the ERL to switch port configuration to another file. See Export Switch Ports, on page 440 for more information.	
Import	Click **Import** to import a set of ERL-to-port mappings into the Emergency Responder configuration. See Import Switch Ports, on page 441 for more information.	

Related Topics

Switch Port Configuration , on page 159

LAN Switch Identification , on page 153

Manually Run the Switch-Port and Phone Update Process , on page 157

E911 and Cisco Emergency Responder Terminology , on page 6

Export Switch Ports

The Export Switch Ports page appears when you click **Export** in the Switch Port Details page (opened when you choose **ERL Membership** > **Switch Ports**).

Authorization Requirements

You must have system administrator or ERL administrator authority to access this page.

Description

Use the Export Switch Ports page to create a file containing the Emergency Responder switch port configuration.

If you must make changes to a large number of port-to-ERL assignments, you can export a file, make your changes in the file using a spreadsheet, and then reimport the file.

You can also download a file using the Download utility, modify it on your local system, then upload it using the Upload utility. See Download File , on page 113 for more information.

The following table describes the Export Switch Ports page.

Table 70: Export Switch Ports Page

Field	Description
Select Export Format	The format to use for the file, such as CSV (comma-separated values).
Enter Export File Name	The name of the file you want to create. Do not include the file extension.
Export button	Click **Export** to create the file. The Status box shows the status of the exportation.
Close button	Click **Close** to close the window.
Download	
Select a File to Download	Use the pull-down menu to select a file and click **Download** to download the file to your local system.

Related Topics

Export Switch Port Information , on page 162

Download File , on page 113

Set Up Large Number of Ports , on page 161

Switch Port Details, on page 438

E911 and Cisco Emergency Responder Terminology , on page 6

Import Switch Ports

The Import Switch Ports page appears when you click **Import** in the Switch Port Details page (opened when you choose **ERL Membership** > **Switch Ports**).

Authorization Requirements

You must have system administrator or ERL administrator authority to access this page.

Description

Use the Import Switch Ports page to add or update several switch port configurations at once to the Emergency Responder configuration. Switch port configurations are mappings of ports to ERLs.

To create the switch port import file, follow these steps:

1. Export the switch port details.
2. Modify the ERK field of these records and save the file.

3. Import the file using switch port import.

You can also create the import file on your local system and then upload the file using the Upload utility. See Upload File , on page 113 for more information.

The following table describes the Import Switch Ports page.

Table 71: Import Switch Ports Page

Field	Description
Select Import Format	Select the format used in the file you are importing. After you select the format, click **view sample file** to see an example of the expected format and of values. You can use this sample information to create your import file in a spreadsheet, but i to export the switch port information from Emergency Responder, modify the export file usir spreadsheet program, and then import the modified file. **Note** See Export Switch Port Information , on page 162 for information about exportin port information.
Select File to Import	Select the file from which you want to import data.
Upload button	Click **Upload** to upload a file from your local system. See Upload File , on page 113 for more infc
Import button	Click **Import** to add data from the information in the import file to your Emergency Respond configuration. ERL assignments in the import file override assignments that already exist in t Emergency Responder configuration. **Note** Port ERL configurations are only updated if Emergency Responder has discover port before you import the port configuration.
Close button	Click **Close** to close the window.
Import Status	Text box that displays status information.

Related Topics

Set Up Large Number of Ports , on page 161

Upload File , on page 113

Export Switch Port Information , on page 162

Switch Port Details, on page 438

E911 and Cisco Emergency Responder Terminology , on page 6

Save Switch Port Configuration

The Save Switch Port Configuration page appears when you click **Save Switch Config** in the Switch Port Details page (opened when you choose **ERL Membership** > **Switch Ports**).

Authorization Requirements

You must have system administrator or ERL administrator authority to access this page.

Description

Use the Save Switch Port Configuration page to save the configuration details in a file containing the Emergency Responder switch port configurations.

Note The Save Switch Configuration functionality can be used only when the IP address of the old switch and the new switch is the same. If the IP address of the old switch and the new switch is different, you must perform an export switch functionality to export the old switch port details, delete the old switch records, and then import the new switch details.

If you need to make changes to an existing switch and replace it with a newer switch, or even change large number of port-to-ERL assignments of an existing switch, you should first save and download the existing configuration details in a CSV file. You can then add or remove an existing switch and add a new switch and run Full Discovery, and then upload the saved CSV file to reuse the existing configuration changes that was saved in the CSV file. For example, you can reuse the ERL name and Location details of the previous switch that you had configured.

You can download the saved CSV files from the Save Switch Port Configuration page.

You can also download or delete saved CSV files using the **File Management Utility** > **Switch Config Files** option.

The following table describes the Save Switch Port Configuration page.

Table 72: Save Switch Port Configuration Page

Field	Description
Select Save Config Format	The format to use for the file, such as CSV (comma-separated values).
Enter Save Config File name	The name of the file you want to create. Do not include the file extension.
Save Config	Click **Save Config** to create the file. The Status box shows the status of the exportation.
Close	Click **Close** to close the window.
Download	
Select a File to Download	Use the drop-down menu to select a file and click **Download** to download the file to your local system.

Upload Switch Port Configuration

The Upload Switch Port Configuration page appears when you click **Upload Switch Config** in the Switch Port Details page (opened when you choose **ERL Membership** > **Switch Ports**).

Authorization Requirements

You must have system administrator or ERL administrator authority to access this page.

Description

Use the Upload Switch Port Configuration page to add or update switch port configurations (ERL Name and Location details) at once to the Emergency Responder switch port configuration. From the **Select File to Upload Config** drop-down list, you can choose one of the saved CSV files and upload the selected file.

Note The Upload Switch Port Configuration functionality can be used only when the IP address of the old and the new switch is the same. If the IP address of the old and new switch is different, you must perform an export switch functionality to export the old switch port details, delete the old switch records, and then import the new switch details.

The following table describes the Upload Switch Port Configuration page.

Table 73: Upload Switch Port Configuration Page

Field	Description
Select Upload config File Format	Select the format used in the file you are importing. For example, CSV format. After you select the format, click **View Sample File** to see an example of the expected format and sequence of values. You can use this sample information to create your saved configuration file in a spreadsheet. See Save Switch Port Configuration, on page 442 for information about exporting saved switch port information.
Select File to Upload Config	From the drop-down list, choose the file which for you want to import data.
Upload	Click **Upload** to upload a file from your local system. The Status box shows the status of the exportation. You can find details on the total number of port updates, and details on the total number of ports that have changed for the location, and ERL changes and updates.
Close	Click **Close** to close the window.

Access Point Details

The Access Point Details page appears when you choose**ERL Membership** > **Access Points**.

Authorization Requirements

You must have system administrator or ERL administrator authority to access this page.

Description

The Access Point Details page lists all the Access Points configured in the corresponding Cisco Unified Communications Manager.

You can assign Access Points to ERLs on the Access Point Details page. This assignment allows Cisco Emergency Responder to assign the correct ERL to phones that connect to the network through the configured Access Point.

The following table describes the Access Point Details page.

Table 74: Access Point Details Page

Field	Description	Notes
Status	It displays various status messages based on the action performed in the Access point page: • Ready—Displays when the Access Point page is loaded successfully. • Update successful—Displays when an ERL assignment is made successfully. • ERL Not Found—Displays when trying to assign an ERL which is not available.	
Access Point Search Parameters		
Find	Enter search criteria to select the Access Points that you want to view or configure. To view all Access Points, click **Find** without entering any criteria. To narrow your search: • From the first **Find** drop-down list, choose one of the following criteria: • Access Point Name • Bssid • ERL Name • From the second **where** drop-down list, choose one of the following criteria: • contains • is not Empty • starts with • Ends with • is Empty • is Exactly • Enter the required search string in next empty field. • From the **and show items per page** drop-down list, choose the appropriate number of results to be displayed on the page. • Click **Find** when you have entered all the search parameters.	

Field	Description	Notes
Access Points	The following list displays the “Find” status information: • Last discovery was done at—Displays the time and date of the last major/AXL discovery if the find result is successful. • No active query—This is displayed if you click the Access Point page without clicking the **Find** button. • No matching records—This is displayed when **Find** is unable to retrieve the matching records. • Phone Location tables are being modified. Please wait and try again—This is displayed when the Cisco Emergency Recorder server is not loaded completely. • Phone Location details are not populated as phone tracking is still in progress. Try after some time—This is displayed when the phone tracking engine is still running. • Cisco Emergency Responder server is not yet initialized completely. Please wait—This is displayed when the Cisco Emergency Responder service is restarted. • Cisco Emergency Responder is not running: Failed to contact Cisco Emergency Responder—This is displayed when the Cisco Emergency Responder service is restarted.	
	The list of Access Points that match your search criteria, one line per Access Point. To assign ERLs to selected Access Point, check the check box to the left of the access details, enter the ERL name in the text box, or click **Search ERL** to find and select the ERL, then click **Assign ERL**. To view the phones associated to that Access Point, click the **View Phones** link in the Access Point's View Phones column. The phone details include Phone, MAC Address, IP Address, Extension, and Phone Type. For more information, see Access Point Phones, on page 447.	Emergency Resp displays a maxin number of 1,000 Point records at the search result than 1,000 acces an error message the search is disp If a large numbe match your searc Emergency Resp several pages to them. Use the **Fi** **Previous**, **Next**, links at the botto page to move be pages. You can a a specific page n the **Page** field ar **Enter** to move t page.
Export	Click **Export** to export the ERL to Access Point configuration to another file. For more information, see Access Point Phones, on page 447.	

Access Point Phones

The Access Point Phones page appears when you choose **ERL Membership** > **Access Points** and click **View Phones** on any one of the records returned by the Access Point search.

Authorization Requirements

You must have a system administrator or ERL administrator authority to access this page.

Description

Use the Access Point Phones page to view the Access Point Name, the Bssid for each Access Point, and the list of phones tracked in that Access point.

Export Access Points

The Export Access Points page appears when you click **Export** on the Access Point Details page (opened when you choose **ERL Membership** > **Access Points**).

Authorization Requirements

You must have a system administrator or ERL administrator authority to access this page.

Description

Use the Export Access Points page to create a file containing the Cisco Emergency Responder access point configuration.

You can export a file and download the exported file using the Download utility. See Download File , on page 113 for more information.

The following table describes the Export Access Points page.

Table 75: Export Access Points Page

Field	Description
Select Export Format	The format to use for the file, such as CSV (comma-separated values).
Enter Export File Name	The name of the file you want to create. Do not include the file extension.
Export button	Click **Export** to create the file. The Status box shows the status of the exportation.
Close button	Click **Close** to close the window.
Download	
Select a File to Download	Use the drop-down menu to select a file and click Download to download the file to your local system.

Find and List IPv4 and IPv6 Subnets(Applicable from Release 15SU1 onwards)

Note From Release 15SU1 onwards, Emergency Responder also supports IPv6 Subnets. Any specific reference to IP Subnets should be understood to mean either IPv4 or IPv6 Subnets. You can configure either IPv4 or IPv6 subnet when you navigate to **ERL Membership** > **IP Subnets**.

The Find and List IPv4 and IPv6 Subnets page appears when you choose **ERL Membership** > **IP Subnets**.

Authorization Requirements

You must have a system administrator or ERL administrator authority to access this page.

Description

Use the Find and List IPv4 and IPv6 Subnets page to locate and view IP subnets that you would like to modify or delete. You can also navigate to add new IPv4 or IPv6 Subnets from this page.

Note Cisco Jabber devices will not work with IPv6 subnets in Emergency Responder.

The following table describes the Find and List IPv4 and IPv6 Subnets page.

Table 76: Find and List IPv4 and IPv6 Subnets Page (Applicable from Release 15SU1 Onwards)

Field	Description
IP Subnet Search Parameters	
Find IP Subnets where...	To list specific IP subnets, select the search criteria and click **Find**.To list all IP subnets, click **Find** without entering any criteria.
IP Subnets	
Add New IPv4 Subnet or **Add New IPv6 Subnet**	

Field	Description
IP Subnets list	Displays results of the IPv4 and IPv6 Subnets search. For the IPv4 and IPv6 Subnets found, the system displays the Subnet ID, Subnet Mask (IPv4)/Prefix Length (IPv6), ERL Name, and Location. Click on one of the preceding records or click the **Edit** icon to modify that IPv4 or IPv6 subnet. The Configure IPv4 Subnet or Configure IPv6 Subnet page appears. Change the Location field or the ERL Name field. **Note** When modifying an existing IPv4 subnet, you cannot change the Subnet ID or the Subnet Mask. **Note** When modifying an existing IPv6 subnet, you cannot change the Subnet ID or the Prefix Length. Click **Update** to save your changes to the IPv4 or IPv6 subnet. Click the **View Phones** icon in any record to view all of the IP subnet phones. The IP Subnet Phones page displays a list of the discovered phones in the IP subnet. See Configure IPv4 Subnet, on page 450 or Configure IPv6 Subnet (Applicable from Release 15SU1 Onwards), on page 451. Click the **Delete** icon to remove an IPv4 or IPv6 subnet. When you click **Delete**, Cisco Emergency Responder asks if you want to run the switch port, and the phone updates the process right away. Click **OK** to run the process immediately or click **Cancel** to delete the IPv4 or IPv6 subnet without running the process immediately.
Cancel Changes button	Click **Cancel Changes** to cancel any changes made on the Configure IPv4 Subnet or Configure IPv6 Subnet page. **Note** The **Cancel Changes** button is viewable only on the Configure IPv4 Subnet or Configure IPv6 Subnet page.
Add New IP Subnet (IPv4)	Click **Add New IP Subnet** to configure new IPv4 subnets. The Configure IPv4 Subnet page appears. See Configure IPv4 Subnet, on page 450 for more information.
Add New IP Subnet (IPv6)	Click **Add New IP Subnet** to configure new IPv6 subnets. The Configure IPv6 Subnet page appears. See Configure IPv6 Subnet (Applicable from Release 15SU1 Onwards), on page 451 for more information.
Export	Click **Export** to create a file containing the IP subnets configuration information. The Export IP Subnet page appears. See Export IP Subnets, on page 452 for more information.
Import	Click **Import** to import IP subnet configuration information from a file. The Import IP Subnet page appears. See Import IP Subnets, on page 453 for more information.

Configure IPv4 Subnet

To reach the Configure IPv4 Subnet page, choose **ERL** > **Membership** > **IP Subnets** and click on **Add New IPv4 Subnet**. The Configure IPv4 Subnet page appears.

Authorization Requirements

You must have a system administrator or ERL administrator authority to access this page.

Description

Use the Configure IPv4 Subnet page to manually define an IP subnet and its ERL. You must manually define an IP Subnet if the Emergency Responder cannot automatically track the type of phone. One example is if the phone is wireless. See Network Hardware and Software Requirements , on page 10 for information about phone support.

You can choose not to track the phones in an IP Subnet by checking the check box **Do not track phones under this IP subnet**. If you do not track the phones in an IP subnet, then you do not need the Emergency Responder User Licenses for these phones.

The following table describes the Configure IPv4 Subnet page.

Table 77: Configure IPv4 Subnet Page

Field	Description
Add New IPv4 Subnet	
Subnet ID	Enter a valid IPv4 subnet address that you want to define. For more information on standardized valid IPv4 address formats, see https://docs.oracle.com/javame/config/cdc/ref-impl/pbp1.1.2/jsr217/java/net/Inet4Address.html.
Subnet Mask	The mask of the subnet you want to define. Based on the bit mask, this value represents the number of IPv4 addresses that are included in this subnet.
Do not track phones under this IP subnet	Check this check box if you do not want this IPv4 subnet and the underlying phones tracked by Cisco Emergency Responder. If you do not track the phones in an IPv4 subnet, then you do not need the Emergency Responder User Licenses for these phones.
Location (optional)	The location of the new IP subnet.
ERL Name	The ERL to assign to the subnet. Type in a valid ERL name or click **Search ERL** to find and select the ERL.
Insert button	Click **Insert** to add the subnet. When you click **Insert**, Emergency Responder asks if you want to run the switch port, and the phone updates the process on the switch immediately. Click **OK** to run the process now, or click **Cancel** to add the IPv4 subnet to the configuration without running the process immediately.

Field	Description
Cancel Changes button	Click **Cancel Changes** to change the fields on this page back to the last saved settings.

Configure IPv6 Subnet (Applicable from Release 15SU1 Onwards)

To reach the Configure IPv6 Subnet page, choose **ERL** > **Membership** > **IP Subnets** and click on **Add New IPv6 Subnet**. The Configure IPv6 Subnet page appears.

Authorization Requirements

You must have a system administrator or ERL administrator authority to access this page.

Description

Use the Configure IPv6 Subnet page to manually define an IP subnet and its ERL. You must manually define an IP Subnet if the Emergency Responder cannot automatically track the type of phone. One example is if the phone is wireless. See Network Hardware and Software Requirements , on page 10 for information about phone support.

You can choose not to track the phones in an IP Subnet by checking the check box **Do not track phones under this IP subnet**. If you do not track the phones in an IP subnet, then you do not need the Emergency Responder User Licenses for these phones.

The following table describes the Configure IPv6 Subnet page.

Table 78: Configure IPv6 Subnet Page

Field	Description
Add New IP Subnet	
Subnet ID	Enter a valid IPv6 subnet address that you want to define. For more information on standardized valid IPv6 address formats, see https://docs.oracle.com/javame/config/cdc/ref-impl/pbp1.1.2/jsr217/java/net/Inet6Address.html.
Prefix Length	(Mandatory) Enter a prefix length for the subnet. The range is 1 to 128.
Do not track phones under this IP subnet	Check this check box if you do not want this IPv6 subnet and the underlying phones tracked by Cisco Emergency Responder. If you do not track the phones in an IPv6 subnet, then you do not need the Emergency Responder User Licenses for these phones.
Location (optional)	The location of the new IP subnet.
ERL Name	The ERL to assign to the subnet. Type in a valid ERL name or click **Search ERL** to find and select the ERL.

Field	Description
Insert button	Click **Insert** to add the subnet. When you click **Insert**, Emergency Responder asks if you want to run the switch port, and the phone updates the process on the switch immediately. Click **OK** to run the process now, or click **Cancel** to add the IPv6 subnet to the configuration without running the process immediately.
Cancel Changes button	Click **Cancel Changes** to change the fields on this page back to the last saved settings.

IP Subnet Phones

The IP Subnet Phones page appears when you choose **ERLMembership/ IPSubnets** and click the **View Phones** icon in any records returned by the IPSubnet Search.

Authorization Requirements

You must have system administrator or ERL administrator authority to access this page.

Description

Use the IP subnet Phones page to view all the IP subnet phones discovered by Emergency Responder.

The IP subnet phones page displays the subnet ID, the subnet mask for each IP subnet and lists all the phones tracked in that IP subnet, and when the last phone was tracked.

Related Topics

Find and List IP Subnets (Applicable only until Release 15)

Configure IP Subnet

Export IP Subnets

To reach the Export IP Subnets page, choose **ERL Membership** > **IPSubnets**. On the Find and List IP Subnets page, click the **Export** link. The Export IP Subnets page appears.

Authorization Requirements

You must have system administrator or ERL administrator authority to access this page.

Description

Use the Export IP Subnets page to create a file containing the Emergency Responder Export IP Subnet configurations.

If you must update a large number of Export IP Subnets, you can export the phone data, make your changes in the file using a spreadsheet, and then reimport the file.

You can also download a file using the Download utility, modify it on your local system, then upload it using the Upload utility. See Download File , on page 113 for more information.

The following table describes the Export IP Subnets page.

Table 79: Export IP Subnets Page

Field	Description
Select Export Format	Select the format used in the file that you are importing. After you select the format, click **view sample file** to see an example of the expected format and sequence of values. Use this sample information to create your import file in a spreadsheet.
Enter Export File Name	The name of the file you want to create. Do not include the file extension
Export button	Click **Export** to add data from the import file to your Emergency Responder configuration.
Close button	Click **Close** to close the window.
Download	
Select a File to Download	Use the pull-down menu to select a file and click **Download** to download the file to your local system.

Related Topics

Download File , on page 113

Find and List IP Subnets (Applicable only until Release 15)

Import IP Subnets, on page 453

Import IP Subnets

To reach the Import IP Subnets page, choose **ERL Membership** > **IPSubnets**. On the Find and List IP Subnets page, click the **Import** link. The Import IP Subnets page appears.

Authorization Requirements

You must have system administrator or ERL administrator authority to access this page.

Description

Use the Import IP Subnet page to create or update many IP subnet phones at once from a file in which you have defined their data. Create this file using a spreadsheet that can save the information in one of the required formats. View the samples from this page before attempting to create or update an import file.

If you must update many IP subnet phones, you can export the phone data, update the export file, and reimport the file.

You can also upload a previously downloaded file that you have modified on your local system. See Upload File , on page 113 for more information.

The following table describes the Import IP Subnets page.

Table 80: Import IP Subnets Page

Field	Description
Select Import Format	Select the format used in the file you are importing. After you select the format, click **view sample file** to see an example of the expected format and sequence of values. Use this sample information to create or update your import file in a spreadsheet.
Select File to Import	Select the file from which you want to import data.
Upload button	Click **Upload** to upload a file from your local system. See Upload File , on page 113 for more information.
Import button	Click **Import** to add data from the import file to your Emergency Responder configuration.
Close button	Click **Close** to close the window.
Import Status	Text box that displays status information.

Related Topics

Find and List IP Subnets (Applicable only until Release 15)

Export IP Subnets, on page 452

Upload File , on page 113

Unlocated Phones

The Unlocated Phones page appears when you choose **ERLMembership** > **Unlocated Phones**.

Authorization Requirements

You must have system administrator or ERL administrator authority to access this page.

Description

Use the Unlocated Phones page to identify phones that are registered with CiscoUnifiedCommunicationsManager, but which Emergency Responder cannot locate. A phone can become unlocated for several reasons:

- The phone is attached to a switch that is not defined in Emergency Responder.
- The phone is connected to an unsupported device, such as a router port, a hub connected to a router, or an unsupported switch.
- The switch to which the phone is connected is currently unreachable; for example, it does not respond to SNMP queries.
- The phone is not found under any configured IP subnet and the phone is not configured as a synthetic phone.
- The phone that was manually assigned.

- The phone that was previously identified as an unlocated phone and assigned an ERL.

Because Emergency Responder cannot assign an unlocated phone to the appropriate ERL, try to identify and resolve all problems that are preventing Emergency Responder from locating these phones on your network. If you cannot resolve the problems by defining switches in Emergency Responder, or by moving phones to supported switch ports, you might have to manually assign a phone to an ERL on this page. See Unlocated Phones , on page 324 for troubleshooting information.

The following table describes the Unlocated Phones page.

Table 81: Unlocated Phones Page

Field	Description
Unlocated Phone Search Parameters	
Find phones where...	Enter search criteria to select the unlocated phones you want to find. To find all unlocated phones, click **Find** without entering any criteria. To narrow your search: • Select **All** to indicate that only phones that match every criteria be selected (an AND s **Any** to indicate that phones that match any search criteria be selected (an OR search) pull-down menu, select the field you want to search on (Phone Extension, Phone MA and so on), select the search relationship (is Exactly, Starts with, and so on), and ente string. • To search on a combination of fields, click the **Plus** icon **(+)** to add additional search (Click the **Minus** icon to (**–**) remove search parameters.) • Click **Find** when you have entered all of the search parameters.
Assign ERL	To assign the ERL, select the phones by checking the check box next to the phones, click to find and select the ERL, and click **Assign ERL**.
Unassign ERL	To unassign a ERL, select the phones and click on **Unassign ERL** button.
List of unlocated phones	A list of the phones Emergency Responder could not assign to a specific ERL. The followin is displayed: • Emergency Responder Group • Phone IPv4 Address • Phone IPv6 Address • Phone Mac Address • Phone Extension • Assigned ERL • Effective ERL • ERL Rule If the phone has moved to a switch served by a different Emergency Responder group, th Responder group name is shown for the phone in the list. **Note** If there are a lot of unlocated phones, Emergency Responder uses more than list them. You can only assign phones to ERLs from one page at a time. Use the bottom of the list to move from page to page.

Related Topics

Identify Unlocated Phones , on page 167
Unlocated Phones , on page 324
E911 and Cisco Emergency Responder Terminology , on page 6
Find and List Manually Configured Phone, on page 457

Export Unlocated Phones

To view the Export Unlocated Phones page, choose **ERL Membership** > **Unlocated Phones** and click **Export**.

Authorization Requirements

You must have system administrator or ERL administrator authority to access this page.

Description

Use the Export Unlocated Phones page to do one of two actions:

- Create a file containing the Emergency Responder Export Unlocated Phones.
- Use the Download utility to download a file containing the Emergency Responder Export Unlocated Phones.

The following table describes the fields found on the Export Unlocated Phones page.

Table 82: Export Unlocated Phones Page

Field	Description
Select Export Format	Select the file format that matches the file being imported. After you select the format, click **View Sample File** to see an example of the expected format and sequence of values. Use this example when creating your imported file.
Enter Export File Name	The name of the file that you want to create. Do not include the file extension.
Export button	Click **Export** to add data from the import file to your Emergency Responder configuration.
Close button	Click **Close** to close the window.
Download	
Select a File to Download	Use the pulldown menu to select a file. Click **Download** to download the file.

Related Topics

Download File , on page 113
Unlocated Phones, on page 454

Find and List Manually Configured Phone

The Find and List Manually Configured Phones page appears when you choose **ERL Membership** > **Manually Configured Phones**.

Authorization Requirements

You must have system administrator or ERL administrator authority to access this page.

Description

Use the Find and List Manually Configured Phones page to locate and view phones that you would like to modify or delete. You can also navigate to add new phones from this page.

The following table describes the Find and List Manually Configured Phones page.

Note When you are performing this search as part of an E.164 dial plan, the "+" is a valid character.

Table 83: Find and List Manually Configured Phones Page

Field	Description
Manual Phone Search Parameters	
Find manual phones where Line Number...	Enter search criteria to select the manually configured phones that you want to find. To find all manually configured phones, click **Find** without entering any criteria. To narrow your search, use the pull-down menu to select the search condition (contains, S and so on) and enter the line number in the text box. You can also select how many results a per page from the pull-down menu. When you have specified your search criteria, click **F**
Manually Configure Phones	
Manually Configured Phones list	Displays the search results. For each phone found, the system displays the Line Number, IPv4 Address, IPv6 Address, and Location. Click on one of these records or click the **Edit** and modify the information for that phone. The Modify Manual Phone page appears. You the MAC Address, IPv4 Address, IPv6 Address, Phone Type, Version, Location, and ERI **Note** When modifying a manual phone, you cannot change the Subnet ID or the Li Click **Update** to save your changes.
Add new Manual Phone	Click **Add new Manual Phone** to add a manually configured phone. The Add New Manua appears. See Add New Manual Phone, on page 458 for more information. **Note** The **Add new Manual Phone** button is also available from the Modify Manu page.
Export	To export Manually Configured Phone information to a file, click **Export** on the Find and L Configured Phones page. See Export Manual Phones, on page 459 for more information.

Field	Description
Import	To import Manually Configured Phone information to a file, click **Import** on the Find and List Configured Phones page. See Import Manual Phones, on page 460 for more information.

Related Topics

- IP Subnet Phones, on page 452
- E911 and Cisco Emergency Responder Terminology , on page 6
- Add New Manual Phone, on page 458
- Export Manual Phones, on page 459
- Import Manual Phones, on page 460

Add New Manual Phone

To reach the Add New Manual Phone page, choose **ERL Membership** > **Manually Configured Phones**. On the Find and List Manually Configured Phones page, click the **Add new Manual Phone** link. The Add New Manual Phone page appears.

Authorization Requirements

You must have system administrator or ERL administrator authority to access this page.

Description

Use the Add New Manual Phone page to manually define a phone ERL. You must manually define a phone if any of these conditions apply:

- Emergency Responder cannot automatically track the type of phone, for example, if the phone is analog. See Network Hardware and Software Requirements , on page 10 for information about phone support.
- The phone is hosted on an unsupported port, such as a router port, a hub connected to a router, or a port on an unsupported switch.

For manually defined phones, Emergency Responder cannot automatically locate and update ERL information. You should regularly review manual phone configurations to ensure that they are correct.

The following table describes the Add New Manual Phone page.

Table 84: Add New Manual Phone Page

Field	Description
Add New Manual Phone	
Line Number	The extension of the phone you want to define.
MAC Address	The MAC address of the phone, if it is an IP phone.
IPv4 Address	The IPv4 address of the phone, if it is an IP phone.
IPv6 Address	The IPv6 address of the phone, if it is an IP phone.
Phone Type	The type of phone, such as analog. This field is for your information only.

Field	Description
Version	The version of the phone software, if any. This field is for your information only.
Location	The location of the phone.
ERL Name	The ERL that you want to assign to the phone. To find and select the ERL, click **Search ERL**.
Insert button	Click **Insert** to add the phone to the list of phones. **Note** The Insert button only appears when you are adding a phone.
Cancel Changes button	Click **Cancel Changes** to change the fields on this page back to the last saved settings.

Related Topics

Manually Define Phones , on page 168
Import Manual Phones, on page 460
Export Manual Phones, on page 459
E911 and Cisco Emergency Responder Terminology , on page 6

Export Manual Phones

To reach the Export Manual Phones page, choose **ERL Membership > Manually Configured Phones**. On the Find and List Manually Configured Phones page, click the **Export** link. The Export Manual Phones page appears.

Authorization Requirements

You must have system administrator or ERL administrator authority to access this page.

Description

Use the Export Manual Phones page to create a file containing the Emergency Responder manual phone configurations.

If you must update a large number of manually configured phones, you can export the phone data, make your changes in the file using a spreadsheet, and then reimport the file.

You can also download a file to your local system using the Download utility, modify the file, and then upload it using the Upload utility. See Download File , on page 113 for more information.

The following table describes the Export Manual Phones page.

Table 85: Export Manual Phones Page

Field	Description
Export Manual Phones	

Field	Description
Select Export Format	Select the format used in the file you are importing. After you select the format, click **view sample file** to see an example of the expected format and sequence of values. Use this sample information to create your import file in a spreadsheet.
Enter Export File Name	The name of the file that you want to create. Do not include the file extension.
Export button	Click **Export** to export the file to a file.
Close button	Click **Close** to close the window.
Download	
Select a file to download	Use the pull-down menu to select a file and then click **Download** to download the file to your local system.

Related Topics

Manually Define Phones , on page 168

Download File , on page 113

Import Manual Phones, on page 460

Find and List Synthetic Phones, on page 461

Import Manual Phones

To reach the Import Manual Phones page, choose **ERL Membership** > **Manually Configured Phones**. On the Find and List Manually Configured Phones page, click the **Import** link. The Import Manual Phones page appears.

Authorization Requirements

You must have system administrator or ERL administrator authority to access this page.

Description

Use the Import Manual Phones page to create or update many manually configured phones at once from a file in which you have defined their data. Create this file using a spreadsheet that can save the information in one of the required formats. View the samples from this page before attempting to create or update an import file.

If you must update a lot of manually configured phones, you can export the phone data, update the export file, and reimport the file.

You can also upload a file from a local system using the Upload utility and then import the data in the file. See Upload File , on page 113 for more details.

The following table describes the Import Manual Phones page.

Table 86: Import Manual Phones Page

Field	Description
Select Import Format	Select the format used in the file you are importing. After you select the format, click **view sample file** to see an example of the expected format and sequence of values. Use this sample information to create your import file in a spreadsheet.
Select File to Import	Select the file from which you want to import data.
Upload	Click **Upload** to upload a file from a local system. The Upload File page appears. See Upload File , on page 113 for more details.
Import button	Click **Import** to add data from the import file to your Emergency Responder configuration.
Close button	Click **Close** to close the window.
Import Status	Displays status messages.

Related Topics

Manually Define Phones , on page 168

Upload File , on page 113

Find and List Synthetic Phones, on page 461

Find and List Synthetic Phones

The Find and List Synthetic Phones page appears when you choose **ERL Membership** > **Synthetic Phones**.

Authorization Requirements

You must have system administrator or ERL administrator authority to access this page.

Description

Use the Find and List Synthetic Phones page to locate and view phones that you would like to modify or delete. You can also navigate to add new synthetic phones from this page.

The following table describes the Find and List Synthetic Phones page.

Table 87: Find and List Synthetic Phones Page

Field	Description
Synthetic Phone Search Parameters	

Field	Description
Find Synthetic phones where MAC Address	Enter search criteria to select the synthetic phones you want to find. To find all synthetic phones, click **Find** without entering any criteria. To narrow your search, use the pull-down menu to select the search condition (contains, Starts with, and so on) and enter the MAC address in the text box. You can also select how many results per page are displayed from the pull-down menu. When you have specified your search criteria, click **Find**.
Synthetic Phones	
Synthetic Phones list	Displays the search results. For each phone found, the system displays the Line Number, ERL Name, IP Address, and Location. Click on one of these records or click the **Edit** icon to view and modify the information for that phone. The Modify Synthetic Phone page appears. You can change the MAC Address, IP Address, Phone Type, Version, Location, and ERL Name. **Note** When modifying a synthetic phone, you cannot change the Subnet ID or the Line Number. Click **Update** to save your changes.
Add new Synthetic Phone	Click **Add new Synthetic Phone** to add a synthetic phone. The Add New Synthetic Phone page appears. See Add New Synthetic Phone, on page 462 for more information. **Note** The **Add new Synthetic Phone** button is also available from the Modify Synthetic Phone page.

Add New Synthetic Phone

To reach the Add New Synthetic Phone page, choose **ERL Membership** > **Synthetic Phones**. On the Find and List Synthetic Phones page, click the **Add new Synthetic Phone** link. The Add New Synthetic Phone page appears.

Note You cannot configure test ERLs for off-premise ERLs and National E911 Service Provider ERLs.

Authorization Requirements

You must have system administrator or ERL administrator authority to access this page.

Description

Use the Add New Synthetic Phone page to manually define a synthetic phone ERL. You must configure synthetic phones in the subnet for testing ERL configurations.

For synthetic phones, Emergency Responder cannot automatically locate and update ERL information. You should regularly review synthetic phone configurations to ensure that they are correct.

The following table describes the Add New Synthetic Phone page.

Table 88: Add New Synthetic Phone Page

Field	Description	Notes
MAC Address	The MAC address of the synthetic phone, or a range of MAC addresses.	The synthetic MAC address must range 00059a3b7700 - 0059a3b8 Enter the MAC address in this fo xx-xx-xx-xx-xx-xx or xxxxxxxxx
ERL Name	The ERL to assign to the synthetic phone. Type in a valid ERL name or select the ERL from the drop-down list.	
Insert button	Click **Insert** to add the synthetic phone to the list of phones.	The **Insert** button only appears w adding a phone.
New button	Click **New** to add another phone.	The **New** button only appears wh viewing an existing phone.
Update button	Click **Update** when viewing an existing phone to save changes you make to the phone.	The **Update** button only appears v viewing an existing phone.
Cancel Changes button	Click **Cancel Changes** to change the fields on this page back to the last saved settings.	

Related Topics

Synthetic Phones , on page 172

E911 and Cisco Emergency Responder Terminology , on page 6

Find and List Users

The Find and List Users page appears when you choose **User Management** > **User**.

Authorization Requirements

You must have system administrator authority to access this page.

Description

Use the Find and List Users page to find and list current users, to add new users, and to modify and delete current users.

The following table describes the Find and List Users page.

Table 89: Find and List Users Page

Field	Description
User Search Parameters	

Field	Description
Find User where User Name	Enter search criteria to select the users that you want to find. To find all users, click **Find** without entering any criteria. To narrow your search: • Select **All** to indicate that only users that match the selected criteria be displayed (an AND • Select **Any** to indicate that users that match any search criteria be selected (an OR searc • From the pull down menu, select the field that you want to search, select its correspondi relationship and select how many results per page are displayed. The search fields and t corresponding relationships are: • Authentication Mode—Both, Remote or Local • User Name— Ends with, Starts with, contains or Exactly. • Unified CM Cluster—Ends with, Starts with, contains or Exactly. • To search on a combination of fields, click the Plus icon (+) to add additional search par (Click the Minus icon (-) to remove search parameters.) • Click **Find** when you have entered all of the search parameters.
User	
Users list	This section of the page displays the search results. If there are no usernames are displayed a completion of the search, then no users have been configured yet.
Username	Displays the users name based on the selection criteria.
Authentication Mode	Displays the authentication mode of the user. The authentication mode can be either Remote
Unified CM Cluster	This value is displayed only when the user is authenticated remotely, with the Unified CM se
Edit icon	Click the user name or the **Edit** icon to display the Modify User page, which allows you to c user authentication mode, password and Unified CM cluster. The Modify User page also displa groups and roles have been assigned to the user.
Delete icon	Click the **Delete** icon to delete the user from the system. **Note** You cannot delete the Administrator.
Add New User button	Click the **Add New User** button to open the Add User page. See Table 90: Add User Page , o 465 for a description of the Add User page.
Delete Users button	Click the **Delete Users** button to delete users in bulk. Select multiple users, both remote and checking the check box and then clicking the **Delete Users** button.
Change to Remote Users button	Click the **Change to Remote Users** button to change local users to remotely authenticated u bulk.
Change to IdP Users button	Click the **Change to IdP Users** button to change local or remote users to IdP users, whose p is maintained in IdP.

Add User

The Add User page appears when you choose **User Management** > **User** and click **Add new User** on the Find and List Users page. You can also access the Add User page from the Modify User page. See Modify User, on page 465 for more information.

Authorization Requirements

You must have system administrator authority to access this page.

Description

Use the Add User page to add a new user to the system.

The following table describes the Add User page.

Table 90: Add User Page

Field	Description
User Name	Enter the username for the new user.
Authentication Mode	Select the authentication mode of the new user. The user can either be a Remote user, Local user, or a IdP user.
Password	Enter the password for the new user.
Reset on Next Logon	Check the **Reset on Next Logon** check box to reset or change the password after a successful sign-in. This field is enabled only for the local users.
Confirm Password	Reenter the password for the new user.
Unified CM Cluster	This field is enabled only when the user is a Remote user. Select a Unified CM cluster, from the drop-down list, to authenticate the remote user.
Insert button	Inserts the new user.
Cancel Changes button	Cancels changes made to the Add User page.

Related Topics

Role-Based User Management , on page 108

Find and List Roles, on page 467

Find and List User Groups, on page 470

Modify User

The Modify User page appears when you choose **User Management** > **User**, search for a user, and then click a user name or on the **Edit** icon associated with the user on the Find and List Users page.

Authorization Requirements

You must have system administrator authority to access this page.

Description

Use the Modify User page to change a current user's password.

The following table describes the Modify User page.

Table 91: Modify User Page

Field	Description
User Name	Displays the name of the user whose information is being modified. **Note** You cannot change the username on the Modify User page.
Authentication Mode	Change the authentication mode for a user. You can change a local user to a remote user and a remote user to local user.
Password	Enter the new password for the user.
Reset on Next Logon	Check the **Reset on Next Logon** check box to reset or change the password after a successful sign-in. This field is enabled only for the local users.
Confirm Password	Reenter the new password for the user.
Unified CM Cluster	Select a Unified CM cluster. This is required when you change a local user to remote user. You can also change the Unified CM cluster of an existing remote user to another Unified CM Cluster. **Note** The Unified CM Cluster drop down box are enabled only when the authentication mode is selected as remote.
Update button	Applies changes made from the Modify User page. **Note** User authentication at passphrase change is valid only for the Cisco ER Administration page. Active sessions of the user in any of the other navigation pages do not get cancelled.
Cancel Changes button	Cancels changes made to the Modify User page.
Add new User	Click this button to add a new user. The Add User, on page 465 page appears. See Table 90: Add User Page , on page 465 for more information.
Activate User	Click **Activate User** to activate the user account. The option is enabled only when that particular user is inactive. The option is always disabled for remote users.
Unlock User	Click **Unlock User** to unlock the account. The option is enabled only when that particular user account is locked. The option is always disabled for remote users.
User Groups for this user	Displays the groups to which the user is assigned.

Field	Description
User Roles for this user	Displays the roles to which the user is assigned.

Change to Remote User

The Change to Remote Users page appears when you choose **User Management** > **User** and click **Change to Remote Users** on the Find and List Users page.

Authorization Requirements

You must have system administrator authority to access this page.

Description

Use the Change to Remote Users page to change the authentication mode of the local user to remote user.

The following table describes the Remote User page.

Table 92: Change to Remote Users Page

Field	Description
Unified CM Cluster	Select the Unified CM Cluster from the drop-down box to remotely authenticate the selected users.
Selected Users	Displays the local users that change to remote users.
Update button	Applies changes made from the Change to Remote Users page.
Close button	Closes the window.

Find and List Roles

The Find and List Roles page appears when you choose **User Management** > **Role**.

Authorization Requirements

You must have system administrator authority to access this page.

Description

Use the Find and List Role page to find, list, modify, and delete current roles, and to add new roles.

The following table describes the Find and List Roles page.

Table 93: Find and List Roles Page

Field	Description
Role Search Parameters	

Field	Description
Find Role where Role Name is	Enter search criteria to select the role you want to find. To find all roles, click **Find** without entering any criteria. To narrow your search, use the pull-down menu to select the search condition (contains, Starts so on) and enter the role in the text box. You can also select how many results per page are di from the pull-down menu. When you have specified your search criteria, click **Find**.
Roles	Section of the page in which the search results are displayed. These default roles are created installation: • Emergency Responder System Admin • Emergency Responder ERL Admin • Emergency Responder Network Admin • Emergency Responder User When you click on the Role Name link or the Description link for any of the default roles, the Role page for that role displays, which displays the following information: • Role Name • Description • List of resources assigned to that role **Note** You cannot modify any of the information for default roles. You can only modify inf for roles that you create. After you create additional roles, they are listed along with the default roles. When you click name, description, or Edit icon for a role that you have created, the Modify Role page appears. 95: Modify Role Page , on page 470 for more information about the Modify Role page.
Edit icon	Click the Edit icon to display the Modify Role page. See Table 95: Modify Role Page , on pa information about the Modify Role page.
Delete icon	Click the **Delete** icon to delete the role from the system. **Note** You cannot delete any of the default roles.
Add New Role button	Click **Add New Role** to display the Add Role page. This button is also available on the Modi and Add Role pages. See Table 94: Add Role Page , on page 469 for information about the A page.

Add Role

The Add Role page appears when you choose **User Management** > **Role** and click **Add new Role** on the Find and List Roles page. You can also access the Add Role page from the Modify Role and Standard Role pages. See Modify Role, on page 469 for more information.

Authorization Requirements

You must have system administrator authority to access this page.

Description

Use the Add Role page to add a new role to the system.

The following table describes the Add Role page.

Table 94: Add Role Page

Field	Description
Add Role	
Role Name	The name of the new role you are adding.
Description	A description of the new role.
Resource Permissions	This section of the page displays a list of all available resources. The check boxes to the left of each resource allow you to select or deselect the resource to be assigned to the new role.
Select All button	Click **Select All** to select all the listed resources.
Clear All button	Click **Clear All** to deselect all currently selected resources.
Insert button	Click **Insert** to add the new role.
Cancel Changes button	Click **Cancel Changes** to cancel the Add Role operation.

Related Topics

Role-Based User Management , on page 108
Find and List Users, on page 463
Find and List User Groups, on page 470

Modify Role

The Modify Role page appears when you choose **User Management** > **Role**, search for a role, and then click on a role name, description, or the Edit icon associated with the role on the Find and List Roles page.

Authorization Requirements

You must have system administrator authority to access this page.

Description

Use the Modify Role page to modify information for an existing role.

Note You cannot modify any information for the four default roles.

The following table describes the Modify Role page.

Table 95: Modify Role Page

Field	Description
Modify Role	
Role Name	The name of the new role you are modifying. **Note** The Role Name cannot be changed.
Description	A description of the role you are modifying. Modify the description by adding new text in the
Resource Permissions	This section of the page displays a list of all available resources. The check boxes to the left o resources indicate which resources have been assigned to this role. Modify the resource assig by checking or unchecking the boxes.
Select All button	Click **Select All** to select all the listed resources.
Clear All button	Click **Clear All** to deselect all currently selected resources.
Update button	Click **Update** to save the changes made to the Modify Role page.
Cancel Changes button	Click **Cancel Changes** to cancel the changes made to the Modify Role page.
Add new Role button	Allows you to add a new role. See the Add Role, on page 468 for information about adding n

Find and List User Groups

The Find and List User Groups page appears when you choose **User Management > User Group**.

Authorization Requirements

You must have system administrator authority to access this page.

Description

Use the Find and List User Groups page to find, list, modify, and delete current user groups, and to add new user groups.

The following table describes the Find and List User Groups page.

Table 96: Find and List User Groups Page

Field	Description
User Group Search Parameters	
Find User Group where User Group Name	Enter search criteria to select the user group you want to find. To find all user groups, click **Find** without entering any criteria. To narrow your search, use the pull-down menu to select the search condition (contains, Starts so on) and enter the user group in the text box. You can also select how many results per page displayed from the pull-down menu. When you have specified your search criteria, click **Fin**

Field	Description
User Groups	Section of the page in which the search results are displayed. When you click on the User link, the Description link, or the Edit icon, the Modify User Group page appears. See Modif on page 472 for information.
Edit icon	Click the **Edit** icon to display the Modify User Group page. See Modify User Group, on p information.
Delete icon	Click the **Delete** icon to delete the user group from the system. **Note** You cannot delete default user groups that were created during installation.
Add New User Group button	Click the **Add New User Group** button to display the Add User Group page. See Table 9 Group Page , on page 471 for information about the Add User Group page.

Add User Group

The Add User Group page appears when you choose **User Management > User Group** and click **Add new User Group** on the Find and List User Groups page. You can also access the Add User Group page from the Modify User Group page. See Modify User Group, on page 472 for more information.

Authorization Requirements

You must have system administrator authority to access this page.

Description

Use the Add User Group page to add a new user group to the system.

The following table describes the Add User Group page.

Table 97: Add User Group Page

Field	Description
Add User Group	
User Group Name	The name of the new user group you are adding.
Description	A description of the new user group.
Add Users to the Group	This section of the page has a text box that displays the names of the users you add to the
Add Users button	Allows you to add users to the new group. When you click **Add Users**, the Add Users page Add User, on page 465 for more information.
Remove Users button	Allows you to remove users from the group. To do so, highlight the username in the text l **Remove Users**.
Assign Roles to Group	This section of the page has a text box that displays the roles you assign to the new user g
Add Roles button	Allows you to assign roles to the new group. When you click **Add Roles**, the Add Roles p See Add Role, on page 468 for more information.

Field	Description
Remove Roles button	Allows you to remove roles from the group. To do so, highlight the role name in the text box **Remove Roles**.
Insert button	Click **Insert** to add the new role.

Related Topics

Role-Based User Management , on page 108

Find and List Users, on page 463

Find and List Roles, on page 467

Modify User Group

The Modify User Group page appears when you choose **User Management > User Group**, search for a user group, and then click a user group name, description, or the **Edit** icon associated with the user group on the Find and List User Groups page.

Authorization Requirements

You must have system administrator authority to access this page.

Description

Use the Modify Role page to modify information for an existing user group.

The following table describes the Modify User Group page.

Table 98: Modify User Group Page

Field	Description
Modify User Group	
User Group Name	The name of the user group you are modifying. **Note** The User Group Name cannot be changed.
Description	A description of the User Group you are modifying. Modify the description by adding or char in the text box.
Add Users to the Group	This section of the page has a text box that displays the names of the users currently in the us
Add Users button	Allows you to add more users to the group. When you click **Add User**, the Add User page app Add User, on page 465 for more information.
Remove Users button	Allows you to remove users from the group. To do so, highlight the username in the text box **Remove Users**.
Assign Roles to Group	This section of the page has a text box that displays the roles currently assigned to the user gr

Field	Description
Add Roles button	Allows you to assign more roles to the group. When you click **Add Roles**, the Add Role p See Add Role, on page 468 for more information. **Note** You cannot add roles to the default roles that were assigned to a default user g installation. If the user group that you are modifying is a default user group, t **Roles** button is not visible.
Remove Roles button	Allows you to remove roles from the group. To do so, highlight the role name in the text b **Remove Roles**. **Note** You cannot remove the default roles that were assigned to a default user grou installation. If the user group you are modifying is a default user group, then **Roles** button is not visible.
Update button	Click **Update** to save the changes made to the Modify User Group page.
Add New User Group button	Allows you to add a new user group. See Add User Group, on page 471 for information.

Credential Policy Page

The **Credential Policy** page appears when you choose **User Management** > **User Settings** > **Credential Policy** or **EnhancedSecurityMode Credential Policy**.

Note

- The Credential Policy option is enabled when the system is in the normal mode.
- The EnhancedSecurityMode Credential Policy option is enabled when the system is in Enhanced Security Mode.
- Local administrator accounts will never expire as they are always configured as standard users. Hence, if you update any credential policy or EnhancedSecurityMode credential policy for a local administrator the changes won't take effect.

Authorization Requirements

You must have system administrator authority to access this page.

Description

Use the **Credential Policy** page to update policy values in the EnhancedSecurityMode or in the normal mode depending on the security level required.

The following table describes the **Credential Policy** field settings.

Table 99: Credential Policy Page

Field	Description
Display Name	Credential Policy or EnhancedSecurityMode Credential Policy name is displayed based on the option selected by you.
Failed Logon	Specify the number of failed sign-in attempts allowed. You can enter a number between 0 to100. To allow unlimited failed sign-ins, enter 0 or check the **No Failed Logon** check box. **Note** The default setting specified for Cisco Emergency Responder (Emergency Responder) in a normal mode is set to 0 (if Emergency Responder is upgraded from pre 11.5 version) or 5 (if Emergency Responder 11.5 is a fresh installation) or 3 (if Emergency Responder is in Enhanced Security Mode).
Reset Failed Logon Attempts Every (minutes)	Specify the number of minutes after which the counter is reset for failed sign-in attempts. You can log in again after the counter is reset. Enter a number between 1 to120. The default setting specified for Emergency Responder in normal mode is 1 (if Emergency Responder is upgraded from pre 11.5 version) or 30 (if Emergency Responder 11.5 is a fresh installation) or 30 (if Emergency Responder is in Enhanced Security Mode).
Credential Expires After (days)	Specify the number of days after which the credential or password expires. Enter a number between 0 to 365. To allow credentials to never expire, enter 0 or check the **Never Expires** check box. The default setting is 0.**Never Expires** check box is checked if Emergency Responder is in normal mode (for both upgrade and fresh installation) and 180 if Emergency Responder is in Enhanced Security Mode.

Field	Description
Minimum Credential Length	Specify the minimum length for user credentials (password). Do not enter 0 as blank passwords are not allowed. Enter a number between1 to 64. Validation of, one uppercase, one lowercase, one numeric, and one special character on password happens only when the value is greater than or equal to four. The default setting is 1 if Emergency Responder is in normal mode (for both upgrade and fresh installation) and 14 if the Emergency Responder is in Enhanced Security Mode.
Minimum number of character changes between successive credentials	Specify the minimum characters that should be changed while updating a new password. Enter a number between of 0 to 64. The value should never be greater than the **Minimum Credential Length** field value. The default setting specified is 1 if Emergency Responder is in normal mode (for both upgrade and fresh installation) and 4 if Emergency Responder is in Enhanced Security Mode.
Stored Number of Previous Credentials	Specify the number of previous user credentials to store. This setting prevents a user from configuring a recently used credential that is saved in the user list. Enter a number between 0 to 25. If you do not want to save any old credentials, enter 0. The default setting specified is 0 if Emergency Responder is in normal mode (for both upgrade and fresh installation) and 12 if Emergency Responder is in Enhanced Security Mode.
Inactive Days Allowed	Specify the number of days that an account can remain inactive before the account gets deactivated. Enter a number between 0 to 5000. If you never want the account to be inactive, enter 0. The default setting specified is 0 for Emergency Responder both in the normal mode (for both upgrade and fresh installation) and in the Enhanced Security Mode.

Field	Description
Expiry Warning Days	Enter a number between 0 to 90 to specify the number of days before a user password expires and to start receiving warning notifications. The value should never be greater than the **Credential Expires After (days)** field. The default setting specified is 0 for Emergency Responder both in the normal mode (for both upgrade and fresh installation) and in the Enhanced Security Mode.
Save	Click the **Save** button to save the changes.
Clear Changes	Click the **Clear Changes** button to clear any change done in the fields and to restore the last saved information.
Set to Default	Click the **Set to Default** button to restore the default values settings depending on the Cisco Emergency Responder mode.

Call History

The Call History page appears when you choose **Reports > Call History**.

Authorization Requirements

You must have system administrator, ERL administrator, network administrator, or user authority to access this page.

Description

Use the Call History page to view the history of emergency calls made from your network. Emergency Responder maintains the most recent 10,000 call history records. There is no restriction on when these calls were placed.

The following table describes the Call History page.

Table 100: Call History Page

Field	Description
Call History Search Parameters	

Field	Description
Search criteria	Enter search criteria to select the calls you want to find. To find all calls, click **Find** without entering any criteria. To narrow your search: • Select **All** to indicate that only calls that match every criteria be selected (an AND se **Any** to indicate that calls that match any search criteria be selected (an OR search). F down menu, select the field that you want to search on (ERL Name, Caller Extension select the search relationship (contains, begins with, and so on), and enter the search • To search on a combination of fields, click the **Plus** icon **(+)** to add additional search Click the **Minus** icon (**–**) to remove search parameters. • When you have entered all of the search parameters, click **Find**.
Call History Matching Records	A list of emergency calls that match your search criteria is displayed with the following in • ERL Name—Click the name to view details about the ERL and its ALI information. Conventional ERL, on page 394 for descriptions of the configuration fields. • Caller Extension—The extension used to place the emergency call. • Time—The time the call was made. • Date—The date the call was made. • Route Pattern-ELIN No.—The route pattern and ELIN combination used for the call Conventional ERL, on page 394 for more detailed information about these fields. • Location—The location of the phone based on whether the phone was configured ma whether it was configured based on the switch port or IP subnet. • Call Acknowledged—The acknowledged status of a call on the Web Alert page. • Acknowledged By—The ID of the user who acknowledged the call. • Time Acknowledged—The time that the call was acknowledged. • Date Acknowledged—The date that the call was acknowledged. • Comments—Any comments entered about the call. If you click the **Edit** icon, the Call appears, on which you can enter or change comments about the call in the **Commen call** text box. If a large number of calls match your search criteria, the system uses several pages to displa the First, Previous, Next, and Last links at the bottom of the page to move between pages. enter a specific page number in the Page field and press **Enter** to move to that page.
Download	Click **Download** to save the call history data to a spreadsheet that you can view or downl local system.
Update	Click **Update** to include your comments in the call history for the call. **Note** Only viewable from the Call Details page.
Cancel Changes	Click **Cancel Changes** to remove unsaved comments. You can then reenter comments. **Note** Only viewable from the Call Details page.
Close	Click **Close** to close the Call Details page. **Note** Only viewable from the Call Details page.

Related Topics

- View Emergency Call History , on page 172
- E911 and Cisco Emergency Responder Terminology , on page 6

ERL Audit Trail

The ERL Audit Trail page appears when you perform one of these actions:

- Choose **Reports** > **ERL Audit Trail**.
- Click **view** in the Audit Trail column for an ERL displayed on the ERL Configuration page (opened by choosing **ERL** > **Conventional ERL**.)

Authorization Requirements

You must have system administrator, ERL administrator, or network administrator authority to access this page.

Description

Use the ERL Audit Trail page to view the change history for ERLs.

The following table describes the ERL Audit Trail page.

Table 101: ERL Audit Trail Page

Field	Description
ERL Audit Trail	
Search criteria	Enter search criteria to select the audit details that you want to find. To find all audit details, click **Find** without entering any criteria. To narrow your search: • Select **All** to indicate that only audit details that match every criteria be selected (an AN select **Any** to indicate that audit details that match any search criteria be selected (an OR From the pull-down menu, select the field that you want to search on (ERL Name, Modi and so on), select the search relationship (contains, begins with, and so on), and enter th string. If searching by ERL Name, you can type in the ERL name or use the pull-down select an ERL. • To search on a combination of fields, click the **Plus** icon **(+)** to add additional search pa Click the **Minus** icon (–) to remove search parameters. • When you have entered all of the search parameters, click **Find**.

Field	Description
Matching Records	A list of ERL change records that match your search criteria. Each change to an ERL is re separate record, so a single ERL may have many audit records. The list displays the followin for each record: • ERL Name—The name of the ERL that was changed. • Modified By—The login ID of the user who changed the ERL. • Modified Time—The date and time the ERL was changed. • Modification Details—A list of the fields that were changed in the ERL or its ALI. U bars to move up and down in the Modification Details text box. **Note** If there are a large number of records match your search, Emergency Respond than one page to list them. Use the links at the bottom of the list to move from You can also enter a page number in the Page field and press **Enter** to go to a s

Related Topics

View Audit Trail for ERL , on page 148

E911 and Cisco Emergency Responder Terminology , on page 6

Export PS-ALI Records

The Export PS-ALI Records page appears when you choose **Tools** > **Export PS-ALI Records**.

Authorization Requirements

You must have system administrator or ERL administrator authority to access this page.

Description

Use the Export PS-ALI Records page to create a file in a NENA format that you can send to your service provider. Your service provider uses this file to update their ALI data for your organization. Your service provider needs this information so that emergency calls from your ERLs can be routed to the correct public safety answering point (PSAP).

Always submit an export file to your service provider. If you do not submit an export file, subsequent export files might not have correct command information for the database update, and you must manually edit the export file to make it uploadable. Your service provider can provide you with error information if the database upload fails.

Note If you change the customer code in your ALI record, Emergency Responder generates two records when exporting ALI: a Delete record to remove the ALI with the old code, and an Insert record to add the ALI with the new code. This Delete and Insert sequence is only generated the first time you export ALI after changing the code. You must ensure that you submit this export file to the service provider.

You can also use export files to back up your ERL configuration. ELIN must be associated to an ERL while exporting PS-ALI records.

The following table describes the Export RS-ALI Records page.

Table 102: Export PS-ALI Records Page

Field	Description
Export PS-ALI Records	
Select NENA Format	The file format to be used in the export file, NENA formats 3.0, 2.1, or 2.0.
File to Export	The name of the file you want to create. Do not include a file extension.
Company Name (NENA Header field)	The name of your company. You cannot have spaces in the name. **Note** The data complies with NENA requirements.
Cycle Counter (NENA Header field)	The sequence in which this export is created. This field is automatically increased each time y data. You can change it if it becomes unsynchronized with the sequence submitted to your se provider. However, changing the sequence number does not affect the data placed in the file; i redoing an export, you must manually edit the export file to change the record status fields. **Note** The data complies with NENA requirements.
End of Line Format	Allows you to select the end-of-line format for the PS-ALI records that is exported for downl can select from the following two formats: • Windows style (\r\n) • Unix/Linux style (\n)
Export button	Click **Export** to create the export file.
Download File	Click **Download File** to download an exported PS-ALI file.
Cancel button	Click **Cancel** to cancel the export operation.

Related Topics

ALI Information, on page 400
ALI Submission and Service Provider Requirements , on page 37
Export ERL Information , on page 146
Export ALI Information for Submission to Your Service Provider , on page 147
ERLs, on page 135
ERL Management , on page 136
E911 and Cisco Emergency Responder Terminology , on page 6

PS-ALI Converter

The PS-ALI Converter page appears when you choose **Tools** > **PS-ALI Converter**.

Authorization Requirements

You must have system administrator or ERL administrator authority to access this page.

Description

Use the PS-ALI Converter tool to generate an ERL file that can be accepted by the Emergency Responder ERL. The PS-ALI Converter tool converts ALI files from a NENA 2.0 format into a csv (comma-separated value) text file. You can then modify the csv file (for example, to add or change an ERL name) and save the modified ERL details by importing the file into Emergency Responder.

Note If you change the customer code in your ALI record, Emergency Responder generates two records when exporting ALI: a Delete record to remove the ALI with the old code, and an Insert record to add the ALI with the new code. This Delete and Insert sequence is only generated the first time you export ALI after changing the code. You must ensure you submit this export file to the service provider.

Table 103: PS-ALI Converter Page

Field	Description
Export PS-ALI Records	
Select PS-ALI file (NENA 2.0 format)	The name of the PS-ALI file to be converted. The file must be in the default format, NENA format 2.0.
Output File (in csv format) Name	The name of the csv file that you want to create.
Convert button	Click **Convert** to create the csv file.
Cancel button	Click **Cancel** to stop the converting process. and close the window.

Related Topics

ALI Information, on page 400
ALI Submission and Service Provider Requirements , on page 37
Export ERL Information , on page 146
Export ALI Information for Submission to Your Service Provider , on page 147
ERLs, on page 135
E911 and Cisco Emergency Responder Terminology , on page 6

PS-ALI Records Download

Download File appears when you choose **Export PS-ALI records->Download**

Authorization Requirements

You must have system administrator or ERL administrator authority to access this page.

Description

The Exported PS-ALI Records can be downloaded from here using the download button.

Table 104: Download PS-ALI Records

Field	Description
Select a file to Download	Use the pull-down menu to select a file and click **Download** to download the file to your loca
Close button	Click **Close** to close the window.

ERL Debug Tool

The ERL Debug Tool page appears when you choose **Tools** > **ERL Debug Tool**.

Authorization Requirements

You must have a system administrator or ERL administrator authority to access this page.

Description

The ERL Debug Tool takes the phone extension as input and displays the ERLs currently being used for routing emergency calls for the phones.

Use this diagnostic tool to verify the Emergency Responder configuration during the ERL creation and the ERL assignment phase and to troubleshoot calls directed to incorrect ERLs.

Note In a scenario where a Dual-stack phone has both the IPv4 and IPv6 addresses configured, and the phone falls under both the IPv4 and IPv6 subnets having the same priority, and one of the subnets is trackable and the other one is non-trackable, the phone is considered to be trackable.

The following table describes the ERL Debug Tool page.

Table 105: ERL Debug Tool Page

Field	Description
ERL Debug Tool	
Find Phones where extension	Enter search criteria to select the extensions that you want to find. To find all extensions, click **Find** without entering any criteria. To narrow your search, use the drop-down menu to select the search condition (contains, Sta and so on) and enter the extension in the text box. You can also select how many results per p displayed from the drop-down menu. When you have specified your search criteria, click **Fi**

Field	Description
Matching records	Section of the page that displays the ERLs currently being used for routing emergency ca phones. For each extension found, the following information is displayed: • Phone extension • ERL • Phone IPv4 Address • Phone IPv6 Address • MAC Address • Why this ERL is Used? If the configurations are not correct, make any required changes.
Export button	Click **Export** to create the export file.

Related Topics

Use Emergency Responder Admin Utility Tool, on page 345
ERLs, on page 135
ERL Management , on page 136

ERL Debug Tool Export

The Export ERL Debug Tool page appears when you click **Export** in the ERL Debug Tool page.

Authorization Requirements

You must have system administrator or ERL administrator authority to access this page.

Description

Use the Export ERL Debug Tool page to create a file which shows phone extension with ERLs currently being used for routing emergency calls for the phones.

Table 106: Export ERL Debug Tool

Field	Description
Select Export Format	The format to use for the file, such as CSV (comma-separated values).
Enter Export File Name	The name of the file you want to create. Do not include the file extension.
Export button	Click **Export** to create the file. The Status box shows the status of the exportation.
Close button	Click **Close** to close the window.
Download	
Select a File to Download	Use the pull-down menu to select a file and click **Download** to download the file to your

ALI Formatting Tool

The ALI Formatting Tool page appears when you choose **Tools** > **ALI Formatting Tool**.

Authorization Requirements

You must have system administrator or ERL administrator authority to access this page.

Description

Use the ALI Formatting Tool page to customize the format of PS-ALI records to facilitate error-free PS-ALI record transactions with service providers.

The ALI Formatting Tool (AFT) reads the NENA file generation by the Emergency Responder and displays all ELIN records. You can then do one or more of the following:

- View the details of the ALI records
- Select a record and update the value for ALI fields, which can be edited using the AFT
- Perform a bulk update operation on multiple ALI records
- Selectively export ALI records based on area code, city code, and so on

The following table describes the ALI Formatting Tool page.

Table 107: ALI Formatting Tool Page

Field	Description
Select a Service Provider	Use the pull-down menu to select a service provider
Select an Input File for the ALI Formatting Tool from the List Below	Use the pull-down menu to select an input file
Submit button	Click the **Submit** button to display the Search for ELINs page, which is described in Table 108: Search for ELINs Page , on page 484.

The following table describes the Search for ELINs page.

Table 108: Search for ELINs Page

Field	Description
Use Search to Filter-out ELINs on Area, City and Local Code(last 4-digits).	Allows you to search ELINs by Local Code, Area Code, or City Code.
Add (+) button	Adds more search parameters
Remove (-) button	Removes search parameters

The following table describes the Bulk Update page.

Table 109: Bulk Update Page

Field	Description
Remove Changes/Generate File button	Shows all the ELINs that have been changed.
Search for ELIN	Displays the ELIN search page.

The following table describes the Review Changes/Generate File page.

Table 110: Review Changes/Generate File Page

Field	Description
Add More ELIN	Displays the remaining ELINs that have not been changed.
Remove ELIN	Removes the selected ELINs from the list
Search for ELIN	Displays the ELIN search screen
Generate File button	Generates the formatted file.

The following table describes the Download Formatted File page.

Table 111: Download Formatted File Page

Field	Description
Download Formatted File button	Displays a Download File dialog box so that the formatted file can be downloaded to the local system.

Related Topics

ALI Information, on page 400
Export ALI Information for Submission to Your Service Provider , on page 147
ALI Formatting Tool for Bell Canada, on page 577
ALI Formatting Tool for SBC Ameritech, on page 579
ALI Formatting Tool for SBC-PacBell, on page 579
ALI Formatting Tool for SBC-Southwestern Bell, on page 580
ALI Formatting Tool for Qwest, on page 581
ALI Formatting Tool for Verizon, on page 581

File Management Utility

The File Management Utility page appears when you choose **Tools** > **File Management Utility**.

Authorization Requirements

You must have system administrator or ERL administrator authority to access this page.

Description

Use the File Management Utility page to search for, download, or delete exported files.

The following table describes the File Management Utility page.

Table 112: File Management Utility Page

Field	Description
Search Parameters	
Please Select:	From the pull-down menu, select the type of file that you want to search for.
Search button	Click **Search** to perform the search.
Exported Files	Area of the page that displays the search results. Displays the File Name, Last Modified data, and File Size for each file found.
Download button	Downloads the selected file. **Note** Before you click **Download**, click in the box next to the file name to select the file. To select all files listed, click in the box next to the File Name column heading.
Delete button	Deletes the selected file. **Note** Before you click **Delete**, click in the box next to the file name to select the file. To select all files listed, click in the box next to the File Name column heading.

Related Topics

Upload and Download Utilities , on page 112

Purge Call History

The Purge Utility for Call History page appears when you choose **Tools** > **Purge Utility**.

Authorization Requirements

You must have system administrator or ERL administrator authority to access this page.

Description

Use the Purge Call History Utility to delete call history records that are older than an age that you specify. You can use this utility to purge records immediately or schedule daily purging of call history records. Emergency Responder logs the results of the purge in the Emergency Responder Administration logs.

The following table describes the purge utility page.

Table 113: Purge Utility for Call History

Field	Description
Status	Displays status messages
Purge Now	
Purge Data older than	Specify the age of record that you want to delete.
Schedule Purge	
Daily Purge at	Specify a time (UTC) during the day at which old records are deleted.
Purge Data older than	Specify the age of record that you want to delete.
Update	Click **Update** to save and activate your changes.
Cancel	Click **Cancel Changes** to change the fields on this page back to the last saved settings.

Related Topics

View Emergency Call History , on page 172

Call History Logs , on page 353

SAML Single Sign-On

The SAML Single Sign-On page appears when you choose **Cisco ER Administration** > **System** > **SAML Single Sign-On**.

Authorization Requirements

You must have system administrator authority to access this page.

Description

SAML Single Sign-On (SSO) page is used to enable or disable Single Sign-On, on Cisco Emergency Responder. It also allows you to import IdP metadata and export Cisco Emergency Responder metadata. You cannot access the**Disaster Recovery System** and **Cisco OS Unified Administration** pages, when Single Sign-On is enabled onCisco Emergency Responder, you need to have the normal admin credentials to access these pages. For more information on the configuration settings, see "SAML Single Sign-On" chapter in *Cisco Emergency Responder Administration Guide* at http://www.cisco.com/c/en/us/support/unified-communications/emergency-responder/products-maintenance-guides-list.html

The following table describes the **SAML Single Sign-On** Page.

Table 114: SAML Single Sign-On Page

Field	Description
Status	Displays status messages.

Field	Description
Server Name	Specifies the names of all the servers in the server group.
SSO Status	Displays one of the following statuses: **Enabled** Indicates that the SAML Single Sign-On is enabled on the server. **Disabled** Indicates that SAML Single Sign-On is disabled on the server.
Re-Import Metadata	**Re-import Metadata** field is enabled only when Single Sign-On is successfully enabled on the subscriber. Click the **Re-import Metadata** icon to import IdP metadata file from the publisher to the subscribers. **Note** This option is displayed as N/A (Not Applicable) for the publisher node.
Last Metadata Import	Specifies the time when the IdP metadata was last imported on the server. This field displays “Never” if you are running the SAML Single Sign-On setup for the first time.
Export Metadata	**Export Metadata** field is enabled only when Single Sign-On is successfully enabled on both publisher and the subscriber. Click the **Export Metadata** icon to download the server metadata file. A SAML metadata file must be generated for the specified server, and downloaded using the browser. You must then import this metadata file to the IdP server. **Important** If you change the hostname or domain of a node, ensure that you download the metadata from that node and upload the file to the IdP server again. The **Export All Metadata** button is enabled by default, regardless of whether the SAML Single Sign-On state set to active.
Last Metadata Export	Specifies the time when the SAML metadata file of the specified server was last exported. This field displays “Never” if you are running the SAML Single Sign-On setup for the first time.

Field	Description
SSO Test	Displays the test results of the SAML configuration with the IdP. The test ensures that the specified server trusts the IdP, and that the IdP trusts the specified server. The trust relationship between the server and the IdP depends on the success of exporting and importing of SAML metadata files. Displays one of the following values: **Never** Indicates that a test has not been performed on this server. **Passed** Indicates that a test has been successfully run on this server, and that the server and the IdP trust one another. **Failed** Indicates that a test was attempted on the specified server, but that either the server does not trust the IdP, or the IdP does not trust the server, or some other network or IdP issue prevented the test from passing.
Run SSO Test	Click **Run SSO Test** to run the Single Sign-On test. You must run this test before enabling SAML Single Sign-On. The SAML Single Sign-On setup cannot be completed until this test is successful. To run this test, there must be at least one LDAP synchronized user with administrator rights. You must also know the password for that user ID. **Note** You cannot run this test until the IdP metadata file is imported to the server, and the server metadata file is exported to the IdP server.
Enable SAML SSO	Click **Enable SAML SSO** to start the SAML Single Sign-On configuration.
Export All Metadata	Click **Export All Metadata** to export the SAML metadata files from each server. These files are converted to a compressed file (.zip) for easy download. You must extract the file and then import each file to the IdP.
Update IdP Metadata File	Click **Update IdP Metadata File** to update IdP metadata on all the servers in the cluster.

Field	Description
Fix All Disabled Servers	Click **Fix All Disabled Servers** to enable SAML Single Sign-On, on the servers on which it is disabled.
View IdP Trust Metadata File	Click **View IdP Trust Metadata File** to download a copy of the IdP metadata file.

APPENDIX B

Change IP Address and Hostname

IP Address and Hostname Overview

You can change the network-level IP address and hostname name of nodes in your deployment for a variety of reasons, including moving the node from one network domain to another or resolving a duplicate IP address problem. The IP address is the network-level Internet Protocol (IP) associated with the node, and the Hostname is the network-level hostname of the node.

This document provides detailed procedures for the following tasks for Cisco Emergency Responder nodes:

- Change the IP address of a node
- Change the hostname of a node

Task lists are provided for each of these procedures that summarize the steps to perform.

Use the *Cisco Emergency Responder 10.5(1) Command Line Interface Guide* to assist you when changing an IP Address or Hostname. This guide replaces the chapter previously found in the Cisco Emergency Responder Administration Guide.

The Emergency Responder Command Line Interface Guide can be found on the Cisco Emergency Responder Command Reference page.

Note You must complete all pre-change tasks and system health checks before you make these changes, and you must complete the post-change tasks after you make any of these changes.

Pre-Change Tasks and System Health Checks

The following sections discuss pre-change tasks and system health checks. You must perform these tasks before you change a Hostname or IP address.

Pre-Change Task List for Cisco Emergency Responder Nodes

The following table lists the tasks to perform before you proceed to change the IP address and hostname for Cisco Unified Communications Manager nodes. You must perform these procedures during a scheduled maintenance window. Perform all system health checks before you perform the pre-change setup tasks.

For details about any of the tasks that are listed, see topics related to performing system health checks on nodes and pre-change setup.

⚠ **Caution** If you do not receive the results that you expect when you perform these tasks, do not continue until you have resolved the issue.

Item	Task
System health checks	
1.	If you have DNS configured anywhere on the Cisco Emergency Responder servers, ensure that forward and reverse records (for example, a record and PTR record) are configured and that the DNS is reachable and working.
2.	Ensure that all servers in the cluster are up and available, and check for any active ServerDown alerts.
3.	Check the database replication status of all Cisco Emergency Responder nodes in the cluster to ensure that all servers are replicating database changes successfully.
4.	Check network connectivity and DNS server configuration.
Pre-change setup tasks	
5.	Use Cisco Emergency Responder Administration to compile a list of all nodes in the cluster. Retain this information for use later.
6.	Run a manual Disaster Recovery System backup and ensure that all nodes and active services are backed up successfully. For more information, see the *Disaster Recovery System Administration Guide* for your release.

Check System Health

Perform the applicable system health checks on the nodes in your deployment as part of the pre-change setup and as part of the post-change tasks that you must perform after you have changed any network identifiers.

Caution If you do not receive the results that you expect when you perform these tasks, do not continue until you have resolved the issue.

Some of the checks in this procedure are required only for post-change verification. See the post-change task list for a complete list of the system health checks to perform.

Note If you are performing system health checks as part of the pre-change setup, you can skip the following steps which are only required when you are performing the post-change tasks:

- Verification that the new hostname or IP address appears on the Cisco Emergency Responder server list.
- Verification that changes to the IP address, hostname, or both are fully implemented in the network.
- Verification that changes to the hostname is fully implemented in the network.

Procedure

Step 1 If you have DNS configured anywhere on the Cisco Emergency Responder servers, ensure that a forward and reverse lookup zone has been configured and that the DNS is reachable and working.

Step 2 Check for any active ServerDown alerts to ensure that all servers in the cluster are up and available. Use the command line interface (CLI) on the first node.

a) Enter the following CLI command on the first node and inspect the application event log: **file search activelog syslog/CiscoSyslog ServerDown**.

Step 3 Check the database replication status on all nodes in the cluster to ensure that all servers are replicating database changes successfully.

Use CLI to get status of DB replication.

To check using the CLI, enter **utils dbreplication status**.

For example output, see topics related to example database replication output. For detailed procedures and troubleshooting, see topics related to verifying database replication and troubleshooting database replication.

Step 4 Enter the CLI command **utils diagnose** as shown in the following example to check network connectivity and DNS server configuration.

```
admin:utils diagnose module validate_network

Log file: platform/log/diag1.log

Starting diagnostic test(s)
===========================
test - validate_network    : Passed

Diagnostics Completed
```

The final output will be in Log file: platform/log/diag1.log.

Use **file view activelog platform/log/diag1.log** command to see the output.

Step 5 If you are performing the pre-change system health checks, you are done; otherwise, continue to perform the post-change verification steps.

Step 6 Verify that the new hostname or IP address appears on the Unified Communications Manager server list. In Cisco Unified CM Administration, select **System** > **Server Settings**.

Note Perform this step only as part of the post-change tasks.

Step 7 Verify that changes to the IP address, hostname, or both are fully implemented in the network. Enter the CLI command **show network cluster** on each node in the cluster. Perform this step only as part of the post-change tasks.

Note The output should contain the new IP address or hostname of the node.

Example

```
admin:show network cluster
10.77.29.191 cer-191-p123.cisco.com cer-191-p123 Publisher callmanager DBPub authenticated
10.77.29.192 cer186-sub.cisco.com cer186-sub Subscriber ciscoer DBSub authenticated using
TCP since Fri Oct 10 18:42:40 2014


Successful
```

Step 8 Verify that changes to the hostname are fully implemented in the network. Enter the CLI command **utils network host <new_hostname>** on each node in the cluster.

Perform this step only as part of the post-change tasks.

Note The output should confirm that the new hostname resolves locally and externally to the IP address.

Example

```
admin:utils network host cer-191-p123
Local Resolution:
cer-191-p123.cisco.com resolves locally to 10.77.29.191 (CER-191-P123.cisco.com)

External Resolution:
cer-191-p123.cisco.com has address 10.77.29.191
```

Pre-Change Setup

Perform all pre-change setup tasks to ensure that your system is prepared for a successful IP address, hostname, domain, or node name change. You must perform these tasks during a scheduled maintenance window.

You should perform the system health checks on your deployment before performing the pre-change setup.

Perform Pre-Change Setup Tasks for Cisco Emergency Responder Nodes

Perform the following pre-change setup tasks before you change the IP address or hostname. You must perform these tasks during a scheduled maintenance window. See the pre-change task list for more information.

Caution If you do not receive the results that you expect when you perform these tasks, do not continue until you have resolved the issue.

Before you begin

Perform the system health checks on your deployment.

Procedure

Step 1 From Cisco Unified Communications Manager Administration on the first node, select **System** > **Server** and click **Find**. A list of all servers in the cluster displays. Retain this list of servers for future reference.

Ensure that you save an inventory of both the hostname and IP address of each node in your cluster.

Step 2 Run a manual Disaster Recovery System backup and ensure that all nodes and active services are backed up successfully. For more information, see the *Disaster Recovery System Administration Guide* for your release.

IP Address and Hostname Changes

The following sections provide important information on IP Address and Hostname Changes. You must read these sections before you change an IP address or Hostname.

Change IP Address and Hostname Task List

The following table lists the tasks to perform to change the IP address and hostname for Cisco Emergency Responder nodes.

Table 115: Change IP Address and Hostname Task List

Item	Task
1.	Perform the pre-change tasks and system health checks.
2.	Change the IP address or hostname for the node using either the Command Line Interface (CLI) or the Unified Operating System GUI.
3.	Perform the post-change tasks.

Change IP Address or Hostname Using Unified Operating System GUI

You can use Cisco Unified Operating System Administration to change the IP address or hostname for publisher and subscriber nodes that are defined by a hostname in your deployment. Unless otherwise stated, each step in this procedure applies to both publisher and subscriber nodes on Cisco Emergency Responder Server Group.

Before you begin

Perform the pre-change tasks and system health checks on your deployment.

Procedure

Step 1 From Cisco Unified Operating System Administration, select **Settings > IP > Ethernet**.

Step 2 Change the hostname, IP address, and if necessary, the default gateway.

Step 3 Click **Save**.

What to do next

Perform all applicable post-change tasks to ensure that your changes are properly implemented in your deployment.

Note Do not proceed if the new hostname does not resolve to the correct IP address. If your cluster is using CA-signed certificates, you will need to have them re-signed. Run the CTL client and update the CTL file if the Cisco Unified Communications Manager cluster security is operating in mixed mode.

Change IP Address or Hostname Using CLI

You can use the Command Line Interface (CLI) to change the IP address or hostname for publisher and subscriber nodes that are defined by a hostname in your deployment. Unless otherwise stated, each step in this procedure applies to both publisher and subscriber nodes on Cisco Emergency Responder Server Group.

Before you begin

Perform the pre-change tasks and system health checks on your deployment.

Procedure

Step 1 Log into the CLI of the node that you want to change.

Step 2 Enter **set network hostname**.

Step 3 Follow the prompts to change the hostname, IP address, or default gateway.

a) Enter the new hostname and press **Enter**.
b) Enter **Yes** if you also want to change the IP address; otherwise, go to Step 4.
c) Enter the new IP address.
d) Enter the subnet mask.
e) Enter the address of the gateway.

Step 4 Verify that all your input is correct and enter **yes** to start the process.

Step 5 Wait for all services to come up on the node where the change is applied.

Step 6 If the change is applied on Publisher and only Hostname is changed, restart Cisco Emergency Responder service on Publisher.

Step 7 If the change is applied on Publisher and IP address is also changed along with the Hostname; restart Cisco Emergency Responder service on both Publisher and Subscriber node.

Step 8 If the node that you have changed is a subscriber node, reboot the node.

What to do next

Perform all applicable post-change tasks to ensure that your changes are properly implemented in your deployment.

Note Do not proceed if the new hostname does not resolve to the correct IP address.

If your cluster is using CA-signed certificates, you will need to have them re-signed. Run the CTL client and update the CTL file if the Cisco Emergency Responder cluster security is operating in mixed mode.

Example CLI Output for Set Network Hostname: Changing Hostname Only of Publisher

The following code shows an example of the CLI Output for Set Network Hostname.

```
admin:set network hostname

WARNING: Changing this setting will invalidate software license
         on this server. The license will have to be re-hosted.
Continue(y/n):
Continue (y/n)?y

ctrl-c: To quit the input.



         ***   W A R N I N G   ***
Do not close this window without first canceling the command.

This command will automatically restart system services.
The command should not be issued during normal operating
hours.

=======================================================
 Note: Please verify that the new hostname is a unique
       name across the cluster and, if DNS services are
       utilized, any DNS configuration is completed
       before proceeding.
=======================================================

Security Warning : This operation will regenerate
       all CUCM Certificates including any third party
       signed Certificates that have been uploaded.

Enter the hostname:: newHostName
Would you like to change the network ip address at this time [yes]:: no


Warning: Do not close this window until command finishes.


Hostname: newHostName

Do you want to continue [yes/no]? yes

calling 1 of 10 component notification script: acluster_healthcheck.sh
calling 2 of 10 component notification script: adns_verify.sh
No Primary DNS server defined
No Secondary DNS server defined
calling 3 of 10 component notification script: aetc_hosts_verify.sh
calling 4 of 10 component notification script: ahostname_callback.sh
Info(0): Processnode query returned using cer195pub123:
hostaddress
============
cer195pub123
updating cerserver table from:'cer195pub123', to: 'newHostName'
Rows: 1
updating cersystemparameters table from:'cer195pub123', to: 'newHostName'
Rows: 3
updating database, please wait 90 seconds
updating database, please wait 60 seconds
updating database, please wait 30 seconds
calling 5 of 10 component notification script: clm_notify_hostname.sh
Verifying update across cluster nodes...
Updating platformConfig.xml: cer195pub123 to newHostName
Updating platformConfig.xml: cer195pub123 to newHostName
Updating platformConfig.xml: cer195pub123 to newHostName
Updating processnode.xml: cer195pub123 to newHostName
\  Restarting Cluster Manager service... Please Wait


cluster update successfull
calling 6 of 10 component notification script: drf_notify_hostname_change.py
calling 7 of 10 component notification script: elm_client_reset_registration
calling 8 of 10 component notification script: idsLocalPrefsUpdateFile.sh
Going to trigger /usr/bin/python /usr/local/er/lib/dblupdatefiles-plugin.py
-f=newHostName,cer195pub123
calling 9 of 10 component notification script: regenerate_all_certs.sh
calling 10 of 10 component notification script: update_idsenv.sh

System services will restart in 1 minute
admin:
```

Example CLI Output for Set Network Hostname: Changing IP Address and Publisher Hostname

The following code shows an example of the CLI Output for Set Network Hostname.

```
admin:set network hostname

WARNING: Changing this setting will invalidate software license
         on this server. The license will have to be re-hosted.
Continue(y/n):
Continue (y/n)?y

ctrl-c: To quit the input.



         ***   W A R N I N G   ***
Do not close this window without first canceling the command.

This command will automatically restart system services.
The command should not be issued during normal operating
hours.

=======================================================
 Note: Please verify that the new hostname is a unique
       name across the cluster and, if DNS services are
       utilized, any DNS configuration is completed
       before proceeding.
```

```
=======================================================

Security Warning : This operation will regenerate
       all CUCM Certificates including any third party
       signed Certificates that have been uploaded.

Enter the hostname:: newHostNameAndnewIPAddress
Would you like to change the network ip address at this time [yes]::


Warning: Do not close this window until command finishes.



ctrl-c: To quit the input.



           ***   W A R N I N G   ***
=======================================================
 Note: Please verify that the new ip address is unique
       across the cluster.
=======================================================

Enter the ip address:: 10.77.29.186
Enter the ip subnet mask:: 255.255.255.0
Enter the ip address of the gateway:: 10.77.29.1
Hostname:       newHostNameAndnewIPAddress
IP Address:     10.77.29.186
IP Subnet Mask: 255.255.255.0
Gateway:        10.77.29.1

Do you want to continue [yes/no]? yes

calling 1 of 6 component notification script: ahostname_callback.sh
Info(0): Processnode query returned using newHostName:
hostaddress
===========
newHostName
updating cerserver table from:'newHostName', to: 'newHostNameAndnewIPAddress'
Rows: 1
updating cersystemparameters table from:'newHostName', to: 'newHostNameAndnewIPAddress'
Rows: 3
updating database, please wait 90 seconds
updating database, please wait 60 seconds
updating database, please wait 30 seconds
calling 2 of 6 component notification script: clm_notify_hostname.sh
Verifying update across cluster nodes...
Updating platformConfig.xml: newHostName to newHostNameAndnewIPAddress
Updating platformConfig.xml: newHostName to newHostNameAndnewIPAddress
Updating platformConfig.xml: newHostName to newHostNameAndnewIPAddress
Updating processnode.xml: newHostName to newHostNameAndnewIPAddress
\  Restarting Cluster Manager service... Please Wait


cluster update successfull
calling 3 of 6 component notification script: drf_notify_hostname_change.py
calling 4 of 6 component notification script: idsLocalPrefsUpdateFile.sh
Going to trigger /usr/bin/python /usr/local/er/lib/dblupdatefiles-plugin.py
-f=newHostNameAndnewIPAddress,newHostName
calling 5 of 6 component notification script: regenerate_all_certs.sh
calling 6 of 6 component notification script: update_idsenv.sh
calling 1 of 3 component notification script: aaupdateip.sh
calling 2 of 3 component notification script: ahostname_callback.sh
```

```
Info(0): Processnode query returned =
name
==================================================
10.77.29.195-AdminUpdateManager
10.77.29.195-SystemUpdateManager
updating server table from:'10.77.29.195', to: '10.77.29.186'
Rows: 1
Rows: 1
updating database, please wait 90 seconds
updating database, please wait 60 seconds
updating database, please wait 30 seconds
calling 3 of 3 component notification script: clm_notify_hostname.sh
Verifying update across cluster nodes...
Shutting down interface eth0:
```

Change IP Address Only

Do not use **set network hostname** CLI command to change IP Address only.

Command Syntax

set network ip eth0 ip-address ip-mask gate-way

Syntax Description

Parameters	Description
eth0	Specifies Ethernet interface 0.
ip-address	The IP address that you want assign.
ip-mask	The IP mask that you want to assign.
gate-way	The IP of default gate way to be assigned.

Example

Note For further information please refer the admin guide IP address change section.

```
admin:set network ip eth0 10.77.34.243 255.255.255.0 10.77.34.1

WARNING: Changing this setting will invalidate software license
         on this server. The license will have to be re-hosted.
Continue(y/n):
Continue (y/n)?y
           ***   W A R N I N G   ***
This command will restart system services
=======================================================
 Note: Please verify that the new ip address is unique
       across the cluster and, if DNS services are
       utilized, any DNS configuration is completed
       before proceeding.
=======================================================
Continue (y/n)?y
calling 1 of 7 component notification script: aaupdateip.sh
calling 2 of 7 component notification script: acluster_healthcheck.sh
calling 3 of 7 component notification script: adns_verify.sh
Verifying 10.77.34.243 against primary DNS server 10.77.34.227 ...
Successfully verified against primary DNS server 10.77.34.227
IPADDR_RETURNED matches 10.77.34.243
calling 4 of 7 component notification script: aetc_hosts_verify.sh
calling 5 of 7 component notification script: ahostname_callback.sh
Info(0): Processnode query returned =
name
==================================================
10.77.34.207-AdminUpdateManager
10.77.34.207-SystemUpdateManager
updating server table from:'10.77.34.207', to: '10.77.34.243'
Rows: 1
Rows: 1
updating database, please wait 90 seconds
updating database, please wait 60 seconds
updating database, please wait 30 seconds
calling 6 of 7 component notification script: clm_notify_hostname.sh
Verifying update across cluster nodes...
Shutting down interface eth0:
```

Post-Change Tasks and Verification

The following sections provide information on post-change tasks and verification. You must read these sections and perform these tasks to complete the IP Address and Hostname changes.

Post-Change Task List for Cisco Emergency Responder Nodes

The following table lists the tasks to perform after you have changed the IP address or hostname of the Cisco Emergency Responder nodes in your cluster.

Perform the tasks that apply to your deployment in the order in which they are presented in the task list. For details about system health checks or generating ITL certificates, see the related topics.

Table 116: Post-Change Task List for Cisco Emergency Responder Nodes

Item	Task
System health checks	
1.	Ensure that all servers in the cluster are up and available, and check for any active ServerDown alerts. **Note** ServerDown alerts in the Syslog are normal during the change process, but should not appear in the log after the change is done.
2.	Check the database replication status of all Cisco Emergency Responder nodes in the cluster to ensure that all servers are replicating database changes successfully.
3.	Check network connectivity and DNS server configuration on the node that was changed using the CLI command **utils diagnose module validate_network**.
Security enabled cluster tasks	

Item	Task
4.	For security-enabled clusters (Cluster Security Mode 1 - Mixed), update the CTL file and then restart all nodes in the cluster before you perform the system health checks and other post-change tasks. For detailed instructions on updating and managing the CTL file, including adding a new TFTP server to an existing CTL file, see the *Cisco Unified Communications Manager Security Guide* .
5.	If you enabled cluster security using Certificate Trust List (CTL) files and USB eTokens, you must regenerate the Initial Trust List (ITL) file and the certificates in the ITL. Skip this step if you have not enabled cluster security using Certificate Trust List (CTL) files and USB eTokens.
Post-change tasks	
6.	Run a manual DRS backup and ensure that all nodes and active services back up successfully. For more information, see the Disaster Recovery System Administration Guide for your release. **Note** You must run a manual DRS backup after you change the IP address of a node, because you cannot restore a node with a DRS file that contains a different IP address or hostname. The post-change DRS file will include the new IP address or hostname.
7.	If you are using the integrated DHCP server that runs on Cisco Unified Communications Manager, update the DHCP server.

Perform Post-Change Tasks for Cisco Emergency Responder Nodes

Perform all post-change tasks to ensure that your changes are properly implemented in your deployment. Perform the tasks in the order in which they are presented in the task list.

Before you begin

Before you perform your post-changes tasks, you must:

- Perform all applicable system health checks to verify the changes that were made to your deployment.
- Perform the security enabled cluster tasks if cluster security is enabled for your deployment.

Procedure

Step 1 Run a manual DRS backup and ensure that all nodes and active services back up successfully. For more information, see the *Disaster Recovery System Administration Guide* for your release.

Note You must run a manual DRS backup after you change the IP address of a node, because you cannot restore a node with a DRS file that contains a different IP address or hostname. The post-change DRS file will include the new IP address or hostname.

Step 2 If you are using the integrated DHCP server that runs on Cisco Unified Communications Manager, update the DHCP server.

Troubleshooting

The following sections provide information on troubleshooting an IP Address and Hostname change. Use this information to diagnose and resolve any issues.

Troubleshoot Cluster Authentication

You can troubleshoot cluster authentication issues on subscriber nodes using the Command Line Interface (CLI).

Procedure

Step 1 Enter **show network eth0 [detail]** to verify network configuration.

Step 2 Enter **show network cluster** to verify the network cluster information.

- If the output displays incorrect publisher information, enter the **set network cluster publisher [hostname/IP address]** CLI command on the subscriber node to correct the information.
- If you are on a publisher node, and the show network cluster CLI command displays incorrect subscriber information, login to Cisco Emergency Responder Administration and choose **System** > **Server Settings** to check the output.
- If you are on a subscriber node and the show network cluster output displays incorrect publisher information, use the **set network cluster publisher [hostname | IP_address]** CLI command to change the publisher hostname or IP address.

Troubleshoot Database Replication

You can use the Command Line Interface (CLI) to troubleshoot database replication on the nodes in your cluster.

- Verify that database replication is in a correct state in the cluster.
- Repair and reestablish database replication for the nodes.
- Reset database replication.

For more information about these commands or using the CLI, see the *Command Line Interface Guide for Cisco Emergency Responder Administration Guide*.

Verify Database Replication

Use the Command Line Interface (CLI) to check the database replication status for all nodes in the cluster. Verify that the Replication STATE is shown as "Active" for both publisher and subscriber replication server.

Anything other than "Active" state (for example, "Dropped", "Connecting") means that there is a problem with database replication and that you need to reset replication for the node. See topics related to database replication examples for example output.

Procedure

Enter **utils dbreplication status** on the publisher and subscriber to check database replication on both the nodes in a Server Group.

Note If replication is not set up for the nodes in your cluster, you can reset database replication for the nodes using the CLI. For more information, see topics related to resetting database replication using the CLI

Example:

```
On Publisher

admin:utils dbreplication status

 -------------------- utils dbreplication status --------------------
Output is in file /var/log/active/er/trace/dbl/sdi/ReplicationStatus.2014_10_13_18_24_02.out

Please use "file view activelog er/trace/dbl/sdi/ReplicationStatus.2014_10_13_18_24_02.out
 " command to see the output
admin:file view activelog er/trace/dbl/sdi/ReplicationStatus.2014_10_13_18_24_02.out

Mon Oct 13 18:24:02 2014 main()  DEBUG:  -->
Mon Oct 13 18:24:02 2014 main()  DEBUG:  Replication cluster summary:
SERVER                 ID STATE    STATUS     QUEUE  CONNECTION CHANGED
-----------------------------------------------------------------------
g_2_cer10_5_0_98000_9000    2 Active   Local           0
g_3_cer10_5_0_98000_9000    3 Active   Connected       0 Oct 13 17:31:15
Mon Oct 13 18:24:03 2014 main()  DEBUG:  <--

end of the file reached
options: q=quit, n=next, p=prev, b=begin, e=end (lines 1 - 7 of 7) :
admin:
On Subscriber:

admin:utils dbreplication status

 -------------------- utils dbreplication status --------------------
Output is in file /var/log/active/er/trace/dbl/sdi/ReplicationStatus.2014_10_13_18_33_14.out

Please use "file view activelog er/trace/dbl/sdi/ReplicationStatus.2014_10_13_18_33_14.out
 " command to see the output
admin:file view activelog er/trace/dbl/sdi/ReplicationStatus.2014_10_13_18_33_14.out

Mon Oct 13 18:33:14 2014 main()  DEBUG:  -->
Mon Oct 13 18:33:14 2014 main()  DEBUG:  Replication cluster summary:
SERVER                 ID STATE    STATUS     QUEUE  CONNECTION CHANGED
-----------------------------------------------------------------------
g_2_cer10_5_0_98000_9000    2 Active   Connected       0 Oct 13 17:31:15
g_3_cer10_5_0_98000_9000    3 Active   Local           0
Mon Oct 13 18:33:15 2014 main()  DEBUG:  <--

end of the file reached
options: q=quit, n=next, p=prev, b=begin, e=end (lines 1 - 7 of 7) :
```

```
admin:
```

Repair Database Replication

Use the Command Line Interface (CLI) to repair database replication.

Procedure

Step 1 Enter **utils dbreplication repair all** on the Publisher to attempt to repair database replication.

Depending on the size of the database, it may take several minutes to repair database replication. Proceed to the next step to monitor the progress of database replication repair.

Example:

```
admin:utils dbreplication repair all
 -------------------- utils dbreplication repair --------------------
Logs for the repair of ~informix/.rhosts file is present in er/logs/repair-rhosts-1818.log
 file
/usr/local/er/db/informix/bin/cdr list server >>
/var/log/active/er/trace/dbl/sdi/ReplicationRepair.2014_10_13_18_38_07.out 2>&1
Output is in file er/trace/dbl/sdi/ReplicationRepair.2014_10_13_18_38_07.out

Please use "file view activelog er/trace/dbl/sdi/ReplicationRepair.2014_10_13_18_38_07.out
 " command to see the output
admin:
```

Step 2 View the ReplicationRepair file as mentioned in step 1 to check whether all tables are scanned and replicated properly. Any error will be reflected in this file.

If errors or mismatches are found, there may be a transient mismatch between nodes. Run the procedure to repair database replication again.

Note If, after several attempts to repair replication, mismatches or errors are being reported, try resetting the replication to resolve this issue.

Reset Database Replication

Reset database replication if replication is not set up for the nodes in your cluster. You can reset database replication using the command line interface (CLI).

Procedure

Step 1 Reset replication on nodes in your cluster. Do the following:

a) Enter **utils db replication reset all** on Publisher node in a CER Server Group.
b) Before you run this CLI command on the Publisher node, first run the command **utils dbreplication stop** on subscriber node, and then on the publisher node.

Step 2 After the command is executed successfully on Publisher node, restart subscriber node.

Troubleshoot Network

You can troubleshoot network issues on nodes using the Command Line Interface (CLI).

Procedure

Step 1 Enter **show network eth0 [detail]** to verify network configuration.

Step 2 If any of the fields are missing, then reset the network interface.

a) Enter **set network status eth0 down**.
b) Enter **set network status eth0 up**.

Step 3 Verify the IP address, mask, and gateway. Ensure that these values are unique across the network.

Troubleshoot Network Time Protocol

The following sections discuss troubleshooting NTP issues on the Publisher and Subscriber nodes. Use this information to resolve any potential issues.

Troubleshoot NTP on Subscriber Nodes

You can troubleshoot Network Time Protocol (NTP) issues on subscriber nodes using the Command Line Interface (CLI).

Procedure

Step 1 Enter **show network eth0 [detail]** to verify network configuration.

Step 2 Enter **utils ntp status** to verify NTP status.

Step 3 Enter **utils ntp restart** to Restart NTP.

Step 4 Enter **show network cluster** to verify the network cluster.

If the output displays incorrect publisher information, use the **set network cluster publisher [hostname/IP_address]** CLI command to reset the publisher.

Troubleshoot NTP on Publisher Nodes

You can troubleshoot Network Time Protocol (NTP) issues on publisher nodes using the Command Line Interface (CLI).

Procedure

Step 1 Enter **show network eth0 [detail]** to verify network configuration.

Step 2 Enter **utils ntp status** to verify NTP status.

Step 3 Enter **utils ntp restart** to Restart NTP.

Step 4 Enter **utils ntp server list** to verify NTP servers.

To add or delete an NTP server, use the **utils ntp server [add/delete]** CLI command.

APPENDIX C

Cisco Emergency Responder Serviceability Web Interface

Control Center

The Control Center page appears when you choose **Tools** > **Control Center**.

Authorization Requirements

You must have serviceability authority to access this page.

Description

Use the Control Center page to view the services running on the server and then start, stop, and restart these services. This page displays a list of services currently running on the server. Radio buttons in front of each service name allows you to select each service to perform the desired action.

The following table describes the Control Center page.

Table 117: Control Center Page

Field	Description
Start button	Starts the selected services.
Stop button	Stops the selected services.

Field	Description
Restart button	Restarts the selected services.
Refresh button	Refreshes the list of currently running services on the selected server.
Service Name	Names of the currently running services on the selected server. To select a service, click the radio button next to the service name.
Status	Current status of the selected service.

Related Topics

Manage Emergency Responder Server , on page 349

Event Viewer

The Event Viewer page appears when you choose **Tools** > **Event Viewer**.

Authorization Requirements

You must have serviceability authority to access this page.

Description

Use the Event Viewer page to view Emergency Responder events for the previous six months.

The following table describes the Event Viewer page.

Table 118: Event Viewer Page

Field	Description
Find Events in the month	Select a specific month to view events from the month.
Type pulldown menu	**Note** This pull-down menu contains two options: Type and Module. When you choose Type or Module, the pull-down menu to the right changes to display the availabl or Module options. Allows you to select which type of event you want to view. The available types are: • ALL • INFO • WARN • ERROR These options are displayed in the pull-down menu to the right of the Type pull-down menu.

Field	Description
Module pulldown menu	**Note** This pull-down menu contains two options: Type and Module. When you cho Type or Module, the pull-down menu to the right changes to display the avai or Module options. Allows you to select the Emergency Responder module for which you want to view event select Module from the pull-down menu, the menu to the right changes to show the availa The available options are: • All • CER_DATABASE • CER_SYSADMIN • CER_REMOTEUPDATE • CER_TELEPHONY • CER_PHONETRACKINGENGINE • CER_AGGREGATOR • CER_ONSITEALERT • CER_GROUP • CER_CALLENGINE • CER_CLUSTER • CER_PROVIDER
Items Per Page menu	Allows you to select the number of events displayed per page. Options are 10, 20, 30, 40,
	Displays search results. **Note** This area of the page is not visible until you perform a search operation.
Type column	Displays the type of event. The Type column displays one of the following: • INFO • WARN • ERROR Use the Up and Down arrows to perform an ascending or descending sort of the results.
Time column	Displays the time of the event. Use the Up and Down arrows to perform an ascending or sort of the results.

Field	Description
Module column	Displays the Emergency Responder module to which the event applies. The modules are: • CER_DATABASE • CER_SYSADMIN • CER_REMOTEUPDATE • CER_TELEPHONY • CER_PHONETRACKINGENGINE • CER_AGGREGATOR • CER_ONSITEALERT • CER_GROUP • CER_CALLENGINE • CER_CLUSTER • CER_PROVIDER Use the Up and Down arrows to perform an ascending or descending sort of the results.
Message column	Displays the message associated with each event. Use the Up and Down arrows at the right o box to scroll through the message.

Related Topics

Use Event Viewer, on page 196

Audit Log Configuration

The Audit Log configuration page appears when you choose **Tools** > **Audit Log Configuration**.

Authorization Requirements

Only a user with an audit role can change the audit log settings. The administrator can assign users to have auditing privileges in the **User Group Configuration** window. The Cisco Emergency Responder Audit Administrator assigns privileges to delete audit logs and also to read and update audit configuration in the Cisco Emergency Responder Serviceability interface.

Description

Use the Audit Log Configuration page to configure audit related settings. This page allows you to set parameters for Audit level, Remote Syslog, and Local Audit Log configuration.

The following table describes the Audit Log ER settings.

Table 119: Audit Log Page

Field	Description
Audit Level Settings	

Field	Description
Audit Event Level **Warning** is the default value.	Choose the required severity level for the audit event from the drop-down list. If you, choose **Debug** all the syslog messages including **Info**, **Error**, and **Warning** are sent to the remote syslog server and stored locally in audit log file if the local audit logging is enabled.
Remote SysLog Settings	
Remote Syslog Server	Enter the hostname or IP address of the remote syslog server to accept syslog messages. This syslog server handles the auditing of the all user-related operations (for example, login, logout, edit settings, and accessing the information). If server name is not specified, Cisco Emergency Responder does not send the syslog messages. 601 is the default port to which the messages are sent and used to communicate to the remote syslog server. **Note** Do not specify a Cisco Emergency Responder node as the destination because the Cisco Emergency Responder node does not accept syslog messages from another server.
Local Audit Log Settings	
Enable Local Audit Log	Check the check box to create an audit log for the application audit log. The application audit log supports configuration updates for Cisco Emergency Responder Administration and Cisco Emergency Responder Serviceability. The option is set to Disabled by default. **Note** The Audit Log Agent Service must be active.
Enable Local Log Rotation	This setting is enabled by default. The system reads this option to rotate the audit log files or to continue to create new files. It begins to overwrite the oldest audit log files after it reaches the maximum number of files. The maximum number of files cannot exceed 500.
Maximum No. of Files	Enter the maximum number of files that you want to include in the log. The default setting is 250 and the maximum number cannot exceed 500.

Field	Description
Maximum File Size (MB)	Enter the maximum file size for the audit log. The file size value must remain between 1 and 5 MB.
Warning Threshold for Approaching Log Rotation Overwrite (%)	Set the threshold at which the system sends you an alert, when the audit logs are approaching the level where they are overwritten. **Note** The total disk space allocated to audit logs is the Maximum No. of Files multiplied by the Maximum File Size. If the size of audit logs on the disk exceeds this percentage of total disk space allocated, the system raises an alert in Event Viewer. The default value is 80% for the warning threshold.
Set to Default	Click the button to set default values for all the parameters.

Note Cisco Emergency Responder always uses the TCP port to connect and send data to the remote syslog server irrespective of the mode (Enhanced Security Mode or Normal). When Cisco Emergency Responder fails to send data to the remote syslog server due to connectivity issues or any other exception, the administrator is notified through email about the failure condition and a notification is sent to the event syslog server that is configured under **System** > **Cisco ER Group Settings**. The data sent to event syslog server uses the UDP port in the normal mode and the TCP port in the Enhanced Security Mode. The **utils remotesyslog** CLI command is not supported in Cisco Emergency Responder.

Related Topics

Audit Log Configuration, on page 512

SNMP Community String Configuration

The SNMP Community String Configuration page appears when you choose **SNMP > V1/V2c Configuration > Community String**.

Authorization Requirements

You must have serviceability authority to access this page.

Description

Use the SNMP Community String Configuration page to view, add, update, and delete community strings. Community strings control access to the Emergency Responder by clients using SNMP V1 and V2c.

The following table describes the SNMP Community String Configuration page.

Table 120: SNMP Community String Configuration Page

Field	Description
Community String Name column	Lists all community strings defined for the selected server. Click the name of the commun update the information for that community string.
Add New button or icon	Add a new community string for the selected server. When you click this button, Emergenc opens a second SNMP Community String Configuration page. **Note** Clicking the **Add New** button brings up the same screen displayed when you **Add New** icon.
Delete Selected button or icon	Deletes the selected community strings. To delete a community string, you must first selec list of community strings. Click the box to the left of the community string name to select all community strings from the selected server, click the box to the left of the **Community S** column heading. **Note** Clicking the **Delete Selected** button initiates the same action as does clicking icon at the top of the page.

Use the second SNMP Community String Configuration page to add new SNMP community strings and to update existing SNMP community strings.

The following table describes the second SNMP Community String Configuration page.

Table 121: SNMP Community String Configuration Page—2

Field	Description
Community String Name	If you are adding a new community string, type the name of the new community string into If you are updating information for an existing community string, the name of community updated is displayed.
Host IP Address Information	
Accept SNMP Packets from any host	Click this radio button to allow any host to access the Emergency Responder using SNMI
Accept SNMP Packets only from these hosts	Click this radio button to specify which hosts can access the Emergency Responder using add hosts that you want to have SNMP access, enter the IP addresses of the new hosts and to remove hosts that you no longer want to have SNMP access, enter the IP addresses of t click **Remove**.
Access Privileges pulldown menu	When adding a new community string, allows you to specify the access privilege for the ne string. When updating a community string, displays the current access privilege level. Th access privilege levels are as follows: • ReadOnly • ReadWrite • ReadWriteNotify • NotifyOnly • None

Field	Description
Insert button or icon	Inserts a new community string for the selected server. You must fill in the other fields on thi before you can insert the new community string.
Clear button or icon	Clears the community string information displayed on the current page.

Related Topics

Set Up SNMP Community String , on page 197

SNMP User Configuration

The SNMP User Configuration page appears when you choose **SNMP** > **V3 Configuration** > **User**.

Authorization Requirements

You must have serviceability authority to access this page.

Description

Use the SNMP User Configuration page to configure new SNMP V3 users.

The following table describes the SNMP User Configuration page.

Table 122: SNMP User Configuration Page

Field	Description
Server pulldown menu	Name of the server for which you want to view, add, update, or delete users. After you select Emergency Responder displays the currently configured information in the following format: • User Name • Authentication Required • Authentication Protocol • Privacy Required • Privacy Protocol • Access Privileges Click user name to display the Add and Update SNMP User Configuration page, from which update the information for that user.
Add New User button or icon	Add a new user for the selected server. When you click this icon, Emergency Responder oper Add/Update SNMP User Configuration page.
Delete Selected button or icon	Deletes the users. To delete a user, you must first select it from the list of users. Click in the b left of the user name to select it. To delete all users from the selected server, click the box to t the **User Name** column heading.

Use the second SNMP User Configuration page to configure new SNMP V3 users.

The following table describes the Add/Update SNMP User Configuration page.

Table 123: SNMP User Configuration Page—2

Field	Description
User Name field	Enter the name of the new SNMP V3 user. **Note** If you reached this page by clicking an existing user name on the SNMP User C page, the fields on this page display the currently configured information.
Authentication Information	Use this section to configure the following information: • If authentication is required for this user, check the check box that is labeled Authentica • Enter the authentication password for the new user in the Password and Reenter Pass boxes. • To select the authentication protocol for the new user, click the radio button for either I
Privacy Information	Use this section to configure the following information: • If privacy is required for this user, check the check box that is labelled Privacy Requ • Enter the privacy password for the new user in the Password and Reenter Password t • To select the privacy protocol for the new user, click on radio button labelled **DES**.
Host IP Addresses Information	Use the radio buttons in this section of the page to do the following: • Specify which hosts can access the Emergency Responder using SNMP. You can inser for new hosts that you want to have SNMP access to the Emergency Responder, or yo IP addresses of hosts that you no longer want to have SNMP access to Emergency R • Allow any host to access Emergency Responder using SNMP.
Access Privileges pulldown menu	When adding a new user, this pull-down menu allows you to specify the access privilege user. When updating a user's information, this field displays the current access privilege le available access privilege levels are as follows: • ReadOnly • ReadWrite • ReadWriteNotify • NotifyOnly • None
Insert button or icon	Insert the new user information for the selected server.
Clear button or icon	Clears the user information displayed on the current page.

Related Topics

Set Up SNMP Users , on page 198

MIB2 System Group Configuration

The MIB2 SystemGroup Configuration page appears when you choose **SNMP > System Group Configuration > MIB2 System Group Configuration**.

Authorization Requirements

You must have serviceability authority to access this page.

Description

Use the MIB2 System Group Configuration page to specify the name and physical location of the contact person for MIB2 managed mode.

The following table describes the MIB2 System Group Configuration page.

Table 124: MIB2 System Group Configuration Page

Field	Description
System Contact	The name of the MIB2 contact.
System Location	The physical location of the managed node.
Update button or icon	Saves the updated MIB2 contact information.
Clear button or icon	Clears the MIB2 contact information displayed on the current page.

Related Topics

Set Up MIB2 , on page 199

CPU and Memory Usage

The CPU and Memory Usage page appears when you choose **System Monitor** > **CPU & Memory Usage**.

Authorization Requirements

You must have serviceability authority to access this page.

Description

Use the CPU and Memory Usage page to view the CPU and memory usage for the Emergency Responder system.

The following table describes the CPU and Memory Usage page.

Table 125: CPU and Memory Usage Page

Field	Description
Disable Auto-Refresh	Check this check box to disable auto-refresh of the information displayed on this page.
Set the screen reset value	Specify in seconds how often this page should be refreshed.
Set CPU Logging Interval	Specify in seconds how often CPU usage is logged. The interval must be between 5 and 600
Processors	This section displays the percentage of CPU time being used by various system components.

Field	Description
Download CPU Log File	Click this link to download the currently displayed CPU and memory usage information to you click on this link, a new page opens that lists all the saved CPU log files. For more in about this screen, see Table 126: CPU Log Files Page , on page 520.
Processor	Name of the processor.
%User	Percentage of processor time being used by the User mode.
%System	Percentage of processor time being used by the System mode.
%Nice	Percentage of processor time being used by nice tasks. **Note** Nice is a value associated with a process that determines when the process is Nice tasks are only those tasks whose nice value is positive.
%Idle	Percentage of time in which the processor is idle.
%Irq	Percentage of processor time being used by interrupt requests (IRQ).
%Softirq	Percentage of processor time being used by soft IRQs. **Note** A soft IRQ is an interrupt request that can be deferred.
%I/O Wait	Percentage of time that the processor is executing read or write operations.
%CPU	The processor's share of the elapsed CPU time (excluding idle time) since last update, exp percentage of CPU time.
Start Log button	Starts a log file of the current CPU usage. **Note** You can create a maximum of 25 CPU log files.
Memory	This section displays the percentage of memory allocated for different uses.
Download Memory Log File	Click this link to download to a file the currently displayed CPU and memory usage inforn you click this link, a new page opens that lists all the saved CPU log files. For more inforn this screen, see Table 127: Memory Log Files Page , on page 520.
Total (KB)	The amount of memory available, in kilobytes.
Used (KB)	Amount of memory currently being used, in kilobytes.
Free (KB)	Amount of memory that is available for use, in kilobytes.
Shared (KB)	Amount of memory used by shared processes, in kilobytes.
Buffers (KB)	Amount of memory used by buffers, in kilobytes.
Cached (KB)	Amount of memory used for caching, in kilobytes.
Total Swap (KB)	Amount of total swap space, in kilobytes
Used Swap (KB)	Amount of swap space currently being used, in kilobytes.

Field	Description
Free Swap (KB)	Amount of available swap space, in kilobytes
%VM Used	Amount of virtual memory being used.
Start Log button	Starts a log file of the current memory usage.

Use the CPU Log Files page to view and download the CPU log files.

The following table describes the CPU Log Files page.

Table 126: CPU Log Files Page

Field	Description
Download button	Download the selected log files. You must first select the file to be downloaded. To do so, cli to the left of the File Name. If you click the box to the left of the File Name column heading, are selected for download.
CPU Log Files	This section displays the details of the saved CPU log files.
File Name	Name of the saved CPU log file. If you click on the file name, a new screen opens and displa contents of the log file.
Last Modified	Date and time of the last modification to the CPU log file.
File Size (KB)	Size of the CPU log file, in kilobytes.

Use the Memory Log Files page to view and download the memory log files.

The following table describes the Memory Log Files page.

Table 127: Memory Log Files Page

Field	Description
Download button	Download the selected log files. You must first select the file to be downloaded. To do so, cli to the left of the File Name. If you click the box to the left of the **File Name** column heading are selected for download.
Memory Log Files	This section displays the details of the saved Memory log files.
File Name	Name of the saved Memory log file. If you click on the file name, a new screen opens and di contents of the log file.
Last Modified	Date and time of the last modification to the Memory log file.
File Size (KB)	Size of the Memory log file, in kilobytes.

Related Topics

Use CPU and Memory Usage Tool , on page 199

Processes

The Processes page appears when you choose **System Monitor** > **Processes**.

Authorization Requirements

You must have serviceability authority to access this page.

Description

Use the Processes page to view and download information about currently running processes.

Note Use the Up and Down arrows next to each column heading on the Processes page to sort the information by each category.

The following table describes the Processes page.

Table 128: Processes Page

Field	Description
Disable Auto-Refresh	Check this check box to disable auto-refresh of the information displayed on this page.
Refresh Rate	To specify in seconds how often this page should be refreshed, enter a number in the text bo the **Set** button to the right of the text box.
Download Log File	Click this link to download log files you have created. You cannot download log files unt first created them.
Select	Check boxes that allow you to select files to be viewed or downloaded.
Process	Name of the process.
PID	ID number of the process.
%CPU	Percentage of processor time being used by the process.
Status	Task's process status: Running (R), Sleeping (S), Uninterruptible disk sleep (D), Zombie ((T), Paging (P)
Nice (Level)	Represents scheduling priority for the process. A nice value of 20 is the highest priority a lowest priority. The default nice value for most processes is 0.
Vm RSS (KB)	Resident set currently in physical memory in kilobytes, including Code, Data and Stack.
Vm Size (KB)	Size of virtual memory, in kilobytes.
Vm Data (KB)	Amount of data currently stored in virtual memory, in kilobytes.
Thread Count	Number of program threads currently running.

Field	Description
Data Stack (KB)	Size of the data stack, in kilobytes.
Page Fault Count	Number of major page faults the task has made requiring loading of memory.

Use the View Selected Processes page to view the selected processes and download the processes log files.

The following table describes the View Selected Processes page.

Table 129: View Selected Processes Page

Field	Description
Disable Auto-Refresh	Check this check box to disable auto-refresh of the information displayed on this page.
Refresh Rate	To specify in seconds how often this page should be refreshed, enter a number in the text box, then click the **Set** button to the right of the text box.
View All Processes button	Returns you to the previous Processes screen, which displays all running processes.
Start Log button	Creates a log of the selected processes displayed on this page.
Download Log File link	Download the selected processes log file.
Processes	This section displays the details of the selected processes. The details are the same as those listed in Table 128: Processes Page , on page 521.

Related Topics

Use Processes Tool , on page 200

Disk Usage

The Disk Usage page appears when you choose **System Monitor** > **Disk Usage**.

Authorization Requirements

You must have serviceability authority to access this page.

Description

Use the Disk Usage page to list the percentage of disk space used by the different partitions in the system.

Note Use the Up and Down arrows next to each column heading on the Disk Usage page to sort the information by each category.

The following table describes the Disk Usage page.

Table 130: Disk Usage Page

Field	Description
Disk Usage Details	
Partition	Name of the partition.
Size	Size of the partition.
Percentage Used	How much disk space is the partition using, as a percentage of total allocated disk space.
Available Space	How much disk space is currently available on the partition.
Used Space	How much disk space is the partition using.

Related Topics

Use Disk Usage Tool , on page 201

System Logs Menu

The System Logs menu contains the following submenus, under which all system logs are grouped:

- **System Logs** > **CER Logs**
- **System Logs** > **Platform Logs**
- **System Logs** > **DB Logs**
- **System Logs** > **CLI Output Files**
- **System Logs** > **SLM Logs**

Authorization Requirements

You must have serviceability authority to access the System Logs pages.

Note Use the Up and Down arrows next to each column heading to sort the information by each category.

The following table describes the System Logs pages.

Table 131: General Description of System Logs Pages

Field	Description
Download button	Download the selected log files. You must first select the file to be downloaded. To do so, to the left of the File Name. If you click the box to the left of the File Name column head are selected for download. **Note** If you select multiple log files, the system creates a Zip file that contains the be downloaded.

Field	Description
File Name	Name of the log file. If you click the file name, the contents of the log file display on a new s **Note** After viewing the contents, click the **Back** button in your browser to return to the page.
Reload Log File button	Reloads the log file currently being viewed, so that any updates can be seen. **Note** This button is only available when you have clicked a file name and are viewing contents of particular log file.
Last Modified	Date the log file was last modified.
File Size (KB)	Size of the log file, in kilobytes.

Table 132: Descriptions of Individual System Log File Pages

Menu/Log File Page	Description
CER Logs > CER Admin	View or download Emergency Responder Admin logs.
CER Logs > CER Server	View or download Emergency Responder Server logs.
CER Logs > CER Phone Tracking	View or download Emergency Responder Phone Tracking logs.
CER Logs > CER Audit	View or download Emergency Responder audit logs.
CER Logs> CER API Services	View or download API service logs.
CER Logs > JTAPI	View or download JTAPI logs.
CER Logs > Tomcat	View or download Tomcat logs.
CER Logs > Event Viewer	View or download Emergency Responder Event logs.
CER Logs > Audio Driver	View or download Emergency Responder Audio Driver logs.
CER Logs > Detailed Logs	View or download Emergency Responder detailed logs.
Platform Logs > CLI	View or download CLI operations logs.
Platform Logs > CLM	View or download CLM (Cluster Manager) logs.
Platform Logs > Certificate Management/IPSec	View or download Certificate Management and IPSec logs.
Platform Logs > DRS	View or download DRS (Disaster Recovery System) logs.
Platform Logs > Install/Upgrade	View or download Installation and Upgrade logs.
Platform Logs > Remote Support	View or download Remote Account creation and operations logs.
Platform Logs > Syslog	View or download Syslog logs.
Platform Logs > Servm	View or download Servm (Services Manager) logs.

Menu/Log File Page	Description
DB Logs > Cerdbmon	View or download Cerdbmon logs.
DB Logs > Install DB	View or download InstallDB Utility logs.
CLI OutputFiles >Platform	View or download Platform log files.
CLI OutputFiles > DB	View or download DB log files.
SLM Logs > SLM	View or download SLM log files.
SLM Logs > GCH	View or download GCH log files.
SLM Logs > TP	View or download TP log files.

Related Topics

Use Emergency Responder Logs , on page 201

APPENDIX D

Cisco Unified Operating System Administration Web Interface

ServerGroup

The ServerGroup page appears when you choose **Show** > **ServerGroup**.

Authorization Requirements

You must have platform administrator authority to access this page.

Description

Use the ServerGroup page to view information about the Emergency Responder servers in the server group.

The following table describes the ServerGroup page.

Table 133: ServerGroup Page

Field	Description
ServerGroup	
Hostname	Displays the name of the host.
IP Address	Displays the IP address of the host.
Alias	Displays the alias of the host
Type of Node	Displays the node type of the host.
Database Replication	Displays the name of the database which will either be a Publisher or Subscriber.

Related Topics

View Hardware Status , on page 207

Hardware Status

The Hardware Status page appears when you choose **Show** > **Hardware**.

Authorization Requirements

You must have platform administrator authority to access this page.

Description

Use the Hardware Status page to view information about the Emergency Responder hardware.

The following table describes the Hardware Status page.

Table 134: Hardware Status Page

Field	Description
Hardware Resources	
Platform Type	Model identity of the platform server
Serial Number	Displays serial number of the virtual machine.
Virtual Hardware	Shows you the status as “Configured” if the hardware is a virtual machine.
Virtual Support	Shows you the status as “Supported” if the support is on a virtual machine.
Processor Speed	Speed of the processor

Field	Description
CPU Type	Type of processor in the platform server
Memory	Total amount of memory in Mbytes
Object ID	Object ID of the platform server
OS Version	Operating system version running on the platform server
RAID Details	Detailed summary of the platform hardware

Related Topics

View Hardware Status , on page 207

Network Configuration

The Network Configuration page appears when you choose **Show** > **Network**.

Authorization Requirements

You must have platform administrator authority to access this page.

Description

Use the Network Configuration page to view information about the network settings.

Note The network status information that displays depends on whether Network Fault Tolerance is enabled. When Network Fault Tolerance is enabled, Ethernet port 1 automatically takes over network communications if Ethernet port 0 fails. If Network Fault Tolerance is enabled, network status information displays for the network ports Ethernet 0, Ethernet 1, and Bond 0. If Network Fault Tolerance is not enabled, status information displays only for Ethernet 0.

The following table describes the Network Configuration page.

Table 135: Network Configuration Page

Field	Description
Ethernet Details	
DHCP Status	Indicates whether DHCP is enabled for Ethernet port 0.
Status	Indicates whether the port is Up or Down for Ethernet ports 0 and 1.
IP Address	Shows the IP address of Ethernet port 0 (and Ethernet port 1 if Network Fault Tolerance (NFT) is enabled).
IP Mask	Shows the IP mask of Ethernet port 0 (and Ethernet port 1 if NFT is enabled).
Link Detected	Indicates whether there is an active link.

Field	Description
Queue Length	Displays the length of the queue.
MTU	Displays the maximum transmission unit.
MAC Address	Displays the hardware address of the port.
RX Stats	Displays information about received bytes and packets.
TX Stats	Displays information about transmitted bytes and packets.
DNS Details	
Primary DNS	Displays the IP address of the primary domain name server.
Secondary DNS	Displays the IP address of the secondary domain name server.
Options	Displays the number of attempts and timeouts.
Domain	Displays the domain of the server.
Gateway	Displays the IP address of the network gateway on Ethernet port 0.

Related Topics

View Network Status , on page 208

Software Packages

The Software Packages page appears when you choose **Show** > **Software**.

Authorization Requirements

You must have platform administrator authority to access this page.

Description

Use the Software Packages page to view the software versions and installed software options.

The following table describes the Software Packages page.

Table 136: Software Packages Page

Field	Description
Partition Versions	Displays the software version that is running on the active and inactive partitions.
Active Version Installed Software Options	Displays the versions of installed software options that are installed on the active version.
Inactive Version Installed Software Options	Displays the versions of installed software options that are installed on the inactive version.

Field	Description
Installed Software Options	Displays the cop file installed on the system.

Related Topics

View Installed Software , on page 208

System Status

The System Status page appears when you choose **Show** > **System**.

Authorization Requirements

You must have platform administrator authority to access this page.

Description

Use the System Status page to view the status of the Emergency Responder system.

The following table describes the System Status page.

Table 137: System Status Page

Field	Description
Host Name	Name of the Cisco UCS host where the Emergency Responder system is installed.
Date	Date and time based on the continent and region that were specified during operating system installation.
Time Zone	Time zone that was chosen during installation.
Locale	Locale of the system.
Product Version	Operating system version.
Uptime	Displays system uptime information.
CPU	Displays the percentage of CPU capacity that is idle, the percentage that is running system processes, and the percentage that is running user processes.
Memory	Displays information about memory usage, including the amount of total memory, free memory, and used memory in kilobytes.
Disk/active	Displays the amount of total, free, and used disk space on the active disk.
Disk/inactive	Displays the amount of total, free, and used disk space on the inactive disk.
Disk/logging	Displays the amount of total, free, and disk space that is used for disk logging.

Related Topics

View System Status, on page 208

IP Preferences

The IP Preferences page appears when you choose **Show** > **IP Preferences**.

Authorization Requirements

You must have platform administrator authority to access this page.

Description

Use the IP Preferences page to view a list of registered ports that can be used by the system. The following table describes the IP Preferences page.

Table 138: IP Preferences Page

Field	Description
Application	Name of the application using (listening on) the port.
Protocol	Protocol used on this port (TCP, UDP, and so on).
Port Number	Numeric port number.
Type	Type of traffic allowed on this port: • Public—All traffic allowed. • Translated—All traffic allowed but forwarded to a different port. • Private—Traffic only allowed from a defined set of remote servers, for example, other servers in the server group.
Translated Port	Traffic destined for this port get forwarded to the port listed in the Port Number column. This field applies to Translated type ports only.
Status	Status of port usage: • Enabled—In use by the application and opened by the firewall. • Disabled—Blocked by the firewall and not in use.
Description	Brief description of how the port is used.

Related Topics

View IP Preferences , on page 209

Ethernet Configuration

The Ethernet Configuration page appears when you choose **Settings** > **IP** > **Ethernet**.

Authorization Requirements

You must have platform administrator authority to access this page.

Description

Use the Ethernet Configuration page to view or change Ethernet settings.

Note All Ethernet settings apply only to Eth0. You can't configure any settings for Eth1. The maximum transmission unit (MTU) on Eth0 defaults to 1500.

Note From Release 14SU2 onwards, the tomcat and tomcat-ecdsa certificates should be exchanged between the publisher and subscriber nodes before and after changing the IP address/hostname.

The following table describes the Ethernet Configuration page.

Table 139: Ethernet Configuration Page

Field	Description
DHCP Information	
DHCP	Indicates whether DHCP is enabled or disabled and allows you to change the DHCP setting using the pull-down menu.
Host Information	
Hostname	Displays the hostname of the node.
Port Information	
IP Address	Displays the IP address of the system. You can change the IP address by entering a new IP address in the text box.
Subnet Mask	Displays the IP subnet mask address. You can change the mask by entering a new subnet mask in the text box.
Gateway Information	
Default Gateway	Displays the IP address of the default network gateway. You can change the gateway IP address by entering a new IP address in the text box.
Save button or icon	Saves any changes made to the Ethernet Configuration page. **Caution** If you click **Save**, the machine reboots. Don't click **Save** unless you want to shut down and reboot your system. **Note** To recognize any new IP addresses, both servers in the server group must be manually rebooted.

Related Topics

Set Up Ethernet Settings , on page 209

Ethernet IPv6 Configuration

Use the **Settings** > **IP** > **Enternet IPv6** menu to enable and configure IPv6 on the node.

Note All Ethernet settings apply only to Eth0. You cannot configure any settings for Eth1. The Maximum Transmission Unit (MTU) on Eth0 defaults to 1500.

Table 140: Ethernet IPv6 Configuration Page

Field	Description
Enable IPv6	Check this check box to enable IPv6 on the node.
Router Advertisement	Choose one of the following IP address sources: • Router Advertisement • DHCP • Manual Entry The three IP address sources are mutually exclusive. **Note** Unless you specify Manual Entry, IPv6 Address, Prefix Length, and Default Gateway fields remain read only.
IPv6 Address	If you chose Manual Entry, enter the IPv6 address of the node. For example, fd6:2:6:96:21e:bff:fecc:2e3a.
Prefix Length	If you chose Manual Entry, enter the prefix length. For example, 64.
Default Gateway	If you chose Manual Entry, enter the default gateway. For example, fe80::3ece:73ff:fea9:c641.
Update with Reboot	If you want the system to reboot immediately after you click Save, check this check box. If you want to reboot later, leave the check box blank. **Note** If you check the Update with Reboot check box, the system reboots after you click Save. For the IPv6 settings to take effect, reboot the system.

Publisher Settings

The Publisher Settings page appears when you choose **Settings** > **IP** > **Publisher.**

Authorization Requirements

You must have platform administrator authority to access this page.

Description

Use the Publisher Settings page to view or change the Publisher hostname or IP address.

Note You can only view and change the publisher hostname IP address only on the Emergency Responder Subscriber, not on the Emergency Responder publisher itself. Changing these fields must be followed by an immediate reboot of the Subscriber.

Table 141: Publisher Settings Page

Field	Description
Hostname	Displays the hostnames of the Emergency Responder Publisher for this Subscriber. To cha hostname, enter the new hostname in the text box, and click **Save**.
IP Address	Displays the IP address of the Emergency Responder Publisher for this Subscriber. To cha address, enter the IP address in the text box, and click **Save**.
Save button or icon	Saves the information in the Publisher Configuration Settings page.

Related Topics

Change IP Addresses for Emergency Responder Servers , on page 212

NTP Server List

The NTP Server List page appears when you choose **Settings** > **NTP Servers**.

Authorization Requirements

You must have platform administrator authority to access this page.

Description

Use the NTP Server List page to add, modify, or delete an NTP server. You can only configure the NTP server settings on the Publisher.

Note Ensure that the external NTP server is stratum 9 or higher (1 to 9).

Note Any change you make to the NTP servers can take up to five minutes to complete. Whenever you make any change to the NTP servers, you must refresh the page to display the correct status.

Caution If you add, modify, or delete an NTP server, you must reboot both the Publisher and the Subscriber.

The following table describes the NTP Server List page.

Table 142: NTP Server List Page

Field	Description
Status	Displays how many configured NTP server were found.
NTP Server	
Hostname or IP Address field	Displays the hostnames or IP addresses of the configured NTP servers. To change a hostnam address, click it, enter the new hostname or IP address, and click **Save**.
Add New button or icon	Adds a new NTP server. After you click **Add New**, enter the hostname of IP address of the n server and click **Save**.
Select All button or icon	Selects all NTP servers listed. When you click this button or icon, a check mark appears in th to the left of each NTP hostname or IP address and to the left of the Hostname or IP Address heading. **Note** The Select All button or icon is only visible if you have previously configured one NTP servers.
Clear All button or icon	Deselects all NTP servers listed. When you click this button or icon, all check marks disappe **Note** The Clear All button or icon is only visible if you have previously configured one NTP servers.
Delete Selected button or icon	Deletes the selected NTP server. To delete an NTP server, you must first select it from the lis servers. Click the box to the left of the NTP server name to select it. To select all listed NTP s click the box to the left of the Hostname or IP Address column heading or click **Select All**. **Note** The Delete Selected button or icon is only visible if you have previously configu or more NTP servers.

The following table describes the NTP Server Configuration page.

Table 143: NTP Server Configuration Page

Field	Description
Status	Displays how many configured NTP server were found.
NTP Server Settings	
Hostname or IP Address field	Displays the hostnames or IP addresses of the configured NTP servers. To change a hostnam address, click it, enter the new hostname or IP address, and click **Save**.
Save button or icon	Saves the information about the new NTP server.

Related Topics

Set Up NTP Servers , on page 210

SMTP Settings

The SMTP Settings page appears when you choose **Settings** > **SMTP**.

Authorization Requirements

You must have platform administrator authority to access this page.

Description

Use the SMTP Settings page to manually configure the SMTP host.

The following table describes the SMTP Settings page.

Table 144: SMTP Settings Page

Field	Description
Status	Displays the status of the SMTP Settings page.
SMTP Host	
Hostname or IP Address	Enter the hostname or IP address of the SMTP server in the text box.
Host Status	Displays the status of the SMTP host server.
Save button or icon	Saves changes made to the SMTP Settings page.

Related Topics

Set Up SNMPv2, on page 149

Time Settings

The Time Settings page appears when you choose **Settings** > **Time**.

Authorization Requirements

You must have platform administrator authority to access this page.

Description

Use the Time Settings page to manually configure the server time.

Note Before you can manually configure the server time, you must delete any NTP servers that you have configured. See NTP Server List, on page 535 for more information.

Caution If you change the server time, you must reboot both the Publisher and the Subscriber.

The following table describes the Time Settings page.

Table 145: Time Settings Page

Field	Description
Date	Allows you to set the month, day, year, hours, minutes, and seconds using the pull-down menus.
Save button or icon	Saves changes made to the Time Settings page.

Related Topics

NTP Server List, on page 535
Set Up NTP Servers , on page 210
Set Up Time Settings , on page 211

Version Settings

The Version Settings page appears when you choose **Settings** > **Version**.

Authorization Requirements

You must have platform administrator authority to access this page.

Description

Use the Version Settings page to restart or shutdown the system and to switch software versions.

Note You must have a different software version installed on the inactive partition to switch versions.

Caution Initiating this action causes the system to restart and become temporarily unavailable.

The following table describes the Version Settings page.

Table 146: Version Settings Page

Field	Description
Status	Displays the current status.
Installed Versions	
Active Version	Displays the version running on the active partition.

Field	Description
Inactive Version	Display the version on the inactive partition.
Restart button or icon	Restarts the system.
Shutdown button or icon	Shuts down the system.
Switch Versions button or icon	Actives the software version on the inactive partition. **Note** The Switch Versions button or icon is only visible if there is a software version installed on the inactive partition.

Related Topics

Manage Software Versions , on page 211

Certificate Management

The Certificate List page appears when you choose **Security** > **Certificate Management**.

Authorization Requirements

You must have platform administrator authority to access this page.

Description

Use the Certificate Management page to do the following:

- Search for existing certificates
- Generate a new certificates
- Upload a certificate
- Upload a CTL
- Generate a CSR

Note From Release 14SU2 onwards, the tomcat and tomcat-ecdsa certificates should be exchanged between the publisher and subscriber nodes before and after changing the IP address/hostname.

Note From Release 14SU3 onwards, Multi-server(SAN) is also supported in Emergency Responder. To generate Certificate Signing Request or Self-signed Certificates for Multi-server(SAN), Tomcat and Tomcat-ECDSA self-signed certs has to be exchanged first between the publisher and subscriber nodes.

The following table describes the Certificate List page.

Table 147: Certificate List Page

Field	Description
Status	Displays the current status.
Certificate List	
Find certificate list where	Enter search criteria for the certificate lists you want to find. To find all certificate lists by file name, select File Name from the pull-down menu and click **Find** without entering any criteria. To find all certificate lists by certificate name, select Certificate Name from the pull-down menu and click **Find** without entering any criteria. To narrow your search: • Select the search relationship (begins with, contains, and so on) from the pull-down menu, and enter the search string in the text box. • To search on a combination of fields, click the **Plus** icon **(+)** to add additional search parameters. Click the **Minus** icon (–) to remove search parameters. Click **Clear Filter** to remove all additional search parameters. • Use the Rows per Page pull-down menu to select how many rows are displayed per page. When you have entered all of the search parameters, click **Find**. If the search finds existing certificates, the information about the certificates (File Name, Certificate Name, and Certificate Type) displays in the Certificate List. Click the File Name link to display the Certificate Configuration page. See Table 154: Certificate Configuration Page , on page 545 for information about the Certificate Configuration Page.
Generate New button or icon	Allows you to generate a new certificate. When you click **Generate New**, the Generate Certificate page appears. See Table 148: Generate New Self-signed Certificate Page , on page 541 for a description of the Generate Certificate page.
Upload Certificate button or icon	Allows you to upload a certificate from a remote server. When you click **Upload Certificate**, the Upload Certificate page appears. See Table 149: Upload Certificate Page , on page 542 for a description of the Upload Certificate page.
Upload CTL button or icon	Allows you to upload a Certificate Trust List (CTL) from a remote server. When you click **Upload CTL**, the Upload Certificate Trust List page appears. See Table 150: Upload CTL Page , on page 542 for a description of the Upload Certificate Trust List page.
Generate CSR button or icon	Allows you to generate a new Certificate Signing Request (CSR). When you click **Generate CSR**, the Generate Certificate Signing Request page appears. See Table 152: Generate CSR Page , on page 544 for a description of the Generate New page.

Field	Description
Download CSR button or icon	Allows you to download a CSR. When you click **Download CSR**, the Download Certificate Signing Request page appears. See Table 153: Download CSR Page , on page 545 for a description of the Download Certificate Signing Request page.

The following table describes the Generate New Self-signed Certificate page.

Table 148: Generate New Self-signed Certificate Page

Field	Description
Status	Displays the current status of the Generate New Self-signed Certificate page.
Generate Self-signed	
Certificate Purpose	Choose the required option from the drop-down list. When you choose any of the following options, the **Key Type** field is automatically set to **RSA**. • tomcat • ipsec When you choose any of the following options, the **Key Type** field is automatically set to **EC** (Elliptical Curve). • tomcat-ECDSA
Distribution	Choose a Emergency Responder server from the drop-down list.
Common / Common Name_SerialNumber	Displays the name of the Emergency Responder server that you have chosen using the **Distribution** drop-down list.
Auto-populated Domains	Appears only if you have chosen any of the following options using the **Certificate Purpose** drop-down list. • tomcat-ECDSA
Key Type	This field lists the type of keys used for encryption and decryption of the public-private key pair. Emergency Responder supports EC and RSA key types.
Key Length	Allows you to choose 2048, 3072, or 4096 from the drop-down list. **Note** Certificates with a key length value of 256, 384, or 521 are chosen only for ECDSA certificates. These options are not available for RSA certificates. • If the key length value is 2048, 3072, or 4096, the supported hash algorithm is SHA256. • If the key length value is 256, 384, or 521, the supported hash algorithms are SHA384 or SHA512.

Field	Description
Hash Algorithm	Choose a value that is greater than or equal to the key length from the drop-down list: **Note** The values in the **Hash Algorithm** drop-down list changes based on the value you have chosen in the **Key Length** field. If your system is running in FIPS mode, it is mandatory to choose SHA256 as the hashing algorithm.
Generate button	Generates a new certificate. You must first select a Certificate Name from the pull-down menu.
Close button	Closes the Generate New Self-signed Certificate page.

The following table describes the Upload Certificate page.

Table 149: Upload Certificate Page

Field	Description
Status	Displays the current status of the Upload Certificate page.
Upload Certificate	
Certificate Name	Use the pull-down menu to select the name of the certificate to upload.
Root Certificate	Enter the name of the root certificate.
Upload File	Use the Browse button to select the file to be uploaded.
Upload File button or icon	Uploads the certificate file specified in the Upload Certificate section.
Close button or icon	Closes the Update Certificate page.

The following table describes the Upload CTL page.

Table 150: Upload CTL Page

Field	Description
Status	Displays the current status of the Upload CTL page.
Upload Certificate	
Certificate Name	Use the pull-down menu to select the name of the CTL file to upload.
Root Certificate	Enter the name of the root certificate.
Upload File	Use the Browse button to select the file to be uploaded.
Upload File button or icon	Uploads the certificate file specified in the Upload Certificate Trust List section.
Close button or icon	Closes the Update CTL page.

The following table lists the Certificate Signing Request Fields.

Table 151: Certificate Signing Request Fields

Field	Description
Certificate Purpose	From the drop-down list, select a value: • **Tomcat** • **Tomcat-ECDSA** • **IPSec** **Note** ITLRecovery and Authz certificates aren't supported in Emergency Responder.
Distribution	Select a Emergency Responder server. When you select this field for multiserver for ECDSA, the syntax is: `Tomcat-ECDSA common name: <host-name>-EC-ms.<domain>`
Common Name / Common Name_SerialNumber	Displays the common name or the common name appended with the serial number of the certificate. Common Name or Common Name_SerialNumber is the file name of the certificate. Shows the name of the Unified Communications Manager application that you selected in the **Distribution** field by default.
Auto-populated Domains	This field appears in Subject Alternate Names (SANs) section. It lists the host names that are to be protected by a single certificate.
Parent Domain	This field appears in Subject Alternate Names (SANs) section. It shows the default domain name. You can modify the domain name, if required.
Key Type	This field identifies the type of key used for encryption and decryption for the public-private key pair.

Field	Description
Key Length	From the **Key Length** drop-down list, select one of the values. Depending on the key length, the CSR request limits the hash algorithm choices. By having the limited hash algorithm choices, you can use a hash algorithm strength that is greater than or equal to the key length strength. For example, for a key length of 256, the supported hash algorithms are SHA256, SHA384, or SHA512. Similarly, for the key length of 384, the supported hash algorithms are SHA384 or SHA512. **Note** Certificates with a **key length** value of 3072 or 4096 can only be selected for RSA certificates. These options aren't available for ECDSA certificates. **Note** Some phone models may fail to register if the RSA **key length** selected for the CallManager **Certificate Purpose** is greater than 2048. From the Unified CM Phone Feature List Report on the Cisco Unified Reporting Tool (CURT), you can check the **3072/4096 RSA key size support** feature for the list of supported phone models.
Hash Algorithm	Select a value from the **Hash Algorithm** drop-down list to have stronger hash algorithm as the elliptical curve key length. From the **Hash Algorithm** drop-down list, select one of the values. **Note** • The values for the **Hash Algorithm** field change based on the value you select in the **Key Length** field. • If your system is running on FIPS mode, it's mandatory that you select SHA256 as the hashing algorithm.

The following table describes the Generate CSR page.

Table 152: Generate CSR Page

Field	Description
Status	Displays the current status of the Generate CSR page.
Generate Certificate Signing Request	
Certificate Name	Use the pull-down menu to select the name of the CTL file to generate.
Generate CSR button or icon	Generates a new CSR.
Close button or icon	Close the Generate CSR page.

The following table describes the Download CSR page.

Table 153: Download CSR Page

Field	Description
Status	Displays the current status of the Download CSR page.
Download Certificate Signing Request	
Certificate Name	Use the pull-down menu to select the name of the CTL file to download.
Download CSR button or icon	Downloads the CSR specified in the Download Certificate Signing Request section.
Close button or icon	Closes the Download CSR page.

The following table describes the Certificate Configuration page.

Table 154: Certificate Configuration Page

Field	Description
Status	Displays the current status of the Certificate Configuration page.
Certificate Settings	Displays the following information about the certificate: • File Name • Certificate Name • Certificate Type • Certificate Group • Description
Certificate File Data	Displays the contents of the certificate file.
Delete button or icon	Deletes the current certificate.
Download button or icon	Downloads the certificate to your local system.

Related Topics

Certificate Management, on page 214

Certificate Monitor

The Certificate Monitor page appears when you choose **Security** > **Certificate Monitor**.

Authorization Requirements

You must have platform administrator authority to access this page.

Description

Use the Certificate Monitor page to do the following:

- Specify the start time
- Specify the frequency
- Enable email notification and provide email addresses of those to be notified

The following table describes the Certificate Monitor page.

Table 155: Certificate Monitor Page

Field	Description
Status	Displays the current status of the Certificate Monitor page.
Certificate Monitor Configuration	
Notification Start Time	Enter the number of days before the certificate expires that you want to be notified.
Notification Frequency	Enter the notification frequency and click one of the radio buttons to indicate days or hours.
Enable Email Notification	Check the box to the enable email notification. **Note** For the system to send notifications, you must configure an SMTP host.
Email ID	Enter the email addresses of those to be notified in the text box. Enter multiple e-mail addresses by separating each address with a semicolon (;). There should be no spaces between the email addresses.
Save button or icon	Saves the information entered on the Certificate Monitor page.

Related Topics

Certificate Management, on page 214

IPSec Policy List

The IPSec Policy List page appears when you choose **Security** > **IPSec Configuration**.

Authorization Requirements

You must have platform administrator authority to access this page.

Description

Use the IPSec Policy List page to display existing IPSec policies, add an additional IPSec policy, or modify an existing IPSec policy.

The following table describes the IPSec Policy List page.

Table 156: IPSec Policy List Page

Field	Description
Status	Displays the current status of the IPSec Policy List page.
IPSec Policy List	Displays the currently configured IPSec policies. Click on the Policy Name link to IPSec Policy Configuration page for that policy.
Add New button or icon	Adds a new IPSec policy. When you click **Add New**, the IPSec Policy Configuration page appears. See Table 157: IPSec Policy Configuration Page, on page 547 for information about the IPSec Policy Configuration page.

The following table describes the IPSec Policy Configuration page in Non Federal Information Processing Standard (Non FIPS) Mode.

Table 157: IPSec Policy Configuration Page

Field	Description
Status	Displays the current status of the IPSec Policy Configuration page.
IPSec Policy Details	
Policy Group Name	Specifies the name of the IPSec policy group.
Policy Name	Specifies the name of the IPSec policy.
Authentication Method	Specifies the authentication method. The Authentication Method field has two options Preshared Key and Certificate. If Preshared Key is selected, the Preshared Key field is editable and the Peer Type and Certificate Name fields are disabled. If Certificate is selected, the Preshared Key field is disabled. The Peer Type and Certificate Name fields are enabled.
Preshared Key	Specifies the preshared key if you selected Pre-shared Key in the Authentication Method field.
Peer Type	Specifies that the peer type is different.
Certificate Name	Specifies the certificate name.
Destination Address	Specifies the IP address of the destination (FQDN is not supported).
Destination Port	Enter the port number at the destination.
Source Address	Specifies the IP address of the source (FQDN is not supported).
Source Port	Specifies the port number at the source.
Mode	Select the Transport mode.
Remote Port	Specifies the port number to use at the destination.

Field	Description
Protocol	Specifies the specific protocol, or Any: • TCP • UDP • Any
Encryption Algorithm	From the drop-down list, choose the encryption algorithm. Choices include: • 3DES • AES 128 • AES 256
Hash Algorithm	Specifies the hash algorithm: • SHA1 • SHA256
ESP Algorithm	From the drop-down list, choose the ESP algorithm. Choices include: • 3DES • AES 128 • AES 256
Phase 1 DH Group	
Phase One Life Time	Specifies the lifetime for phase One, IKE negotiation, in seconds.
Phase One DH	From the drop-down list, choose the phase One DH value. Choices include: 2, 5, 14, 15, 16, 17, and 18.
Phase 2 DH Group	
Phase Two Life Time	Specifies the lifetime for phase Two, IKE negotiation, in seconds.
Phase Two DH	From the drop-down list, choose the phase Two DH value. Choices include: 2, 5, 14, 16, 17, and 18.
IPSec Policy Configuration	
Enable Policy	Check the check box to enable the policy.
Save button or icon	Saves the changes made to the IPSec Policy List page.

The following table lists the field names that are displayed when the system is in FIPS Mode or ESM Mode.

Note In case you’re planning to upgrade to Release 15, note that the IPSec policy with 3DES Algorithm isn't supported in FIPS mode. You must delete and recreate the IPSec policy with the Encryption and ESP Algorithms other than 3DES in both the nodes between which the IPSec tunnel is to be established, and then plan an upgrade or migration.

When you enable FIPS mode in Emergency Responder Release 15, the 3DES algorithm is not supported for IPSec communication. If you have already configured the IPSec policies with ESP and Encryption Algorithm as 3DES and enabled FIPS mode, the upgrade to Emergency Responder Release 15 is blocked.

Table 158: IPSec Policy Configuration Page

Field	Description
Status	Displays the current status of the IPSec Policy Configuration page.
IPSec Policy Details	
Policy Group Name	Specifies the name of the IPSec policy group.
Policy Name	Specifies the name of the IPSec policy.
Authentication Method	Specifies the authentication method. By default, certificate is selected. **Note** Preshared key is not present in FIPS Mode.
Peer Type	Specifies the peer type is different.
Certificate Name	The name of the certificate.
Destination Address	Specifies the IP address or FQDN of the destination.
Destination Port	Enter the port number at the destination.
Source Address	Specifies the IP address or FQDN of the source.
Source Port	Specifies the port number at the source.
Mode	Specifies the Transport mode.
Remote Port	Specifies the port number to use at the destination.
Protocol	Specifies the specific protocol, or Any: • TCP • UDP • Any
Encryption Algorithm	From the drop-down list, choose the encryption algorithm. Choices include: • AES 128 • AES 256

Field	Description
Hash Algorithm	Specifies the hash algorithm: • SHA1 • SHA256
ESP Algorithm	From the drop-down list, choose the ESP algorithm. Choices include: • AES 128 • AES 256
Phase 1 DH Group	
Phase One Life Time	Specifies the lifetime for phase One, IKE negotiation, in seconds.
Phase One DH	From the drop-down list, choose the phase One DH value. The choices are from 14 to 18.
Phase 2 DH Group	
Phase Two Life Time	Specifies the lifetime for phase Two, IKE negotiation, in seconds.
Phase Two DH	From the drop-down list, choose the phase Two DH value. The choices are from 14 to 18.
IPSec Policy Configuration	
Enable Policy	Check the check box to enable the policy.
Save button or icon	Saves the changes made to the IPSec Policy Configuration page.

Related Topics

IPsec Management , on page 219

Cipher Management

Cipher management enables you to control the set of security ciphers that is allowed for every TLS and SSH connection. Cipher management allows you to disable weaker ciphers and thus enable a minimum level of security.

The **Cipher Management** page has no default values. Instead, the Cipher Management feature takes effect only when you configure the allowed ciphers. Certain weak ciphers are never allowed, even if they are configured on the **Cipher Management** page.

For more details, see Cipher Restrictions, on page 556.

TLS Interfaces

The following table details the TLS interfaces fields:

Fields	Description
All TLS	The ciphers assigned in this field will apply on all server and client connections that support the TLS protocol.
HTTPS TLS	The cipher selection in this field will apply on all connections to Tomcat on ports 443 and 8443 that support the TLS protocol.
Cipher String	This field accepts an OpenSSL formatted cipher string that will apply to the designated interface. For more information about syntax, see the OpenSSL documentation at https://www.openssl.org/docs/manpages.html.
Cipher Expansion String	When you **Save** this page, this field shows the expansion of the configured ciphers in the field “Cipher String” for the respective interface.

For more details on how to configure the cipher string, see the “Cipher Management” section in the *Security Guide for Cisco Unified Communications Manager* at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

SSH Interfaces

The following table details the SSH interfaces fields:

Fields	Description
SSH Ciphers	The ciphers assigned in this field will apply to SSH connections.
Cipher String	This field accepts OpenSSH formatted cipher string. For more information about syntax, see the OpenSSH documentation at https://www.ssh.com/manuals/server-admin/44/Ciphers_and_MACs.html.
Cipher Expansion String	This field shows the expansion of the configured cipher in the field “Cipher String” for the SSH interface.
SSH Key Exchange	Key exchange algorithm configured here will be associated with the SSH Key Exchange interface on Emergency Responder.
Algorithm String	This field accepts OpenSSH formatted algorithm string. For more information about syntax, see the OpenSSH documentation at https://tools.ietf.org/id/draft-ietf-curdle-ssh-kex-sha2-09.html.

Fields	Description
Algorithm Expansion String	This field shows the expansion of the configured SSH Key algorithms in the field “Algorithm String” for the interface.
SSH MAC	MAC algorithm configured here will be associated with the SSH MAC interface on Emergency Responder.
Algorithm String	This field accepts OpenSSH formatted algorithm string. For more information about syntax, see the OpenSSH documentation at https://www.ssh.com/manuals/server-admin/44/Ciphers_and_MACs.html.
Algorithm Expansion String	This field shows the expansion of the configured MAC algorithm in the field “Algorithm String” for the SSH interface.

For more details on how to configure the cipher string, see the “Cipher Management” section in the *Security Guide for Cisco Unified Communications Manager* at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

Recommended Ciphers

Warning Ensure the ciphers configured include the recommended ciphers as listed below. Make sure that the ciphers configured are part of the recommended ciphers. Otherwise, you may encounter interoperability issues with other products over secure interfaces. After configuring the recommended ciphers, restart the affected services or reboot the server for the changes to take effect.

Warning Configuring hmac-sha2-512 in SSH MAC interface affects the DRS functionality.

Configuring ciphers aes128-gcm@openssh.com, aes256-gcm@openssh.com in "SSH Cipher's" field or configuring only ecdh-sha2-nistp256 algorithm in "SSH KEX" will break the DRS functionality.

We recommend the following cipher strings for the TLS and SSH interface configuration:

TLS

```
ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-SHA384:
ECDHE-RSA-AES256-SHA:AES256-GCM-SHA384:AES256-SHA256:AES256-SHA:
ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-SHA256:
ECDHE-RSA-AES128-SHA:AES128-GCM-SHA256:AES128-SHA256:AES128-SHA
```

SSH Ciphers

```
aes128-ctr,aes192-ctr,aes256-ctr
```

SSH MAC

```
hmac-sha1,hmac-sha2-256
```

SSH KEX for FIPS and Non-FIPS

```
diffie-hellman-group14-sha1,diffie-hellman-group16-sha512,diffie-hellman-group14-sha256,ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521
```

Cipher Limitations

Although the **Cipher Management** configuration page allows you to configure any number of ciphers, each application has a list of ciphers it supports on its interfaces. For example, **All TLS** interfaces may show ECDHE or DHE or ECDSA based ciphers, but an application such as Emergency Responder may not support these ciphers because EC curves or DHE algorithms are not enabled for this application's interfaces. See the "Application Ciphers Support" section below for a list of ciphers supported by individual application interfaces.

Validation in GUI

The ciphers on the **Cipher Management** page are validated according to the OpenSSL guidelines. For example, if a cipher configured is ALL:BAD:!MD5, the cipher string will be considered as valid although "BAD" is not a recognized cipher suite. OpenSSL considers this as a valid string. If AES128_SHA is configured instead of AES128-SHA (using an underscore instead of a hyphen) however, OpenSSL will identify this as an invalid cipher suite.

Application Ciphers Support

The following table represents the application interfaces and the all corresponding ciphers and algorithms that are supported on TLS and SSH interfaces:

Table 159: Emergency Responder Cipher Support for TLS Ciphers

Application / Process	Protocol	Port	Supported Ciphers
DRS	TCP / TLS	4040	`ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-SHA384:ECDHE-RSA-AES256-SHA:DHE-RSA-CAMELLIA256-SHA:AES256-GCM-SHA384:AES256-SHA256:AES256-SHA:CAMELLIA256-SHA:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-SHA256:ECDHE-RSA-AES128-SHA:DHE-RSA-CAMELLIA128-SHA:AES128-GCM-SHA256:AES128-SHA256:AES128-SHA:CAMELLIA128-SHA`

Application / Process	Protocol	Port	Supported Ciphers
Cisco Tomcat	TCP / TLS	8443 / 443	ECDHE-RSA-AES256-GCM-SHA384: ECDHE-RSA-AES256-SHA384: ECDHE-RSA-AES256-SHA: DHE-RSA-AES256-GCM-SHA384: DHE-RSA-AES256-SHA256: DHE-RSA-AES256-SHA: DHE-RSA-CAMELLIA256-SHA: AES256-GCM-SHA384:AES256-SHA256: AES256-SHA:CAMELLIA256-SHA: ECDHE-RSA-AES128-GCM-SHA256: ECDHE-RSA-AES128-SHA256: ECDHE-RSA-AES128-SHA: DHE-RSA-AES128-GCM-SHA256: DHE-RSA-AES128-SHA256: DHE-RSA-AES128-SHA: DHE-RSA-CAMELLIA128-SHA: AES128-GCM-SHA256:AES128-SHA256: AES128-SHA:CAMELLIA128-SHA: ECDHE-RSA-DES-CBC3-SHA: EDH-RSA-DES-CBC3-SHA: DES-CBC3-SHA ECDHE-ECDSA-AES256-GCM-SHA384: ECDHE-ECDSA-AES256-SHA384: ECDHE-ECDSA-AES256-SHA: ECDHE-ECDSA-AES128-GCM-SHA256: ECDHE-ECDSA-AES128-SHA256: ECDHE-ECDSA-AES128-SHA: ECDHE-ECDSA-DES-CBC3-SHA

Table 160: Cipher Support for SSH Ciphers

Service	Ciphers/Algorithms
SSH Server	• Ciphers: aes128-ctr aes192-ctr aes256-ctr aes128-gcm@openssh.com aes256-gcm@openssh.com • MAC algorithms: hmac-sha2-256 hmac-sha1 • Kex algorithms: ecdh-sha2-nistp521 ecdh-sha2-nistp384 ecdh-sha2-nistp256 diffie-hellman-group14-sha1 diffie-hellman-group1-sha1 diffie-hellman-group-exchange-sha256 diffie-hellman-group-exchange-sha1

Service	Ciphers/Algorithms
SSH Client	• Ciphers: aes128-ctr aes192-ctr aes256-ctr aes128-gcm@openssh.com aes256-gcm@openssh.com • MAC algorithms: hmac-sha2-256 hmac-sha1 • Kex algorithms: ecdh-sha2-nistp521 ecdh-sha2-nistp384 ecdh-sha2-nistp256 diffie-hellman-group14-sha1 diffie-hellman-group1-sha1 diffie-hellman-group-exchange-sha256 diffie-hellman-group-exchange-sha1
DRS Client	• Ciphers: aes256-ctr aes256-cbc aes128-ctr aes128-cbc aes256-ctr blowfish-cbc • MAC algorithms: hmac-md5 hmac-sha2-256 hmac-sha1 hmac-sha1-96 hmac-md5-96 • Kex algorithms: ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 diffie-hellman-group14-sha1 diffie-hellman-group1-sha1 diffie-hellman-group-exchange-sha256 diffie-hellman-group-exchange-sha1

Service	Ciphers/Algorithms

SFTP client	• Ciphers:
	`aes128-ctr`
	`aes192-ctr`
	`aes256-ctr`
	• MAC algorithms:
	`hmac-sha2-256`
	`hmac-sha1`
	• Kex algorithms:
	`ecdh-sha2-nistp521`
	`ecdh-sha2-nistp384`
	`diffie-hellman-group14-sha1`
	`diffie-hellman-group1-sha1`
	`diffie-hellman-group-exchange-sha256`
	`diffie-hellman-group-exchange-sha1`

Cipher Restrictions

The **Cipher Management** page allows configuration of any ciphers as supported by OpenSSL or OpenSSH. However, some of the ciphers are disabled internally based on the security standards of Cisco to avoid accidental exposure of critical data.

When you configure ciphers on the **Cipher Management** page, the following ciphers are disabled:

TLS Disabled Ciphers

```
EDH-RSA-DES-CBC-SHA:EDH-DSS-DES-CBC-SHA:ADH-DES-CBC-SHA:
DES-CBC-SHA:KRB5-DES-CBC-SHA:KRB5-DES-CBC-MD5:EXP-EDH-RSA-DES-CBC-SHA:
EXP-EDH-DSS-DES-CBC-SHA:EXP-ADH-DES-CBC-SHA:EXP-DES-CBC-SHA:EXP-RC2-CBC-MD5:
EXP-KRB5-RC2-CBC-SHA:EXP-KRB5-DES-CBC-SHA:EXP-KRB5-RC2-CBC-MD5:EXP-KRB5-DES-CBC-MD5:
EXP-ADH-RC4-MD5:EXP-RC4-MD5:EXP-KRB5-RC4-SHA:EXP-KRB5-RC4-MD5:ADH-AES256-GCM-SHA384:
ADH-AES256-SHA256:ADH-AES256-SHA:ADH-CAMELLIA256-SHA:ADH-AES128-GCM-SHA256:ADH-AES128-SHA256:
ADH-AES128-SHA:ADH-SEED-SHA:ADH-CAMELLIA128-SHA:ADH-DES-CBC3-SHA:ADH-RC4-MD5:
AECDH-AES256-SHA:AECDH-AES128-SHA:AECDH-DES-CBC3-SHA:AECDH-RC4-SHA:AECDH-NULL-SHA:
DES-CBC3-MD5:IDEA-CBC-MD5:RC2-CBC-MD5:RC4-MD5:ECDHE-RSA-RC4-SHA:ECDHE-ECDSA-RC4-SHA:
ECDH-RSA-RC4-SHA:ECDH-ECDSA-RC4-SHA:RC4-SHA:RC4-MD5:PSK-RC4-SHA:KRB5-RC4-SHA:
KRB5-RC4-MD5:IDEA-CBC-SHA:KRB5-IDEA-CBC-SHA:KRB5-IDEA-CBC-MD5:DHE-RSA-SEED-SHA:
DHE-DSS-SEED-SHA:SEED-SHA:KRB5-DES-CBC3-MD5:NULL-MD5:PSK-AES256-CBC-SHA:
PSK-AES128-CBC-SHA:PSK-3DES-EDE-CBC-SHA:ECDHE-RSA-NULL-SHA:ECDHE-ECDSA-NULL-SHA:
ECDH-RSA-NULL-SHA:ECDH-ECDSA-NULL-SHA:NULL-SHA256:NULL-SHA
```

SSH Disabled Ciphers

```
3des-cbc,aes128-cbc,aes192-cbc,aes256-cbc,rijndael-cbc@lysator.liu.se
```

SSH Disabled KEX Algorithms

```
curve25519-sha256@libssh.org,gss-gex-sha1-,gss-group1-sha1-,gss-group14-sha1-
```

SSH Disabled MAC Algorithms

```
hmac-sha1-etm@openssh.com,hmac-sha2-256-etm@openssh.com
```

Software Installation/Upgrade

The Software Installation/Upgrade page appears when you choose **Software Upgrades** > **Install/Upgrade**.

Authorization Requirements

You must have platform administrator authority to access this page.

Description

Use the Software Installation/Upgrade page to install or upgrade software from a DVD/CD or from a file system on a remote server.

The following table describes the Software Installation/Upgrade page.

Table 161: Software Installation/Upgrade Page

Field	Description
Status	Displays the current status of the Software Installation/Upgrade page.
Software Location	
Source	Pull-down menu used to specify the source for the installation/upgrade. Options are **DVD/C** **Filesystem**.
Directory	The name of the directory containing the files. **Note** If the upgrade file is on a Linux or Unix server, you must enter a forward slas beginning of the directory path that you want to specify. For example, if the u is in the **patches** directory, you must enter **/patches**. If the upgrade file is on server, check with your system administrator for the correct directory path.
Server	The hostname or IP address of the remote server from which the software is downloaded.
User Name	The name of a user who is configured on the remote server.
User Password	Password that is configured for this user on the remote server.
Transfer Protocol	Pull-down menu used to specify which transfer protocol to use. Options are **ftp** or **sftp**. **Note** These options are available only if you selected **Remote Filesystem** from the pull-down menu. If you selected **DVD/CD**, this pull-down menu is grayed ou
Cancel Install button or icon	Cancels the installation or upgrade procedure.
Next button or icon	Continues with the installation or upgrade procedure.

Branding

The **Branding** page appears when you choose **Software Upgrades** > **Branding**.

Authorization Requirements

You must have platform administrator authority to access this page.

Description

You can upload customized branding for Cisco Emergency Responder. Use the **Branding** page to upload the `branding.zip` folder which contains the “ CER” directory.

Once the `branding.zip` folder is uploaded successfully, you can enable or disable Branding using either the command line or graphical user interface and then refresh the page for the changes to take effect. For more information, refer to the “Branding” chapter.

The following table describes the Branding page.

Table 162: Branding Page

Field	Description
Status	Displays status of the **Branding** page.
Upload Branding File	
Browse	Click the **Browse** button to locate the `branding.zip` folder on the server.
Upload File	Click the **Upload File** button to upload the file to the server. It uploads the file successfully a validates the required contents of the `branding.zip` folder.
Enable Branding	After you have uploaded the `branding.zip` file, click this button to enable branding custo on this Cisco Emergency Responder node. After you enable branding, refresh your browser. **Note** Ensure that you use only one among GUI and CLI to enable branding as well as t it. For example, if you enable branding using the GUI interface, you must use th interface itself to disable branding. Else, it will not function properly.
Disable Branding	Click this button to disable customized branding from Cisco Emergency Responder. **Note** Ensure that you use only one among GUI and CLI to enable branding as well as t it. For example, if you enable branding using the GUI interface, you must use th interface itself to disable branding. Else, it will not function properly.

Related Topics

Branding File Requirements, on page 232
Enable Branding, on page 231

Ping Configuration

The Ping Configuration page appears when you choose **Services** > **Ping**.

Authorization Requirements

You must have platform administrator authority to access this page.

Description

Use the Ping Configuration page to send ping requests to test if other systems are reachable over the network.

The following table describes the Ping Configuration page.

Table 163: Ping Configuration Page

Field	Description
Status	Displays the current status of the Ping Configuration page.
Ping Settings	
Hostname or IP Address	Text box into which you enter the IP address or network name for the system that you want to ping.
Ping Interval	Text box in which you enter the amount of time between ping requests, in seconds.
Packet Size	Text box into which you enter the packet size of the ping request.
Ping iterations	Pull-down menu that allows you to choose the number of times you want to send ping requests to the other system. Available options are 1, 5, 25, or 100 times **Note** When you specify multiple pings, the **ping** command does not display the ping date and time in real time. Be aware that the **ping** command displays the data after the number of pings that you specified are complete.
Validate IPsec	Select the check box to have the system validate IPsec.
Ping Results	Text box in which the ping results are displayed.
Ping button or icon	Sends the ping request.

Related Topics

Ping Another System , on page 229

Remote Access Configuration

The Remote Access Configuration page appears when you choose **Services** > **Remote Support**.

Authorization Requirements

You must have platform administrator authority to access this page.

Description

Use the Remote Access Configuration page to set up a remote account that Cisco support personnel can use to access the system for a specified period of time. If the account duration limit expires, Cisco support can not access the remote support account.

When you establish a remote account, the system generates a pass phrase.

Follow this procedure to complete the remote account setup:

1. Call Cisco support and provide them with the remote support account name and pass phrase.
2. Cisco support enters the pass phrase into a decoder program that generates a password from the pass phrase.
3. Cisco support logs into the remote support account on the customer system by using the decoded password.

If you have not already created a remote account, when you navigate to the Remote Access Configuration page you can create a new account.

The following table describes the Remote Access Configuration page.

Table 164: Remote Access Configuration Page

Field	Description
Status	Displays the current status of the Remote Access Configuration page.
Remote Access Account Information	
Account Name	Name for the new remote account. Account names must be at least six-characters long and co all lowercase, alphabetic characters
Account Duration	The amount of time that the remote account exists, in days.
Save button or icon	Creates a new remote account. You must provide the Account Name and Account Duration be click **Add**. Remote Access Configuration page redisplays. See Table 165: Remote Access Conf Page , on page 560 for a description of the fields on the Remote Access Configuration page.
Delete button or icon	Deletes the currently configured remote account. **Note** The Delete button or icon is only visible if there is an existing remote account.

If you have already created a remote account, when you navigate to the Remote Access Configuration page you view and delete the remote account.

The following table describes the Remote Access Configuration page.

Table 165: Remote Access Configuration Page

Field	Description
Remote Access Account Information	
Account Name	Displays the name of the remote support account.
Expiration	Displays the date and time when access to the remote account expires.

Field	Description
Passphrase	Displays the generated pass phrase.
Decode Version	Indicates the version of the decoder in use.
Delete button or icon	Deletes the remote access account information.

Related Topics

Set Up Remote Support , on page 230

APPENDIX E

Disaster Recovery System Web Interface

Backup Device List

The Backup Device List page appears when you choose **Backup** > **Backup Device**.

Authorization Requirements

You must have platform administrator authority to access this page.

Description

Use the Backup Device List page to list, add, and delete backup devices.

The following table describes the Backup Device List page.

Table 166: Backup Device List Page

Field	Description
Backup Device List	Lists the configured backup devices and displays the Device Name, Device Type, and Device Path. Click on the Device Name link to bring up the Backup Device page for that device.
Add New button	Adds a new backup device. When you click the Add icon, the Backup Device page appears. See Table 167: Backup Device Page , on page 564 for information about the Backup Device page.
Select All button and icon	Selects all the listed backup devices.
Clear All button and icon	Deselects all selected backup devices.

Field	Description
Delete Selected button and icon	Deletes the selected backup devices.

The following table describes the Backup Device page, which you use to add new backup devices.

Table 167: Backup Device Page

Field	Description
Backup device name	Enter the device name in the text box (required).
Select Destination	To select the backup destination, click the **Tape Device** or **Network Directory** radio button (required).
Tape Device	Select the name of the tape device from the pull-down menu.
Network Directory	In the fields provided, enter the Server name, Path name, User name, and Password for the Network Directory.
Number of backups to store on the Network Directory	Select the number of backups using the pull-down menu.
Save button and icon	Saves the information about the new backup device.
Back button and icon	Returns to the Backup Device List page.

Related Topics

Add Backup Devices , on page 242

Schedule List

The Schedule List page appears when you choose **Backup** > **Scheduler**.

Authorization Requirements

You must have platform administrator authority to access this page.

Description

Use the Schedule List page to list currently scheduled backups, to add new schedules, to enable schedules, and to disable schedules. You can schedule a backup to start at a specified date and time and configure it either to run once or at a specified frequency, as well as specifying the features to be backed up.

The following table describes the Schedule List page.

Table 168: Schedule List Page

Field	Description
Schedule List	Lists all scheduled backups. Displays the Schedule List name, the Device Path, and the Sch Click the Schedule List name link to view the details of that schedule. **Note** After you have created a scheduled backup, you must enable the schedule. To the schedule in the Schedule List and click the **Enable Selected Schedules** bu
Add New button or icon	Adds a new schedule. When you click the Add button or icon, the Scheduler page appear 167: Backup Device Page , on page 564 for information about the Scheduler page.
Select All button or icon	Selects all the listed schedules. **Note** The Select All button only appears if no schedules have been configured.
Clear All button or icon	Deselects all selected schedules. **Note** The Clear All button only appears if no schedules have been configured.
Delete Selected button or icon	Deletes the selected schedules. **Note** The Delete Selected button only appears if no schedules have been configure
Enable Selected Schedules button or icon	Enables the selected schedules. **Note** The Enable Selected Schedules icon only appears if no schedules have been
Disable Selected Schedules button or icon	Disables the selected schedules. **Note** The Disable Selected Schedules button only appears if no schedules have been

The following table describes the Scheduler page.

Table 169: Scheduler Page

Field	Description
Status	Displays the status of the Scheduler page.
Schedule Name	Enter the name of the schedule in the text box.
Select Backup Device	Select the name of the backup device from the pull-down menu.
Select Features	Select **Emergency Responder** as the feature to be backed up.
Start Backup at	
Date	From the pull-down menus, enter the year, month, and day on which the backup sta
Time	From the pull-down menus, enter the hour and minute at which the backup starts.
Frequency	

Field	Description
Once	Click this radio button to schedule a single backup.
Daily	Click this radio button to schedule a daily backup.
Weekly	Click this radio button to schedule a weekly backup. Check the check boxes to specify on which the weekly backup is scheduled.
Monthly	Click this radio button to schedule a monthly backup.
Save button or icon	Saves the backup schedule information.
Set Default button or icon	Saves the information entered as the default for scheduled backups.
Disable Schedule button or icon	Disables the Schedule. If the Schedule is currently disabled, this button is grayed out.
Enable Schedule button or icon	Enables the Schedule. If the Schedule is currently enabled, this button is grayed out.
Back button or icon	Returns to the Scheduler List page.

Related Topics

Backup History and Restore History, on page 567

Backup Status, on page 569

Create and Edit Backup Schedules , on page 243

Manage Backup Schedules , on page 244

Manual Backup

The Manual Backup page appears when you choose **Backup** > **Manual Backup**.

Authorization Requirements

You must have platform administrator authority to access this page.

Description

Use the Manual Backup page to start a manual backup.

Note Before starting a manual backup, make sure that all servers in the clusters are running and are reachable over the network. Servers that are not running or are not reachable over the network are not backed up.

Note From Release 14SU2 onwards, tomcat and tomcat-ecdsa certificate must be exchanged between the publisher and subscriber nodes before taking drs backup. Certificate exchange is also required if the ipaddress/hostname changes.

The following table describes the Manual Backup page.

Table 170: Manual Backup Page

Field	Description
Select Backup Device	Select the name of the backup device from the pulldown menu.
Select Features	Check **Emergency Responder** as the feature to be backed up.
Start Backup button or icon	Starts a manual backup.
Estimate Size button or icon	Estimates the backup size for the selected feature
Select All button or icon	Selects all the listed features.
Clear All button or icon	Deselects all selected features.

Related Topics

Schedule List, on page 564

Start Manual Backup , on page 245

Backup History and Restore History

The Backup History page appears when you choose **Backup** > **History**. The Restore History page appears when you choose **Restore** > **History**.

Authorization Requirements

You must have platform administrator authority to access this page.

Description

Use the Backup History page to view information about past backups. Use the Restore History page to view information about past restore operations.

The following table describes the Backup History page.

Table 171: Backup History Page

Field	Description
Backup History information	The following information about past backups is displayed: • Tar Filename • Backup Device • Completed On • Result • Backup Type • Version • Features Backed Up • Features Returned Warning • Failed Features
Refresh button or icon	Refreshes the information in the Backup History page.

The following table describes the Restore History page.

Table 172: Restore History Page

Field	Description
Restore History information	The following information about past backups is displayed: • Tar Filename • Backup Device • Version • Completed On • Result • Features Restored • Failed Features
Refresh button or icon	Refreshes the information in the Restore History page.

Related Topics

Schedule List, on page 564
Manual Backup, on page 566
Backup Status, on page 569
Restore Wizard, on page 569
Restore Status, on page 571
Backup and Restore History , on page 249

Backup Status

The Backup Status page appears when you choose **Backup** > **Current Status**.

Authorization Requirements

You must have platform administrator authority to access this page.

Description

Use the Backup Status page to view status information about the current backup.

The following table describes the Backup Status page.

Table 173: Backup Status Page

Field	Description
Status	Provides information about the status of the current backup.
Backup Details	The following information about the current backup is displayed: • Tar Filename • Backup Device • Operation • Percentage Complete • Feature • Server • Component • Status • Result • Start Time • Log File
Refresh button or icon	Refreshes the information about the current backup.
Cancel Backup button or icon	Cancels the current backup.

Related Topics

Schedule List, on page 564
Check Backup Status , on page 245

Restore Wizard

The Restore Wizard page appears when you choose **Restore** > **Restore Wizard**.

Authorization Requirements

You must have platform administrator authority to access this page.

Description

Use the Restore Wizard page to restore a backup file to a server or to restore all servers in a cluster. The Restore Wizard consists of four web pages.

Use the Step1 Restore—Choose Backup Device page to select the backup device to be used for the backup.

The following table describes the Step1 Restore—Choose Backup Device page.

Table 174: Step 1 Restore—Choose Backup Device Page

Field	Description
Status	Indicates the current status of the recovery operation.
Select Backup Device	Select the backup device using the pull-down menu.
Next button or icon	Advances to the next page in the Restore Wizard.
Cancel button or icon	Cancels the restore operation.

Use the Step2 Restore—Choose the Backup Tar File page to select the backup tar file to be restored.

The following table describes the Step2 Restore—Choose the Backup Tar File page.

Table 175: Step 2 Restore—Choose the Backup Tar File Page

Field	Description
Status	Indicates the current status of the restore operation.
Select Backup File	Use the pull-down menu to select the tar file for backup
Back button or icon	Returns to the previous page in the Restore Wizard.
Next button or icon	Advances to the next page in the Restore Wizard.
Cancel button or icon	Cancels the restore operation.

Use the Step3 Restore—Select the Type of Restore page to select the features to be restored.

The following table describes the Step3 Restore—Select the Type of Restore page.

Table 176: Step 3 Restore—Select the Type of Restore Page

Field	Description
Status	Indicates the current status of the restore operation.
Select Features	Click the box to the left of the Emergency Responder feature name to select the Emergency Responder feature for backup.
Back button or icon	Returns to the previous page in the Restore Wizard.

Field	Description
Next button or icon	Advances to the next page in the Restore Wizard.
Cancel button or icon	Cancels the restore operation.

Use the Step4 Restore—Final Warning for Restore page to select the servers to be restored.

The following table describes the Step4 Restore—Final Warning for Restore page.

Table 177: Step 4 Restore—Final Warning for Restore Page

Field	Description
Status	Indicates the current status of the restore operation.
Warning	Displays a warning message stating that the restore operation overwrites all existing data on the selected servers.
Select the Servers to be restored for each Feature	Under the Emergency Responder feature name, select the servers to be restored. To do so, click the check box to the left of the server name.
Back button or icon	Returns to the previous page in the Restore Wizard.
Restore button or icon	Initiates the restore operation. Before you click **Restore**, you must first select the server to be restored. You can select a Publisher or a Subscriber to be restored, but not both. **Caution** The restore operation overwrites any existing data on the selected servers.
Cancel button or icon	Cancels the restore operation.

Related Topics

Backup History and Restore History, on page 567
Restore Status, on page 571
Restore Backup File , on page 245
Restore Entire Server Group , on page 246

Restore Status

The Restore Status page appears when you choose **Restore** > **Status**.

Authorization Requirements

You must have platform administrator authority to access this page.

Description

Use the Restore Status page to view the status of restore operations.

The following table describes the Restore Status page.

Table 178: Restore Status Page

Field	Description
Status	Provides information about the status of the current restore operation.
Restore Details	The following information about the current restore operation is displayed: • Tar Filename • Backup Device • Operation • Percentage Complete • Feature • Server • Component • Status • Result • Start Time • Log File
Refresh button or icon	Refreshes the information about the current restore operation.

Related Topics

Restore Wizard, on page 569
Backup History and Restore History, on page 567
View Restore Status, on page 249
Backup and Restore History , on page 249

APPENDIX F

Admin Utility Web Interface for Cisco Emergency Responder

Update Cisco Unified Communications Manager Version

The Upgrade CUCM Version page appears when you choose **Update** > **CUCM Version**.

Authorization Requirements

You must have system administrator authority to access this page.

Description

Use the Upgrade CUCM Version page to select a different version of CiscoUnifiedCommunicationsManager.

The following table describes the Upgrade CUCM Version page.

Table 179: Upgrade CUCM Version Page

Field	Description
Status	Displays the current CiscoUnifiedCommunicationsManager version.
CUCM Version Details	
Choose the CiscoUnifiedCommunicationsManager version to upgrade	Use the pull down menu to select a version of CiscoUnifiedCommunicationsManager.
Go button	Click **Go** to begin the update process. **Note** Change the CUCM version separately on the Publisher and Subscriber nodes.

Field	Description
Cancel button	Cancels the CiscoUnifiedCommunicationsManager update.

Related Topics

Change Cisco Unified Communications Manager Version , on page 305

Update Cluster DB Host

The Update Cluster DB Host page appears when you choose **Update > Cluster DB Host**.

Authorization Requirements

You must have system administrator authority to access this page.

Description

Use the Update Cluster DB Host page to designate a new server as the Emergency Responder cluster database host server.

The following table describes the Update Cluster DB Host page.

Table 180: Update Cluster DB Host Page

Field	Description
Status	Displays the name of the current cluster database host
Cluster DB Host Details	
ClusterDB Hostname/IP Address	Enter the hostname (if DNS is configured) or the IP address of the new cluster database host. **Note** If the cluster is spread across domains, then enter a fully qualified hostname.
Password	Enter the password for the new cluster database host
Confirm Password	Reenter the password for the new cluster database host.

Field	Description
Go button	Click the **Go** button to designate the new server as the new cluster database host. **Note** The Emergency Responder Cluster DB host details are updated. Emergency Responder services must be restarted for this change to take effect. You must restart Emergency Responder Services by rebooting the Emergency Responder publisher and subscriber servers. Only restarting Emergency Responder services does not work because the IP address is cached by other services and this updates the Emergency Responder Cluster DB host details for this server group only. Other servers in this Emergency Responder cluster are NOT updated automatically. For further details, see Update Emergency Responder Cluster Database Host Details , on page 306.
Cancel button	Cancels the Update Cluster DB Host operation.

Related Topics

Set Up Emergency Responder Cluster and Cluster DB Host , on page 134

Update Emergency Responder Cluster Database Host Details , on page 306

APPENDIX G

Using AFT for Specific Service Providers

ALI Formatting Tool for Bell Canada

The following topics describe how to use AFT for Bell Canada.

Transaction Code Modifications

When using the AFT with Bell Canada as your service provider, ensure that the Transaction Code for Bell Canada is either A or D. Otherwise, Bell Canada rejects the record and returns it in an Error Return file with an error message.

The following table shows the values displayed in the Function Field in NENA records and the corresponding values for the Transaction Code in Bell Canada records.

Table 181: NENA and Bell Canada Function/Transaction Fields

NENA Function Code Field	Bell Canada Transaction Code Field
I for Insert a new record.	A for Add a new record.
C for Change a record.	A for Change a record. **Note** The NENA Function Code C is mapped to Bell Canada's Transaction Code A.
D for Delete a record.	D for Delete a record.

Bell Canada Data

The following table describes the remaining Bell Canada-specific fields. Some fields require data to generate ALI files in the format specified in Bell Canada's ALI data support documentation; other fields can remain blank.

If there is an error in these fields, Bell Canada rejects the record and sends back an Error Return file with an error code.

Note You do not configure the Language Indicator field using AFT; AFT sets the field to E for English.

Table 182: Modifying Bell Canada-Specific Fields

Field	Description	Format	Notes
Service Class	Type of telephone service of the customer's Terminal Number.	3 alphanumeric characters	Required field.
Postal Code	Postal code of the customer's service address.	6 alphanumeric characters	Required field. The first must be alphabetic.
Municipality Code	Unique code assigned to each municipality.	3 alphanumeric characters	Required field.
Class of Service	Code that identifies the grade, class, and type of service.	5 alphanumeric characters	Required field.
System Source	Identifies the source database of the Transaction Record.	1 alphabetic character	Required field.
Location Type	Type of location within a building (for example, apartment).	15 alphanumeric characters	Optional field.
Location Number	Number of the location identified in the Location Type field (for example, apartment 2, floor 2).	6 alphanumeric characters	Optional field.
Service Municipality	City, town, village, borough, or locality.	35 alphanumeric characters	Required field.
LSP ID	Unique code provided to the PS ALI customer by Bell Canada that denotes the provider of local telephone service.	5 alphanumeric characters	Required field. Must be the valid LSP Ic provided to the PS ALI c by Bell Canada.

ALI Formatting Tool for SBC Ameritech

SBC Ameritech (Ameritech) does not have any service provider-specific fields that you must modify using the AFT. However, when using AFT to format records for Ameritech, you may need to modify the Function Code.

Cisco Emergency Responder (Emergency Responder) sets the Function Code to one of the following:

- I for Inserting a new ALI record (the default)
- C for Updating an ALI record, such as changing a street name
- D for Deleting an ALI record

If you make changes to an ALI record in Emergency Responder to correct errors reported by Ameritech, you may need to use AFT to change the Function Code for ELIN records.

For example, Emergency Responder initially generates ALI records with a function code of I for Insert. After you format a file and export it to Ameritech using AFT, Ameritech may reject the file because of an error, such as the street suffix is incorrect. You cannot change the street suffix in AFT because this field is disabled. Instead, you must change the ALI record using Emergency Responder.

When Emergency Responder generates the ALI record the second time after you make the change, it sets the Function Code to C because it assumes that the first file was accepted. Use AFT to change the Function Code for ELIN records from C to I. Then, generate the format using AFT and send the reformatted file to Ameritech.

ALI Formatting Tool for SBC-PacBell

The following sections describe how to use the AFT for SBC-PacBell.

Call Back for ELIN Enablement

Emergency Responder displays the ELIN at the PSAP. If the emergency call is cut off for any reason, or if the PSAP needs to talk to the caller again, the PSAP can then dial to reconnect to the emergency caller.

The call back for this ELIN option allows you to specify a direct inward dial (DID) number that can be used by the PSAP when a call from a fictitious number is made to 911.

The call back for this ELIN option performs two important functions:

- It alerts the PSAP that the phone they are calling back may not have generated the 911 call.
- It enables the PSAP to call back to a phone that is located near the fictitious telephone number that did place the call.

We recommend that you always enable this option by checking the call back for this ELIN field. (The default is to leave the field blank, which defaults to No.)

Function Code Modifications

Emergency Responder sets the function code to one of the following:

- I for Inserting a new ALI record (the default)
- C for Updating an ALI record, such as changing a street name
- D for Deleting an ALI record

If you make changes to an ALI record in Emergency Responder to correct errors reported by your service provider, you may need to use AFT to change the function code for ELIN records.

For example, Emergency Responder initially generates ALI records with a function code of I for Insert. After you format a file and export it to SBC Pacific Bell (PacBell) using AFT, PacBell may reject the file. The error may be that the street suffix is incorrect, for example. You cannot change the street suffix in AFT because this field is disabled. You must change the ALI record using Emergency Responder.

When Emergency Responder generates the ALI record the second time after you make the change, it sets the function code to C because it assumes that the first file was accepted. Use AFT to change the Function Code for ELIN records from C to I. Then, generate the format using AFT and send the reformatted file to PacBell.

ALI Formatting Tool for SBC-Southwestern Bell

The following sections describe how to use the AFT for SBC-Southwestern Bell.

PS Code for SBC-Southwestern Bell

To make the ELIN records readable by Southwestern Bell, you may need to use AFT to update the PS Code field; this field is specific to Southwestern Bell. The PS Code is a four-digit code that the Southwestern Bell system assigns whenever the system configures a new PS site. This code is associated with the PS user's login and source.

The PS Code is a feature that allows only records with the correct PS Code to be processed into tables for the PS Site. If the PS Code does not match the configured Source Name that is assigned to the PS Site, the record will not process. Before you generate a formatted file using AFT, make sure that PS Code and the Source Name match. For more information, see the Southwestern Bell documentation.

Function Code Modifications

Emergency Responder sets the function code to one of the following:

- I for Inserting a new ALI record (the default)
- C for Updating an ALI record, such as changing a street name
- D for Deleting an ALI record

If you make changes to an ALI record in Emergency Responder to correct errors reported by your service provider, you may need to use AFT to change the function code for ELIN records.

For example, Emergency Responder initially generates ALI records with a function code of I for Insert. After you format a file and export it to Southwestern Bell using AFT, Southwestern Bell may reject the file. The error may be that the street suffix is incorrect, for example. You cannot change the street suffix in AFT because this field is disabled. You must change the ALI record using Emergency Responder.

When Emergency Responder generates the ALI record the second time after you make the change, it sets the function code to C because it assumes that the first file was accepted. Use AFT to change the function code for ELIN records from C to I. Then, generate the format using AFT and send the reformatted file to Southwestern Bell.

ALI Formatting Tool for Qwest

Qwest does not have any service provider-specific fields that you must modify using the AFT. However, when using AFT to format records for Qwest, you may need to modify the function code.

Cisco Emergency Responder (Emergency Responder) sets the function code to one of the following:

- I for Inserting a new ALI record (the default)
- C for Updating an ALI record, such as changing a street name
- D for Deleting an ALI record

If you make changes to an ALI record in Emergency Responder to correct errors reported by Qwest, you may need to use AFT to change the function code for ELIN records.

For example, Emergency Responder initially generates ALI records with a function code of I for Insert. After you format a file and export it to Qwest using AFT, Qwest may reject the file because of an error. The error may be that the street suffix is incorrect, for example. You cannot change the street suffix in AFT because this field is disabled. You must change the ALI record using Emergency Responder.

When Emergency Responder generates the ALI record the second time after you make the change, it sets the function code to C because it assumes that the first file was accepted. Use AFT to change the function code for ELIN records from C to I. Then, generate the format using AFT and send the reformatted file to Qwest

ALI Formatting Tool for Verizon

The following sections describe how to use the AFT for Verizon.

Function Code Modifications

Verizon does not have any service provider-specific fields that you must modify using the AFT. However, when using AFT to format records for Verizon, you may need to modify the function code.

Emergency Responder sets the function code to one of the following:

- I—Inserting a new ALI record (the default)
- C—Updating an ALI record, such as changing a street name
- D—Deleting an ALI record
- U—Unlocking an ALI Record (included to support Local Number Portability)
- M—Migrating an ALI Record (included to support Local Number Portability)

If you make changes to an ALI record in Emergency Responder to correct errors reported by Verizon, you may need to use AFT to change the function code for ELIN records.

For example, Emergency Responder initially generates ALI records with a function code of I for Insert. After you format a file and export it to Verizon using AFT, Verizon may reject the file because of an error. The error may be that the street suffix is incorrect, for example. You cannot change the street suffix in AFT because this field is disabled. You must change the ALI record using Emergency Responder.

When Emergency Responder generates the ALI record the second time after you make the change, it sets the function code to C because it assumes that the first file was accepted. Use AFT to change the function code for ELIN records from C to I. Then, generate the format using AFT and send the reformatted file to Verizon.

Verizon New England State Disability Indicator Modifications

To make the ELIN records readable by Verizon's New England states (MA, ME, NH, RI, VT), you may need to use AFT to update the Disability Indicator field; this field is specific to Verizon. The Disability Indicator is a reserved 20-character field that the carrier can use to enter disability information.

The following table shows the Disability Indicator designations that you can use to populate the location field of an ALI record.

Table 183: Disability Indicator Descriptions

Disability Indicator	Description
LSS	Life Support System
MI	Mobility Impaired
B	Blind
DHH	Deaf and Hard of Hearing
TTY	Teletypewriter
SI	Speech Impaired
DD	Developmentally Disabled

AFT intelligently identifies the New England states (from the state field of the ALI record) and allows you to update the Disability Indicator field individually (by selecting an New England ELIN record from the tree) or in bulk (through the Bulk Update feature).

Customer Name for Verizon West State Modifications

The Verizon West states (CA, HI, ID, IL, IN, MI, NC, OH, OR, SC, TX, WA, WI) read the Customer Name field in the following format which uses a comma followed by a space between the last name and the first name. For example, Last Name, First Name.

This format prevents display errors at the PSAP. You can use AFT to update the field so that it follows the format that is used by Verizon West states.

AFT intelligently identifies the Verizon West states (from the state field of the ALI record) and allows you to update the Customer Name field individually (by selecting a Verizon West ELIN record from the tree) or in bulk (through the Bulk Update feature).

When you use AFT to make updates, it creates two different entries for the Customer Name field—one in the Emergency Responder database and one in the Service Provider's database. To avoid future discrepancies, you should also make the same update in the Customer Name field in the Emergency Responder GUI.

New Jersey Location Modifications

Verizon's New Jersey (NJ) system is a keyword-driven system that is based on a state requirement that location data be uniformly displayed at all PSAPs. Data is extracted from the location field only when one or more keywords, associated data, and delimiters are present in exact prescribed format. The NJ system location has four separate and distinct location type fields which can be simultaneously displayed at the PSAP. The location type fields are as follows:

- Unit Type (APT, BOX, LOT, PIER, RM, ROOM, RU, SUIT, SUITE, UNIT, WING)
- Floor Number (FLR)
- Building Description (BLDG)
- Coin Location Description (DES)

AFT intelligently identifies the NJ system-specific requirement for Location (from the state field of the ALI record) and allows you to update the location individually (by selecting a New Jersey ELIN) as well as in bulk (through the Bulk Update feature).

When you use AFT to make updates, it creates two different entries for the Customer Name field—one in the Emergency Responder database and one in the Service Provider's database. To avoid future discrepancies, you should also make the exact update in the Location field in Emergency Responder GUI.

APPENDIX H

Event Log Messages

CER_DATABASE

Table 184: CER_DATABASE Event Log Messages

Type	Message
INFO	Failed to get the fully qualified host name. DNS might not be enabled. Putting Ipaddress in Cluster database.
ERROR	CER Server Memory Usage is HIGH - above threshold value of 80%
ERROR	Database replication BROKEN.
ERROR	Number of <NUM> limit exceeded. Fetching only a maximum of *** <NUM> *** entries

CER_SYSADMIN

Table 185: CER_SYSADMIN Event Log Messages

Type	Message
ERROR	Failed to add this CER group to CER cluster.

Type	Message
WARNING	Cisco ER cluster functionality will not work till this problem is fixed. 1. Check if "CERCluster password" is same as in Cisco ER ClusterDB. 2. Check if Cisco Tomcat and Database services are running on Cisco ER ClusterDB. 3. Check if Cisco ER ClusterDB Hostname is correct and accessible. For more details see EventViewer on ER Server.<Error reason>.
ERROR	Failed to initialize LDAP. <Error Message>

CER_TELEPHONY

Table 186: CER_TELEPHONY Event Log Messages

Type	Message
WARNING	Emergency call from<CALLING ADDRESS>has been routed to default ERL because calling party failed. Please make sure that the check box "Enable Calling Party Number Modification" is checked on t Manager user page for the CER user. PSAP callbacks MAY NOT work correctly. The CER servic to be restarted once the flag is checked on the Call Manager User page.
WARNING	Emergency call from<calling address>could not be routed using the following Routepatterns. <LIST OF RP's> Call Routed to <RP/NUMBER> Please check the availability of the above routes. Also, check for the following error conditions. 1. If FAC and/or CMC are configured on the route patterns used for CER, please disable them. 2. If the "Calling Party Number Modification" flag on the CER user page in the call manager is please enable it.
ERROR	Failed to load class <CLASS NAME>.
ERROR	CCMString is empty can't load telephony classes.
WARNING	Got OutOfService event from provider: <PROVIDER_NAME>.
INFO	Got InService event from provider: <PROVIDER_NAME>.
WARNING	Logged out of the duplicate provider - <CTI_Manager> from CER. Specify the CTI Ports (if any) provider, in a different CCM node.
WARNING	Cannot register media terminal for port: <PORT_NUMBER>.

Type	Message
WARNING	CTI Port: <PORT_NUMBER> is in OUTOFSERVICE, trying after 10 seconds.
ERROR	Media channel creation failed: <ERROR>.
WARNING	Failed to create media channel for: <PORT_NUMBER>.
ERROR	Failed to initiate call to security: <NUMBER> <ERROR>. <ERROR> corresponds to: • PrivilegeViolationException • InvalidPartyException • MethodNotSupportedException • InvalidArgumentException • InvalidStateException • E911CallRouterException • <Other Exceptions (if any)>
ERROR	Failed to register route point: <ROUTE_PATTERN> with Provider: <PROVIDER_NAME>.
ERROR	RouteAddress: <ADDRESS> is in OUTOFSERVICE.
WARNING	<ADDRESS> Route Point received IN_SERVICE event from Provider <NAME>.
WARNING	<ADDRESS> Route Point received OUT_OF_SERVICE event from Provider <NAME>.
ERROR	<msg>Address = <CALLING ADDRESS> ; Terminal = <CALLING TERMINAL> because, returned :<CAUSE> <msg> corresponds to Call failed to reach PSAP for : /PSAP Callback failed for : <CAUSE> corresponds to CAUSE_ INVALID_DESTINATION/CAUSE_ROUTING_TIMER_EXPIRED/CAUSE_ PARA SUPPORTED/CAUSE_STATE_INCOMPATIBLE/CAUSE_UNSPECIFIED_ ERROR
ERROR	<msg>Address = <CALLING ADDRESS> ; Terminal = <CALLING TERMINAL> because, returned : CAUSE_CTIERR_FAC_CMC_REASON_CMC_NEEDED. Please Uncheck the R FAC/CMC codes on the Route points used by the Cisco Emergency Responder.
WARNING	Call from <CALLER ID> could not be routed to the Offpremise ERL : <ERL NAME>. Possible reasons: The phone-location association has not yet happened or has met with errors. Device Name: <DEVICE NAME> Caller ID: <CALLER ID>
WARNING	Failed to get the JTAPI Provider for: <NAME_STRING> trying infinitely.

Type	Message
WARNING	Not registering the provider: <PROVIDER_NAME> as is already registered/in the same CCM C of:<element>.
WARNING	JTAPI logs are not enabled as the logs path is empty in E911Bootstrap properties.
ERROR	Failed to get the JTAPI Provider for: <IP Address/Host Name> after <NUMBER> attempts.
WARNING	Currently, no CTI Ports are available to place the call for <CallingAddress>. Phone notification w in the next 60 seconds.

CER_AGGREGATOR

Table 187: CER_AGGREGATOR Event Log Messages

Type	Message
WARNING	Device <ipaddress> is SNMP unreachable. Please check SNMP settings in CER and also on this CCM. Please confirm proper access privilege (READ_ONLY) set on this box for SNMP service. Also, verify n/w connectivity.
WARNING	During discovery some devices are unreachable. List of Unreachable Switches <List>.
WARNING	WARNING During discovery some devices are unreachable. List of Unreachable CCMs <List>.
WARNING	CERServer could not communicate with CERPhoneTrackingEngine.
WARNING	CERServer could not communicate with CERPhoneTrackingEngine.
INFO	Device <IP Address> is SNMP unreachable. Please check SNMP settings in CER and also on this CCM. Please confirm proper access privilege (READ_ONLY) set on this box for SNMP service. Also, verify n/w connectivity.
INFO	Error in resolving HostName -> IPAddress through DNS, ignoring the seed from DE <IP Address>.
INFO	IP Address mismatch detected,OLD_IP <IP Address> NEW_IP <IP Address> SEED <IP Address> for any changed configuration, deletion and re addition of seed device is recommended.
INFO	Device <IP Address> is not a valid switch.
INFO	Device <IP Address> is SNMP Un-reachable.
INFO	Device <IP Address> is not supported.
INFO	This Device <IP Address> is identified for a different device family than earlier discovered, ignored for this discovery cycle.

Type	Message
INFO	Failed to retrieve SysOid of a device <IP Address> Please check if device is SNMP reachable.
INFO	This device is not supported <seed>.
INFO	This Device <IPADDRESS> is earlier discovered with different device family for changed device config (ipAddress, deviceFamily, dnsName). Delete and re-add the device is must; also you need to re-enter SNMP community string if changed from earlier one.
INFO	The device <IP Address> is not a valid switch...please confirm.
INFO	This device not a valid CCM to discover <IP Address>.
INFO	Error in resolving HostName -> IPAddress, ignoring the seed for discovery <IP Address>.
INFO	IP Address mismatch detected,OLD_IP <IP Address> NEW_IP <IP Address> SEED <IP Address> for any changed configuration, deletion and re addition of seed device is recommended.
	During discovery some devices are unreachable List of Unreachable Switches<SWITCH LIST> Cisco CallManager(s)<CCM LIST>.
	Device <IPADDRESS> is SNMP unreachable. Please check SNMP settings in CER and also on device. IF this is a CCM box then please confirm proper access privilege (READ_ONLY) set on this box for SNMP service. Also, verify n/w connectivity.
INFO	Device <IP Address> is not a valid CCM.

CER_GROUP

Table 188: CER_GROUP Event Log Messages

Type	Message
INFO	Active Cisco Emergency Responder set to : <Server Details>.
INFO	Connection established with Cisco Emergency Responder: <PEER>
WARNING	Disconnected from Cisco ER: <PEER>.
ERROR	Cisco ER Couldn't open socket at port <NUMBER>, Exiting.
WARNING	Failed to open connection with Cisco Emergency Responder: <_remoteAddress>/<_remotePort>

CER_CALLENGINE

Table 189: CER_CALLENGINE Event Log Messages

Type	Message
INFO	Cisco ER Exiting: Graceful shutdown.
ERROR	Problem in initializing SERVER (Server Group). Cannot continue... <EXCEPTION>.
ERROR	Problem in initializing Database (E911ServerGroupParameters). Retried... <COUNT> times.
ERROR	Problem in initializing SERVER (Server). Cannot continue... <EXCEPTION>.
ERROR	Problem in initializing Database (Server). Cannot continue... <EXCEPTION>.
ERROR	Problem in initializing Database (CERServers). Retried... <COUNT> times.
ERROR	Problem in initializing SERVER (License). Cannot continue... <EXCEPTION>.
ERROR	Problem in initializing SERVER (Zone). Cannot continue... <EXCEPTION>.
ERROR	Problem in initializing SERVER (DiscoveryEngine). Cannot continue... <EXCEPTION>.
ERROR	Problem in initializing SERVER (CERIPSubnetManager). Cannot continue... <EXCEPTION>.
ERROR	Problem in initializing SERVER (CERVHMPhoneManager). Cannot continue... <EXCEPTION>.
ERROR	Problem in initializing SERVER (CCM Cluster - No Call Manager seeds configured). Cannot continue... <EXCEPTION>.
ERROR	Problem in initializing SERVER (Seed Switch). Cannot continue... <EXCEPTION>.
ERROR	Problem in initializing SERVER (Discrepant entry). Cannot continue... <EXCEPTION>.
ERROR	Problem in initializing SERVER (Security Contact). Cannot continue... <EXCEPTION>.
ERROR	Problem in refreshing LDAP (Server Group). Cannot continue... <EXCEPTION>.
ERROR	Problem in refreshing LDAP (Zone). Cannot continue... <EXCEPTION>.
ERROR	Problem in refreshing LDAP (Server). Cannot continue... <EXCEPTION>.
ERROR	Problem in refreshing LDAP (Seed Switch). Cannot continue...<EXCEPTION>.
ERROR	Problem in refreshing LDAP (CCM Cluster). Cannot continue... <EXCEPTION>.
ERROR	Problem in refreshing LDAP (Discrepant entry). Cannot continue... <EXCEPTION>.
ERROR	Problem in refreshing LDAP (Security Contact). Cannot continue... <EXCEPTION>.

Type	Message
ERROR	Problem in refreshing LDAP (Security Contact). Cannot continue...<EXCEPTION>.
ERROR	Problem in refreshing zone port tree (Switchport to zone map). Cannot continue... <EXCEPTION>.
ERROR	LicenseManager: End Of 60 Day Evaluation Period. CER Will not work. Please upload a valid License file.
WARNING	Warning!!! You have insufficient number of user licenses. Total phones tracked by the group of CER instances added to the Smart Software Manager exceed the user licenses available.

CER_CLUSTER

Table 190: CER_CLUSTER Event Log Messages

Type	Message
WARNING	IntraCluster Communication failed to ServerGroup with servers Master:<SERVER DETAILS> StandBy: <SERVER DETAILS>.

CER_ONSITEALERT

Table 191: CER_ONSITEALERT Event Log Messages

Type	Message
WARNING	Backup Cisco ER <hostname> has taken control as Active Cisco ER. Transition time: <timestamp>.
WARNING	Master Cisco ER <hostname> has taken control as Active Cisco ER. Transition Time: <timestamp>.
WARNING	Emergency call DetailsCaller Extension:<Extn>Call Time :<TimeStamp>
WARNING	Emergency call DetailsCaller Extension:<Extn>Zone/ERL :<zone>LOCATION :<Location>Call Time :<Timestamp>

CER_PHONETRACKINGENGINE

Table 192: CER_PHONETRACKINGENGINE Event Log Messages

Type	Message
WARNING	Unified Communication Manager : <IP address> configured for tracking in Cisco Emergency Responder doesn't have Phones registered to it or unable to send Phone details to CER. Please check on Unified Communication Manager.

APPENDIX

Cisco Emergency Responder Port Usage

Cisco Emergency Responder (Emergency Responder) uses the following ports:

Table 193: Port Usage in Emergency Responder

Protocol	TCP /UDP	Port Range	For this protocol, app or box is: <Client, Server, or Peer>	What is other end?	Relevance to Product	What it doe
CTI	UDP	16384 to 32767				Used for co between En Responder Communica
CTI	TCP	2748				Used for En Responder connections Communica for CTI rou CTI ports
CTI	TCP	2749				Used for En Responder connections Communica for CTI rou CTI ports.
SNMP	UDP	161				Provides se SNMP-base app.
SNMP	UDP	6161				Native SNM for requests SNMP mas
TCP	TCP	7161				Used for co between SN agent and s

Protocol	TCP /UDP	Port Range	For this protocol, app or box is: <Client, Server, or Peer>	What is other end?	Relevance to Product	What it does
TCP	TCP	1500				IDS DB
TCP	TCP	1501				IDS DB
XML	TCP	1515				IDS DB
Proprietary	TCP	8500				IPsec Cluster M
N/A	TCP	22			sshd	Secure File Tra Protocol
TCP	TCP	22			sshd	SSH port for re
N/A	UDP	123				NTP port used Communicatio server
N/A	UDP	546				DHCPv6 Clien
N/A	UDP	6666			netdump	Port should be systems runnin netdump serve
HTTPS	TCP	443				HTTPS
N/A	TCP	9443			haproxy	Searches authe contacts
N/A	UDP	500				Internet Securi Association an Management P
N/A	UDP	514				System Loggin
Proprietary	TCP	2444				Used by CTL C communicate v Provider to set security mode a the CTL file
TCP	TCP	3804				Certificate Aut Function (CAP listening to inc requests from e
XML	TCP	5555				License Manag license request
TCP	TCP	7070				Certificate Ma Daemon

Protocol	TCP /UDP	Port Range	For this protocol, app or box is: <Client, Server, or Peer>	What is other end?	Relevance to Product	What it doe
TCP	TCP	7999				Cellular Dig Protocol
HTTPS	TCP	50000-50004				HTTPS to I
N/A	UDP	67 and 68				DHCP port CM server
N/A	UDP	ephemeral				Package Ma
N/A	UDP	ephemeral				DNS
N/A	TCP	32768:61000				Generic Ep
N/A	UDP	32768:61000				Generic Ep
N/A	IP	GRE: IP 47, ESP: IP 50, AH: IP 51, IPSec: UDP 500.				IPsec confi
SMTP	TCP	25	client	SMTP Mail Server(*)	core	Send e-pag notification
CDP			client		core	Discovery c phones
CLM	TCP	8500	server	clm	core	cluster man
CLM	UDP	8500	server	clm	core	cluster man
SYSLOGD	UDP	514	server	syslog server	optional	event syslo
SYSLOGD	TCP	601	server	syslog server	optional	audit syslog
SYSLOG	UDP	8888	client	syslog client	optional	syslog port
HTTPS	TCP	8443	server	Browser	core	secure web
HTTP	TCP	8080	server	Browser	core	web access
HTTP	TCP	80	server	Browser	core	web access
NTPD	UDP	123	client	NTP server	optional	network tim
Peer TCP	TCP	17001	peer	Emergency Responder Server	core	Emergency Master Bac

Protocol	TCP /UDP	Port Range	For this protocol, app or box is: <Client, Server, or Peer>	What is other end?	Relevance to Product	What it does
Peer RMI	TCP	7777	server	Emergency Responder Server	core	Emergency Res Server RMI po
Peer RMI	TCP	7778	server	Emergency Responder Admin	core	Emergency Res Admin RMI po
Applet	TCP	55000	server	Applets	core	Web alert
SNMP	UDP	162	server	SNMP Agents	optional	Network Mana
DBLRPC	TCP	1515	server	dblrpc	core	Db replication
RACOON	ESP		client	Emergency Responder Server	optional	IPsec traffic
RACOON	UDP	500	client	Emergency Responder Server	optional	IPsec setup por
IDS	TCP	1500	server	IDS		Informix datab
TCP	TCP	1099			AMC	AMC RMI Reg
TCP	TCP	1090			AMC	AMC RMI Obj
TCP	TCP	4040			CiscoDRFMaster	DRS Master A

APPENDIX J

Cisco Emergency Responder API Documentation

API Configuration Overview

Cisco Emergency Responder offers a suite of Application Programming Interface (APIs) through which client applications can be integrated to access the server data and managing functionalities.

These APIs provide users the flexibility to manage their network or their customers' networks by providing services and make them available to their end users. Partners can easily integrate these APIs with their internal tools, systems, and applications. Using industry standard authentication and role-based authorization, these APIs provide a trusted scalable platform to support multiple deployment models.

APIs are introduced to better manage users and their roles remotely, and ELIN/ERL Management. Also, to ease inter-operability with Cisco Unified Communications Manager. For more information on the APIs and their configuration, see Cisco Emergency Responder (CER) API Documentation.

Role Permissions for Different API

Users obtain Cisco Emergency Responder system API access privileges via the roles that are associated to the access groups of which the user is a member. Each role contains a set of permissions that is attached to a specific resource or application, such as Access Points or Audit Log Configuration.

For a user who has Role Permissions as "ERL", the role may contain permission that allows the user to view or edit the Conventional ERL using APIs available in the application. In this case, the ERL can be created, updated, and deleted using the corresponding APIs.

Following table lists all the available resources in Cisco Emergency Responder API documentation and their access privileges information:

Table 194: Standard Resources and Their Privileges

Resource Permissions	Access Criteria
Access Point	Access to CER System Administrator and access to Access Points tab
Add Subscriber	Access to CER System Administrator and access to Add Subscriber

Resource Permissions	Access Criteria
ALI Formatting Tool	Access to CER System Administrator and access to ALI Formatting Tool
All Logs	Access to CER Serviceability and able to see all logs of CER
Audit Log Configuration	Access to CER Serviceability and change Audit Log Configuration
Call History	Access to CER System Administrator and access to Call History
Call Manager Details	Access to CER System Administrator and access to Call Manager Details
CER Groups in Cluster	Access to CER System Administrator and access to CER Groups in Cluster
Cluster DB Host setting	Access to admin utility page and Update Cluster DB Host Details
Control Centre	Access to CER Serviceability page and access control centre
CPU & Memory Usage	Access to CER Serviceability page and access to CPU And Memory Usage
Device SNMP Settings	Access to CER System Administrator and access to Device SNMP Settings
Disk Usage	Access to CER Serviceability page and access to Disk Usage
ERL	Access to CER System Administrator and access to conventional ERL
ERL Audit Trail	Access to CER System Administrator and access to ERL Audit Trail
ERL Debug Tool	Access to CER System Administrator and access to ERL Debug Tool
ERL Migration	Access to CER System Administrator and access to ERL Migration
Event Viewer	Access to CER Serviceability page and access to Event Viewer
File Management Utility	Access to CER System Administrator and access to File Management Utility
Functional role	Access to create, read, update, delete Role details

Resource Permissions	Access Criteria
National E911 Service Provider ERL	Access to CER System Administrator and access to National E911 Service Provider ERL
IP Subnet	Access to CER System Administrator and access to IP Subnet
License Management	Access to CER System Administrator and access to License Management
Mail Alert Configurations	Access to CER System Administrator and access to Mail Alert Configurations
Manually Configured Phones	Access to CER System Administrator and access to Manually Configured Phones
Change CCM Version	Access to admin utility page and Change CCM version
Off-Premises ERL	Access to CER System Administrator and access to Off-Premises ERL
OnsiteContact	Access to CER System Administrator and access to OnsiteContact
Pager and Email Alert Configurations	Access to CER System Administrator and access to Pager and Email Alert Configurations
Phone Search	Access to CER User and access to Phone search
Processes	Access to CER Serviceability page and access to Processes
PS ALI Convert	Access to CER System Administrator and access to PS ALI Convert
PS ALI Export	Access to CER System Administrator and access to PS ALI Export
Purge	Access to CER System Administrator and access to Purge
Run Tracking	Access to CER System Administrator and access to Run Tracking
Saml Sso	Access to CER System Administrator and access to Saml Sso
Tracking Schedule	Access to CER System Administrator and access to Schedule
Server	Access to CER System Administrator and access to Server settings

Resource Permissions	Access Criteria
Server Group	Access to CER System Administrator and access to Server Group
MIB2 system group configuration	Access to CER Serviceability page and access to system group configuration
SNMP V1/V2c configuration	Access to CER Serviceability page and access to SNMP V1/V2c configuration
SNMP v3 configuration	Access to CER Serviceability page and access to SNMP v3 configuration
LAN Switches	Access to CER Serviceability page and access to LAN Switches
Switch Port	Access to CER System Administrator and access to Switch Port
Synthetic Phone	Access to CER System Administrator and access to Synthetic Phone
Telephony	Access to CER System Administrator and access to Telephony
Unlocated Phones	Access to CER System Administrator and access to Unlocated Phones
Application User	Access to CER System Administrator and access to User management
User Setting	Access to create, read, update, delete User details
User Call History	Access to CER User and access to User Call History
User Group	Access to create, read, update, delete User Group details
National E911 Service Provider VUI Settings	Access to CER System Administrator and access to National E911 Service Provider VUI Settings
Web Alert	Access to CER User and access to Web Alert