Remote Teleworker and Off-Premises User—E911

- Remote Teleworker and Off-Premises User—E911 Overview, on page 1
- Remote Teleworker Emergency Calling Prerequisites, on page 2
- Initial Configurations for Setting Up Remote Teleworker Emergency Calling , on page 3
- Configure Remote Teleworker Emergency Calling For Off-Premises Locations, on page 9
- Verify the Remote Teleworker Off-Premises Locations in Emergency Responder, on page 10
- Configuring Mobile and Remote Access Connected Devices, on page 11

Remote Teleworker and Off-Premises User—E911 Overview

Cisco Emergency Responder can be configured to provide E911 support to remote teleworker and off-premises users. These users, when registering over Virtual Private Network (VPN) or Mobile Remote Agent, can update their location through the phone display or through Cisco Emergency Responders Off-premises User Page. The Enterprise requires an arrangement with a National Emergency Service Provider to perform location updates, Master Street Address Guide (MSAG) address validation, and call completion.

Currently, Cisco Emergency Responder supports integrations with National E911 Service Provider as National Emergency Service Providers.

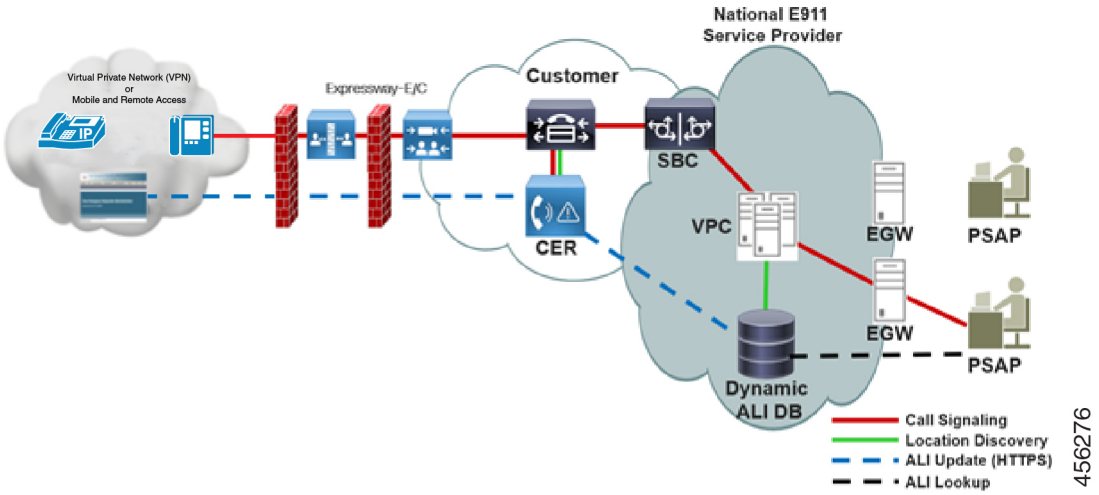
Cisco Unified Communications Manager (Unified Communications Manager) requires users with off-premises phones to set their current location before allowing any outbound call from the phone. Users that have an off-premises phone rely on Unified Communications Manager to route their emergency calls to a National Emergency Service Provider to deliver the emergency call to the appropriate Public Service Answering Point (PSAP) along with the current address.

A legal disclaimer notice is displayed on any phone device that is dynamically identified as an off-premises device (that is, connected remotely to the customer network). The disclaimer advises the users that their administrator has identified their device as outside the customer network and the user must select their current location before being able to place outbound calls. Users can confirm their current location or select another previously stored location from their device display.

If the user's current location has not been previously defined, the user is directed to the Cisco Emergency Responder Off-Premises User web page to create a new location. After the new location has been defined and the address has been validated in the MSAG, emergency calls placed from off-premises phones will then be completed through the National Provider.

Note Remote Teleworker or Off-premises user can have up to 8 preconfigured locations.

Note Extension Mobility is not supported for off-premises users.



Remote Teleworker Emergency Calling Prerequisites

- Configure National E911 Service Provider Enterprise Services. For more information, see chapter Configure Emergency Responder and National E911 Service Provider Enterprise Services.
- Enhanced e911 feature is supported only on X/Open System Interface (XSI) capable phones. For more information on XSI, see Cisco Unified IP Phone Services Application Development Notes for Cisco Unified Communications Manager and Multiplatform Phones.
  - Cisco IP Phone 7800 Series
  - Cisco IP Phone 8800 Series
  - Cisco IP Phone 7941/7945
  - Cisco IP Phone 7961/7965
  - Cisco IP Phone 7970/7971/7975
  - Cisco IP Phone 8941/8945
  - Cisco IP Phone 8961
  - Cisco IP Phone 9951/9971
  - Cisco IP Communicator

• Cisco Virtual Desktop (VXCC)

Initial Configurations for Setting Up Remote Teleworker Emergency Calling

• Unified Communications Manager Configurations Task Flow, on page 3
• Emergency Responder Configurations Task Flow, on page 6

Unified Communications Manager Configurations Task Flow

Perform the following tasks to set up Emergency Responder Location Management feature in the Unified Communications Manager server before you can use it to enter the off-premises locations.

Procedure

	Command or Action	Purpose
Step 1	Set Up AXL Application User , on page 3	Allows you to configure the AXL application user for Emergency Responder on Unified CM.
Step 2	Set Up Application Server in Unified CM, on page 4	Allows you to add an application server in Unified CM to define the configuration details for the Emergency Responder (Phone Tracking Menu page in Emergency Responder).
Step 3	Associate End User to a Device, on page 5	Associates the end user to a phone or device.
Step 4	Configure Off-Premises Location Facility, on page 5	Configure this option for remote or mobile devices that change locations frequently.
Step 5	Configure a Directory Number, on page 5	You can configure the directory number configuration settings for the phone or device.

Set Up AXL Application User

When configuring the off-premises user feature, Emergency Responder uses an application user to perform AXL queries and device registration checks. This application user should be different than the CTI Manager User Name. The CTI Manger User Name is used to control the CTI Route Points and the CTI Ports. The AXL User is used to perform device and user queries in the Unified Communications Manager database and device registration status.

Procedure

Step 1 In Cisco Unified CM Administration user interface, choose **User Management** > **Application User** and click **Add New**.

Step 2 Complete the following required fields:

- **User ID**—Use a descriptive name such as AXL Application User.
- **Password**—Enter a password for this user.
- **Confirm Password**—Reenter the password for this user.

Step 3 Click **Save**.

Step 4 Choose **User Management > User Group** in the CiscoUnifiedCommunications Manager menu.

Step 5 At search criterion, enter **standard** and click **Find**.

Step 6 Click **Standard CCM Admin Users** to display the User Group configuration page.

Step 7 Click **Add App Users to Group**.

Step 8 Enter the User ID created in Step 2 as the search criterion and click **Find**.

Step 9 Click the check box next to the user ID. Click **Add Selected**.

Unified CM adds the selected user to the **Standard CCM Admin Users** user group.

Step 10 Choose **User Management > User Group**.

Step 11 Enter **standard** as the search criterion and click **Find**.

Step 12 Click the **Standard TabSync User** group.

Step 13 Repeat steps 7-9 to add the user to the Standard TabSync User group.

Step 14 Choose **User Management > User Group**.

Step 15 Enter **standard** as the search criterion and click **Find**.

Step 16 Click the **Standard RealtimeAndTraceCollection** group.

Step 17 Repeat steps 7-9 to add the user to the Standard RealtimeAndTraceCollection group.

Set Up Application Server in Unified CM

You must configure the Emergency Responder Location Management server on the Unified CM server before your users can use it to enter their off-premise locations.

Procedure

Step 1 From Cisco Unified CM Administration, choose **System > Application Server**.

Step 2 Click **Add New**.

Step 3 From the Application Server Type drop-down list, choose **CER Location Management** and click **Next**.

Step 4 Enter a name that identifies Emergency Responder Off-Premise application.

Step 5 Enter details for the following:

- **IP Address**—IP Address of the Emergency Responder to which Unified Communications Manager is connected.
- **Selected Application Users**—Select the AXL application user that was created in the previous step.

Step 6 Enter the End User URL for users to access the Emergency Responder Off-Premises page.

The URL takes the form of `http://cer_host/ofpuser` , where `cer_host` is the FQDN of the Emergency Responder server or the IP address of the Emergency Responder. The end user URL is the URL

that is presented to the user when they select **Add New** on the device when the user wants to define a new location.

Step 7 Click **Save**.

Associate End User to a Device

Required devices should be associated with the user on the End User page as Controlled Devices (From Cisco Unified CM Administration user interface, navigate to **User Management > End User** and associate the device in the Controlled Devices section) and also on the Phones page in the **Owner User ID** field.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device > Phone**.

Step 2 Enter the device details.

Step 3 In Device Information, select the **Owner** as **User** and set the **Owner User ID** to the user that this device is assigned to.

Step 4 Click **Save**.

Configure Off-Premises Location Facility

To trigger the off-premises notification sequence, the administrator must configure the device to invoke the off-premise location check during the registration process. Perform the following:

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device > Phone**.

Step 2 In the Device Information section, check the **Require off-premises location** option if the device requires off-premises location check upon registration. Off-premises location update is required when the device's location is associated with an off-premises ERL (as defined in Emergency Responder).

Step 3 Click **Save**.

Configure a Directory Number

Configure the following in the Directory Number configuration page to ensure proper call routing for Remote Teleworkers:

Procedure

Step 1 In the Phone Configuration page, select the **DN** from the Association section on the left side of the page.

Step 2 In the Directory Number Configuration page, verify that the **External Phone Number Mask** will make the actual directory number into a 10-digit North American Numbering Plan (NANP) number.

If the DN on the phone is not a 10-digit NANP number, define the external phone number mask to create a 10-digit NANP number. If the **External Phone Number Mask** is used, the mask must include at least one X to be considered valid for the Remote Teleworker feature.

Step 3 Click **Save**.

Emergency Responder Configurations Task Flow

Perform the following tasks to set up Emergency Responder Location Management feature in the Emergency Responder server.

Procedure

	Command or Action	Purpose
Step 1	Set Up and Test National E911 Service Provider Connectivity, on page 6	Validate connectivity to National E911 Service Provider.
Step 2	Set Up an National E911 Service Provider Route Pattern, on page 7	Sets the route patterns for routing the call to National E911 Service Provider.
Step 3	Set Up AXL Authentication , on page 7	Allows you to configure the AXL credentials and port information.
Step 4	Set Up Off-Premises ERL , on page 8	Adds a new emergency response location (ERL) for Off-Premises phones.
Step 5	Configure Default ALI Values for National E911 Service Provider ERLs, on page 8	Adds the Default ALI Values for National E911 Service Provider URLs.
Step 6	Configure IP Subnet, on page 9	Defines the IP subnet and associated URL.

Set Up and Test National E911 Service Provider Connectivity

You can use the National E911 Service Provider VUI configuration page to enter the account information that is required for Emergency Responder to interoperate with National E911 Service Provider Validation and Update Interface (VUI). After entering the required information, you can test the connectivity to National E911 Service Provider from this page.

Contact your chosen National Emergency Service Provider (National E911 Service Provider) to obtain the required National E911 Service Provider configuration details. For more information on the National E911 Service Provider VUI configuration settings in Emergency Responder, see National E911 Service Provider VUI Settings.

Before you begin

- DNS must be configured in Emergency Responder and Unified Communications Manager to reach the National Providers VUI services.

Note To configure the Domain Name System (DNS) in both the Unified Communications Manager and Emergency Responder, execute the **set network dns primary** command.

Run the **set network domain** command to set the network domain.

Procedure

Step 1 From Cisco ER Administration, choose **System** > National E911 Service Provider **VUI Settings**.

Step 2 Upload the certificate from your local drive to the Emergency Responder server.

Step 3 Enter the **Certificate Password** and the **VUI URL** that was specified by the provider.

Step 4 Test and Validate the Certificate.

Step 5 After verifying the validity of the certificate, add the **VUI Schema URL** and **Account ID**.

Step 6 Click **Test Connectivity** to verify whether Emergency Responder can successfully connect to National E911 Service Provider VUI or not.

On the 'Test National E911 Service Provider Connectivity' pop-up window, the Test Results section should show status “200 OK” after pressing the **Connect** button. This response indicates that both the certificate and account information are valid.

Set Up an National E911 Service Provider Route Pattern

Before any emergency calls can be completed by National E911 Service Provider for Enterprise Service, you must configure the route patterns for routing the call to National E911 Service Provider.

Procedure

Step 1 From Cisco ER Administration, choose **System > Telephony Settings**.

Step 2 Under National E911 Service Provider Route Pattern Settings, enter the National E911 Service Provider **Route/Translation Pattern** and click the **Add** button.

What to do next

Verify that the lock icon next to the **ERL > Off Premise ERL** is removed and the page is accessible.

Set Up AXL Authentication

When setting up Emergency Responder for supporting Remote Teleworkers, Emergency Responder will use the AXL user to access information about device configuration and status through the AXL interface. You must define and test AXL connectivity to the Unified Communications Manager in Emergency Responder to ensure that the user has access to the AXL resources. This procedure verifies that the user information entered has connectivity to the required AXL resources.

Procedure

Step 1 From Emergency Responder, choose **Phone Tracking > Cisco Unified Communications Manager**.

Step 2 Select the Unified CM cluster for which you will be providing the off-premises user support.

You can find the previously defined Unified CM clusters at the bottom of the page.

Step 3 Under AXL Setting, enter the following information:

- AXL Username
- AXL Password
- AXL Port Number

Step 4 Click the **Text AXL Connectivity** URL.

Step 5 Click **Connect**.

If the AXL user is correctly defined, the result displays "Connection succeeded". If an error comes back, try reentering the user and password information and try the connection again.

Step 6 Click **Update** to save the information.

Set Up Off-Premises ERL

Use this procedure to create a new emergency response location (ERL) for Off-Premises phones. For most installations, users need only a single Off-Premise ERL to route Off-premises calls to the National Provider.

Procedure

Step 1 From Cisco ER Administration, choose **ERL > Off-Premises ERL > Off-Premises ERL (Search and List)** from Emergency Responder.

Step 2 Click **Add New ERL**.

Step 3 Enter an ERL name and description.

Step 4 Enter the National E911 Service Provider Route/Translation Pattern.

Step 5 Select the Off-Premises users who should be notified when an emergency call is made from this ERL.

Step 6 Click **Insert** to save the Off-Premises ERL information.

Configure Default ALI Values for National E911 Service Provider ERLs

Use the Default ALI Values page to set the default values that automatically populate the respective ALI fields when a user updates their National E911 Service Provider ERL settings.

Procedure

Step 1 From Cisco ER Administration, choose **ERL >** National E911 Service Provider **ERL > Default ALI Values**.

Step 2 Enter the **Company ID**.

Step 3 Enter the **Customer Name**.

Step 4 Click **Save**.

Configure IP Subnet

Use the Configure IP Subnet page to manually define an IP subnet and its ERL. The IP Subnet used to identify the off-premises devices will be the internal address of the Expressway E/C nodes or the VPN subnet/VPN concentrator.

Procedure

Step 1 From Cisco ER Administration, choose **ERL Membership > IP subnets** and click **Add new IP subnet**.

Step 2 Enter the Subnet ID and Mask details.

- For VPN connected devices, the IP Subnet should be a subnet/mask format.
- For Mobile Remote Agent connected devices, the IP Subnet may be subnet/mask or a specific IP address.

Step 3 Click **Search ERL** to select the ERL you want to assign to the subnet.

Step 4 In the ERL Search Parameters, set the find value to **Off-Premise ERL** and click **Find**.

Step 5 Click the radio button next to the Off-Premise ERL (defined previously) and click **Select ERL**.

Step 6 Click **Insert** to add the subnet on the Configure IP Subnet page.

Configure Remote Teleworker Emergency Calling For Off-Premises Locations

Add New Location

Before a user can associate a location to their phone or device, the user must first enter a location into Emergency Responder. All locations defined in Emergency Responder are user-specific. Each user must add their own locations. When a user has multiple locations, each location must have a unique name to identify that unique location.

Procedure

Step 1 Log in to the Cisco Emergency Responder Off-Premises User page at **https://<CER_FQDN>/ofpuser** using the end user credentials.

Note Emergency Responder Off-Premises User page does not support SSO logins.

Step 2 From the Cisco Emergency Responder Off-Premises User page, select **Locations** and click **Add New Locations**.

Enter a valid address. Use this location name to identify this address when you associate your phone with this address.

Step 3 Click **Validate** to verify the address with your National Provider.

Step 4 If the address validation fails, the user must correct the address before saving the location.

Step 5 Click **Save** to save the location information in Emergency Responder.

Note Saving the location does not immediately update the National Provider, but stores the location information in Emergency Responder. When a user selects the location from the device, the stored address information is sent to the National Provider to update the address for the user's E.164 number.

Associate Your Location to Your Phone

After a user defines a location in Emergency Responder, the user should associate and verify that the device is associated to the desired location.

Procedure

Step 1 From the Cisco Emergency Responder Off-Premises User page, choose **Phones**.

Step 2 To associate a location to a phone, click the corresponding **Assign** link.

Step 3 In the Associate Location page, select the desired location from the **Select New Location** drop-down list. The new location becomes active when you click the **Associate Location** button.

The Status field show displays that the "Location Association Is Successful." This indicates that the address is valid and has been updated with the National Provider.

Step 4 Once the location is associated, the device on the Phones page should display the device status as **Off Premises** and the Associated Location should match the one that was selected. Additionally, ensure that the Direct Inward Dial (DID) is a properly formatted 10-digit NANP number.

Verify the Remote Teleworker Off-Premises Locations in Emergency Responder

Note If the remote or off-premises user chooses not to update their current location, the Disclaimer prompts the user to acknowledge that calls may be restricted until the location is updated. 911 calls will not work until the user decides to associate their device to the desired location.

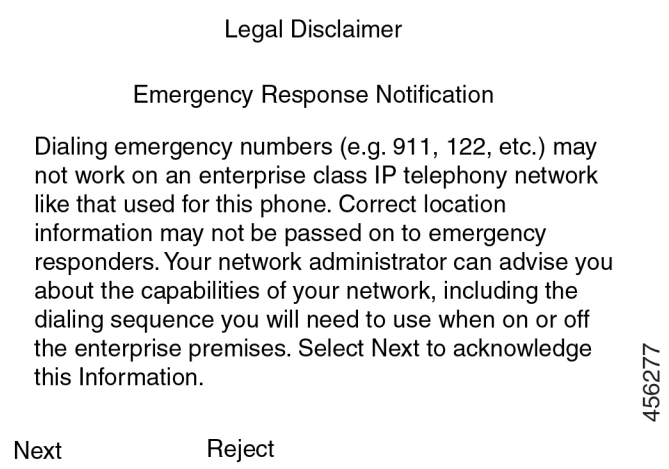
As the System Administrator, you can configure to select and mandate location update so that the device user has to acknowledge the disclaimer and provide current location information before the device is enabled for normal use. (From Cisco Unified CM Administration, choose **System > E911 Messages** to configure the mandatory location update disclaimer message.)

Procedure

Step 1 Reset the phone or device.

After the phone has rebooted and after 2-5 seconds after registering, the device should display the Remote Teleworker legal notification. At this point, the remote teleworker location selection process should start.

Step 2 Ensure that the following legal disclaimer message appears on the phone.



Step 3 Click **Next**.

You will get the details of all the locations added through Cisco Emergency Responder Off-premises URL.

Step 4 Using the toggle buttons on the phone or device, choose a location and press the **Select** button.

A few seconds later, the phones user interface should indicate the successful settings of the off-premises user's location.

What to do next

Administrators should instruct the users on how to validate the accuracy of the E911 address based on the user-defined setting. This process should follow the company's procedure for emergency address validation. When a user dials 911 as per the company process for validating the emergency dispatch address, the call should be routed to public-safety answering point (PSAP) using the off-premises ERL and the address reported by the PSAP should be the address currently assigned to the device through the Cisco Emergency Responder Off-Premises User Page.

Configuring Mobile and Remote Access Connected Devices

Configuring devices connected over the Mobile and Remote Access Edge (Cisco Expressway-E/C) will occur in the same way as the VPN connected phones. The IP Subnet used to identify Mobile and Remote Access clients will be the Expressway-C's IP Address. All phones or devices registered to Unified Communications Manager using Mobile and Remote Access will have the same IP Address as the Unified CM.

The configuration procedures for Mobile and Remote Access clients are the same as for VPN clients except that the Mobile and Remote Access setup requires one additional configuration step on the Expressway-C to work. In order to allow the HTTP requests from the phones to the E911Proxy service to obtain the XSI messages, the external Cisco Expressway server must have an explicit HTTP service mapping. This mapping is required to map the external request to an internal resource.

The following configuration must be set up in the Cisco Expressway:

Procedure

Step 1 From the Cisco TelePresence Video Communication Server Control, navigate to **Configuration > Unified Communications > HTTP allow list > Editable inbound rules**.

Step 2 Enter a description.

Step 3 Enter the **URL** to reach the E911Proxy service. The URL should be **https://cucmfqdn:8080/e911proxy** .

Step 4 Enter the **Allowed Methods** and **Match type**.

Note Because E911Proxy HTTP requests are node-specific, the Expressway administrator must add the 'E911Proxy' service for all call processing nodes in the cluster. Any node that has phone registrations must have an Expressway-C entry to allow the XSI messages to be retrieved to complete the remote teleworker location selection process.