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 2
Understanding Cisco Emergency Responder, on page 5

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 1
Understanding Cisco Emergency Responder, on page 5

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:

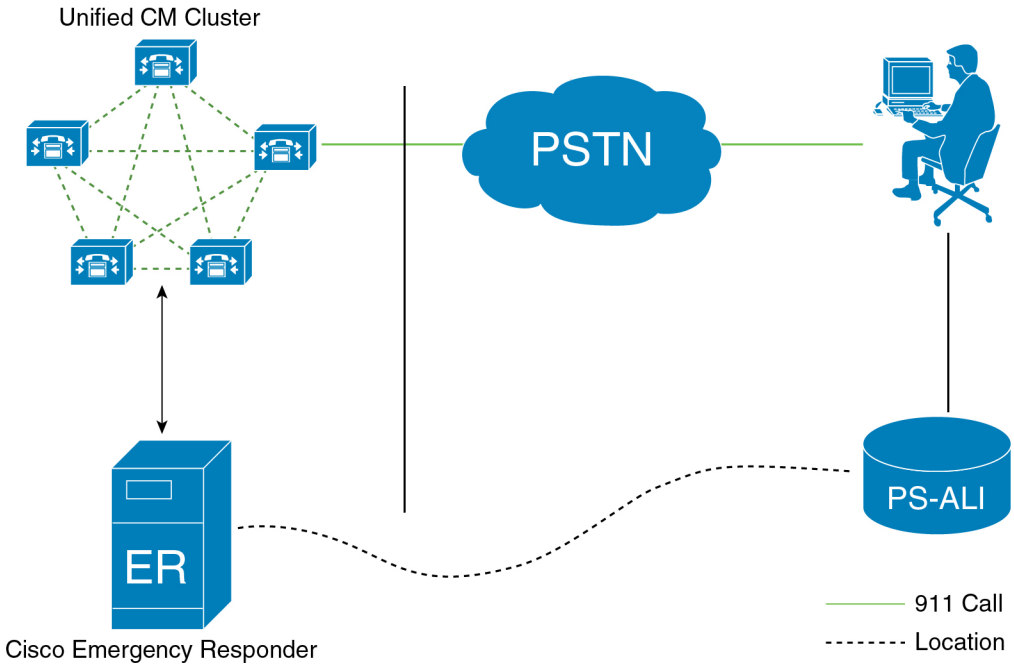
- **Telephone Call to Preconfigured DN**—Includes information like Calling Line Number and time of the 911 call.
- **Web-Notification to Authenticated Users**—Includes information like Calling Line Number, name of the originator, location, and time of the 911 call.
- **Email Notification to Configured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

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).

Cisco Emergency Responder supports integrating with an E911 National Service Provider (like Intrado V911 or RedSky E911Anywhere service) 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 Intrado V9-1-1 Enterprise Services.

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 6 or Cisco Smart Software Manager Satellite, on page 7
- 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

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.

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 8.	Use this procedure to generate a product instance registration token for your virtual account.
Step 2	Configure Transport Settings, on page 9.	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 11.	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 9.

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 8.

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 11.

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 9.

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 12.

  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 13.

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 13.

  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 14.

  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 8.

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.

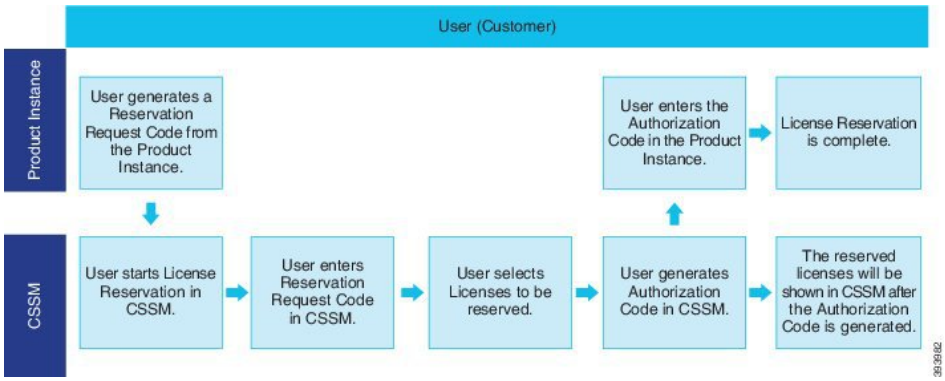
Note Usage information is updated once every 6 hours automatically. For more information, see the online help.

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.

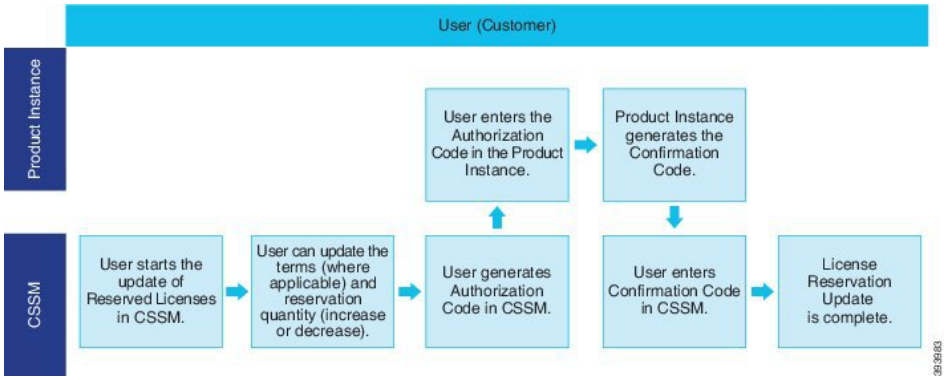
Users can specify and reserve perpetual or term-based licenses against the Emergency Responder product. No regular synchronization is required from the product once authorization code is exchanged unless there are any changes in the reservation requests. Reserved licenses remain blocked in Cisco Smart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

Figure 1: Reserve Licenses



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

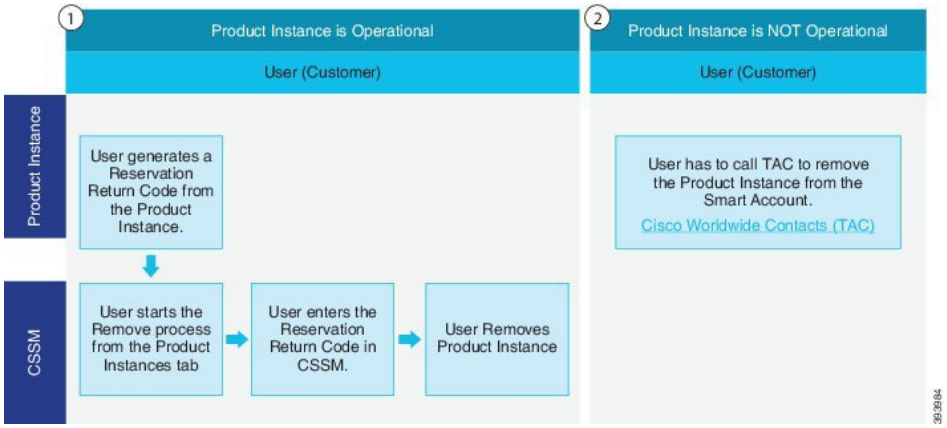


When licenses are reserved on a Product Instance (Emergency Responder), there are two ways to remove your product from the smart account and release all the licenses that are reserved for that Product Instance (Emergency Responder):

- **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



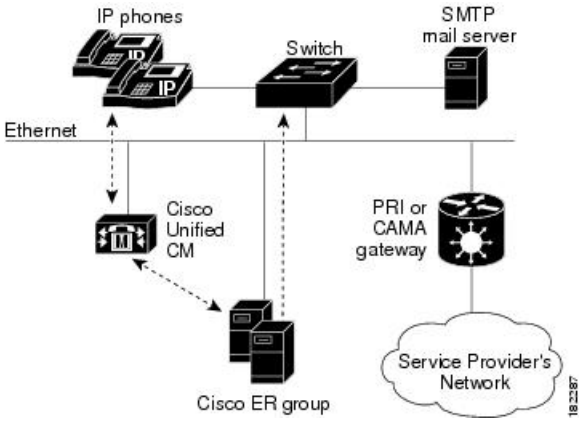
Customer entitled to License reservation feature on their Smart Account can reserve licenses from their virtual account, tie them to a devices UDI and use their device with these reserved licenses in a disconnected mode. The customer reserves specific licenses and counts for a UDI from their virtual 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>"

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 for more information about setting up switches for Emergency Responder. See Phone Management 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 19 for an explanation of the path an emergency call takes when managed by Emergency Responder.

Related Topics

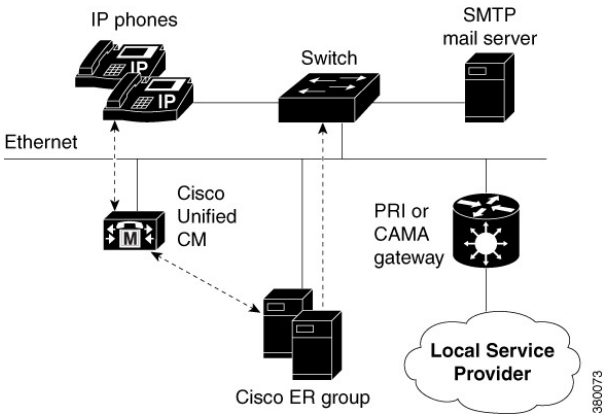
Determine Required Cisco Emergency Responder Groups , on page 27
Emergency Responder Deployment , on page 32

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 18 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 29.

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 18 or a dedicated National Emergency Call Delivery Service such as Intrado as shown in Figure 7: Cisco Emergency Responder and Intrado , on page 19.

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

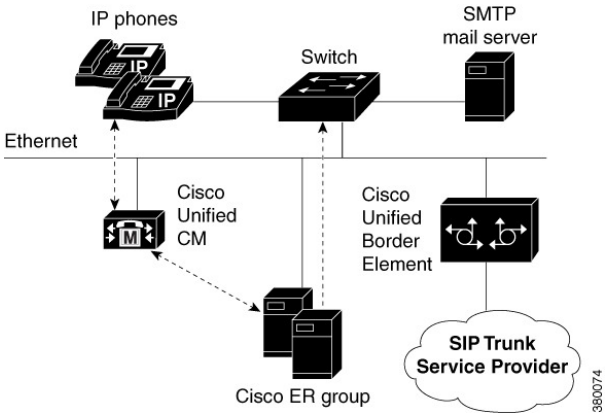
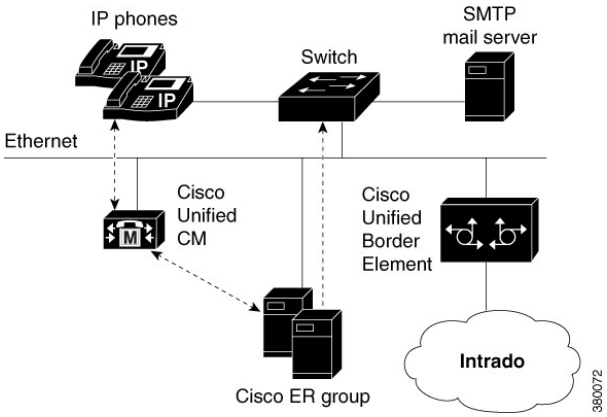


Figure 7: Cisco Emergency Responder and Intrado



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

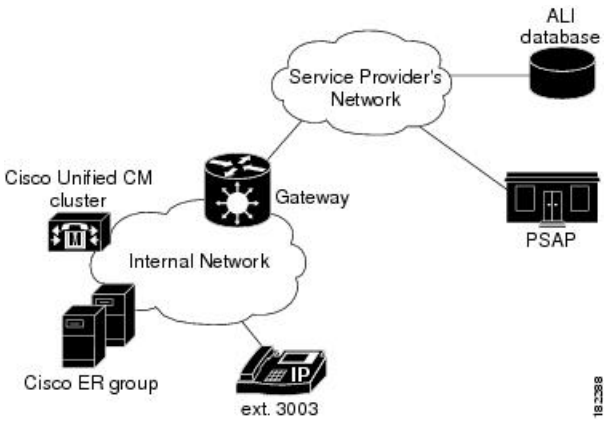
For more information on Intrado, see Configure Emergency Responder and Intrado V9-1-1 Enterprise Services.

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 20 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 and Set Up Test ERLs.

- 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.
- 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.
- Unlocated Phones—The MAC address of an IP Phone is assigned to an ERL. See Identify Unlocated Phones.
- 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.

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) 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 2
Data Integrity and Reliability, on page 28
ERLs
ELIN Numbers Emergency Calls and PSAP Callbacks
Set Up Calling Search Space for Gateway and PSAP Connection
Network Preparations , on page 29

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.

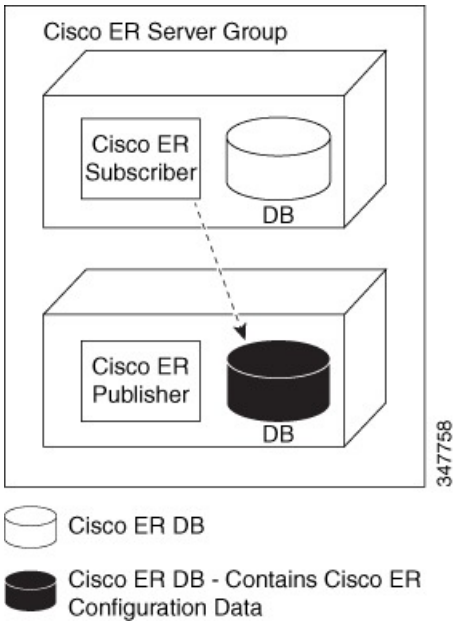
Configuration data for the server groups is stored in a database on the Publisher. This data is replicated to the Subscriber.

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:

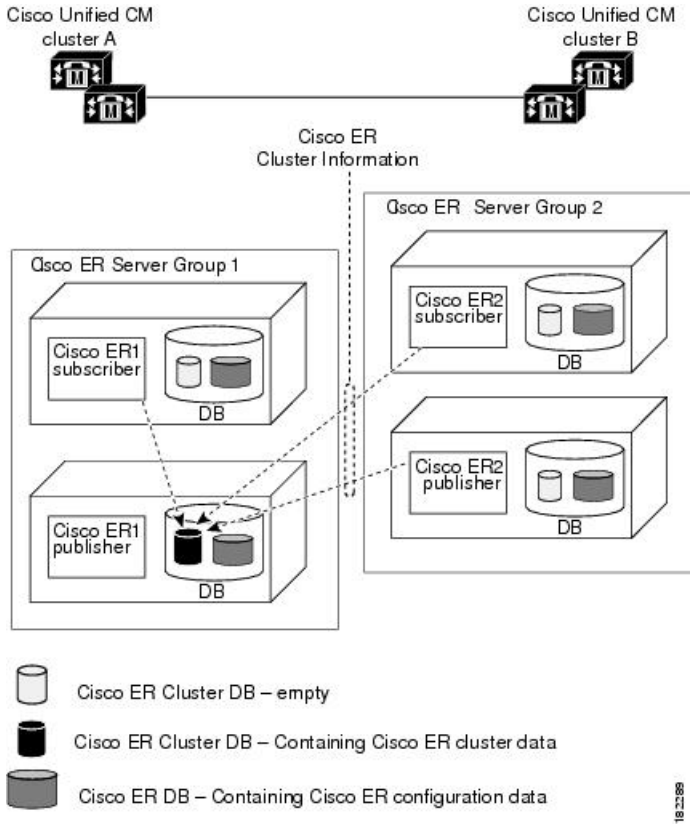
- A database that stores Emergency Responder configuration information.
- A database that stores Emergency Responder cluster information.

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.

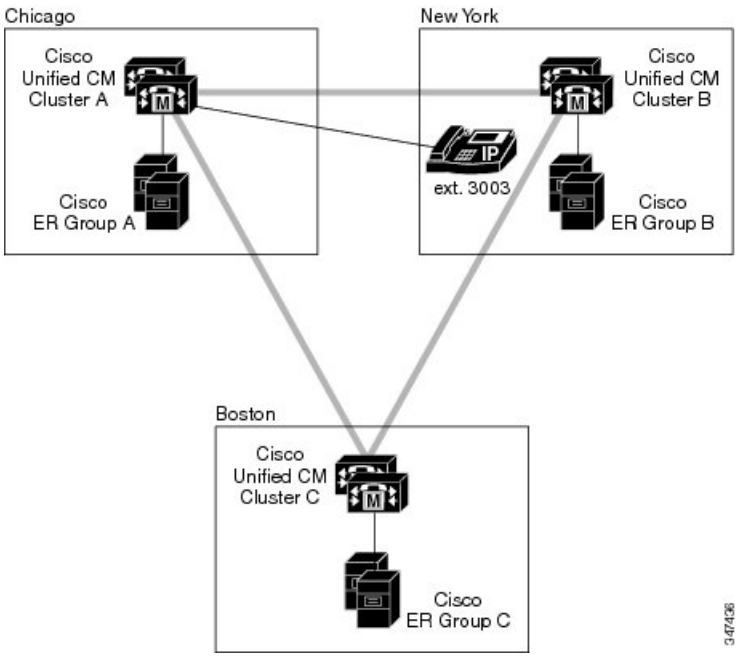
Note If you enter the system administrator email account in the System Administrator Mail ID field when you configure the Emergency Responder Server Group Settings, the system administrator receives an email notification when the standby server handles a call or when the standby server takes over for 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 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) 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 32
ALI Submission and Service Provider Requirements , on page 31
Export ALI Information for Submission to Your Service Provider
ALI Formatting Tool
ALI Formatting Tool

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 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.

- 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 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 and Emergency Responder ERL Administrator Role 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 and Export ALI Information for Submission to Your Service Provider for more information.

Related Topics

Emergency Call Process , on page 19
Determine Required Cisco Emergency Responder Groups , on page 27
Cisco Emergency Responder User Preparation

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

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

ERL Creation

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
ERL Management
ERL Creation
Export ERL Information

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 6 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
Phone Management

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 28 for more information about maintaining data integrity.

Related Topics

Emergency Responder Onsite Alert Personnel Preparations
Emergency Responder ERL Administrator Role
Emergency Responder Network Administrator Role
Emergency Responder System Administrator Role

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.

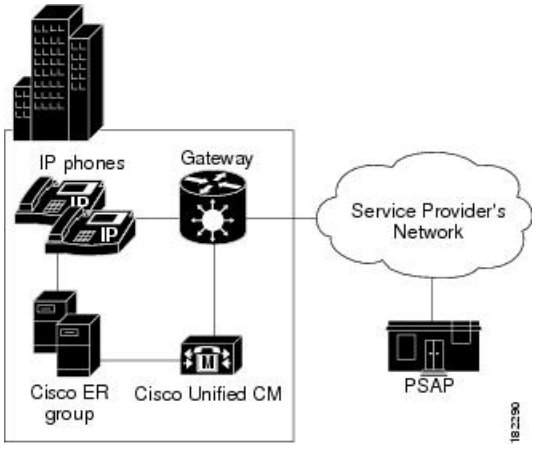
Deployment in Main Site and PSAP

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 33
- Deployment in Main Site with Satellite Offices , on page 35
- Deployment in Main Site Serving Multiple Sites , on page 36
- Two Main Site Deployments , on page 38

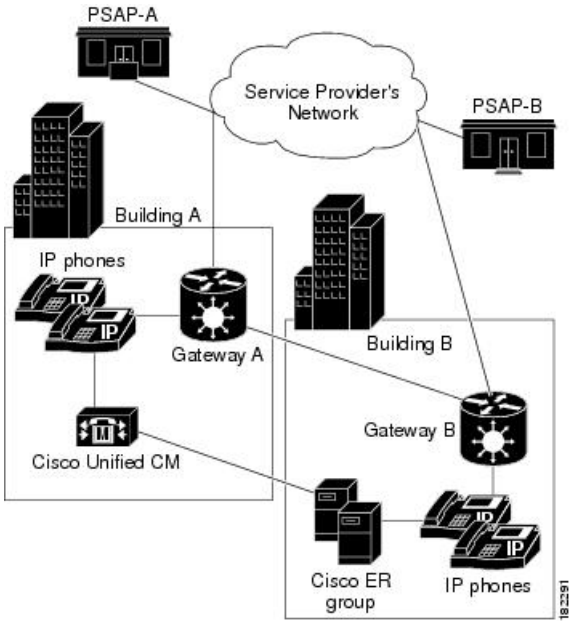
Related Topics

Emergency Call Process , on page 19
Emergency Responder and Your Network , on page 16
Determine Required Cisco Emergency Responder Groups , on page 27
Installation on a New System
Configure Cisco Unified Communications Manager

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 38.

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 32
- Deployment in Main Site with Satellite Offices , on page 35
- Deployment in Main Site Serving Multiple Sites , on page 36
- Two Main Site Deployments , on page 38

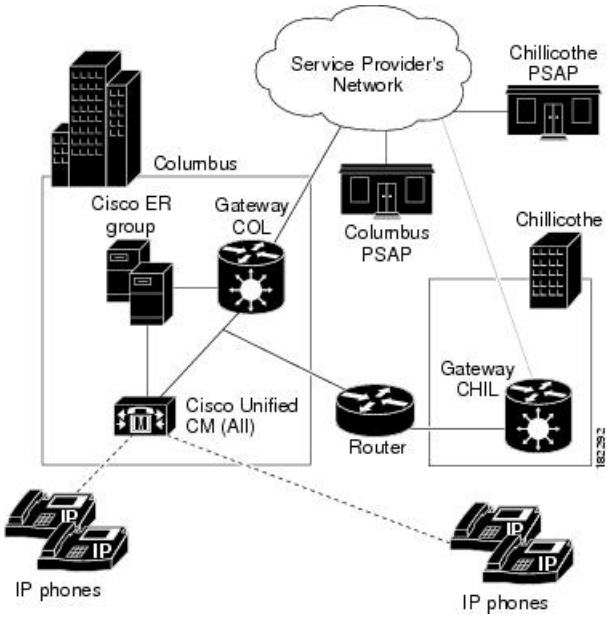
Related Topics

Emergency Call Process , on page 19
Emergency Responder and Your Network , on page 16
Determine Required Cisco Emergency Responder Groups , on page 27
Installation on a New System
Configure Cisco Unified Communications Manager

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 38.

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 for more information.

See these examples to extend this example to other networks:

- Deployment in Main Site and PSAP , on page 32
- Deployment in Main Site with Two or More PSAPs, on page 33
- Deployment in Main Site Serving Multiple Sites , on page 36
- Two Main Site Deployments , on page 38

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.

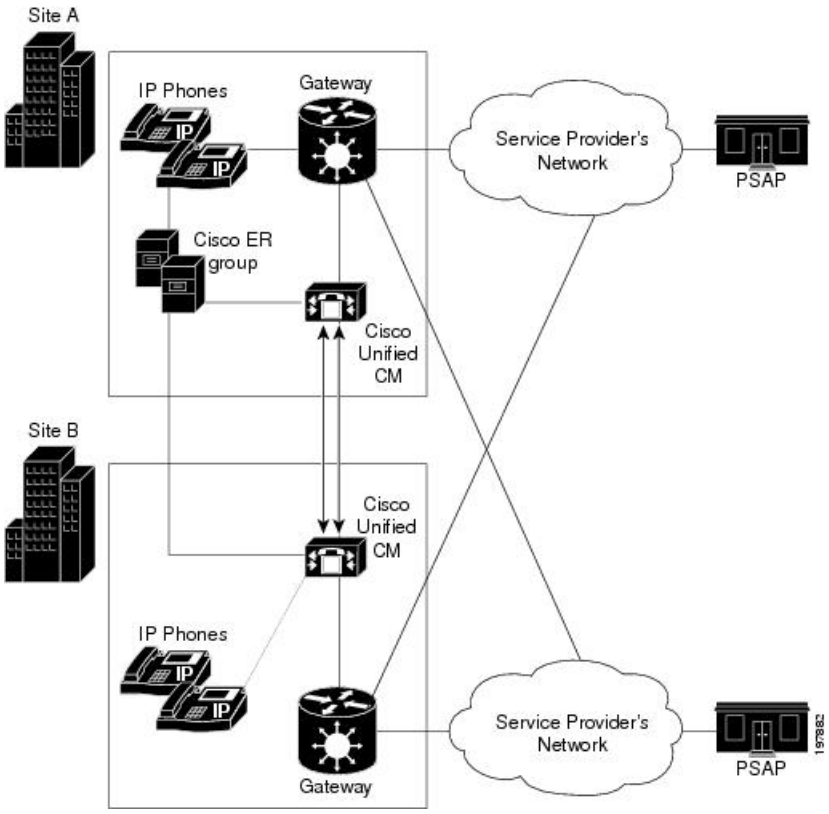
Related Topics

Emergency Call Process , on page 19
Emergency Responder and Your Network , on page 16
Determine Required Cisco Emergency Responder Groups , on page 27
Installation on a New System
Configure Cisco Unified Communications Manager

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 37 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 32
- Deployment in Main Site with Two or More PSAPs, on page 33
- Deployment in Main Site with Satellite Offices , on page 35
- Two Main Site Deployments , on page 38

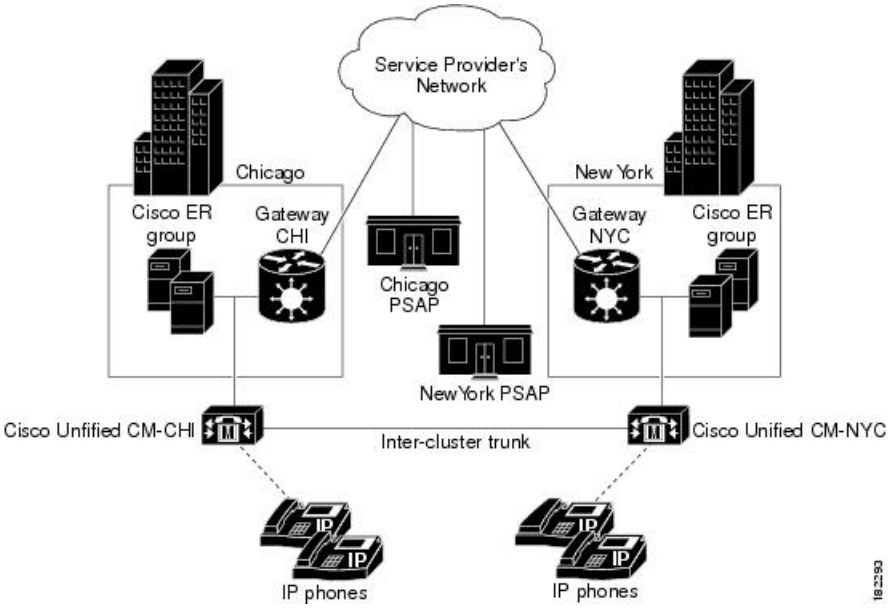
Related Topics

Emergency Call Process , on page 19
Emergency Responder and Your Network , on page 16
Determine Required Cisco Emergency Responder Groups , on page 27
Installation on a New System
Configure Cisco Unified Communications Manager

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 35 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 33 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.
- 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.

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.

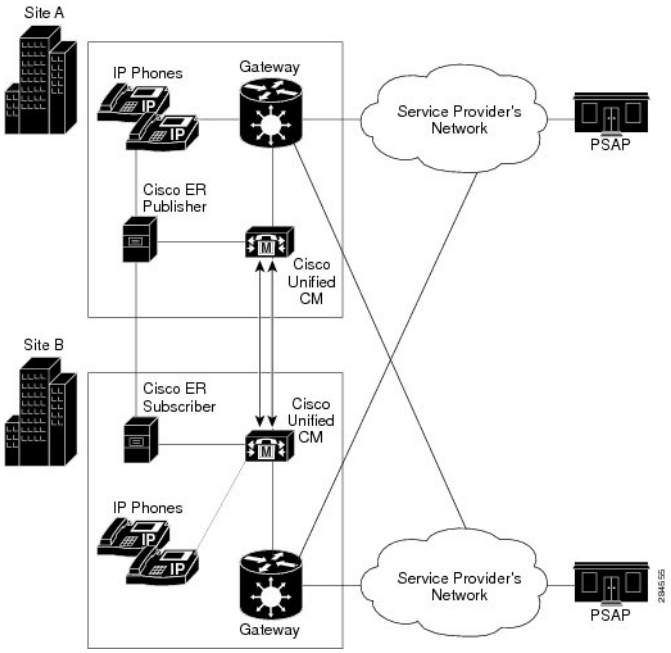
To enable phone movement between Chicago and New York, you must also configure an inter-cluster trunk to link the CiscoUnifiedCommunicationsManager clusters, and create an inter-Emergency Responder group route pattern so that Emergency Responder can transfer calls between CiscoUnifiedCommunicationsManager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

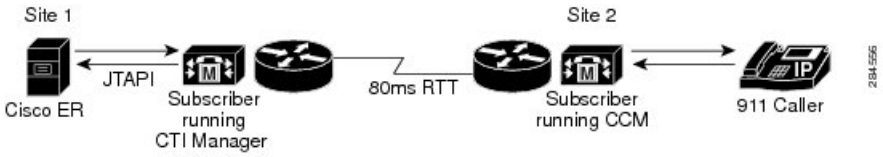
- At least 1.544 Mbps available bandwidth between ER publisher and ER subscriber (for data replication)
- No more than 80 msec RTT between any Unified CM server and either ER server

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.

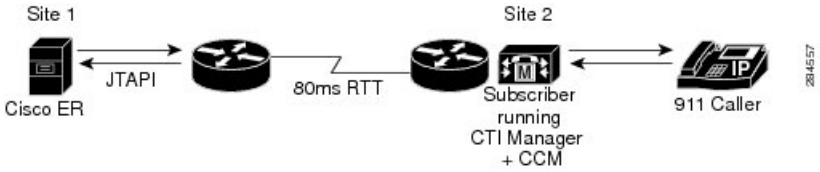
Figure 17: JTAPI Over the WAN During Normal Operations



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 39 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 32
- Deployment in Main Site with Two or More PSAPs, on page 33
- Deployment in Main Site with Satellite Offices , on page 35

- Deployment in Main Site Serving Multiple Sites , on page 36

Related Topics

Emergency Call Process , on page 19
Emergency Responder and Your Network , on page 16
Determine Required Cisco Emergency Responder Groups , on page 27
Installation on a New System
Configure Cisco Unified Communications Manager

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 19
Emergency Responder and Your Network , on page 16
Determine Required Cisco Emergency Responder Groups , on page 27
Installation on a New System
Configure Cisco Unified Communications Manager