Configure Cisco Emergency Responder

Cisco Emergency Responder Configuration Overview

After you install Cisco Emergency Responder (Emergency Responder) and configure Cisco Unified Communications Manager (Unified CM), you can configure Emergency Responder so that it begins managing emergency calls.

Configuration Overview

Emergency Responder provides several features, including expanded administrative website interfaces, role-based user management, and upload and download utilities.

Note Emergency Responder is compatible with Cisco EnergyWise, including provisions to detect user activity on powered-down phones.

Website Interfaces

Emergency Responder provides several web sites from which you can access and use different parts of the system. From the main Emergency Responder web page, you can access the following areas:

- Emergency Responder Serviceability
- Emergency Responder Administration (default home)
- CiscoUnifiedOS Administration
- Disaster Recovery System
- Emergency Responder User
- Emergency Responder Admin Utility

Each of these web sites allows a user access to different parts of the system and requires a separate login and password. Access to these web sites is controlled through the role-based user management mechanism (for more information, see Role-Based User Management , on page 2).

When the Emergency Responder system is first installed, a default Emergency Responder Administrator user is created. The default Administrator has full access to all web sites except the Cisco Unified OS Administration and Disaster Recovery System websites, and can create users, roles, and user groups. The default Administrator cannot be deleted from the system.

Related Topics

Cisco Emergency Responder Administration Web Interface
Cisco Emergency Responder Serviceability Web Interface
Cisco Unified Operating System Administration Web Interface
Disaster Recovery System Web Interface

Role-Based User Management

Emergency Responder uses a role-based user management mechanism. The information in the following topics describe this mechanism.

User Management

On installation, the system creates one default user, Emergency Responder Administrator. The Emergency Responder Administrator has access to all system administration screens except the Platform Administration and Disaster Recovery System screens. By default, the Emergency Responder Administrator user is assigned to the Emergency Responder System Administrator, Emergency Responder Serviceability, Emergency Responder Admin Utility, and Emergency Responder User user groups and has access to the resources defined for the Emergency Responder System Admin, Emergency Responder Serviceability, Emergency Responder Admin Utility, and Emergency Responder User roles.

Note The default Emergency Responder Administrator user cannot be deleted.

You can add additional users. After the additional users are added, you assign them to user groups. The new user then inherits the roles that were defined for that user group.

Related Topics

Emergency Responder User Management , on page 12
Find and List Users

Role Management

On installation, the system creates six default roles. The following table lists and describes the default roles.

Note Default roles cannot be deleted.

Table 1: Default Roles

Role	Description
Emergency Responder System Admin	Has access to all system administration screens.
Emergency Responder Serviceability	Has access to all serviceability screens.
Emergency Responder Admin Utility	Has access to all Admin Utility screens.
Emergency Responder Network Admin	Has access to Cisco Unified Communications Manager, LAN switch, and SNMP settings screens.
Emergency Responder ERL Admin	Has access to all ERL-related screens.
Emergency Responder User	Has access to the user screens.

When creating a new role or modifying an existing role, you specify which system resources are assigned to the role. A resource is the same thing as a web page or a menu item within the Emergency Responder administration website. For example, the **Find and List Roles** web page is a resource, as is the **User Management > Role menu** item.

The following table shows the resources that are available to each default role.

Note Some resources are groups of menu items. For example, the Logs menu in the Cisco Emergency Responder Serviceability website is one resource but it contains many submenus.

Table 2: Resources Assigned to Default Roles

Resource	Emergency Responder System Admin	Emergency Responder Network Admin	Emergency Responder ERL Admin	Emergency Responder Serviceability	Emergency Responder Admin Utility	Emergency Responder User
Add Subscriber	x					
Admin Utility	x					

Resource	Emergency Responder System Admin	Emergency Responder Network Admin	Emergency Responder ERL Admin	Emergency Responder Serviceability	Emergency Responder Admin Utility	Emergency Responder User
ALI Formatting Tool	x					
All Logs				x		
Application User	x					
Call History	x					
Unified CM Details	x	x				
Emergency Responder Groups in Cluster	x					
Change Unified CM Version					x	
Cluster DBHost Setting					x	
Control Center				x		
CPU and Memory Usage				x		
Device SNMP Settings	x	x				
Disk Usage				x		
ERL	x		x			
ERL Audit Trail	x					
ERL Debug Tool	x					
ERL Migration	x		x			

Resource	Emergency Responder System Admin	Emergency Responder Network Admin	Emergency Responder ERL Admin	Emergency Responder Serviceability	Emergency Responder Admin Utility	Emergency Responder User
Event Viewer				x		
File Management Utility	x					
Functional role	x					
Intrado ERL	x		x			
Intrado VUI Settings	x					
IP subnet	x		x			
License Management	x					
Mail Alert Configurations	x					
Manually Configured Phones	x		x			
MIB2 System Group Configuration				x		
Off-Premises ERL	x		x			
Onsite Contact	x		x			
Pager Alert Configurations	x		x			
Phone Search						x
Point to New Publisher					x	
Processes				x		
PS ALI Convert	x					

Resource	Emergency Responder System Admin	Emergency Responder Network Admin	Emergency Responder ERL Admin	Emergency Responder Serviceability	Emergency Responder Admin Utility	Emergency Responder User
PS ALI Export	x					
Purge	x					
Run Tracking	x	x				
Tracking Schedule	x	x				
Server	x					
Server Group	x					
LAN Switches	x	x				
SNMP V1/V3c Configuration				x		
SNMP V3 Configuration				x		
Switch Port	x		x			
Synthetic Phone	x		x			
Telephony	x					
Unlocated Phones	x		x			
User Call History						x
User Group	x					
User Settings	x					
Web Alert						x

Related Topics

Emergency Responder Role Management , on page 16
Find and List Roles

User Group Management

On installation, the system creates six default user groups. The following table lists and describes the default user groups.

Note Default user groups cannot be deleted.

Table 3: Default User Groups

User Group	Description
Emergency Responder System Administrator	Assigned System Administration roles
Emergency Responder Network Administrator	Assigned Network Administration role
Emergency Responder ERL Administrator	Assigned ERL Administration role
Emergency Responder Serviceability	Assigned Serviceability role
Emergency Responder Admin Utility	Assigned Admin Utility role
Emergency Responder User	Assigned User role

You can create additional user groups. When you create a user group, you assign roles and add users to the group. Multiple roles can be assigned to a single group. The users in the group have access to all the resources defined by the roles assigned to the group.

Related Topics

Emergency Responder User Group Management , on page 18
Find and List User Groups

Upload and Download Utilities

Emergency Responder includes download and upload utilities that allow you to transfer bulk data in the form of csv files from a Emergency Responder server to a local system (download) and from a local system to a Emergency Responder server (upload).

For example, you can export database details to a csv file and then download the csv file to a local system. On the local system, you can modify the csv file, upload it the Emergency Responder server, and import the data in the csv file into the Emergency Responder database.

The following table lists the Emergency Responder administrative web pages from which you can use the upload and download utilities and gives the navigation path to each page.

Note You can upload only four file types: xml, csv, lic, and txt. Filenames must not contain spaces.

Table 4: Administrative Web Pages Containing the Upload and Download Utilities

Page Name	Navigation Path
Find Conventional ERL Data	**ERL > Conventional ERL**
Find Off-Premises ERL Data	**ERL >Off-premises ERL >Off-premises ERL (Search and List)**
Find Intrado ERLs Data	**ERL > Intrado ERL > Intrado ERL (Search and List)**
LAN Switch Details	**Phone Tracking > LAN Switch Details**
Switch Port Details	**ERL Membership > Switch Ports**
Find and List IP subnets	**ERL Membership > IP subnets**
Find and List Manually Configured Phones	**ERL Membership > Manually Configured Phones**

Download File

Procedure

Step 1 From one of the pages listed in Table 4: Administrative Web Pages Containing the Upload and Download Utilities , on page 8, click **Export**. The Export page appears.

Step 2 If you have previously exported the data to a file, skip to Step 3. If you have not previously exported data to a file, use the **Select Export Format** pulldown menu to select the file format, then enter the name of the file to be created in the **Enter Export File Name** field. Click **Export**. The data is exported to the specified file.

Step 3 Use the Select a File to Download pulldown menu to select the file that you want to download, then click **Download**. The file is downloaded to your local system.

Upload File

Before you begin

Before beginning the procedure, make sure the file to be uploaded exists on your local system. The file can be one that was previously downloaded from a Emergency Responder server, or one that you created.

Procedure

Step 1 From one of the pages listed in Table 4: Administrative Web Pages Containing the Upload and Download Utilities , on page 8, click **Import**. The Import page appears.

Step 2 Click **Upload**. The Upload File page appears.

Step 3 Click **Browse** to select the file to be uploaded. A Choose File window opens and displays the files on your local system.

Step 4 Select the file to be uploaded and click **Open**. The pathname of the file to be uploaded appears in the **Select the file to be uploaded** field of the Upload File page.

Step 5 Click **Upload**. The file is uploaded to the Emergency Responder server. You can then import the data from the file.

Related Topics

Conventional ERL
LAN Switch Details
Switch Port Details
Find and List IP Subnets
Find and List Manually Configured Phone
File Management Utility

Emergency Responder Configuration

The following procedure provides information about the tasks that must be completed to configure Emergency Responder and indicates which user types can complete the tasks, with pointers to more detailed information.

Note Some of the following tasks listed can be done in parallel.

Procedure

	Command or Action	Purpose
Step 1	Create and set up Emergency Responder users and groups.	This step can be completed by the System Administrator.
Step 2	Identify the switches and configure the connection to them.	This step can be completed by the Network Administrator.
Step 3	Identify the onsite alert (security) personnel, create the emergency response locations (ERLs), assign them to phones, and transmit your ALI data to your service provider.	This step can be completed by the ERL Administrator.
Step 4	Set up Emergency Responder with Intrado V9-1-1 for Enterprise Service.	

Related Topics

Set Up Users and Groups , on page 9
Set Up Switch Connection , on page 10
Manage Onsite Alerts, ERLs, and ALI Data , on page 11
Set Up Emergency Responder with Intrado V9-1-1 for Enterprise Service , on page 12

Set Up Users and Groups

The following procedure provides information about the tasks that must be completed to set up Emergency Responder users and groups. This task can be completed by a System Administrator.

Procedure

	Command or Action	Purpose
Step 1	Create the users your organization requires for Emergency Responder administration.	
Step 2	Create the Emergency Responder group.	
Step 3	Set up the Emergency Responder group telephony settings.	
Step 4	Update Emergency Responder servers to the Emergency Responder group.	
Step 5	Upload the product license key.	
Step 6	Identify and configure the Unified CM clusters whose emergency calls this Emergency Responder group handles.	The network administrator can also perform this step.
Step 7	Understand recurring system administration tasks.	
Step 8	If you use Intrado V9-1-1 Service Provider for Enterprise Service, configure Emergency Responder to support Intrado V9-1-1 Service Provider for Enterprise Service.	
Step 9	If you support off-premise users, configure AXL authentication information with Unified CM.	

Related Topics

Emergency Responder Configuration , on page 9
Emergency Responder User Management , on page 12
Log In to Emergency Responder , on page 20
Set Up a Server Group, on page 23
Set Up Group Telephony Settings for Server , on page 24
Configure Servers , on page 26
Upload License File, on page 26
Identify Cisco Unified Communications Manager Clusters , on page 27
Emergency Responder System Administrator Role
Set Up Intrado VUI Settings
Set Up AXL Authentication

Set Up Switch Connection

The following procedure provides information about the tasks that must be completed to set up Emergency Responder switch connection. This task can be completed by a Network Administrator.

Procedure

- Enter the SNMP read community strings.

- Define the schedule Emergency Responder should use for updating information from the switches.
- Identify the switches that can have phones connected to them.
- Run the switch-port and phone update process so that Emergency Responder can identify the ports on the switches and whether phones are attached to them.
- Understand recurring network administration tasks.

Related Topics

Emergency Responder Configuration , on page 9
Set Up SNMPv2, on page 44
Define Phone Tracking and Switch Update Schedules, on page 46
LAN Switch Identification , on page 47
Manually Run the Switch-Port and Phone Update Process , on page 51
Emergency Responder Network Administrator Role

Manage Onsite Alerts, ERLs, and ALI Data

The following procedure provides information about the tasks that must be completed to Manage onsite alerts, ERLs, and ALI data. This task can be completed by an ERL Administrator.

Procedure

- Identify the onsite alert (security) personnel that should receive alerts from Emergency Responder.
- Create the ERLs.
- Assign the ERLs to switch ports.

Note The network administrator must add the switches and run the switch-port and phone update process before you can do this task.

- Add phones that Emergency Responder does not directly support.

Note Emergency Responder does not automatically track the movement of these phones.

- Identify the unlocated phones and work with the network administrator to resolve problems that are preventing Emergency Responder from locating these phones. Assign ERLs to the phones that remain.
- Export the ALI data and transmit it to your service provider. Work with your service provider to determine transmission requirements.
- Understand recurring ERL administration tasks.

Related Topics

Emergency Responder Configuration , on page 9
ERLs, on page 30
ERL Management , on page 30
Add Onsite Security Personnel, on page 32
ERL Creation , on page 33
Switch Port Configuration , on page 53
Manually Define Phones , on page 63

Identify Unlocated Phones , on page 61
Export ERL Information , on page 40
Export ALI Information for Submission to Your Service Provider , on page 41
Emergency Responder ERL Administrator Role

Set Up Emergency Responder with Intrado V9-1-1 for Enterprise Service

The following tasks apply when you use Emergency Responder with Intrado V9-1-1 for Enterprise Service:

Procedure

Step 1 Create Intrado ERL and verify the validity and consistency of the ALI data for the Intrado ERL against the Intrado TN database.

Step 2 Assign Intrado ERLs to switch ports, IP subnets, and unlocated phones.

Step 3 If you support off-premise users, create off-premise ERLs and assign to IP subnets and unlocated phones.

Note You cannot assign off-premise ERLs to switch ports.

Related Topics

Emergency Responder Configuration , on page 9
Set Up Intrado ERLs
Reconcile ALI Discrepancies
Switch Port Configuration , on page 53
Set Up Off-Premise ERL
Identify Unlocated Phones , on page 61

Emergency Responder User Management

When you install Emergency Responder, the system defines one default Emergency Responder Administrator user (see User Management , on page 2 for more information). You can also define additional users or modify existing users.

The information in the following sections describe how to add new users and how to modify and delete existing users.

Add Users

You can add users to the system and then assign them to user groups. The security levels for new users are determined by which user groups you assign them to.

In Emergency Responder, you can add a user either as a local user or a remote user. Remote users must use their Unified CM credentials or Active Directory credentials for authentication.

You can add users to either the primary and standby servers within a single Emergency Responder group. Because access is allowed based on the combination of the user groups defined on the two servers, a user that is defined only on the primary server can log into the backup server.

Before you begin

Develop a list of users for each security level. You must know the user names of all onsite alert personnel, and you should determine who should have access to each of the administration security levels.

Note You can use this procedure to add or remove users. However, you cannot remove the administrative user created at the time of Emergency Responder installation.

Procedure

Step 1 From the Emergency Responder Administration web interface, select **User Management** > **User**.

The Find and List Users page appears.

Step 2 Click the **Add New User** button. The User Configuration page appears.

Step 3 Enter the required information in the User Name, Authentication Mode, Password, Confirm Password and Unified CM Cluster fields.

Step 4 Click **Insert**.

Step 5 Repeat these steps to add additional users.

Step 6 To assign security levels to the new users, you must add them to one or more user groups.

Step 7 Repeat this procedure on the other Emergency Responder server in the Emergency Responder server group.

Note To remove a user from a group, you must remove the user from groups on both the primary and standby servers.

Modify Users

After you have created a user, you can change user authentication mode, change the password for a local user, or change a Unified CM cluster for a remote user.

Change User Authentication Mode

Procedure

Step 1 From the Emergency Responder Administration web interface, select **User Management** > **User**.

The Find and List Users page appears.

Step 2 Enter search criteria to find the specific user that you want to modify and click **Find**, or click **Find** without any search criteria to display all configured users. The search results are displayed.

Step 3 Click on the user name.
The User Configuration—Modify User page appears.

Step 4 Select the authentication mode that you want to assign to the user from the drop-down box:

- If you select Remote as the authentication mode, select a Unified CM Cluster from the drop-down box.
- If you select Local as the authentication mode, enter a password and reconfirm the password.

Step 5 Click **Update**.

Change Password for a Local User

Procedure

Step 1 From the Emergency Responder Administration web interface, select **User Management** > **User**.

The Find and List Users page appears.

Step 2 Enter search criteria to find the specific user that you want to modify and click **Find**, or click **Find** without any search criteria to display all configured users. The search results are displayed.

Step 3 Click on the user name.
The Modify User page, used for user configuration, appears.

Step 4 Select the authentication mode that you want to assign to the user from the drop-down box.

If you select Local as the authentication mode, enter a new password and reconfirm the new password.

Step 5 Click **Update**.

Change a Unified CM Cluster for a Remote User

In Emergency Responder, you can also change the Unified CM cluster of an existing remote user to another Unified CM Cluster.

Procedure

Step 1 From the Emergency Responder Administration web interface, select **User Management** > **User**.

The Find and List Users page appears.

Step 2 Enter search criteria to find the specific user that you want to modify and click **Find**, or click **Find** without any search criteria to display all configured users. The search results are displayed.

Step 3 If you select Remote as the authentication mode, select a Unified CM Cluster from the drop-down box.
The User Configuration—Modify User page appears.

Step 4 Select the new Unified CM Cluster for all the remote users.

Step 5 Click **Update**

Delete Users

Emergency Responder enables you to perform batch operations in which you can either delete a single user or delete multiple users in bulk.

Note You cannot delete the default administrative user created at the time of installing Emergency Responder.

Procedure

Step 1 From the Emergency Responder Administration web interface, select **User Management** > **User**.

The Find and List Users page appears.

Step 2 Enter search criteria to find the specific user that you want to delete and click **Find**, or click **Find** without any search criteria to display all configured users. The search results appear.

Step 3 Find the user that you want to delete and click the **Delete** icon for that user.

The system displays a warning prompting you to confirm the deletion.

You also can select multiple users from the list, both local and remote, by checking the check box and then clicking the **Delete Users** button to delete users in bulk.

The system displays a warning prompting you to confirm the deletion.

Step 4 Click **OK**. The user is removed from the system and all User Group associations to the user are deleted.

Related Topics

Log In to Emergency Responder , on page 20
Cisco Emergency Responder User Preparation

Changing Users to Remote in Bulk

Emergency Responder allows you to change the user to either local or remote. A remote user is authenticated using the Unified CM Cluster.

Before you begin

Note You must have system administrator or ERL administrator authority to access this page.

Procedure

Step 1 From the Emergency Responder Administration web interface, select **User Management** > **User**.

The Find and List Users page appears.

Step 2 Enter search criteria to find the specific user that you want to delete and click **Find**, or click **Find** without any search criteria to display all configured users. The search results appear.

Step 3 Click **Username**. The Modify User page, used for user configuration, appears.

Step 4 Select the authentication mode that you want to assign to the user. You can change a local user to remote user.

Step 5 Select an Unified CM Cluster from the drop-down box if you have changed the user to remote user.

Step 6 Click **Update**.

Note To change users in bulk, select the users that you want to change by checking the check box and then clicking the **Change to Remote Users** button. Select the Unified CM cluster from the drop-down box, as described in Step 6.

Emergency Responder Role Management

When you install Emergency Responder, the system defines six default roles (see Role Management , on page 3 for more information about the default roles). You can also define additional roles or modify existing roles.

The following topics describe how to add new roles and how to modify and delete existing roles.

Add Roles

You can add additional roles to the system and assign resources to them.

Note The default roles cannot be removed or modified.

Before you begin

Decide what additional roles you want to create and determine if any existing default role meets your needs.

Procedure

Step 1 From the Emergency Responder Administration web interface, select **User Management > Roles**.

The Find and List Roles page appears.

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

The Role Configuration page appears.

Step 3 Enter the Role Name (required) and Description (optional) in the text boxes.

Step 4 From the list of resources, check the check box next to the resources to which the new role should have access.

Step 5 Click **Insert** to add the new role to the system.

Step 6 Verify that you successfully added the new role by returning to the **User Management > Roles** page and performing a role search. Enter search criteria to find the specific role you just created and click **Find**, or click

Find without any search criteria to display all configured roles. The search results appear. Verify that the new role is listed.

Modify Roles

Note You cannot modify default roles.

Procedure

Step 1 From the Emergency Responder Administration web interface, select **User Management** > **Roles**.

The Find and List Roles page appears.

Step 2 Enter search criteria to find the specific role that you want to modify and click **Find**, or click **Find** without any search criteria to display all configured roles. The search results appears.

Step 3 Click the role name.

The Role Configuration—Modify Role page appears.

Step 4 If desired, modify the Role Name and Description (if one is listed) in the text boxes.

Step 5 From the list of resources, checking or unchecking the check boxes next to the resources to which the modified role should have access.

Step 6 Click **Update** to add the updated role information to the system.

Step 7 Verify that you successfully modified the new role by returning to the **User Management** > **Roles** page and perform a role search. Enter search criteria to find the specific role that you just modified and click **Find**, or click **Find** without any search criteria to display all configured roles. The search results appear. Click the role name and verify that the modified role information appears on the Role Configuration—Modify Role page.

Delete Roles

Note You cannot delete a default role.

Procedure

Step 1 From the Emergency Responder Administration web interface, select **User Management** > **Roles**.

The Find and List Roles page appears.

Step 2 Enter search criteria to find the specific role that you want to delete and click **Find**, or click **Find** without any search criteria to display all configured roles. The search results appear.

Step 3 Click the **Delete** icon for the role to be deleted.

A warning message displays asking you to verify that you want to delete the role.

Step 4 Click **OK** to delete the role.

The Find and List Roles page refresh and the roles are no longer listed in the Role Names list.

Emergency Responder User Group Management

When you install Emergency Responder, the system defines six default user groups (see User Group Management , on page 7 for more information about the default user groups). You can also define additional user groups or modify existing user groups.

You can create a user group to receive web alert from a specific ERL. You must associate this User Group with the Onsite Alert ID assigned for an ERL. For additional information, see Add Onsite Security Personnel.

Note The group members can still view all web alerts in the system, if applicable.

The following topics describe how to add new user groups and how to modify existing user groups.

Add User Groups

You can add user groups to the system and assign users and roles to each new user group.

Before you begin

Before you begin, you should decide what additional user groups that you want to create and determine if any existing default user groups meets your needs.

Procedure

Step 1 From the Emergency Responder Administration web interface, select **User Management > User Group**.

The Find and List User Groups page appears.

Step 2 Click **Add a User Group**.

The User Group Configuration—Add User Group page appears.

Step 3 Enter the User Group Name (required) and Description (optional) in the text boxes.

Step 4 Click **Add Users**.

The User Names page appears.

Step 5 Enter search criteria to find a specific user and click **Find**, or click **Find** without any search criteria to display all configured users. The search results appear.

Step 6 Check the check box to the left of the user names to be added and click **Add**.

The User Name page closes and the added names appears in the Add User to Group text box on User Group Configuration—Add User Group page.

Note To delete users from this list, select the user name and click **Remove Users**.

Step 7 Click **Add Roles**.

The Role Names page appears.

Step 8 Enter search criteria to find a specific role and click **Find**, or click **Find** without any search criteria to display all configured roles. The search results appear.

Step 9 Check the check box to the left of the roles to be added and click **Add**.

The Role Names page closes and the added roles appear in the Add Roles to Group text box on User Group Configuration page.

Note To delete roles from this list, select the user name and click **Delete Roles**.

Step 10 Click **Insert** to add the new role to the system.

Modify User Groups

Note You cannot modify default user groups.

Procedure

Step 1 From the Emergency Responder Administration web interface, select **User Management > User Group**.

The Find and List User Groups page appears.

Step 2 Enter search criteria to find the specific user group that you want to modify and click **Find**, or click **Find** without any search criteria to display all configured user groups. The search results appear.

Step 3 Click the user group name.

The User Group Configuration—Modify User Group page appears.

Step 4 (Optional) Modify the description of the User Group (if one is listed) in the **Description** text box.

Step 5 The **Add Users to Group** text box displays the names of the users currently assigned to the user group. To add additional users, follow the procedure given in the Add User Groups , on page 18.

To remove users, highlight the name of the users and click **Remove Users**.

Step 6 The **Assign Roles to Group** text box displays the names of the roles currently assigned to the user group. To add additional roles, follow the procedure given in the Add Roles , on page 16.

To remove roles, highlight the name of the roles and click **Remove Roles**.

Step 7 When you are finished, click **Update** to save the updated user group information to the system.

Step 8 Verify that you successfully modified the user group by returning to the **User Management > User Group** page and performing a search. Enter search criteria to find the specific user group that you just modified and click **Find**, or click **Find** without any search criteria to display all configured user groups. The search results appear. Click the user group name and verify that the modified user group information appears on the User Group Configuration—Modify User Group page.

Delete User Groups

Note You cannot delete the default user groups. You can only delete user groups that you have created.

Procedure

Step 1 From the Emergency Responder Administration web interface, select **User Management > User Group**.

The Find and List User Groups page appears.

Step 2 Enter search criteria to find the specific user group that you want to delete and click **Find**, or click **Find** without any search criteria to display all configured user groups. The search results appear.

Step 3 Click the **Delete** icon for the user group to be deleted.

Note You cannot delete the default user groups. You can only delete user groups that you have created.

A warning message appears asking you to verify that you want to delete the user group.

Step 4 Click **OK** to delete the user group.

The Find and List Roles page refresh and the deleted user group is no longer be listed in the User Groups list.

Cisco Emergency Responder Credential Policy

Cisco Emergency Responder includes an option to modify credential policy settings values. The system administrator can now enhance the security for all local and remote user accounts by modifying the default policy settings either in Credential Policy or in EnhancedSecurityMode Credential Policy.

For more information about the fields and their configuration options, see Credential Policy Page.

Log In to Emergency Responder

You must log into the Emergency Responder web interfaces to view or change the system configuration. The system administrator controls access using the Role-Based User Management mechanism. See Role-Based User Management , on page 2 for more information.

Before you begin

You must have a valid user ID and password before you can log into Emergency Responder. Contact the main Emergency Responder administrator if you cannot log into the interface and you are supposed to have administrative access.

Procedure

Step 1 From an supported browser, open this URL, where servername is the DNS name or IP address of the Emergency Responder server: http://servername/ceradmin.

The browser opens the Emergency Responder Server Administration page.

Step 2 Use the Navigation pull-down menu to select the website that you want to log into. The Emergency Responder websites are as follows:

- Emergency Responder Serviceability
- Emergency Responder Administration
- CiscoUnified OS Administration
- Disaster Recovery System
- Emergency Responder User
- Emergency Responder Admin Utility

To open the Log-in page, click one of websites in the list.

Step 3 Click **Go.**

The login screen for the selected website appears.

Step 4 Enter your user name and password, and click **Login**.

Emergency Responder logs you into the selected website. Unless you log in as a system administrator, some commands in the menus may have lock icons. These locks indicate pages that you cannot view because of your authorization level.

When you are finished, click **Logout** above the menu bar to log out.

Note In Emergency Responder 8.5 and above, the validation for Username is not case sensitive.

Related Topics

Emergency Responder User Management , on page 12
Emergency Responder Role Management , on page 16
Emergency Responder User Group Management , on page 18
Cisco Emergency Responder User Preparation

Restrict Maximum Number of Concurrent Sessions

Emergency Responder allows the administrator to restrict the maximum number of concurrent sessions that can be active at a time for any user. If this restriction is enabled, the administrator can specify a maximum limit (between 1 and15) for the number of concurrent sessions allowed.

This limit is applicable to all users configured in Emergency Responder.

Emergency Responder restricts users from creating more than the specified number of concurrent sessions. Users who attempt to create additional sessions that exceed the concurrent session limit are prevented from logging in to Emergency Responder and will see the following error message: **Session limit exceeded. Please log out of any existing sessions and try again**.

Note This limit is applicable to all users that exceed the limit.

Note This limit is imposed separately for each Emergency Responder website:

- Emergency Responder Administration
- Emergency Responder Serviceability
- Emergency Responder User
- Emergency Responder Admin Utility

Warning If a user logs in to an Emergency Responder website and closes the browser without logging out, the session remains active until it times out after a period of 30 minutes. During this period, if the user attempts to establish additional sessions beyond the prescribed limit, he will be unable to do so.

Before you begin

You must have system administrator authority to configure an Emergency Responder server group.

Procedure

Step 1 Select **System > CiscoER Group Settings**.

Emergency Responder opens the Emergency Responder Group Settings page.

Step 2 Check the **Limit Concurrent Sessions** check box. This option is used to enable limiting the number of concurrent sessions and enables the **Max. number of concurrent sessions** drop-down box.

Step 3 Select the maximum number of concurrent sessions that you want to impose on the Emergency Responder user, from the **Max. number of concurrent sessions** drop-down box.

Step 4 Click the **Update Settings** button to apply the new change.

Note You can disable the maximum number of concurrent settings by selecting **System > Emergency Responder Group Settings** and uncheck the **Limit Concurrent Sessions** check box.

Related Topics

Group Settings

Server and Server Group Configuration

The information in the following topics describe how to configure Emergency Responder servers and server groups, and the telephony connection between the Emergency Responder groups and Unified CM.

Set Up a Server Group

To configure a Emergency Responder server group, you must connect to the administration interface on one of the servers that is part of the group. An Emergency Responder server group consists of up to two Emergency Responder servers, a primary and a standby, or backup, server. This redundancy helps ensure that Emergency Responder remains available in case one server becomes disabled.

Consider placing the two servers in a group in separate physical locations so that problems that might affect one server do not affect the other, such as a fire, flood, or network disruption. See Data Integrity and Reliability for more information.

Before you begin

You must have system administrator authority to configure an Emergency Responder server group.

Procedure

Step 1 Select **System > CiscoER Group Settings**.

Emergency Responder opens the Emergency Responder Group Settings page.

Step 2 Fill in the group settings. Many fields have defaults that should work for most networks. At minimum, you must configure these fields:

- **CiscoER Group Name**—Enter a name for the group. This name is mainly for your use, so choose a name that you find meaningful.
- **SMTP Mail Server** and **Source Mail ID**—If you want Emergency Responder to send email alerts to your Emergency Responder system administrator and onsite alert personnel (security), enter the IP address or DNS name of a mail server, and the name of an account on that server to use for sending email. If you configure email addresses for onsite alert personnel, they receive email alerts from this account when an emergency call is made in their assigned area. If their email address is for an email-based paging system, they are paged.
- **Enable Secured connection**— If you want to send mails from the SMTP Mail Server in a secure mode, ensure to configure the SMTP Mail Server in a secure mode and the SMTP server certificate is added to the Tomcat trust store of the Cisco Emergency Responder prior to enabling the Enable Secure connection checkbox. Failing to do so may result in email alert delivery failure.
- **System Administrator Mail ID**—If you want Emergency Responder to send email alerts in the case of critical errors, enter the email account information for the system contact.
- **Calling Party Modification flag**—You must set this flag if you enabled Calling Party Modification when you created Emergency Responder as a Cisco Call Manager user.
- **Enable Syslog** and **Syslog Server**—You can configure Emergency Responder to send log messages to the Syslog Server. To do this, select **Enable Syslog** and enter the fully qualified DNS name of the Syslog server.

- **Security end user web interface language**—To display the Emergency Responder User web pages in French (Canada) or Spanish(Spain), select it in the drop-down box. The default language is English(US).
- **Enable AXL & Cluster Secured connection**—To secure cluster communication and AXL communication with other products. Ensure the Cisco Unified Communications Manager tomcat-trust certificate and the Cisco Emergency Responder server group certificate is added to the Tomcat trust store of the Cisco Emergency Responder (in both publisher and subscriber). Failing to do so may result in breaking of AXL communication between Cisco Unified Communications Manager and Cisco Emergency Responder, along with the cluster communication within the Cisco Emergency Responder group.

Step 3 When you are satisfied with your settings, click **Update Settings**.

Emergency Responder creates the Emergency Responder group.

Related Topics

Configure Servers , on page 26
Group Settings
Collect Information From Syslog

Set Up Group Telephony Settings for Server

You must configure the telephony settings to tell Emergency Responder which phone numbers it should use for emergency calls and ELINs.

Before you begin

You must have system administrator authority to configure the telephony settings.

Before you configure these settings, create the required route points and route patterns in Unified CM. See these topics for more information:

- Create Emergency Call Route Points
- Create Route Patterns for Inter-Cisco Emergency Responder Group Communication

Procedure

Step 1 Select **System > Telephony Settings**.

Emergency Responder opens the Telephony Settings page.

Step 2 Enter the telephony settings, as described in the Telephony Settings:

- **UDP Port Begin**—The first UDP port Emergency Responder can use for telephone calls. For example, 32000.
- **Inter Cisco ER Group Route Pattern**—The route pattern that other Emergency Responder groups use to route emergency calls to this group, for example, 1000.911.
- **PSAP Callback Route Point Pattern**—The CTI route point you created to receive calls from the PSAP. For example, 913XXXXXXXXXX (913 plus 10 Xs).
- **ELIN Digit Strip Pattern**—The digits to strip from the PSAP callback route point to reveal the ELIN. For example, 913.

- **Default ELIN Digit Translation**— If the Emergency Responder does not find a mapping between the caller's extension and ELIN, it will translate ELIN to Default ELIN Digit Translation Number and complete the PSAP call back.
- **Route Point for Primary Cisco ER Server**—The route point you created for the Emergency Responder primary server to use. For example, 711. You may change this number. See Modify the Emergency Number , on page 25.
- **Route Point for Standby Cisco ER Server**—The route point you created for the Emergency Responder standby server to use. For example, 912.
- **IP Type of Service (00-FF)**—The value of the type of service (ToS) byte in the IP header. The default 0xB8 implies a ToS class of Priority Queue. We recommend that this default value be used for Emergency Responder.
- **Onsite Alert Prompt Repeat Count**—The number of times a prompt is given on the onsite security phone.
- **Intrado Route Pattern**—The route pattern for an Intrado emergency response location (ERL).

Step 3 Click **Update Settings** to save your changes.

Modify the Emergency Number

You can configure or modify the emergency number that was automatically set at installation time by entering the number in the **Route Point for Primary CiscoER Server** field**.** Before you configure or change the emergency number, you must configure the new route point and associate it with the Emergency Responder user in Unified CM.

Caution Modify the emergency number during off-peak hours.

Procedure

Step 1 Associate the new route point with the Emergency Responder user in Unified CM. See Create Emergency Responder Cisco Unified Communications Manager User.

Step 2 Modify the route point for the new number: enter the number in the **Route Point for Primary CiscoER Server.** field.

Step 3 Click **Update Settings**.

Note Emergency Responder can still support only one emergency number. After you change it, Emergency Responder starts routing calls received at the new emergency number route point.

Related Topics

Telephony Settings
Create Emergency Call Route Points
Create Route Patterns for ERLs
Create Route Patterns for Inter-Cisco Emergency Responder Group Communications
Identify Cisco Unified Communications Manager Clusters , on page 27

Configure Servers

After you create an Emergency Responder group, you can use the Server Settings page to update Emergency Responder server settings (for example, to change the server name or to change the trace and debug settings) and to delete servers.

Before you begin

You must have system administrator authority to update or delete a Emergency Responder server.

Procedure

Step 1 Select **System > Server Settings**.

Emergency Responder opens the Server Settings page.

Step 2 Select the server name in the left-hand Servers list to change the server settings (Server Name or Debug Package List, or Trace Package List settings). Emergency Responder loads the server settings into the edit boxes. Make your changes and click **Update**.

Step 3 Select the server and click **Delete** to remove a server from the group. If you are permanently removing the server from your network, ensure that you make any required changes to your telephony network so that calls are not misdirected or dropped.

Step 4 When you are satisfied with your settings, click **Update**.

Emergency Responder saves your changes and displays them in the list of servers at the top of the page.

Related Topics

Installation on a New System
Set Up a Server Group, on page 23
Set Up Group Telephony Settings for Server , on page 24
Identify Cisco Unified Communications Manager Clusters , on page 27
Server Settings for Emergency ResponderServerGroup

Upload License File

Cisco Prime License Manager maintains the licensing for Cisco Emergency Responder 10.0 and later versions.

Use the Prime License Manager tool to obtain licenses from Cisco, to install the licenses, and to manage and view your inventory of licenses. This tool also tracks license compliance or noncompliance.

Related Topics

Emergency Responder Licensing
License Manager

Identify Cisco Unified Communications Manager Clusters

You must identify one Unified CM server per Unified CM cluster that you want to manage with the Cisco Emergency Responder group that you are configuring. Cisco Emergency Responder obtains the list of phones registered with these Unified CM servers and tracks the movements of these phones

CiscoEmergency Responder provides three levels of CTI failover. To enable the three levels of CTI failover, enter an IP address or DNS name for the primary CTI Manager, the Backup CTI Manager 1, and the Backup CTI Manager 2.

Before you begin

You must have system administrator or network administrator authority to identify the Unified CM clusters.

You must activate Cisco Unified Communications Manager on the server before Emergency Responder can access the Unified CM cluster list. For more information, refer to CSCsx52550 using the Software Bug Toolkit.

Every Unified CM server in the Unified CM cluster must be running SNMP services so that Emergency Responder can obtain the required information from the server.

Before configuring these settings, create the required users and CTI ports. This information must be complete before Cisco Emergency Responder tries to create a provider with the Cisco Emergency Responder cluster. Cisco Emergency Responder only registers the CTI ports and route points that are associated with the user when the provider is created. See these topics for more information:

- Create Emergency Responder Cisco Unified Communications Manager User
- Create Required CTI Ports

To identify one Unified CM server per Unified CM cluster that you want to manage with the Cisco Emergency Responder group you are configuring, follow these steps:

Procedure

Step 1 Select **Phone Tracking > CiscoUnifiedCommunicationsManager Details**.

Cisco Emergency Responder opens the Unified CM Details page.

Step 2 Enter the details for the Unified CM server:

- **CiscoUnifiedCommunicationsManager**—The IP address or DNS name of the server. This server must be running Unified CM and SNMP services. Do not define more than one Unified CM server within the same Unified CM cluster in the Emergency Responder configuration.
- **CTI Manager**—The IP address or DNS name of the CTI manager for the cluster to which the server belongs.
- **CTI Manager User Name**—The user you created for CiscoEmergencyResponder. See Create Emergency Responder Cisco Unified Communications Manager User for more information.
- **CTI Manager Password**—The user password.
- **Backup CTI 1 Manager**—The IP address or DNS name of the first backup CTI manager for the cluster.
- **Backup CTI 2Manager**—The IP address or DNS name of the second backup CTI manager for the cluster.
- **Telephony Port Begin Address**—The first CTI port address in the sequence of ports you created for Emergency Responder use. See Create Required CTI Ports for more information.

- **Number of Telephony Ports**—The number of CTI ports in the sequence you created for Emergency Responder use.

Step 3 To establish secure JTAPI communications, do the following:

a) Check the **Enable Secure Connection** check box.

b) Enter the following required information:

- TFTP Server IP Address
- TFTP Server Port

Note The TFTP Server Port field is pre-populated with a default value. If in Unified CM you entered a different value for the TFTP Server Port, you must enter that value here, replacing the default value.

- CAPF Server IP Address
- CAPF Server Port

Note The CAPF Server Port field is pre-populated with a default value. If in Cisco Unified CommunicationsManager you entered a different value for the CAPF Server Port, you must enter that value here, replacing the default value.

- Instance ID for Publisher
- Secure Authentication String for Publisher
- Instance ID for Subscriber
- Secure Authentication String for Subscriber

Note You must also configure secure JTAPI communications on your Cisco Unified CommunicationsManager cluster. See Create Required CTI Ports for details.

Step 4 To configure the AXL Settings, do the following:

a) Enter the AXL Username configured on the Cisco Unified Communications Manager.

b) Enter the password for the AXL User.

c) Enter the Port Number. By default Port 8443 is chosen.

Step 5 Select the **SNMP Settings** checkbox if the Cisco Unified Communications Manager has SNMPv3 enabled and Emergency Responder should discover it using SNMPv3.

Step 6 Click **Insert**.

Emergency Responder adds the Unified CM server to the list of servers. Repeat this procedure if you are supporting other Unified CM clusters with this Emergency Responder group.

Tip

- To view or change a Unified CM server settings, click the server in the list of servers. The settings are loaded into the edit boxes. To change a setting, edit it and click **Update**.
- To remove a Unified CM server from the Emergency Responder configuration, click it in the list of servers, then click **Delete.**

Related Topics

Cisco Unified Communications Manager Clusters

Set Up Emergency Responder Cluster and Cluster DB Host

Procedure

Step 1 Identify the following:

- All the Emergency Responder groups participating in the Emergency Responder cluster
- One of the Emergency Responder publishers as “Cluster DB Host”
- A password that is the same across the Cluster as “Cluster password”

Step 2 Using the Emergency Responder Admin Utility web interface, navigate to **Update > ClusterDB Host,** and enter the values from Step 1.

Step 3 Repeat steps 1 and 2 for each Emergency Responder server group in the cluster.

Step 4 Restart Emergency Responder services.

Note Emergency Responder server groups can communicate with Emergency Responder1.3, 2.x, 7.1 and 8.0 and later versions of Emergency Responder server groups in an Emergency Responder cluster.

Related Topics

Update Cluster DB Host
Update Emergency Responder Cluster Database Host Details

Cisco Unified Communications Manager Cluster Changes

If you change or upgrade the Unified CM cluster identified in Emergency Responder to a later version, you must use the Admin Utility to identify Emergency Responder with the later Unified CM version.

To change the Unified CM cluster that is identified in Emergency Responder to a different version, see Change Cisco Unified Communications Manager Version.

Work with Emergency Responder Locations

An emergency response location (ERL) defines the area in which an emergency call is made. Security personnel and emergency response teams use ERL information to locate an emergency caller.

Note Unified CM supports alerts to onsite security personnel from Cisco Emergency Responder and PSAP Callback on phones that have the Do-Not-Disturb or Call Forwarding feature enabled. For phones with a shared line, the PSAP Callback rings on the original device that had placed the emergency call.

Emergency Responder system administrators or ERL administrators can create and modify ERLs. The following sections explain ERLs in greater detail and explain how to work with them in Emergency Responder.

ERLs

An emergency response location (ERL) is a building, area within a building, or outside area (if you extend phone service outdoors) that is to be considered as a single location for emergency response purposes. All telephones within the ERL are treated as coming from the same location.

When someone makes an emergency call, the public safety answering point (PSAP) and your onsite alert (security) team are notified of the ERL. If the emergency requires locating the individual who placed the emergency call, the response teams will have to find the person within the ERL. You can include more specific information using the Phone Location field for individual switch ports. This level of detail is only available for automatically tracked phones, and only appears on the Web Alert screen for onsite alert personnel.

This is similar to the way emergency calls are handled for individual home users: emergency response teams know the house from which the call was placed, but have to search from room to room until they find the caller. The bigger the house, the longer the potential search. Likewise, the larger you make your ERLs, the longer it might take a response team to find an emergency caller.

The laws relating to size of ERLs can vary for different cities, states, and countries. You are responsible for learning your local statutes and developing ERLs that satisfy those statutes. Work with your telephone service provider; they can help you understand the laws. Ultimately, you have to submit the automatic location information (ALI) for your ERLs to your service provider so that calls from your ERLs are routed to the appropriate PSAPs.

Here are some examples of possible ERLs:

- You have a 25-story building, each floor has 10,000 square feet of office space. You might create 25 ERLs, one per floor, or you could divide each floor in half and create 50 ERLs, two per floor.
- You have 5 buildings. Each building was a former home, and they are approximately 3000 square feet. You might create 5 ERLs, one per building, even though some of the buildings are multistory.
- You have a 5-story building, but the building is very large, so that each floor has 100,000 square feet of office space. You might create 20 ERLs per floor for a total of 100 ERLs, each ERL covering approximately 5,000 square feet.
- You have a high concentration of telephones, and local standards require that an ERL have no more than 48 telephones. In this case, you have to define zones based on telephone coverage, rather than on physical space. Try to create zones that are recognizable as a physical location, for example, BldJFloor5Row3.

Related Topics

ERL Management , on page 30
ERL Creation , on page 33
Export ERL Information , on page 40
E911 and Cisco Emergency Responder Terminology
Emergency Call Process

ERL Management

To establish a useful set of ERLs, consider following these steps:

1. Become familiar with local statutes on emergency call requirements. Local laws might have specific requirements or recommendations on the maximum size of an ERL (for example, no larger than 7,000 square feet).

2. Talk to your service provider to learn about their rules or recommendations.
3. Work with the security personnel in your organization to determine what they feel is required for them to effectively respond to an emergency call. Besides having suggestions about the size of the various zones, security personnel should also review the ERL-naming strategy because the ERL name is one of the major data points they use to locate the emergency caller.

   Security personnel also can use these fields to help locate a caller:

   - The Location field in the ALI, which you can use to clarify ERL names, for example, by including the complete street address of the building. Although security can also view the ALI from the Emergency Responder user interface, it takes a few extra steps to view the entire ALI, so including a complete address in the Location field can expedite response.
   - The Phone Location field associated to the switch port. You can use this field to fine-tune the location, for example, by specifying the office or cube number that the port serves.

4. Use Emergency Responder to enter information about your security (onsite alert) personnel. You should enter this information before defining the ERLs, because during ERL definition you assign personnel to each ERL.
5. Use Emergency Responder to define the ERLs and their ALI. See ERL Creation , on page 33 for more information.
6. Assign switch ports to the correct ERL and define the phone location for the port. See Switch Port Configuration , on page 53 for more information. Someone with network administrator authority must first add the switches to the Emergency Responder configuration before you can complete this task.
7. Define any phones that are not directly supported by Emergency Responder. See Manually Define Phones , on page 63, for more information.
8. After you are satisfied with the ERL and ALI definitions, export the ALI information and submit it to your service provider. Work with your service provider to determine the file format and submission requirements. You must submit this information so that emergency calls from your ERLs can be routed to the correct public safety answering point (PSAP). See Export ERL Information , on page 40 and the Export ALI Information for Submission to Your Service Provider , on page 41 for more information.

   After you complete this task, emergency calls from your ERLs should result in the correct onsite response personnel receiving notification of an emergency call, and the correct local PSAP receiving the actual emergency call.

Note Ensure that you submit each ALI export file as you create it. The ALI export records include an indication that the record is either new or modified. If you do not submit an ALI export file, the subsequent file you submit might have incorrect status indications, which can result in your service provider rejecting some, or possibly all, of your submitted records.

9. Ensure you update the ERL, ALI, and switch port information as you:
   - Add or remove switches or ports
   - Add or remove manually defined phones
   - Add or remove ERLs
   - Update ALIs

Any time you update the ELINs for an ERL, or the ALI, you should reexport ALI data and submit it to your service provider.

Related Topics

ERLs, on page 30
Emergency Responder ERL Administrator Role

Add Onsite Security Personnel

You must identify your security, or onsite alert personnel so that you can assign them to your emergency response locations (ERLs). If an emergency call is made from an ERL, the associated onsite alert personnel receive:

- A web-based alert on the Emergency Responder end-user interface specific to emergency calls originating from the assigned ERL. They also can view all alerts in the system.
- An email message. If you use an email-based paging address, the message results in a page.
- A telephone call indicating that an emergency call was made.

Before you begin

You must log into Emergency Responder with system administrator or ERL administrator authority.

Collect information about all of your onsite alert personnel, including names, telephone numbers, and email addresses. Also, develop a unique identification name for each, if you do not already have one readily available (such as badge number).

Procedure

Step 1 Select **ERL > Onsite Alert Settings**.

Emergency Responder opens the Onsite Alert Settings page.

Step 2 Enter the unique ID, name, telephone number, email address, and pager address, and User Group of a security or onsite alert person.

Unique ID might be a badge number, email name, or other site-specific unique name. You use this ID to assign the person to an ERL, so ensure that you use a naming strategy useful to you.

You can use an email-based paging address for the email address, so that onsite alert personnel receive a page rather than an email.

Step 3 Click **Insert**.

Emergency Responder adds the person to the list of onsite personnel. Repeat until you define all security or onsite personnel.

Tip

- To delete a person, first remove the person from all ERL definitions. Then, in the Available Onsite Alerts list on the Onsite Alerts Settings page, click the **Delete** icon corresponding to that person's record.
- To modify onsite alert settings, click on the person's Onsite Alert ID, Onsite Alert Name, Onsite Alert Number, Onsite Alert Email Address or Onsite Alert Pager Address in the Available Onsite Alerts list. The information for that person displays in the Modify Onsite Alert Contact section of the page. Modify the information as needed and then click **Update**. You cannot change a person's Onsite Alert ID: to change the Onsite Alert ID, delete the person's entry and create a new one.

ERL Creation

The following sections describe how to create emergency response locations (ERLs).

Set Up Default ERL

Emergency Responder does not automatically assign new switch ports and unlocated phones to the default emergency response location (ERL). New switch ports and unlocated phones are treated as ERLs that are not configured.

You must not configure the default ERL to any of the Switch Ports, Unlocated Phones, Manually Configured Phones or IP subnets. The default ERL is used internally by Emergency Responder only if no other ERL is configured for that phone.

Emergency Responder also uses the default ERL for all emergency calls when the Emergency Responder server is first started (or restarted when there is no standby Emergency Responder server) until the initial switch port update is finished. (This process is started immediately.)

Before you begin

You must log into Emergency Responder with system administrator or ERL administrator authority.

You must first configure the required ELINs in Unified CM.

Procedure

Step 1 Select **ERL > Conventional ERL**.

Emergency Responder opens the Find Conventional ERL Data page.

Step 2 Click **Configure Default ERL**.

Emergency Responder opens the ERL Information for Default window.

Step 3 Fill in the ERL Information for Default window.

Step 4 Click **ALI Details**.

Emergency Responder opens the ALI Information window.

Step 5 Fill in the ALI Information window.

When finished filling in the ALI, click **Update ALI Info**. Emergency Responder saves your ALI. Click **Close** to close the window.

Step 6 Make the ERL Information for Default window the active window if it is not, and click **Update**.

Emergency Responder saves the ERL and its ALI.

Step 7 Click **Close** to close the window.

Tip You cannot delete the default ERL. In addition, you cannot configure other ERLs unless the default ERL is configured.

Related Topics

Conventional ERL
Add New ERL
ALI Information
ALI Information
Set Up Individual ERL and Automatic Location Information (ALI) , on page 35
ERLs, on page 30
ERL Management , on page 30

Set Up ERLs for Non-PSAP Deployment

You may want to deploy Emergency Responder for on-site alerts only. That is, instead of routing emergency calls to a public safety answering point (PSAP), you route emergency calls to a specified security phone.

There are two ways to set up non-PSAP deployments:

- **Configure Security IDs Only**—In this scenario, you configure security IDs for the zones for any ERL; you do not configure route/translation patterns. All emergency calls are routed to the ERL security. If this fails, the calls are routed to the default ERL security. Emergency Responder then initiates a call to the configured security phone and plays prompts to alert security personnel to the emergency call.
- **Configure Security IDs and Route/Translation Patterns**—In this scenario, you configure security IDs for the zones for any ERL and you also configure a route/translation pattern without an ELIN number. Emergency Responder displays a popup warning message alerting you that this zone will not have an ELIN. The emergency call is routed using the route/translation pattern; If this fails, the default pattern is used. Emergency Responder then initiates a call to the configured security phone and plays prompts to alert security personnel to the emergency call.

Note In this scenario, you must use a different route/translation pattern for each zone.

Procedure

Step 1 Identify the security personnel to be notified in case of an emergency call (see Add Onsite Security Personnel, on page 32).

For example, configure security A with directory number 1000.

Step 2 Add an ERL with no route pattern or ELIN, but only with security IDs for that ERL (see ERL Creation , on page 33).

For example, add ERL X with security A.

Step 3 Go to the switch port screen and assign discovered switch ports to the already configured ERLs (see Switch Port Configuration , on page 53).

For example, associate switch ports of switch IP Y to ERL X.

All emergency calls from any phone connected to switch IP Y use ERL X and ring on the security A directory number 1000.

Note If you use Layer 3 (IP) roaming for wireless IP phones or wireless phones register using their Wireless Access Point's IP address, then Emergency Responder cannot automatically track movement of these phones. This is because Emergency Responder uses the IP address of the phone to determine the phone's location. Do not use Layer 3 roaming if you need Emergency Responder to automatically track movement of wireless phones in your network.

Set Up Individual ERL and Automatic Location Information (ALI)

This section explains how to define a single ERL. Because several ERLs often have similar information, see "Import Several ERLs" section for strategies for simplifying the definition of similar ERLs.

Before you begin

You must log into Emergency Responder with system administrator or ERL administrator authority.

Procedure

Step 1 Select **ERL > Conventional ERL**.

Emergency Responder opens the Find conventional ERLs page.

Step 2 Click **Add New ERL**.

Emergency Responder opens the Add New ERL window.

Step 3 Fill in the Add New ERL window.

Step 4 Click the **Add ALI** button.

Emergency Responder opens the ALI Information window.

Step 5 Fill in the ALI Information window.

When finished filling in the ALI, click **Save and Close**.

Step 6 Make the Add New ERL window the active window if it is not, and click **Insert**.

Emergency Responder saves the ERL and its ALI.

Step 7 Click **Close** to close the window.

Tip

- To create an ERL that is similar to an existing ERL, click **Find** to list the existing ERLs, then click copy for the similar ERL. Emergency Responder creates a copy of some ERL and all ALI information, which you can modify for the new ERL.
- You can create or update tags to simplify the ALI definition process. Navigate to the ALI Information window, and look for information about the location of the samplevalidate.txt file. The sample file explains how to set up tags. When you have created or updated the desired tags, select the tag name on the ALI Information window and the ALI fields are loaded with the settings associated with the tag.

Related Topics

Conventional ERL
Add New ERL
ALI Information
Import Several ERLs , on page 36
ERLs, on page 30
ERL Management , on page 30

Import Several ERLs

Rather than defining ERLs one at a time, you can create a file that contains more than one ERL definition, and import these ERLs at the same time into your Emergency Responder configuration. This is especially useful if you already have ERL definitions set up in a spreadsheet, or if you are recovering an Emergency Responder configuration using ERL data exported from Emergency Responder.

Before you begin

You must log into Emergency Responder with system administrator or ERL administrator authority.

Prepare an import file. Emergency Responder includes detailed information about the required file format on the Import ERL data page. The page also includes the location in which you must place the file to import it.

You can import conventional, off-premise, or Intrado ERLs. Click the **Import** link in the upper-right corner of the Find Conventional ERL Data Page, Find Off-Premises ERLs Data page, and the Find Intrado ERLs Data page.

Use the following procedure to view the format, create or update your file, copy the file to the required location, and then follow the procedure to import the file.

Procedure

Step 1 In the Find ERL page (Find Conventional ERL data page, Find Off-Premises ERLs data page, or the Find Intrado ERLs data page), click **Import**.

Emergency Responder opens the Import ERL data page.

Step 2 Select the format of your import file (csv or xml) from the pull-down menu.

Step 3 Click **Upload** to upload the file from your local machine.

Step 4 Select your import file.

Step 5 Click **Import**.

Emergency Responder imports your ERL and associated ALI data, and displays the status of the import as it proceeds. The imported data overwrites existing conflicting data in the Emergency Responder configuration.

Step 6 Click **Close** to close the Import ERL Data window.

Related Topics

Import ERL Data
Set Up Individual ERL and Automatic Location Information (ALI) , on page 35
ERLs, on page 30
ERL Management , on page 30
Upload File , on page 8
ERL Creation , on page 33
Set Up Off-Premise ERL
Set Up Intrado ERLs

Convert ALI Data

Use the PS-ALI Converter tool to generate an ERL csv (Comma Separated Value) text file that can be accepted by the Emergency Responder ERL. You must first upload an existing ALI file in NENA 2.0 format to Emergency Responder before converting it.

Before you begin

You must log into Emergency Responder with system administrator or ERL administrator authority.

To convert ALI data, follow these steps:

Procedure

Step 1 Select **Tools > PS-ALI Converter.**

Emergency Responder displays the PS-ALI Converter page.

Step 2 Click the **Upload PSALI file** button to upload an ERL file in NENA 2.0 format. The Upload File page appears.

Step 3 Follow the instructions in the Upload File , on page 8 to upload the ERL file.

Step 4 Select the uploaded file from pulldown menu.

Step 5 In the Output file (in csv format) Name field, enter the name of the converted csv file you want to create.

Step 6 Click **Convert** to create the csv file.

The generated csv file is in the following folder:

```
%cerroot%/import
```

You can import the file or download the file using the File Manager utility.

Step 7 Modify the converted csv file as needed. For example, add the ERL name, route pattern, and security details to update the ERL.

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

Related Topics

Import ERL Data
Set Up Individual ERL and Automatic Location Information (ALI) , on page 35
ERLs, on page 30
ERL Management , on page 30

Set Up IP Subnet-based ERLs

In addition to supporting switch port-based ERLs, Emergency Responder supports IP subnet-based (Layer 3) ERLs. You can configure IP subnets and assign ERLs to the configured IP subnets; Cisco Emergency Responder then routes the emergency calls based on the configured IP subnet and ERL associations.

This feature is useful in environments where strict IP addressing rules are followed and cubicle-level location is not required, such as configurations with wireless phones.

Use IP subnet-based ERLs to locate and track wireless endpoints, such as CiscoUnifiedWirelessIPPhone7920 series devices and Cisco clients using wireless IP connection. Cisco Emergency Responder cannot locate or track wireless endpoints to a CiscoAccessPoint.

Note Subnet-based tracking is limited by the IP subnet addressing plan. It cannot distinguish location within a same IP Subnet.

Before you begin

You must have system administrator or ERL administrator authority to access this page.

Procedure

Step 1 Select **ERL Membership > IP subnets** and click the **Add new IP subnet** link on the Find and List IP Subnets page.

Emergency Responder opens the Configure IP Subnets page.

Step 2 At the Subnet ID field, enter the IP address of the subnet that you want to define, for example,10.76.35.0.

Step 3 At the Subnet Mask field, enter the mask of the subnet that you want to define, for example, 255.255.255.224.

Step 4 To select the ERL you want to assign to the subnet, click the **Search ERL** button next to the ERL Name field. The Find ERL page appears.

Step 5 Enter the ERL Search Parameters and click **Find**. The search results appear.

Step 6 Click the radio button next to the ERL that you want to assign to the subnet and click **Select ERL**. The Find ERL page closes.

Step 7 On the Configure IP Subnet page, click **Insert** to add the subnet.

A popup message requests that you force a switch port update. You can do this after all the IP subnets have been added.

Step 8 To change the fields on this page back to the last saved settings, click **Cancel Changes**.

Step 9 To return to the Find and List IP Subnets page, click **Back to IP Subnet Search**.

Related Topics

Find and List Synthetic Phones
Add New Synthetic Phone

Set Up Test ERLs

You can use Cisco Unified Operations Manager to monitor the health and functionality of Emergency Responder.

To use Cisco Unified Operations Manager with Emergency Responder, you configure a test ERL for conventional ERLs, then add a synthetic phone and associate the synthetic phone to the test ERL. When a synthetic phone makes an emergency call, Emergency Responder uses the associated test ERL to route the call.

Note You can configure test ERLs only to synthetic phones.

Note You cannot configure test ERLs for off-premise ERLs and Intrado ERLs.

All synthetic phones used for Emergency Responder testing must belong to one of the configured test ERLs. For phones used for test ERLs, you enter the MAC address or address range allotted for synthetic phones.

The following conditions apply to test ERLs:

- Calls from synthetic phones are not logged in Call History logs.
- Web alerts are not generated for emergency calls from synthetic phones.
- Email alerts are not generated for emergency calls from synthetic phones.
- PS-ALI records for test ERLs are not exported in NENA export files.

Tip You do not need to enter ALI data for test ERLs. Non-test ERLs must contain ALI data.

Before you begin

You must have system administrator or ERL administrator authority to reach this page.

Procedure

Step 1 Select **ERL** > **Conventional ERL** and click **Add New ERL** on the ERL Configuration page.
Step 2 At the ERL field, enter a name for the test ERL.
Step 3 At the Test ERL field, check the box to select it.

Note This setting is not available on the ERL Information for Default; default ERLs may not be used as test ERLs.

Note Do not click **ALI Details** to enter ALI data. You do not need to enter ALI data for test ERLs; only non-test ERLs must contain ALI data.

Step 4 Click **Insert** to save the test ERL and click **Close** to close the window.

Step 5 Select **ERL Membership > Synthetic Phones** and click **Add New Synthetic phone** on the Find and List Synthetic Phones page.

Step 6 In the MAC Address field, enter the MAC address or the range of MAC addresses allotted for synthetic phone.

Enter the MAC address in this format:

xx-xx-xx-xx-xx-xx

or

xxxxxxxxxxxx

The synthetic MAC address must be within the following range:

00059a3b7700 - 0059a3b8aff

Step 7 In the ERL Name field, enter the test ERL that you want to assign to the synthetic phone. Select the configured test ERL from the drop-down list or type in a valid test ERL name.

Step 8 Click **Insert** to add the phone to the list of defined synthetic phones.

Step 9 To change the fields on this page back to the last saved settings, click **Cancel Changes**.

Related Topics

Find and List Synthetic Phones

Add New Synthetic Phone

Export ERL Information

Use the Export ERL page to create ERL export files for your own use, for example, to back up or move an ERL configuration. You can export conventional, off-premise, or Intrado ERLs. Click the **Export** link in the upper-right corner of the Find Conventional ERL Data page, Find Off-Premises ERLs Data page, and the Find Intrado ERLs Data page.

Note Do not submit ERL export files to your service provider; they are not exported in a format that your service provider can use.

For information about exporting ALI information, see Export ALI Information for Submission to Your Service Provider , on page 41.

For information about reformating ALI data to be accepted by the ERL, see Export ALI Information for Submission to Your Service Provider , on page 41.

Before you begin

You must log into Emergency Responder with system administrator or ERL administrator authority.

Procedure

Step 1 In the Find ERL page (Find Conventional ERL Data page, Find Off-Premises ERLs Data page, or the FindIntrado ERLs Data page), click **Export**.

Emergency Responder opens the Export ER Data window.

Step 2 Select the Export Format (csv or xml) from the pull-down menu.

Step 3 Enter the name of the file to be exported in the Enter Export File Name field.

Step 4 Click **Export**.

Emergency Responder creates the export file, and tells you the location where the file was created and how many records were exported.

Step 5 Select the exported file from the pull-down menu and click **Download** to download it to your local machine.

Step 6 Click **Close** to close the Export ERL Data window.

Related Topics

Export ERL Data
ERLs, on page 30
ERL Management , on page 30
ERL Creation , on page 33
Set Up Off-Premise ERL
Set Up Intrado ERLs

Export ALI Information for Submission to Your Service Provider

Your service provider and their database provider need your automatic location information (ALI) so that emergency calls from your conventional ERLs can be routed to the correct public safety answering point (PSAP). The PSAP can also use this information to dispatch emergency response teams (such as police, fire, medical) to deal with the emergency. As you create and update your ERLs and their ALIs, make sure that you export the data and send it to your service provider or the database provider they identify.

See ALI Formatting Tool chapter for information about sending ALI details to your service provider.

Before you begin

You must log into Emergency Responder with system administrator or ERL administrator authority.

Caution Ensure that you submit each ALI export file as you create it. The ALI export records include an indication that the record is either new or modified. If you do not submit an ALI export file, the subsequent file you submit might have incorrect status indications, which can result in your service provider rejecting some, or possibly all, of your submitted records.

Procedure

Step 1 Select **Tools > Export PS-ALI Records**.

Emergency Responder opens the Export PS-ALI Records page.

Step 2 At the **Select the NENA Format** field, choose the format required by your service provider from the drop-down list.

Step 3 At the File to Export field, enter the name of the file to export.

Step 4 At the **Company Name** field, enter your company name.

Note Emergency Responder automatically increments the Cycle Counter each time you export data. You do not need to change this counter unless you are redoing or correcting a previous exportation. However, changing the sequence number does not affect the data placed in the file. If you are redoing an export, you have to manually edit the export file to change the record status fields.

Step 5 Click **Export**.

Emergency Responder creates the export file and tells you how many records were exported.

Step 6 Click **Download** to download the file to your local machine.

Step 7 Click **Close** to close the Export ALI Records window.

Step 8 Use your service provider's method of transmitting the file to the service provider.

Related Topics

ALI Information
Export ERL Data
Export PS-ALI Records
ERLs, on page 30
ERL Management , on page 30

View Audit Trail for ERL

You can view the audit trail for an ERL to determine how, when, and by whom an ERL was created or changed.

Before you begin

You must have system administrator, ERL administrator, or network administrator authority to view the audit trail.

Procedure

Step 1 Select **Reports > ERL Audit Trail**.

Emergency Responder opens the ERL Audit Trail page.

Step 2 Enter search criteria to select the ERLs whose audit history you want to view.

To view all ERLs, click **Find** without entering any criteria.

To narrow your search:

a) Select the field that you want to search on, select the search relationship, and enter the search string. For some fields, you can select valid strings from the right-most drop-down list.
b) To search on a combination of fields, click **More** to add additional search fields. Select **Any** at the top of the list to indicate that ERLs that match any search criteria be selected (an OR search); select **All** to indicate that only ERLs that match every criteria be selected (an AND search).
c) Click **Find** when you have entered all of the search criteria.

Emergency Responder lists the matching audit records. If there are a lot of matches, Emergency Responder uses several pages to display them. Use the links at the bottom of the list to change pages.

Tip To view the audit trail of a specific ERL, click **View** in the Audit Trail column in a list of ERLs shown on the Find and List ERLs page.

Related Topics

ERL Audit Trail
Work with Emergency Responder Locations , on page 29

Emergency Responder Switch Configuration

Before you can assign switch ports to ERLs, you must identify the switches used in your network to Emergency Responder. The following topics describe the switch requirements and how to identify switches to Emergency Responder.

Switch Requirements for Emergency Responder

Emergency Responder uses Cisco Discovery Protocol (CDP) to locate phones, so you should enable CDP on all of your switches. If you do not enable CDP, Emergency Responder must use the Content Addressable Memory (CAM) table on the switch to track phones. Using the CAM table is less efficient than using CDP.

If some of the phones on your network do not use CDP, Emergency Responder tracks them using the CAM table.

Ensure that the switches to which phones are attached are supported by Emergency Responder, and that the switches are running the required software version. The Network Hardware and Software Requirements lists the supported switches and software versions.

If you are using Catalyst 3500 switch clusters, you must assign IP addresses to every switch. Emergency Responder cannot work with a switch unless the switch has an IP address.

Related Topics

Set Up SNMPv2, on page 44
Define Phone Tracking and Switch Update Schedules, on page 46
LAN Switch Identification , on page 47
Manually Run the Switch-Port and Phone Update Process , on page 51

Set Up SNMP Connection

Emergency Responder uses SNMP to obtain information about the ports on a switch. Emergency Responder must obtain this port information so that you can assign the ports to ERLs, and so that Emergency Responder can identify phones that are attached to the ports and update their ERL assignments.

Emergency Responder only reads SNMP information, it does not write changes to the switch configuration, so you only have to configure the SNMP read community strings.

When you configure the SNMP strings for your switches, you must also configure the SNMP strings for your Unified CM servers. Emergency Responder must be able to make SNMP queries of all Unified CM servers in the cluster that it supports.

If your Cisco Emergency Responder servers, Unified CM servers, and Cisco IP Phones are in a different subnet than your switches, you must either configure both the subnets for the servers and phones as well as the subnet for the switches or use *.*.*.*.

Related Topics

SNMP Settings
LAN Switch Identification , on page 47

Set Up SNMPv2

Before you begin

You must have the system administrator or the network administrator authority to define the SNMP settings.

Obtain the read community strings from all of the switches you define in Emergency Responder. If you use different strings for different sets of switches, determine whether you can define an IP address pattern for these sets. For example, if you use the same string for all switches that begin with 10.1, and another string for switches that begin with 10.2, you can use the patterns 10.1.*.* and 10.2.*.*.

If two or more patterns match an IP address, Emergency Responder uses the SNMP string associated with the most closely matching pattern. For example, if you define *.*.*.* and 10.1.*.*, and the IP address is 10.1.12.24, Emergency Responder uses the SNMP string defined for 10.1.*.*. The sequence of entries on this page does not affect the selection.

Procedure

Step 1 Select **Phone Tracking > SNMPv2 Settings**.

Emergency Responder opens the SNMP Settings page.

Step 2 Enter an IP address pattern to which you want to associate an SNMP read community string.

Use the asterisk (*) as a wildcard character. You can also use number ranges for octets, such as 15—30. Because the Emergency Responder only tries to contact the switches you identify on the LAN Switch Details page (see LAN Switch Identification , on page 47 for more information), it does not matter if the IP address patterns cover devices other than switches.

- If all of your switches use the same read community string, enter *.*.*.*. You only need to create one entry.
- If subsets of your switches use the same strings, create a mask that covers those subsets, if possible. For simplicity, try to create the fewest number of patterns.

- If you use a separate string for each switch, you must enter each switch on this page.

Step 3 Enter the timeout and retries values.

These values work together to determine how often and how long Emergency Responder tries to obtain SNMP information from a switch before giving up. The first attempt lasts as long as the timeout value. If you enter 1 or higher for retries, Emergency Responder tries again, and each retry lasts twice as long as the previous try. For example, if you specify 10 for timeout, the first retry lasts for 20 seconds, the second retry lasts for 40 seconds, and so forth.

The optimal values are 10 to 15 seconds for timeout, and 2 to 3 for retries.

Step 4 Enter the read community string, for example, **public**.

Note Community string does not support special characters like angle brackets (< >), backslash (\), colon (:), quotation marks (" "), and tilde (~).

Step 5 Click **Insert**.

Emergency Responder adds the SNMP setting to the list of settings.

Step 6 If you must create more than one setting, return to Step 2, on page 44.

If you change the SNMP read community string on a switch, you must update the associated setting in Emergency Responder:

- To change an SNMP setting, select it in the list. Emergency Responder loads the setting in the edit boxes. Make your changes and click **Update**. Then, run the switch port and phone update process on the switch after you update the SNMP setting. Select **Phone Tracking > LAN Switch Details**, select the switch in the LAN Switches list, and then click **Locate Switch Ports**. If you are changing the setting for many switches, run the process on all switches by selecting **Phone Tracking > Run Switch-Port & Phone Update**.
- To delete a setting, click the delete icon on the setting's entry.

Set Up SNMPv3

Procedure

Step 1 Select **Phone Tracking > SNMPv3 Settings**.

Emergency Responder opens the SNMPv3 Settings page.

Step 2 Enter the User information for which you want to provide access.

Enter an IP address pattern to which you want to associate an SNMP read community string. Use the asterisk (*) as a wildcard character. You can also use number ranges for octets, such as 15–30.

Step 3 To require authentication, check the **Authentication Required** check box, enter the password in the Password and Reenter Password fields, and choose the appropriate protocol.

Step 4 If you checked the **Authentication Required** check box, you can specify privacy information. To require privacy, check the **Privacy Required** check box, enter the password in the Password and Reenter Password fields, and choose the appropriate protocol.

Step 5 Enter the timeout and retries values.

These values work together to determine how often and how long Emergency Responder tries to obtain SNMP information from a switch before giving up. The first attempt lasts as long as the timeout value. If you enter 1 or higher for retries, Emergency Responder tries again, and each retry lasts twice as long as the previous try. For example, if you specify 10 for timeout, the first retry lasts for 20 seconds, the second retry lasts for 40 seconds.

The optimal values are 10 to 15 seconds for timeout, and 2 to 3 for retries.

Step 6 Click **Insert**.

Step 7 If you must create more than one setting, return to Step 2.

Whenever you change the SNMPv3 settings on a switch or Unified CM server, you must update the associated setting in Emergency Responder:

- To change an SNMPv3 setting, select it in the list. Emergency Responder loads the setting in the edit boxes. Make your changes and click **Update**. Then, run the switch port and phone update process on the switch after you update the SNMPv3 setting. Select **Phone Tracking > LAN Switch Details**, select the switch in the LAN Switches list, and then click **Locate Switch Ports**. If you are changing the setting for a large number of switches, run the process on all switches by selecting **Phone Tracking > Run Switch-Port & Phone Update**.
- To delete a setting, click the delete icon on the setting's entry.

Related Topics

SNMP Settings

LAN Switch Identification , on page 47

Define Phone Tracking and Switch Update Schedules

To track phones successfully, Emergency Responder must periodically contact switches to obtain port and device information. Emergency Responder updates network information using two processes:

- Phone Tracking—A periodic comparison of the phones registered with Unified CM to the location information obtained from the switches. If a phone moves, Emergency Responder updates the phone's ERL. Phones that cannot be located are classified as unlocated phones (see Identify Unlocated Phones , on page 61).

Note If you do not configure a switch port phone update schedule, the default schedule runs at midnight.

- Switch-Port and Phone Update—The phone tracking process plus a more extensive check of the network switches, which can identify new or changed switch modules (additional or removed ports). Any newly-discovered ports are assigned to the Default ERL. Ensure that your ERL administrator updates the ERL assignment for new ports.

Before you begin

You must have system administrator or network administrator authority to define the schedule.

Procedure

Step 1 Select **Phone Tracking > Schedule**.

Emergency Responder opens the Schedule page.

Step 2 Enter the incremental phone tracking schedule in minutes and click **Update**.

Emergency Responder runs the phone tracking process this number of minutes after finishing the previous phone tracking process.

Step 3 Enter the AXL incremental location phone tracking schedule in minutes and click **Update**.

Emergency Responder runs the enhanced location phone tracking for wireless devices after this number of minutes from the start of previous location tracking process.

Note By default, Emergency Responder actively queries the Cisco Jabber client every 2 minutes through AXL discovery on receipt of the device location.

Step 4 Enter the schedule for the switch port and phone update process. You should run this process at least once per day (but not more than four times per day).

For example, if you want to run the process at midnight Monday through Friday, but at 6 PM on Saturday and Sunday, create two schedule entries:

- Select **Mon**, **Tue**, **Wed**, **Thu**, and **Fri**, and **00** for **Hour**, **00** for **Minute**, then click **Insert**. Emergency Responder adds the schedule to the list.
- Select **Sat** and **Sun**, and **18** for **Hour**, **00** for **Minute**, then click **Insert**. Emergency Responder adds the schedule to the list.

  If you define schedules that overlap, Emergency Responder only runs one process.

Note The Emergency Responder Administrator must ensure that ccmPhoneStatusUpdateStorePeriod (CISCO-CCM-MIB) value in Unified CM must be set to a value greater than the Emergency Responder incremental phone tracking interval, for tracking phone changes efficiently.

To change a switch port and phone update schedule, click the schedule in the list. Emergency Responder loads the schedule's settings in the schedule fields. Make your changes and click **Update**. To delete a schedule, click the delete icon on the schedule's list entry.

Related Topics

Phone Tracking Schedule

Manually Run the Switch-Port and Phone Update Process , on page 51

LAN Switch Identification

You must tell CiscoEmergency Responder (Emergency Responder) which switches to manage. Emergency Responder tracks port changes, including changes to the devices connected to those ports, and can recognize

which ports have phones connected to them. Identify all switches that might have phones attached to them, essentially all edge switches.

Because Emergency Responder must obtain information from the switches, you must ensure that the information you supply to Emergency Responder is correct and kept up-to-date. After you have created the initial switch list, you can make mass changes to switch definitions by exporting the switch definitions, editing the export file, and reimporting the file.

The following sections describe how to identify switches to Emergency Responder, and how to export switch information.

Identify LAN Switches One at a Time

You can enter switches into the Emergency Responder configuration one at a time. If you have a large number of switches to add, consider creating an import file to add them instead of using this procedure. See Import a Group of Switches , on page 49 for more information.

Before you begin

You must have system administrator or network administrator authority to add, remove, or change switch definitions.

Determine if your network includes phones that do not use the Cisco Discovery Protocol (CDP) to announce themselves to the network. For non-CDP phones, Emergency Responder must use the CAM information about the switch to identify phones. See Network Hardware and Software Requirements for information about which phones require CAM access.

Ensure that you configure the SNMP read community strings before adding switches. See Set Up SNMPv2, on page 44 for more information.

Note Emergency Responder performs a full discovery scan for all the switches when you either reboot the Emergency Responder server or while upgrading to a higher version. This process can be time consuming, depending on network size and number of switches.

Note Always delete the LAN Switches from **Emergency Responder Administration > Phone Tracking > LAN Switch Details**, if this has been removed from the network.

Procedure

Step 1 Select **Phone Tracking > LAN Switch Details**.

Emergency Responder opens the LAN Switch Details page.

Step 2 Enter information about the switch:

- Enter the IP address or Hostname of the switch.

  Note The hostname can begin with a numerical value.

- If there might be non-CDP-enabled phones attached to the switch, select **Enable CAM-based Phone Tracking**.
- If you want to display the switch port descriptions that are configured on the switch in the locations field in Emergency Responder, select **Use port description as port location.**

Step 3 Click **Insert** to add the switch to the Emergency Responder configuration.

Emergency Responder asks if you want to run the switch port and phone update process. You must run this process so that Emergency Responder can identify the ports on the switch and so that your ERL administrator can then assign the ports to the right ERLs.

If you are adding more than one switch, you can skip running the process until you add the last switch. When you select to run the process, Emergency Responder runs the process on all switches added since the last time the switch port and phone update process was run.

If you do not choose to run the process, you can run it later by selecting **Phone Tracking > Run Switch-Port & Phone Update**.

In either case, newly discovered ports are assigned to the Default ERL.

Note Emergency Responder expects only one IP address or hostname per chassis and needs access to the following MIBs:

- mib-2
- IF-MIB
- CISCO-CDP-MIB
- ENTITY-MIB
- CISCO-VLAN-MEMBERSHIP-MIB
- RIDGE-MIB*
- CISCO-STACK-MIB
- Mib-2
- interface
- CISCO-2900-MIB

Click a switch in the LAN Switches list to view the switch's Emergency Responder configuration. To change the configuration, make your changes and click **Update**.

Click **Add LAN Switch** to add another switch if you are viewing an existing switch's configuration.

To delete a switch, select it from the LAN Switches list and click **Delete**. If you do not remove the switch from the network, Emergency Responder identifies any phones connected to the switch as unlocated phones.

Related Topics

Import a Group of Switches , on page 49
Export Switch Information , on page 51
LAN Switch Details
Switch Requirements for Emergency Responder , on page 43

Import a Group of Switches

You can define a large number of switches at one time by importing a file that contains the required switch information. You can create this file by exporting switch information from your network management software,

and then using a spreadsheet program to modify the records to match the Emergency Responder file format requirements (that is, by deleting columns, adding columns, rearranging columns, and so forth).

If you have a large network, importing switch definitions can save you a lot of time.

Before you begin

You must have system administrator or network administrator authority to import switch definitions.

Prepare an import file. Emergency Responder includes detailed information about the required file format on the Import LAN Switch page. The page also includes the location in which you must place the file to import it. Use the following procedure to go to the page and view the format, create your file, copy the file to the required location, and then follow the procedure to import the file.

Ensure that you configure the SNMP read community strings before adding switches. See Set Up SNMPv2, on page 44 for more information.

Procedure

Step 1 Select **Phone Tracking** > **LAN Switch Details**.

Emergency Responder opens the LAN Switch Details page.

Step 2 Click **Import** in the left-hand switch list.

Emergency Responder opens the Import LAN Switch page.

Step 3 Select the file format, and the name of the file you want to import.

Step 4 Click **Import**.

Emergency Responder asks you whether you want to run phone tracking on the imported switch. You must run phone tracking before you can configure the switch ports, so normally you should select **OK**. If you select **Cancel**, Emergency Responder imports the switches but does not run the phone tracking process.

After you make your selection, Emergency Responder adds the switch configurations and shows you the status of the import.

Step 5 Click **Close** to close the window.

Step 6 If you did not run phone tracking on the imported switches, select **Phone Tracking** > **Run Switch-Port & Phone Update**.

Emergency Responder contacts each switch to discover the ports on the switch and any phones attached to the ports.

Alternatively, you can view each switch's configuration on the LAN Switch Details page and click **Locate Switch Ports** to run the process only on the selected switch.

Related Topics

Identify LAN Switches One at a Time , on page 48
Export Switch Information , on page 51
LAN Switch Details
Switch Requirements for Emergency Responder , on page 43

Export Switch Information

You can export your Cisco Emergency Responder (Emergency Responder) configuration. By exporting this information, you can back up your data, or create a file for updating a large number of switch definitions in Emergency Responder. You can edit the export file, make your changes, then reimport the file and overwrite the information in Emergency Responder.

Before you begin

You must have system administrator or network administrator authority to export switch definitions.

Procedure

Step 1 Select **Phone Tracking > LAN Switch Details**.

Emergency Responder opens the LAN Switch Details page.

Step 2 Click **Export** in the switch list.

Emergency Responder opens the Export LAN Switch page.

Step 3 Select the file type and enter the file name for the export file. Do not include a file extension.

Step 4 Click **Export**.

Emergency Responder creates the export file. Click **Close** to close the window.

Related Topics

Identify LAN Switches One at a Time , on page 48
Import a Group of Switches , on page 49
LAN Switch Details
Switch Requirements for Emergency Responder , on page 43

Manually Run the Switch-Port and Phone Update Process

Before you can assign ERLs to switch ports, Emergency Responder must identify the ports on the switch using the switch port and phone update process. Although Emergency Responder runs this process according to the schedule you set (see Define Phone Tracking and Switch Update Schedules, on page 46 for more information), you might want to run it manually when you make a lot of changes to the switch configuration without running phone tracking on individual switches.

Because the switch port and phone update process does extensive checking, only run it if you are trying to refresh the entire Emergency Responder tracking results. Alternatively, if you are only trying to update the results for a limited number of switches, you can run phone tracking on individual switches. To run on individual switches, select **Phone Tracking > LAN Switch Details**, select the switch in the left-hand column then click **Locate Switch Ports**.

These are some reasons you might run phone tracking on an individual switch:

- You add a switch to Emergency Responder. When you add a switch, Emergency Responder asks if you want to run the process. If you select to run it at that time, you do not have to click **Locate Switch Ports**.

Emergency Responder runs the process for all switches you added to the Emergency Responder configuration since the last time the full switch port and phone update process was run.

- You add, remove, or change a module in a switch already defined to Emergency Responder.
- You can add and delete IP subnet-based ERLs.

Manually run the switch port and the following phone update process if:

- You want to refresh the Emergency Responder tracking results.
- You add switches to Emergency Responder by importing switch definitions, as described in the Import a Group of Switches , on page 49, but you did not run phone tracking during the importation.
- If you find a large number of entries in the unlocated phones list (see Identify Unlocated Phones , on page 61), run this process to see if Emergency Responder can find some of those phones. See Unlocated Phones for issues you should address to help resolve these problems before running the switch-port and phone update process.

Before you begin

You must have system administrator or network administrator authority to manually run the switch port and phone update process.

Procedure

Select **Phone Tracking > Run Switch-Port & Phone Update**.

Emergency Responder runs the process without changing the page you are viewing. Any newly discovered ports are assigned to the Default ERL.

Note When a 911 call is placed, and the phone matches multiple ERLs via Phone Tracking, Cisco Emergency Responder will use the following hierarchy to select an ERL:

- Switch Port
- IP Subnet
- Manually configured phone

Related Topics

Define Phone Tracking and Switch Update Schedules, on page 46
Identify Unlocated Phones , on page 61
Switch Requirements for Emergency Responder , on page 43

Track Change of Switch IP Address Dynamically

Emergency Responder allows you to dynamically track the change in a LAN switch IP address managed by Emergency Responder. This feature is intended for LAN switches that have been added using the switch hostname.

Before you begin

You must have system administrator authority to enable dynamic tracking of a LAN switch IP address.

Procedure

Step 1 Select **System** > **CiscoER Group Settings**.

Emergency Responder opens the Emergency Responder Group Settings page.

Step 2 Select the **Dynamic Tracking of Switch IP Address** check box to dynamically track a switch's IP address.

Step 3 Click the **Update Settings** button to apply the change.

You must wait for the next Incremental Discovery cycle to start. During this cycle Emergency Responder detects the new IP address of the LAN switch and updates its database. You will be notified of this change detection from an entry in the Emergency Responder Event Viewer and with an administrative email alert.

Note It is recommended that you enable Dynamic Tracking of Switch IP Address only during a scheduled maintenance window when the switch is subject to an actual change of IP address. It is recommended that you disable this option during normal periods as this operation is CPU intensive.

Note For a LAN switch that has been added using the IP address, Emergency Responder cannot track any change in its IP address. In this case, you must delete the switch and add it again with the new IP address.

Related Topics

Group Settings

Define Phone Tracking and Switch Update Schedules, on page 46

Phone Management

The following topics describe how to assign switch ports and phones to the appropriate emergency response locations (ERLs), and how to view the history of emergency calls handled by Emergency Responder.

Switch Port Configuration

After the network administrator adds switches to the Emergency Responder configuration, and runs the switch port and phone update process, you can assign the switch ports to emergency response locations (ERLs). When you assign a port to an ERL, make sure that you assign the ERL based on the location of the device attached to the port, not the location of the port itself.

For example, your wiring closet is on Floor 1. Half of its ports serve Floor 1, the other half serve Floor 2. Also, you have defined two ERLs, Floor1 and Floor2. Although the switch is on Floor 1, only half its ports belong in the Floor1 ERL; the other half belong in the Floor2 ERL.

Before you assign ports to ERLs, ensure that you have a reliable mapping of switch ports to their end points (for example, cubicle numbers or office numbers). Your assignments are only reliable if this map is kept static, that is, so long as wires are not indiscriminately moved from port to port on the switch. Work with your network administrator to ensure the integrity of the wiring closet. See Data Integrity and Reliability for more information.

Set Up Individual Switch Ports

You can assign switch ports to ERLs a few at a time. If you have a large number of ports to map, it is much easier to create an import file to add them instead of using this procedure. See Set Up Large Number of Ports , on page 55 for more information.

Before you begin

You must have system administrator or ERL administrator authority to assign ports to ERLs.

You can only configure ports defined for the Emergency Responder group to which you are logged in.

Procedure

Step 1 Select **ERL Membership** > **Switch Ports**.

Emergency Responder opens the Switch Port Details page.

Step 2 Enter search criteria to list the ports that you want to configure.

- **Find** displays a maximum of 1,000 records. Refine your search accordingly. To limit the number of ports that are displayed, check the check box next to **Collapse search results.** The search displays the IP address or name of the switches found. To display all ports associated with a switch and display the expanded view, click the + button next to the switch. To display just the switch and collapse the list, click the - button next to the switch.
- If you want to list all ports on a specific switch, select **Switch IP Address** or **Switch Host Name**, enter the IP address or host name, and click **Find**. Emergency Responder lists all ports discovered on the switch.
- If you want to narrow your search by using multiple criteria, click the + button to add search fields. Select **Any** at the top of the list to indicate that ports that match any search criteria be selected (an OR search); select **All** to indicate that only ports that match every criteria be selected (an AND search).
- For all searches, select the Emergency Responder group that you want to search. If your initial search does not list the ports you are looking for, it might be because the ports are managed by a different Emergency Responder group. You can only search one Emergency Responder group at a time.

Note Emergency Responder remembers the previous search criteria for the login session.

Step 3 Assign ports to ERLs:

a) Check the check box next to the switch port that you want to assign an ERL.

If you want to assign all listed ports for a switch, select the check box for that switch. You can only assign ports on one page at a time, so if there is more than one page of ports in the listing, complete this task for each page separately.

b) Select the ERL you want to assign to the ports.

c) Optionally, enter more specific location information in the **Phone Location** field. Click **view** to open a window so that you can enter information. For example, you could enter the cubical or office number that the port serves.

This information is sent to the onsite alert (security) personnel to help them locate the emergency caller. You can only update the phone location information if you are logged into the primary Emergency Responder server in the Emergency Responder group.

d) To select the ERL you want to assign to the selected ports, click the **Search ERL** button next to the ERL Name field. The Find ERL page appears.
e) Enter the ERL Search Parameters and click **Find**. The search results appear.
f) Click the radio button next to the ERL that you want to assign to the switch ports and click **Select ERL**. The Find ERL page closes.
g) Click **Assign ERL**.

Emergency Responder assigns the ERL to the selected ports. You can continue assigning ports on this page of the ports list, but do not change the search results page before completing these steps.

Emergency Responder commits your ERL assignments. From here, you can continue to the other page of the listed ports, or click **Find** to enter new search criteria to obtain another list of ports.

Click **Edit View** to change the fields and arrangement of fields in the port list. If you want to revert to the standard view, then click **Restore Defaults**.

The phone location information is saved on the primary Emergency Responder server. Back up this data regularly.

Related Topics

Switch Port Details
Import Switch Ports
Set Up Large Number of Ports , on page 55
Export Switch Port Information , on page 56
Work with Emergency Responder Locations , on page 29

Set Up Large Number of Ports

You can assign a large number of ports to ERLs at one time by importing a file that contains the required information.

If you have a large network, importing port-to-ERL mappings can save you a lot of time.

Before you begin

You must have system administrator or ERL administrator authority to import switch port definitions.

Prepare an import file. The easiest way to create this file is to first export the switch port details from Emergency Responder (see Export Switch Port Information , on page 56), and then use a spreadsheet program to change the ERL to the desired ERL and add phone location information. Ensure that the switch port and phone update process is run before creating the export file, so that the file includes records for every switch port.

Before you import the file, you must copy it to the location identified on the Import Switch Port page. The following procedure explains how to get to this page. Links on the page also displays the detailed information about the required file format for the import file if you need it.

Emergency Responder must already be aware of the ports before you import the file. Ensure that all ports you are importing have been located by Emergency Responder.

You can only configure ports defined for the Emergency Responder group to which you are logged in.

Procedure

Step 1 Select **ERL Membership** > **Switch Ports** .

Emergency Responder opens the Switch Port Details page.

Step 2 Click **Import**.

Emergency Responder opens the Import Switch Ports page.

Step 3 Select the format of your import file (csv) from the pull–down menu.

Step 4 Click **Upload** to upload the file from your local machine. See Upload File , on page 8 for information about using the Upload utility.

Step 5 Select your import file using the Select File to Import pull–down menu.

Step 6 Click **Import**.

Emergency Responder imports the file and shows you the import results. The ERL-to-port mappings and port location information in the import file overwrite any existing data in the Emergency Responder configuration.

Step 7 Click **Close** to close the Import Switch Port page.

Related Topics

Switch Port Details
Export Switch Ports
Set Up Individual Switch Ports , on page 54
Export Switch Port Information , on page 56
Switch Requirements for Emergency Responder , on page 43

Export Switch Port Information

You can export your Emergency Responder port configuration. By exporting this information, you can back up your data, or create a file that you can use to update a large number of switch port mappings in Emergency Responder. You can edit the export file, make your changes, then reimport the file and overwrite the information in Emergency Responder.

Before you begin

You must have system administrator or ERL administrator authority to export switch port definitions.

Procedure

Step 1 Select **ERL Membership** > **Switch Ports** .

Emergency Responder opens the Switch Port Details page.

Step 2 Click **Export**.

Emergency Responder opens the Export Switch Ports page.

Step 3 Select the file format and enter the desired file name, and click **Export**.

Emergency Responder exports the file to the export location.

Step 4 To download the exported file to your local system, select the file name from the Select file to download pull–down menu and click **Download**.

Step 5 Click **Close** to close the Export Switch Port page.

Related Topics

Switch Port Details
Set Up Individual Switch Ports , on page 54
Set Up Large Number of Ports , on page 55
Work with Emergency Responder Locations , on page 29

Switch-Port Change Reporting for Wired Cisco Unified IP Phones

Emergency Responder detects changes in the switch port association of wired CiscoUnifiedIPPhones. An incremental or full discovery cycle detects CiscoUnifiedIPPhones that have changed switch port associations or are newly discovered. Cisco UnifiedIPPhones that become missing during a complete discovery are also reported. Emergency Responder notifies the system administrator of these changes by email.

Note A missing CiscoUnifiedIPPhone is one that is registered in Cisco UnifiedCommunicationsManager but is not found behind a switch port of any switch tracked by Emergency Responder. CiscoUnifiedIPPhones that appear on the Unlocated Phones page in Emergency Responder Administration web interface are also included in the missing list. Switch-port Change Reporting reports the location changes for CiscoUnifiedIPCommunicator when it is connected to a switch that is tracked by Emergency Responder.

The change notification email contains the following information:

- The time at which the change was detected. This is the approximate completion time of the discovery cycle that detected the change.
- The previous switch IP and port number of the CiscoUnifiedIPPhone. If the CiscoUnifiedIPPhone is new, this field is blank.
- The current switch IP and port number of the CiscoUnifiedIPPhone. If the CiscoUnifiedIPPhone is missing, this field is blank.
- The details of the CiscoUnifiedIPPhone, including the MAC address, device name, Phone Type, IP address and IP phone extensions.

Procedure

Step 1 Select **System > Mail Alert Configurations**.

The Email Alert Settings page appears.

Step 2 In the **Misc parameters** section, check the check box to the right of Switch Port location change reporting parameter to enable or disable email alerts.

Check the **Include event viewer contents in mail check box** if you want to include the details from the event viewer in the email message.

Step 3 Click **Update Settings**.

What to do next

Note Configure the email client settings to allow line breaks in the email to improve readability.

Supported CiscoUnifiedIPPhones—This feature supports only wired CiscoUnifiedIPPhones that meet both of these conditions:

- Wired CiscoUnifiedIPPhones discovered behind a LAN switch port using Cisco Discovery Protocol (CDP) tracking or Content-Addressable Memory (CAM) tracking.
- Wired CiscoUnifiedIPPhones actively registered in Unified CM. The only exception for this rule is CiscoUnifiedIPPhones previously registered in Unified CM. These CiscoUnifiedIPPhones are reported as missing.

Cluster Scenario—The active server in each server group within a cluster sends separate notifications for the CiscoUnifiedIPPhones it discovers and tracks.

Server Group Scenario—Within a server group, Emergency Responder performs change detection and notification on the active Emergency Responder server only.

Feature Activation—The change detection and notification feature requires manual activation.

Change Notification conditions - Emergency Responder sends change notification email when a full discovery cycle completes under any of these circumstances:

- During a normally scheduled discovery.
- After a manual start from the Emergency Responder Administrator web interface.
- Because of a Unified CM addition from the web interface by the system administrator.

Similarly, a partial discovery cycle sends email notifications under these circumstances:

- During a normally scheduled discovery.
- Because of a LAN switch addition to Emergency Responder the system administrator starts the discovery process.
- Because the system administrator selecting the **Locate Switch Ports** button on the LAN switch details page.

Note An Incremental Discovery does not locate missing CiscoUnifiedIPPhones from Unified CM if no phone registrations take place during the discovery cycle. A full discovery detects all missing CiscoUnifiedIPPhones that are located since the previous full discovery.

The following events do not result in a change notification:

- When the Emergency Responder Server starts following the first discovery cycle.
- When a Publisher returns to an online state following the first discovery cycle.
- When no phone location changes occur following a discovery cycle.

Related Topics

Set Up a Server Group, on page 23

Access Point Configuration and Discovery

An Access Point is a standalone device which connects to a router through a wired network. It can also be an essential component of the router. Each Access Point is identified through a Service Set Identifier (SSID) or Basic Service Set Identifier (BSSID). Wireless phones connect to the network over Wi-Fi or any equivalent standard through an Access Point.

SSID— The Service Set Identifier (SSID) is a unique name assigned to each WLAN network. A unique name is assigned to each WLAN as multiple WLANs can coexist in one airspace.

BSSID—The Basic service set identifier (BSSID) identifies access points and their associated clients within a WLAN network when there are multiple access points present within each WLAN. BSSID is included in all the wireless packets.

Cisco Unified Communications Manager, provides support to sync Access Points through a Wireless Controller.

Cisco Emergency Responder via the configured Cisco Unified Communications Manager identifies all the " Access Points", either through direct Cisco Unified Communications Manager database access during a Major Discovery or AXL Change Notification every two minutes.

Cisco Emergency Responder administrator can assign ERLs to the Access Points. For more information on Access Point details, see the Related Topics section.

EnergyWise

Cisco EnergyWise allows administrators to measure and reduce the energy consumption of devices connected to a Cisco network, such as IP telephones. Because each telephone reports its power consumption to a switch or router, you can monitor energy consumption across a network. You can then manage the power state of a phone by determining what phones are powered up, when they receive power, and how much power they receive.

Cisco EnergyWise Phone User Experience

When a phone enters Power Save Plus mode, it becomes unregistered from Unified CM and powers down after negotiating with the EnergyWise switch. Administrators configure the sleep and wakeup times, which are communicated to the switch by the phone.

Users can wake up the Cisco Unified IP Phone 6900, 8900, and 9900 series phones from Power Save Plus mode but cannot wake up the Cisco Unified IP Phone 7900 series.

Phone Discovery Scenarios Common to EnergyWise Users

The following three phone discovery scenarios are common to EnergyWise users. These scenarios can help you to understand this feature.

Scenario 1 — When the phone is connected to a switch that is configured on Emergency Responder for discovery:

- A phone is configured with EnergyWise on the Unified CM.
- The phone is connected to the switch and is discovered by Emergency Responder. The phone is displayed on the Switch Port page, connected to a switch port.

- Before the next Major Discovery, the phone enters Power Save Plus mode and it becomes unregistered with Unified CM.
- During the next Major discovery, Emergency Responder retains the phone location information. It is listed on the Switch Port page as being connected to the same switch port.
- When the phone is powered up again, the correct location is available if the user can make a 911 call without waiting for the next Incremental or Major discovery.

Note When a phone in Power Save Plus mode is unplugged, the EnergyWise configurations on the switch are lost. And if a Major Discovery takes place, the phone location information is lost also. Even if the phone is plugged back into the same port, powers up and registers with the switch, Emergency Responder treats this phone as a newly registered phone in the next discovery cycle.

Note If an EnergyWise phone is connected to a supported switch that is configured on Emergency Responder for discovery, the phone must be discovered at least once before entering Power Save Plus mode. This ensures that Emergency Responder retains the phone location and configuration information into the next Major Discovery. If the phone enters Power Save Plus mode without being discovered, it is not listed on the Switch page. But instead the phone is listed on the IP Subnet page (if configured) or the Unlocated Phone page in the next discovery. When it wakes up, registers with the switch and is discovered, the phone is listed on the Switch Port page.

Scenario 2 — IP subnet-based phone discovery in Emergency Responder:

- The phone is configured with EnergyWise on the Unified CM.
- The phone is discovered by Emergency Responder, based on the IP subnet. It is listed on the IP Subnet page.
- Before the next Major Discovery, the phone enters Power Save Plus mode and becomes unregistered with Unified CM.
- During the next Major Discovery, Emergency Responder retains the phone location information and the phone is listed on the IP Subnet page.
- When the phone is powered up again, the correct location is available if the user makes a 911 call without waiting for the next Incremental or Major discovery.

Scenario 3 — Unlocated phones in Emergency Responder:

- The phone is configured with EnergyWise on Unified CM.
- The phone is listed on the Unlocated Phones page in Emergency Responder after discovery.
- Before the next Major discovery, the phone enters Power Save Plus mode and it becomes unregistered with Unified CM.
- During the next Major discovery, Emergency Responder retains the phone location information. It is listed on the Unlocated Phones page.

- When the phone is powered up again, users can make a 911 call without waiting for the next Incremental or Major discovery. But the phone is in the default ERL or the ERL assigned to the Unlocated Phone switch.

Power Save Plus Mode Limitations

Consider the following limitations for users making 911 calls from phones in Power Save Plus mode:

- Users cannot wake up Cisco Unified IP Phones 7900 series that are in Power Save Plus mode because the sleep and wake-up times are configured on the Unified CM. The phone location information is not deleted from Emergency Responder, but users cannot make a 911 call until the phone reaches the configured wake-up time.
- Users can wake up Cisco Unified IP Phones 6900, 8900, 9900 in Power Save Plus mode. But the phone takes a few minutes to wake up and register with Unified CM and you should consider this delay during emergencies.
- You can track phones connected to a switch on the Emergency Responder page. But if the phones go into Power Save Plus mode before they are discovered, they are considered unlocated and are listed on the Unlocated Phones page.
- If a network has a standalone Emergency Responder with no backup subscriber, you should consider the impact of a system or Emergency Responder restart. Because there is no backup server, the existing discovery data is lost when the system is restarted. And when discovery occurs, it is considered a fresh discovery and Emergency Responder does not identify the switch location information for any phones that entered Power Save Plus mode before the restart.

  In Emergency Responder, these phones are listed on the Unlocated Phones page or IP Subnet page (if configured). When the phones are powered up and are discovered, they are listed on the Switch Port page. Consider these sleeping phones and their wake-up time when you assign the ERL.

  To avoid losing phones in the Power Save Plus mode when Emergency Responder is stopped, we recommend that you configure a backup Emergency Responder subscriber. If the publisher Emergency Responder service is stopped or the server goes down, the subscriber accesses the backup version of the discovery data, including the phones in Power Save Plus Mode. And when a restart occurs, the discovery data is retrieved from the subscriber and the phones in Power Save Plus mode are not lost.

Identify Unlocated Phones

If Emergency Responder cannot locate a phone, it places the phone in the Default ERL and puts it in a list of unlocated phones. Using this list, you can reassign the phones to a different ERL, or you can use the list to help identify the problems that are preventing Emergency Responder from locating the phones.

These are some things that can prevent Emergency Responder from locating a phone:

- The phone is attached to a switch that is not defined in Emergency Responder.
- The phone is connected to an unsupported device, such as a router port, a hub connected to a router, or an unsupported switch.
- The switch to which the phone is connected is currently unreachable, for example, it does not respond to SNMP queries.
- The phone has moved to a switch served by a different Emergency Responder group. If this is the case, the Emergency Responder group name is shown for the phone in the unlocated phones list.
- No IP subnet is configured for the phone.

Because Emergency Responder cannot assign an unlocated phone to the appropriate ERL, try to identify and resolve all problems that are preventing Emergency Responder from locating these phones on your network. If you cannot resolve the problems by defining switches in Emergency Responder, or by moving phones to supported switch ports, you can manually assign a phone to an ERL. See Unlocated Phones for more detailed information about resolving these problems.

In addition, Emergency Responder also displays the following in the unlocated phone list:

- The phone that was manually assigned.
- The phone that was previously identified as an unlocated phone and assigned an ERL.

Before you begin

You must have system administrator or ERL administrator authority to view or configure unlocated phones.

Procedure

Step 1 Select **ERL Membership > Unlocated Phones**.

Emergency Responder opens the Unlocated Phones page.

Step 2 Enter search criteria to list the unlocated phones.

Step 3 Check the check box next to the phone that you want to assign an ERL.

Step 4 Click the Search **ERL button** next to the ERL Name field to select the ERL you want to assign to the selected phone. The Find ERL page appears.

Step 5 Enter the ERL Search Parameters and click **Find**. The search results appear.

Step 6 Click the radio button next to the ERL that you want to assign to the unlocated phones and click **Select ERL**. The Find ERL page closes.

Step 7 Click the **Assign ERL** button.

Emergency Responder assigns the phone to the ERL, but leaves it in this list. If you later resolve the problem that is preventing Emergency Responder from locating this phone, Emergency Responder removes it from the list and assigns it the correct ERL based on port assignment.

Note To unassign a ERL, select the phones and click on **Unassign ERL** button.

You can select all the phones on the displayed page by selecting the check box in the list title. You can only assign phones to ERLs on a single page at a time. If there is more than one page of phones, use the links at the bottom of the list to move from page to page.

Note Emergency Responder does not automatically discover analog phones or phones connected to PBXs. As a result, these phones do not appear on the Unlocated Phones list. These phones must be manually configured. See Manually Define Phones , on page 63 for more information.

Related Topics

IP Subnet Phones
Switch Port Configuration , on page 53
Manually Define Phones , on page 63

Manually Define Phones

To manage all emergency calls in your network, Emergency Responder must know about every phone whose calls are routed by Unified CM, even if Emergency Responder does not directly support the phone. Emergency Responder handles emergency calls from these manually defined phones in the same way it handles calls from phones attached to supported switch ports. The only difference is that Emergency Responder cannot dynamically change the ERL of a manually defined phone if that phone is moved.

You must manually define a phone if any of these conditions apply:

- The phone is hosted on an unsupported port, such as a router port, a hub connected to a router, or a port on an unsupported switch.
- No IP subnet is configured for the phone.

For any phones you must manually define, you should regularly audit the location of those phones to determine if you must update the ERL assignment for the phone in Emergency Responder.

Note New switch ports and unlocated phones are NOT associated to Default ERLs automatically. They are treated as "ERL not configured." The Default ERL is used only internally by Emergency Responder if no other ERL is configured for that phone. Emergency Responder will not allow the Default ERL to be configured to switch ports, unlocated phones, manually configured phones, or IP subnets.

Note You cannot manually add a phone that is used with Unified CM Extension Mobility. With Unified CM Extension Mobility, a user can log into a phone and the phone is assigned the user's extension. However, with manually defined phones, you are defining the phone based on extension, not on device, so the extension of the logged-in person does not get assigned the appropriate ERL. Ensure that all phones used with Unified CM Extension Mobility are connected to supported switch ports.

Before you begin

You must have system administrator or ERL administrator authority to manually define phones.

Note Manually configured phones can have E.164 and non-E.164 line numbers.

Procedure

Step 1 Select **ERL Membership > Manually Configured Phones**.

Emergency Responder opens a new page, the Find and List Manually Configured Phones page.

Step 2 Enter the extension and click **Find** to search for phones that you must modify. Emergency Responder performs a search and displays the results of your search.

From the search result on the Find and List Manually Configured Phones page, you can remove a phone, change an existing phone or add a new phone:

Step 3 Click the **Delete** icon on the phone entry to remove a phone.

Step 4 To change an existing phone:

a) Click the phone entry in the list. Emergency Responder opens the Add/Modify Phones page with the phone information displayed in the edit boxes.
b) Make your changes and click **Update**. Emergency Responder updates the phone.
c) Click **Back to Phone Search** to return to the Find and List Manually Configured Phones page.

Step 5 To add a new phone:

a) Click **Add New Manual Phone**. Emergency Responder opens the Add New Manual Phone page.
b) Enter information about the phone you want to define. You must enter the line number and select an ERL. If the phone is an IP phone, you must also enter the IP address and MAC address for the phone. Other fields are optional and are mainly for your information.
c) To select the ERL you want to assign to the selected ports, click the **Search ERL** button next to the ERL Name field. The Find ERL page appears.
d) Enter the ERL Search Parameters and click **Find**. The search results appear.
e) Click the radio button next to the ERL that you want to assign to the manual phone and click **Select ERL**. The Find ERL page close.
f) Click **Insert**. Emergency Responder adds the phone to the list of manually defined phones.
g) Click **Back to Phone Search** to return to the Find and List Manually Configured Phones page.

Related Topics

Add New Manual Phone
Identify Unlocated Phones , on page 61
Network Hardware and Software Requirements
Assign Large Number of Manually Configured Phones to ERLs , on page 64
Export Manually Configured Phone Information , on page 65

Assign Large Number of Manually Configured Phones to ERLs

You can assign a large number of manually configured phones to ERLs at one time by importing a file that contains the required information.

If you have a large network, importing a manually configured phone to ERL mappings can save you a lot of time.

Before you begin

You must have system administrator or ERL administrator authority to import switch port definitions.

Prepare an import file. The easiest way to create this file is to first export the manually configured phone details from Emergency Responder (see Export Manually Configured Phone Information , on page 65), and then use a spreadsheet program to change the ERL to the desired ERL and add phone location information. Ensure that the manual phone configuration and phone update process is run before creating the export file, so that the file includes records for every manually configured phone.

Before you import the file, you must copy it to the location identified on the Import Manual Phones page. The following procedure explains how to get to this page. Links on the page also display the detailed information about the required file format for the import file if you need it.

Emergency Responder must already be aware of the manually configured phones before you import the file. Ensure that all manually configured phones you are importing have been located by Emergency Responder.

You can only configure manually configured phones defined for the Emergency Responder group to which you are logged in.

Procedure

Step 1 Select **ERL Membership > Manually Configured Phones**.

The Find and List Manually Configured Phones page appears.

Step 2 Click **Import**.

The Import Manually Configured Phones page appears.

Step 3 Select the Import Format (csv) using the pull-down menu.

Step 4 Click **Upload** to upload the file from your local machine. See Upload File , on page 8 for information about using the Upload utility.

Step 5 Select the import file using the Select File to Import pull-down menu.

Step 6 Click **Import**.

Emergency Responder imports the file and shows you the import results. The ERL-to-port mappings and the location information for manually configured phones in the import file overwrite any existing data in the Emergency Responder configuration.

Step 7 Click **Close** to close the Import Manually Configured Phone page.

Related Topics

Switch Port Details
Export Switch Ports
Set Up Individual Switch Ports , on page 54
Export Switch Port Information , on page 56
Work with Emergency Responder Locations , on page 29

Export Manually Configured Phone Information

You can export your Emergency Responder manually configured phone configuration. By exporting this information, you can back up your data or create a file that you can use to update a large number of manually configured phone mappings in Emergency Responder. You can edit the export file, make your changes, then reimport the file and overwrite the information in Emergency Responder.

Before you begin

You must have system administrator or ERL administrator authority to export switch port definitions.

Procedure

Step 1 Select **ERL Membership > Manually Configured Phones**.

Emergency Responder opens the Find and List Manually Configured Phones page.

Step 2 Click **Export**.

Emergency Responder opens the Export Manual Phones page.

Step 3 Select the export format (csv) from the Select Export Format pulldown menu.

Step 4 Enter the desired file name in the Enter Export File Name field and click **Export**.

Emergency Responder exports the file to the export location.

Step 5 To download the exported file to your local system, select the file name from the Select file to download pulldown menu and click **Download**.

Step 6 Click **Close** to close the Export Manual Phones page.

Related Topics

Manually Define Phones , on page 63
Assign Large Number of Manually Configured Phones to ERLs , on page 64
Work with Emergency Responder Locations , on page 29
Synthetic Phones , on page 66

Synthetic Phones

With Emergency Responder, you can use Cisco Unified Operations Manager to monitor the health and functionality of Cisco Emergency Responder. To use Cisco Unified Operations Manager with Cisco Emergency Responder, you configure a synthetic phone in Emergency Responder and associate the synthetic phone to an ERL that is used as a test ERL. When a synthetic phone makes an emergency call, Emergency Responder uses the associated test ERL to route the call.

Note You can only configure test ERLs for conventional ERLs. You cannot configure test ERLs for off-premise ERLs and Intrado ERLs.

For more information, see Set Up Test ERLs , on page 39.

View Emergency Call History

You can view the history of emergency calls made in your network that are handled by Emergency Responder. Emergency Responder sends emergency call notifications to the onsite alert personnel that you identify in your ERLs, and these people respond to the notifications. From the administrator interface, you can view the same call history that your onsite alert personnel can view, and see comments they make about the calls. You might need to review the call history to report on usage or to troubleshoot call routing problems.

Tip From the Call History page, you can view detailed information about the 10,000 most recent calls. You can find records of older calls in Emergency Responder raw call log files. See Call History Logs for more information.

Procedure

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

Emergency Responder opens the Call History page.

Step 2 Click **Find**.

All call summary information appears.

Step 3 Enter the search criteria that you want to use to create a list of emergency calls.

To view a list of all calls, click **Find** without entering any search criteria.

To narrow your search, select the item you on which you want to search, and click **Find**. For example, you can view calls that were made in a specific ERL, or calls that were made from a specific phone extension. If you want to search on more than one criteria, click **More** to add additional search fields. Select **All** at the top of the list to perform an AND search (a call only matches the search if each of the criteria is met), or **Any** for an OR search (a call matches the search if it matches one or more of the criteria).

Step 4 From the list of calls that Emergency Responder shows you in response to your search criteria, you can:

- View the call characteristics.
- Click the ERL name to view the ERL details. From the ERL details, you can also view the ALI for the call.
- Click **edit** in the comment field to change the comment. Emergency Responder opens a separate window where you make your editorial changes.

Tip If a large number of calls match your search criteria, Emergency Responder uses additional pages to list the calls. Use the links at the bottom of the list to move through these additional pages.

Related Topics

Call History Logs

SAML Single Sign-On Overview

Use SAML Single Sign-On (SSO) to access a defined set of Cisco applications after signing into one of those applications. SAML describes the exchange of security-related information between trusted business partners. It is an authentication protocol used by service providers (such as Cisco Emergency Responder) to authenticate a user. With SAML, security authentication information is exchanged between an identity provider (IdP) and a service provider. The feature provides secure mechanisms to use common credentials and relevant information across various applications.

SAML Single Sign-On establishes a circle of trust (CoT) by exchanging metadata and certificates as part of the provisioning process between the IdP and the service provider. The service provider trusts user information of the IdP to provide access to the various services or applications.

Note During upgrade, SAML SSO login does not respond.

The client authenticates against the IdP, and the IdP grants an Assertion to the client. The client presents the assertion to the service provider. Because a CoT established, the service provider trusts the assertion and grants access to the client.

Note SSO is not supported for Cisco Unified OS Administration or Disaster Recovery System. If you log in to Cisco Unified OS Administration or Disaster Recovery System when SSO is enabled, and try to access Cisco ER Administration or Cisco ER Serviceability or Cisco ER User or Cisco ER Admin Utility, then Cisco Emergency Responder authorizes the user but not authenticate through IdP. To authenticate the user through IdP, close the web browser and access the Cisco Emergency Responder again. SSO is not supported for Cisco Emergency Responder Off-Premises User page.

SAML Single Sign-On Prerequisites

- DNS configured for the Cisco Emergency Responder cluster
- An identity provider (IdP) server
- Add the same users present in IdP to Cisco Emergency Responder.
- To configure the trust relationship between IdP and Cisco Emergency Responder servers, obtain the trust metadata file from your IdP and import it to all your servers.
- Export metadata from Cisco Emergency Responder and upload it on to the IdP server.

The following IdPs using SAML 2.0 are tested for the SAML Single Sign-On feature:

- OpenAM 10.0.1
- Microsoft® Active Directory® Federation Services 2.0, 3.0, and 4.0
- PingFederate® 6.10.0.4
- F5 BIP-IP 11.6.0

The third-party applications must meet the following configuration requirements:

- The mandatory attribute “uid” must be configured on the IdP. This attribute must match the attribute that is used for the user ID in Cisco Emergency Responder.

Note Cisco Emergency Responder currently supports only the sAMAccountName option as the LDAP attribute for user ID settings.

For information about configuring mandatory attribute mapping, see the IdP product documentation.

NTP Setup

In SAML SSO, Network Time Protocol (NTP) enables clock synchronization between the Cisco Emergency Responder and IdP. SAML is a time sensitive protocol and the IdP determines the time-based validity of a SAML assertion. If the IdP and Cisco Emergency Responder clocks are not synchronized, the assertion

becomes invalid and stops the SAML SSO feature. The maximum allowed time difference between the IdP and Cisco Emergency Responder is 3 seconds.

Note For SAML SSO to work, you must install the correct NTP setup and make sure that the time difference between the IdP and Cisco Emergency Responder does not exceed 3 seconds.

For information about synchronizing clocks, see NTP Server List.

Domain Name Server (DNS) Setup

Cisco Emergency Responder can use DNS to resolve Fully Qualified Domain Names (FQDNs) to IP addresses. The Service Providers and the IdP must be resolvable by the browser.

SAML Single Sign-On Task Flow

Follow these tasks to activate SAML Single Sign-On in Cisco Emergency Responder.

Procedure

	Command or Action	Purpose
Step 1	Add An IdP User, on page 69	Use this procedure to add an IdP user.
Step 2	Enable SAML Single Sign-On, on page 70	Use this procedure to enable SAML Single Sign-On.
Step 3	Disable SAML Single Sign-On, on page 71	Use this procedure to disable SAML Single Sign-On.

Add An IdP User

Procedure

Step 1 From Cisco ER Administration, choose **User Management** > **User**.
The **Find And List Users** page appears.

Step 2 Click **Add New User**.
The **Add User** page appears.

Step 3 Enter the username in the **User Name** field.

Step 4 From the **Authentication Mode** drop-down list, choose “IdP”.

Step 5 From the **CUCM Cluster** drop-down list, choose the Cisco Unified Communications Manager cluster IP address.

Note The users can login into the recovery url by using the password set in Cisco Unified Communications Manager through AXL, if the same user name exists in Cisco Unified Communications Manager.

Local credential policy is applicable only for the local users. IdP users have the same credential policy as remote users have in Cisco Emergency Responder.

Step 6 Click **Insert**.

What to do next

Enable SAML Single Sign-On, on page 70

Enable SAML Single Sign-On

Perform the following steps to enable SAML Single Sign-On:

Before you begin

Ensure that the following prerequisites are met before proceeding with the steps:

- Add An IdP User, on page 69—Ensure to manually add at least one IdP user in Cisco Emergency Responder.

Procedure

Step 1 From Cisco ER Administration, choose **System** > **SAML Single Sign-On**.

Step 2 Click **Enable SAML SSO**.

A warning message is displayed to notify that the change made takes a few minutes to reflect on the user interface.

Step 3 Click **Continue**.

A dialog box that allows you to import IdP metadata displays. To configure the trust relationship between the IdP and your servers, you must obtain the trust metadata file from your IdP and import it to all your servers.

Step 4 Click **Browse** to locate and upload the IdP metadata file.

Step 5 Click **Import IdP Metadata**.

Step 6 Click **Next**.

Note The **Next** button is enabled only if the IdP metadata file is successfully imported on at least one node in the cluster.

A new status message is added in the **SAML Single Sign-On Configuration** window. It provides optional information to either skip or continue further with steps to upload the server metadata to the IdP.

Step 7 Click **Download Trust Metadata Fileset** to download server metadata to your system.

Step 8 Upload the server metadata on the IdP server.

After you install the server metadata on the IdP server, run a Single Sign-On test to ensure that the metadata files are correctly configured.

Step 9 Click **Next** to continue.

Step 10 Select an ldP user with administrator rights from the list of valid administrator IDs.

Step 11 Click **Run Test**.

The IdP sign-in window displays.

Note You cannot enable SAML Single Sign-On until the Run Test succeeds.

Step 12 Enter a valid username and password.

After successful authentication, the following message is displayed:

```
SSO Test Succeeded
```

Close the browser window after you see this message.

If the authentication fails or takes more than 60 seconds to authenticate, a "sign-in Failed" message is displayed on the IdP sign-in window. The following message is displayed on the SAML Single Sign-On window:

```
SSO Metadata Test Timed Out
```

To attempt signing in to the IdP again, repeat Steps 11 and 12.

Step 13 Click **Finish** to complete the SAML Single Sign-On setup.

SAML Single Sign-On is enabled and it may take one to two minutes for the changes to take effect.

Disable SAML Single Sign-On

Perform the following steps to disable SAML Single Sign-On:

Procedure

Step 1 From Cisco ER Administration, choose **System** > **SAML Single Sign-On**.

Step 2 Click **Disable SAML SSO**.

A warning message is displayed to notify that the changes made take a few minutes to reflect on the user interface.

Access the Recovery URL

Use the recovery URL to bypass SAML Single Sign-On and log in to the Cisco Emergency Responder interface for troubleshooting. For example, enable the recovery URL before you change the domain or hostname of a server. Logging in to the recovery URL facilitates an update of the server metadata.

Before you begin

- Only application users with administrative privileges can access the recovery URL.
- If SAML Single Sign-On is enabled, the recovery URL is enabled by default. You can enable and disable the recovery URL from the CLI. For more information about the CLI commands to enable and disable the recovery URL, see *Cisco Emergency Responder Command Line Interface Guide*.

Procedure

In your browser, enter `https://<hostname/hostip>/ceradmin/servlet/showRecovery`.

Update Server Metadata After a Domain or Hostname Change

After a domain or hostname change either in IdP or Cisco Emergency Responder, update the server metadata and clear the browser cache, to ensure that SAML Single Sign-On is functional.

Before you begin

If the recovery URL is disabled, it does not appear for you to bypass the Single Sign-On link. To enable the recovery URL, log in to the CLI and execute the following command: **utils sso recovery-url enable**.

Procedure

Step 1 In the address bar of your web browser, enter the following URL:

`https://<CER-server-name>` where `< <CER-server-name>` is the hostname or IP address of the server.

Step 2 Click **Recovery URL to bypass Single Sign-On (SSO)**.

Step 3 Enter the credentials of an application user with an administrator role and click **Login**.

Step 4 From Cisco ER Administration, choose **System** > **SAML Single Sign-On**.

Step 5 Click **Export Metadata** to download the server metadata.

Step 6 Upload the server metadata file to the IdP.

Step 7 Click **Run SSO Test**.

Step 8 Enter a valid User ID and password.

Step 9 After you see the success message, close the browser window.

Manually Provision Server Metadata

To provision a single connection in your IdP for multiple UC applications, you must manually provision the server metadata while configuring the Circle of Trust between the Identity Provider and the Service Provider. For more information about configuring the Circle of Trust, see the IdP product documentation.

The general URL syntax is as follows:

`https://<SP FQDN>:8443/ssosp/saml/SSO/alias/<SP FQDN>`

Procedure

To provision the server metadata manually, use the Assertion Customer Service (ACS) URL.

Example:

Sample ACS URL: `<md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://cucm.ucsso.cisco.com:8443/ssosp/saml/SSO/alias/cucm.ucsso.cisco.com" index="0"/>`

The remaining services are accessible only after providing valid local, IdP or Remote user credentials. In case of testing the SAML SSO Rest APIs using any rest client, valid credentials is necessary. The client validates the local, IdP or Remote(CER Users) authentication is same as Recovery URL, and the authentication grants an Assertion to the client. After successful authentication, the client presents the Assertion to the Service Provider. Since there is a CoT established, the Service Provider validates the Assertion and grants access to the client.

Note When you try to EnableSSO through the rest client, the server restarts. During this period, when 911 call is made, it may fetch the default ERL and the server also takes some time to publish all node information under **Cisco Emergency Responder Administration** > **System** > **SAML Single Sign-On**.