Dedicated Instance

Configuring Emergency Responder with a National E911 Service Provider

Version 1.1

© 2022 Cisco and/or its affiliates. All rights reserved.

Contents

© 2022 Cisco and/or its affiliates. All rights reserved.

National Emergency Calling Service Provider Integration with the Emergency Responder—Overview

As employees move to a hybrid work model, employers must provide calling services to remote users with the same level of service available in the office. This includes the need for remote workers to set their location for emergency call dispatch. And starting in January of 2022, RAY BAUM'S Act requires all employers to provide an accurate emergency dispatch address for remote workers. This federal regulation has led many employers to extend their calling solution to include a National Emergency Calling Service Provider (National Provider) to meet these federal regulations.

Using a National Emergency Calling Service Provider for call routing enables a customer to deliver an emergency call to any PSAP in the US and Canada. A National Emergency Calling provider also eliminates the need to have physical connections (i.e., PRI or analog) in each service area that users work in.

Hybrid workers that use Cisco call control, including Dedicated Instance (DI), can integrate with a National Emergency Calling Service Provider and allow an administrator to simplify the on-premises location tracking as well as off-premises user location updates. The integration with the National Providers requires Cisco Emergency Responder (CER).

Although CER integration with a National Provider simplifies the on-premises location management solution, the ability to support nomadic users makes the CER with the National Provider integration critical to meeting federal regulations. For identifying the location of a nomadic user, Cisco recommends that when a hybrid worker is working on-premises at a company site, the user's location should be defined by the calling system administrator. But when a hybrid worker is working outside their company's facility, each worker should be responsible for updating their location. The integration with a National Provider gives hybrid employees the ability to update their location based on their current location without any administrator intervention.

Cisco's calling solution offers emergency calling support for all calling products, but the mechanism for providing location updates differs based on the device or client. For example, on-premises physical phones normally use CDP neighbor information or IP subnet to determine location. Soft clients (on PCs or MACs) are normally tracked by wireless AP association or IP Subnet. Soft clients that are installed on mobile devices (iPhone or Android) use the native dialer to deliver emergency calls, even when located on-premises. When nomadic clients and endpoints are off premises, the location updates must be provided by each user because their location is outside the administrator's area of responsibility. For deployments that need to support nomadic users when both on-premises and off-premises, Cisco recommends the following methods for location updates:

Device	On-Premises	Off-Premises
Cisco IP Phone (all models)	CER-CDP/IP Subnet	RedSky-MyE911
Jabber (Mac/Win/Tab)	CER-AP/IP Subnet	RedSky-MyE911
Jabber (iPhone/Android)	Native Dialer	Native Dialer
Webex App (DI) (Mac/Win/Tab)	Native UI (HELD+)	Native UI (HELD+)
Webex App (iPhone/Android)	Native Dialer	Native Dialer

© 2022 Cisco and/or its affiliates. All rights reserved.

In a Dedicated Instance deployment, both the Cisco Emergency Responder (CER) and RedSky will be utilized to track phones and clients. On-premises phones will be tracked using the Emergency Responder to identify the location of the phone and setting the appropriate dispatch location before routing the call to RedSky for call delivery. Webex App users will be tracked in RedSky using HELD+ protocol.

When integrating CER with a National Provider, an administrator will perform traditional tasks in CER toidentify the physical location of a device/user and the identification number. Administrators will create Emergency Response Locations (ERLs), which specify a specific location that emergency services will bedispatched to. The definition of an ERL depends on the building, but typically an ERL is the building address and a floor of the building (in a multi-story building) or a "zone" within the building based on state regulations. Administrators must also assign the Emergency Location Identification Number (ELIN) to each location. The use of ERLs and ELINs is currently how Cisco ER should be configured to supporton-premises device location discovery. But an advantage of having a National Provider integration is that the ERL and ELIN information can be automatically synchronized with the National Provider. This synchronization process allows an administrator to update their on-premises location information and have the definition and updates take effect immediately. Additionally, using a National Provider relievesthe administrator from having to update each emergency service PSAP. Instead, the administrator sends all updates to the National Provider.

This document will discuss how to integrate CER with a National Emergency Calling Service Provider tosimplify the provisioning aspects of Emergency Response Locations (ERL) and Emergency Response Identification Numbers (ELIN). The ability to define ERLs and ELINs with a National Emergency Calling Service provider allows an administrator to update the emergency dispatch addresses for all of their facilities across the US and Canada. The support for nomadic users using the MyE911 app from RedSky will also be covered in this document.

Creating National Emergency Calling Service Provider Account

Webex Calling customers with users in the U.S. are entitled to get an account. To request an account, you will need to contact your partner to begin the process. Partners must go through a one-time onboarding call with RedSky to understand this solution. Partners or customers can request an account. To create an account, you must be prepared to provide the following information and answer the following questions:

- Customer Name
- Organizational ID
- Administrator Email ID and Name
- Partner Name
- Partner Admin Email ID and Name
- Number of Users (approximate number of users in the U.S)
- Have you purchased a Dedicated Instance license?

You can submit account creation requests using a Webex bot – E911Account@webex.bot. This is also where you will submit the previous information.

Note: If your partner is not onboarded, the support team will contact the partner administrator and help with the onboarding process. This may take some time so please plan accordingly.

© 2022 Cisco and/or its affiliates. All rights reserved.

Setting up the Emergency Responder and Test National Provider Connectivity

After you have received confirmation that your company's emergency service account has been created with the National Provider, you must configure the Emergency Responder to verify connectivity with the National Provider's configuration web services. Connectivity is required toallow CER to send ERL and ELIN information to the National Provider for on-premises and off-premises devices.

You must complete the tasks described in the following procedure to unlock the CER menus that allow the creation, modification, and updates with the National Provider's services.

Note: Although the Emergency Responder uses the name Intrado for all configuration tasks, both Intrado and RedSky, an Everbridge company, are approved third-party National Emergency Calling Service Providers with CER. Any reference to Intrado should be understood to mean either Intrado or RedSky, depending on your chosen provider.

Note: You must configure the IP address of the DNS server to resolve the URLs provided by the National Provider before completing these tasks. See Cisco Unified Operating System Administration Web Interface for the Emergency Responder.

	Command or Action	**Purpose**
Step 1	Set up the Intrado VUI Setting.	Uploads the certificate, defines the VUI URL and sets up the configuration account details.
Step 2	Configure the default ALI Values for Intrado ERL.	Sets the default VUI account settings.
Step 3	Set up the dialing patterns for routing calls to the National Provider on CER.	Configures the route patterns for routing emergency calls to the National Provider.
Step 4	Set up the route pattern for routing calls to the National Provider through Dedicated Instance	Configures the route pattern to route emergency calls to the National Provider.

Setting up Intrado VUI Settings

For any deployment that supports users in the United States, the CER services come with the Intrado VUI settings preconfigured with the RedSky certificate, cloud service URL and proxy information. The only configuration that must be set before using the VUI services is the Intrado account ID. Each customer has a unique Intrado account ID available on the RedSky administration portal. An Intrado account ID is a five-digit number.

Procedure

1. From the Emergency Responder, select **System > Intrado VUI Settings**.
2. Steps 1 and 2 for the configuration will already be configured.
3. In Step 3, change the Intrado Account ID to the value specified in the RedSky administration portal.

© 2022 Cisco and/or its affiliates. All rights reserved.

4. Click **Test Connectivity** to verify whether Emergency Responder can successfully connect to the customer specific account through the Intrado VUI.

   Note: On the "Test Intrado Connectivity" pop-up window, the Test Results section should show status "200 OK" after you click Connect. This response indicates that both the certificate and account information are valid. If the preceding steps are successful, then Intrado related ERL, search list, and so on are unlocked.

5. Click **Update**.

Configuring the Default ALI Value for Intrado ERL

When integrating with a National Provider, there will be certain operations that occur that require the customer to define default values for any updates that occur with the National Provider. This section describes the default settings that must be defined before sending calls to the National Provider.

Procedure

1. From CER Administration, select ERL > Intrado ERL > Default ALI Values.
2. Fill in the parameters with the following values:

Parameter	Value
Type of Service	Non-Pub (recommended)
Class of Service	VOIP Default (recommended)
Company ID	Provided by the National Provider
Customer Name	Name of Company

3. Click Save/Update.

Setting up Dialing Patterns for Routing Calls to the National Provider (CER)

Before any emergency calls can be delivered to a National Emergency Calling Service Provider, the Emergency Responder must have at least one routing pattern configured for routing emergency calls to the National Provider. Since all emergency calls that are routed to a National Emergency Calling Service Provider use the same path, only one Intrado routing pattern is needed. Call delivery and redundancy is accomplished using a route list and route group configuration. So, defining additional Intrado route patterns is only needed if the deployment uses different route patterns for different call paths (like SIP and PRI).

The method for routing emergency calls to the National Provider can be a direct routing pattern or a translation pattern. The route pattern should be one that can be easily identified and transformed into the properly formatted 911 pattern that's sent to the National Provider. Cisco recommends against using 911 as the Intrado route pattern in the CER to avoid confusion with the other 911 patterns in the system. By choosing an Intrado routing pattern like 119911, the administrator should configure a route pattern of 119.911 to discard the predot and send the call with the called party of 911 to the National Provider.

Procedure

1. From the CER Administration, select **System > Telephony Settings**.
2. Under Intrado Route Pattern Settings, type the Intrado Route/Translation pattern, and then click **Add**.

© 2022 Cisco and/or its affiliates. All rights reserved.

Setting Up the Route Pattern for Routing Calls to the NationalProvider through Dedicated Instance

All emergency calls that need to be routed to the National Provider must match a route pattern that directs the call to a Route Group, Route List and SIP Trunk or PRI gateway that can reach the National Provider. Most customers choose to integrate with the National Providers using SIP Trunks, but PRI will provide comparable service in most situations. Cisco recommends using SIP Trunks to connect with the National Provider. This is the default method for Dedicated Instance. To simplify the deployment, customers that are using Dedicated Instance will have pre-defined Route Groups set up for delivering calls to the National Provider.

If using a SIP trunk, the administrator must use a pre-defined LUA script to ensure proper customer identification. For Dedicated Instance deployments, the LUA script is included in the installation. The LUA script allows for only one parameter, which is the RedskyOrgID.

Procedure

1. In UC Manager admin, navigate to **Call Routing > Route/Hunt > Route Pattern**.
2. Add a new route pattern.
3. Add the same pattern that was defined in the previous step. If the pattern 119911 was used, the Route patternshould be 119.911. Set the route partition to one that the CER Route Point has access to, and then set the Discard Digits to “PreDot”.
4. Before saving, the route pattern must have a Gateway/Route List specified. For Dedicated Instance, use the predefined trunk of “xUS-<DC>-e911-RedSky-Trk”. For non-DI deployments, select the admin-created Route List to reach the SIP Trunk and then the National Provider.
5. Click **Save**.

Configuring Emergency Responder for National Provider Integration for On-Premises Phones

Use the following workflow to guide you through the setup ERLs and ELINs that will be used by the National Provider for on-premises devices for location setting. This process can only be done after the VUI Integration process covered earlier has been completed.

Procedure

	Command or Action	Purpose
Step 1	Create the Intrado ERLs.	Configures the ERLs that will be sent to the National Provider.
Step 2	Add the scheduled Intrado updates.	Creates the ALI and Secondary Status update schedules between the Emergency Responder and RedSky.
Step 3	Update the scheduled Intrado updates.	Updates the schedules.
Step 4	Optional – Migrate conventional ERL to Intrado ERL (for existing CER deployments).	Migrates ERLs from the CER to a National Provider.

© 2022 Cisco and/or its affiliates. All rights reserved.

	Command or Action	Purpose
Step 5	Create infrastructure references and assign ERLs.	Describes basic wire map. (TBD)

Creating Intrado ERLs

Before you begin

The CER Administrator must first configure at least one Intrado route pattern before any Intrado ERLs can be added to the system.

The creation of Intrado ERLs will need to be performed by an administrator to route emergency calls to a National Provider for delivery to the correct PSAP. If this is a new CER deployment, then the administrator should use the Intrado ERL configuration for all ERL definitions. If this is an existing CER deployment, read the next section to learn about migrating conventional ERLs to Intrado ERLs.

Intrado ERLs will be configured basically the same as Conventional ERLs. One minor difference is that the route pattern for routing the calls can only be selected from the route pattern previously defined in the Intrado Route/Translation pattern section. This is because all ERLs that are set up as Intrado ERLs must route to the National Provider.

All Intrado ERLs will be sent to the National Provider. The update process with the National Provider is a push process to create or update ALI records. The updates to the National Provider are not a synchronization, so any changes in the ALI record in the National Provider's database will be overwritten by the CER records during the next scheduled update. Additionally, any ERL's that are deleted on CER will not be deleted in the National Provider's database. All ERL deletions in the National Provider's database, are a manual process.

Procedure

1. From the Emergency Responder, select **ERL > Intrado ERL > Intrado ERL** (Search and List).
2. Click **Add New ERL**. The Emergency Responder opens the Add New ERL window.
3. Fill in the ERL Information with a Name and Description.
4. Select the Route/Translation pattern defined earlier and add the ELIN Number to represent this location.
5. Select any Onsite Alert IDs that should be notified if an emergency call originates from this location.
6. Click ALI Details. Emergency Responder opens the ALI Information window.
7. Define the required fields for the ALI record.

   Note: To allow for a common location name between the National Provider's location and CERs ERL name, Cisco recommends that the ERL name be put in the Comments field.

   Note: The Location field is limited to 20 characters total. ERLs with a location field longer than 20 characters will be rejected by the National Provider.

   Note: The Query from Intrado and Pre-Validate from Intrado operations do not work with RedSky Horizon Mobility.
8. Click **Save and Close**.

© 2022 Cisco and/or its affiliates. All rights reserved.

9. Click **Insert**.
10. After saving the record, the record is ready for conveyance to the National Provider. Click Update to Intrado to send the record immediately. Otherwise, the record will be sent to the National Provider when the next scheduled update is to occur.

What to do next

This step is for new installations, but if this deployment has existing ERLs, the existing Conventional ERLs can be migrated to an Intrado ERLs using the **ERL Migration Tool** page. Information about how to migrate conventional ERLs to Intrado ERLs can be found later in this chapter.

Adding Scheduled Intrado Updates

To ensure consistency between the Emergency Responder's Intrado ERLs and the National Emergency Calling Service Provider, an administrator can create ALI and secondary status update schedules between the CER and a National Provider. A scheduled ALI update sends newly created Intrado ERL records to the National Provider. A scheduled secondary status update sends queries to the National Provider requesting information about records with errors that have been corrected.

Procedure

1. Select **ERL > Intrado ERL > Intrado Schedule** from the Emergency Responder.
2. Select the days of the week and the time of day that you want to schedule an update. Cisco recommends that you complete the update at least once a day at a time that least impacts your system (for example, 2 AM).
3. Select the Enable Schedule check box if you want to activate this schedule.
4. Select either ALI Update Schedule or Secondary Status Update Schedule.
5. Click Add to add the schedule to the list of schedules.

Updating the Scheduled Intrado Update

Procedure

1. From the Emergency Responder, select **ERL** > Intrado ERL > Intrado Schedule.
2. Click the **Edit** link adjacent to the schedule that you want to update.
3. Select the days of the week and the time of day.
4. Select or clear the **Enable Schedule** check box to activate this schedule.
5. Click **Update** to change the schedule on the list of schedules.

Conventional ERL to Intrado ERL Migration for Existing CER Deployments

Existing deployments that have already defined ERLs and ELINs for on-premises location identification will have access to the ERL Migration Tool to migrate and synchronize their existing ERLs with the National Provider. The ERL Migration option will be available once the administrator has successfully configured CER integration with a National Provider. This process is optional and should not be used unless there are previously defined Conventional ERLs.

Cisco Emergency Responder has three different types of ERLs. The three ERL types are off-premisesERL, conventional ERL and Intrado ERL. The off-premises ERL that is used to manage hybrid workers that are off-

© 2022 Cisco and/or its affiliates. All rights reserved.

premises will be covered later in this document. This section will cover the difference between conventional ERLs and Intrado ERLs and the migration from conventional to Intrado ERLs.

A conventional ERL is one that is defined in CER and will be exported and provide to the local carrier or service provider. A conventional ERL is only defined in CER and the administrator must manually export and update the ALI records with the local telco or telephony service provider. An Intrado ERL is an ERL that is defined in CER but is automatically uploaded to the National Emergency Calling Service Provider. The configuration of a Conventional and Intrado ERL is the same from a definition standpoint. The main difference is when you save Intrado ERL. After savingan Intrado ERL, the administrator has the option of sending the ERL ALI information to Intrado or saving the ERL records and waiting for the next synchronization scheduled update.

As previously mentioned, a National Provider can provide emergency dispatch to all PSAPs across the US and Canada. By uploading the ERL records to the National Provider, the addresses are validated and stored for call dispatch. And since the dispatch address will be synchronized with the National Provider, the address can be updated at any time. Once uploaded, the change takes effect immediately.

Cisco recommends that customers use Intrado ERLs to simplify their solution for ALI Management.Although the recommendation will simplify the management and update of ALI records, Cisco doesnot require customers to make this change. Customers can continue to use their existing CER setup and enable just the off-premises location updates for hybrid users.

The procedure in this section will allow administrators to bulk migrate their existing configuration tothe National Provider. Cisco recommends that you bulk update all existing ERLs to ensure that the ERL name is present in the National Providers interface. Cisco highly recommends that you use a common ERL name in CER and the National Provider.

The first part of this process is to update all conventional ERLs to add the ERL name into the Comments field of the ALI. This ensures location name consistency and uniqueness in the National Provider’s location database.

The second part of the process is to migrate the Conventional ERLs to Intrado ERLs.

Procedure

1. In CER administration, navigate to **ERL > Conventional ERL.** Select Export from the top of the display window.
2. Export the file to CSV and provide a filename. Click **Export**.
3. After exporting the records, in the Download section, select the file that was exported, and then download it.
4. Open the file in an application that supports CSV files (for example, Excel). Select and copy all the values inthe ERL Name column and paste them into the Comments column. Pay special attention to paste the values in row 2. Verify that the ERL and the value in the Comments column match.
5. Check the Location field for length. National Providers can only accept 20 characters for the Location field. Any location value longer that 20 characters will be rejected and must be fixed. Save the file to the local system.
6. In CER administration, navigate to **ERL > Conventional ERL**. Select **Import** from the top of the display window.
7. Select **Upload** and choose the file modified in Step 5. After uploading the file, **Close** the upload file window.
8. On the **Import ERL Data** page, select the file that was just uploaded and click **Import.** The import status results should have the records inserted matching the number of exported records from Step 2.
9. Check a few records to make sure the ALI records have the proper information after the import. After verification, the next step is to migrate to Intrado ERLs using the ERL Migration Tool.

© 2022 Cisco and/or its affiliates. All rights reserved.

This procedure will convert a Conventional ERL into an Intrado ERL.

Procedure

1. In CER administration, navigate to **ERL** > ERL Migration Tool.
2. In the ERL search parameters, select **Conventional ERL** as the search criteria, and then select **Find**.

   Note: The default search returns only 20 ERLs. To migrate more ERLs as a time, set the **Show** value to 50 (max value).

3. Select all the ERLs to migration using the check boxes. Navigate to the bottom of the page and select Migrate to Intrado ERL.
4. In the **Enter Values for ERL Migration** pop-up select the Route/Translation pattern set for reaching the National Provider and set the **Class of Service** and **Type of Service** to "VOIP Default" and "Non-Pub", respectively. Click the **Migrate to Intrado ERL**.
5. When you finish, the page should indicate that CER was able to migrate successfully. Continue migrating the existing conventional ERLs to Intrado ERLs.
6. After migrating all conventional ERLs to Intrado ERLs, the Intrado ERLs are migrated within CER, but have not been sent to the National Provider. Intrado ERLs are uploaded with the next scheduled Intrado update.

   After completing the ERL migration and the first schedule synch is completed, verify that the CER ERLs have been imported into the National Providers Location database. Once completed, infrastructure can be assigned to ERLs in the National Provider's database or in CER.

Configuring Cisco Emergency Responder for Off-Premises Users

When a hybrid user is off-premises, the Cisco Emergency Responder must be able to identify the off-premises users to preserve the calling party of the caller and pass that number to the NationalProvider. Off-premises users are identified based on the IP subnet of their connection to Dedicated Instance. There are three primary methods for a hybrid worker to connect to calling services: VPN client, Hardware VPN (Virtual office), or through an ExpresswayE/C deployment (MRA)

This section explains how to configure CER to identify an off-premises user and route the call to the National Provider for emergency call handling.

Procedure

	Command or Action	Purpose
Step 1	Verify the off-premises MyE911 service setting.	Confirms that the Intrado VUI configuration has the MyE911 flag set to True.
Step 2	Set up the Intrado off-premised ERLs.	Ensures that you configure the Intrado route patterns before you add the Intrado off- premises ERLs.
Step 3	Configure the IP subnet for off-premises users in the Emergency Responder.	Defines the IP subnet for off-premises phone and associated ERL.

© 2022 Cisco and/or its affiliates. All rights reserved.

	Command or Action	Purpose
Step 4	Instruct users on using MyE911 to set their location when off-premises.	Ensures that off-premises phone users add locations and associate their devices to those locations.

Verifying Off-Premises MyE911 Flag Setting

When CER is integrated with a National Emergency Calling Service Provider and you want remote users to use an application to set their location, then you must configure CER to pass the calls to the National Provider without the user setting their location in CER. Examples of an application that can set the off-premises location of a user are RedSky MyE911, Intrado Remote Location Manager and Cisco Webex App (running HELD+).

Procedure

1. From the CER Administration page, Select **System > Intrado** VUI Settings.
2. Ensure that the **MyE911 for Location Updates** is set to True.

Setting up Intrado Off-Premises ERLs

In situations where a hybrid worker sets their location through an application or through the Webex App, CER must have an ERL created to route the call to the National Provider while preserving the calling party's number. At the National Provider, the calling party number will be used to associate the calling party to the location of the caller. In the CER, there must be at least one off-premises ERL to ensure the calling party number is sent instead of an ELIN, like on-premises devices sent to the National Provider.

Although multiple off-premises ERLs can be defined, only one is needed per customer.

Procedure

1. From CER, select **ERL > Intrado ERL > Off-Premises ERL** (Search and List).
2. Click Add New ERL.

   CER opens the Add New ERL window.
3. Fill in the ERL Name and Description information.
4. Select the Route/Translation pattern defined for reaching the National Provider and any user that should be notified when an off-premises call is placed.

   Note: When configuring the off-premises ERL, there is no option to set an ELIN. Passing the user's calling party to the National Provider will uniquely identify the caller and their specific location.
5. Click Insert.

Configuring IP Subnet for Off-Premises Users in Emergency Responder

Use the Configure IP Subnet page to define an IP Subnet for devices that are off premises. The IP subnet should be the IP address of the Expressway-C inside address or the IP Subnet of a VPN concentrator for a client VPN session or Hardware VPN solutions.

When defining client or hardware VPN IPSubnets, these subnets should have /26 or /24 masks to coverthe ranges of IP addresses that might be used by the clients. When defining an Expressway-C as the interface, define them as /32 addresses with an IPSubnet defined for each Expressway-C gateway.

© 2022 Cisco and/or its affiliates. All rights reserved.

1. From CER Administration, **select ERL Membership > IP subnets** and click **Add new IP subnet**.
2. Enter the Subnet ID and Mask details.
3. Click Search ERL to select the ERL you want to assign to the subnet.
4. In the ERL Search Parameters, set the find value to Off-Premises ERL and click Find.
5. Click the radio button next to the Off-Premises ERL (defined previously) and click Select ERL.
6. Click Insert to add the subnet on the Configure IP Subnet page.
7. Repeat for each Expressway-C or VPN IP range.

Instructing Users to Set and Configure Remote Teleworker Emergency Calling forOff-Premises Locations

Users need instruction on how to set their address when prompted by the application. The training procedure depends on which application is deployed to users.

Since the location setting and validation occur directly with the National Provider, there is no additional configuration required in the CER for supporting off-premises users.

Configuring RedSky Horizon Mobility for Off-Premises Users

When a hybrid worker is outside the enterprise, the worker must be able to set their location for emergency dispatch. To do that, the user must install the MyE911 application. The MyE911 application from RedSky is a standalone application that monitors network connections, communicates with the RedSky Horizon Mobility services, and allows users to set their locationwith the MyE911 web service. The MyE911 application runs independently of Dedicated Instance. Since the MyE911 program runs independently, this program supports both Webex App and Jabber deployments.

All users that will be using the MyE911 client must be imported into RedSky's administrative portal. You can do this using bulk upload. Once users have been added to the administrative portal, clients will download the application. The first launch of the MyE911 client prompts usersfor their email. The RedSky service sends a one-time password to the client and after that, the client can set the location through the RedSky web portal.

See the RedSky MyE911 documentation for additional details.

Configuring Cisco Emergency Responder for National Provider Integration for On-Premises Clients

The ability for a hybrid user to work both on-premises and off-premises provides convenience forthese workers but poses a challenge for an administrator to support these users. This ability requires planning by the system administrator to ensure that the client can be accurately tracked in both scenarios. When a worker is off premises, the accuracy of the address of the worker is upto the user. But when that same worker is on premises, the accuracy and identification of the workers location is the responsibility of the employer. When a worker is on premises, CER tracksthem through switch port, access point or IP subnet. Even though the worker is tracked through the CER, this does not disable the MyE911 client from requesting that a user set the location.

Since an end user should never set the location when on-premises, the MyE911 application needs to associate to a campus-wide IPSubnet so that MyE911 will not request a location but allow the CER to set the location.

© 2022 Cisco and/or its affiliates. All rights reserved.

Procedure

	Command or Action	Purpose
Step 1	Create a RedSky location for the campus.	Configures a single location in RedSky for on-premises clients to associate with to suppress the MyE911 client location prompting.
Step 2	Create an IP address range for on-premises clients.	Configures an IPSubnet at the NationalProvider for voice and data VLANs.
Step 3	Define trusted IP address ranges.	Defines an IP address range for the external IP addresses used by the customer to reach the Internet.
Step 4	Verify that the client has correctly associated to the IPSubnet when on premises.	Confirms that a client that is on-premisesis associated with the correct IPSubnet.

Creating a RedSky Location for the Campus

When hybrid users visit a company-owned location, their MyE911 client should not prompt the user for their location. Creating a campus-wide overlay location is needed to accomplish this task. Since this location is not used for the actual location of the caller, the address and phone number can be the company's main location information.

Procedure

1. Log into your RedSky administrator portal.
2. Navigate to **Configuration > Locations**.
3. Click **Add a Building**.
4. Set the Name field to a generic value and provide an address of a building managed by the company.

   For example, defining the campus for Cisco would have the following values:

   Name: Cisco Campus

   Address: 300 East Tasman Drive, San Jose, CA 95134
5. Click **Save**.
6. Expand the Building Name that was just created, and then click **Add Location**.
7. Add a location that indicates the location match is a campus-wide setting. For example:

   Name: San Jose Cisco Campus

   Location Information: Campus OverlayPhone

   Number: 408-525-1000
8. Click **Save**.

© 2022 Cisco and/or its affiliates. All rights reserved.

Creating an IP Address Range for On-Premises Clients

Before you begin

Before you can configure the IP address range, an administrator must obtain the different on- premises IP subnets that a client will use to connect to calling services. A typical deployment will need to define at least one voice VLAN and one data VLAN. A Jabber client on a PC will normally connect to the calling service over the data VLAN, that is why both the voice and data VLAN IP addresses need to be defined. The IP addresses used in this step will be large when including a campus-type environment. A /20 or even a /16 address range is not uncommon for a campus environment. Although a large IP address range cannot provide location specificity, the purpose of the IP address range is to provide the My911 client to associate with a location so the client will not prompt the user to enter the location. When nomadic users are on-premises, location tracking and setting is performed by CER.

Procedure

1. Log into your RedSky administrator portal.
2. Navigate to **Configuration > Network Discovery**.
3. Select **IP Ranges** from the Network Discovery banner.
4. Click **Add IP Range Mapping**.
5. Add a Starting address and an Ending address for the Data VLAN. Select the overlay “Building” that was created in the previous section. Click **Save** to save the configuration.

   Note: The start and end address range does not need to follow traditional IP subnetting rules. RedSky does not enforce /xx routing rules on IP range mappings.
6. Complete Steps 1 to 5 for the Voice VLAN.
7. If the deployment supports IPv6, then there must be additional entries for the IPv6 voice and data VLANs.

Defining Trusted IP Address Ranges

For a device to successfully associate with the internal (Private) IP address just defined in the previous step, an administrator must provide RedSky with their Public IP address. In a typical enterprise deployment, the IP addresses assigned to IP phones and PC/MAC devices are not public addresses. Because these addresses are typically private, many customers could deploy the same range and cause overlap within the RedSky solution. The RedSky service avoids this conflict by using a company’s public address and private address to uniquely identify valid location requests/updates from the MyE911 client.

Most deployments will have both an IPv4 and an IPv6 public address. Both addresses must be addedas trusted IP addresses in RedSky to allow MyE911 clients to match the campus overlay IP subnet.

The RedSky service requires that each trusted IP address be owned by a single company. If the trusted IP address range overlaps with any other defined trusted IP address in the database, the entry will be denied. This even applies to a single company with multiple organizations under a common company account.

© 2022 Cisco and/or its affiliates. All rights reserved.

Procedure

1. Log into your RedSky administrator portal.
2. Navigate to **Configuration > Network Discovery**.
3. Select **IP Ranges** from the Network Discovery banner.
4. Click on the slider to the **Trusted IP Range** value
5. Click **Add IP Range Mapping**.
6. Add a Starting address and an Ending address for the public IP address for the company. Click **Save**.

   Note: The start and end address range does not need to follow traditional IP subnetting rules. RedSky does not enforce /xx routing rules on IP range mappings.

7. Complete Steps 1 to 5 for any IPv6 address range.

Verifying the MyE911 Client Associated to IP Subnet when On Campus

After creating the building, location, private IP address range, and trusted IP address range, the MyE911 client should be tested to verify the association to the campus overlay location.

As a hybrid user comes onto the campus environment, the MyE911 app in the task bar should appear, indicating that the client has been discovered and associated to the overlay location. If the association with the overlay has occurred, then the MyE911 application does not prompt the user to set a locationas the user roams around the campus.

Procedure

1. Log into your RedSky administrator portal.
2. Navigate to **Configuration > Users**.
3. Using the search box, find the user that is being tested.

   The Current Location column should contain the Overlay location.

   Once the overlay location is confirmed, the Webex App client is tracked in CER using the access point or IPSubnet of the user's location.

Document history

Described in	Version	Date
Initial version	1.0	December 2021
Updated Template	1.1	January 2022

© 2022 Cisco and/or its affiliates. All rights reserved.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at https://www.cisco.com/c/en/us/about/contact-cisco.html.

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

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