



The bridge to possible

Partner Onboarding
Cisco Confidential

Webex App

Configuring United Communications Manager for Nomadic E911 Support

Version 1.1

Contents

Overview of Nomadic E911 for Webex App	3
Prerequisites for Deployment	3
Configuring Unified CM for Emergency Call Routing to RedSky	3
Configuring Service Profile in Unified CM for RedSky Integration	4
Testing Nomadic E911 Service and Address Verification.....	4
Determining On-Premises and Off-Premises Devices	6
Configuring RedSky Horizon Mobility for On-Premises Devices.....	6
Identifying Dispatch Locations.....	7
Defining the Dispatchable Address and Location	7
Adding Infrastructure and Associates to a Location.....	8
Verifying Device to Infrastructure Mappings.....	10

Overview of Nomadic E911 for Webex App

Cisco's Nomadic E911 services are required for almost all enterprises that operate in the US. This requirement comes in response to a general move towards hybrid work and to RAY BAUM'S Act, which states that off-premises users must be able to set their location for emergency services.

The ability for users to define their own location for emergency services dispatch must be simple and easy to use. Nomadic E911 service is available in Webex App when using Dedicated Instance. Nomadic E911 enables administrators to address the requirements of RAY BAUM'S Act by letting users update their location natively in Webex App.

The Webex App user experience is designed to minimize end user location prompting by remembering personal locations and automatically reassociating to the location upon return. This association to a location can be via a wireless network, a wired network, or over a VPN. Only when a user roams to a new location is the user prompted to set a location. The Nomadic E911 solution provides end users the ability to verify their location at any time by using the 933-route pattern.

Prerequisites for Deployment

Prior to deploying Nomadic E911 for in Dedicated Instance, the customer or partner must enroll in a RedSky account. To configure the required services in the Webex App, the administration must have the following information:

- RedSky account number
- RedSky secret key
- RedSky HELD+ URL
- Emergency numbers that route to RedSky

Configuring Unified CM for Emergency Call Routing to RedSky

When deploying Dedicated Instance, Cisco recommends you use Webex App for messaging, meetings, and telephony services. The Webex App is enhanced to use HELD+ to locate a user and set the user's emergency dispatch address. Although the Webex App client sets the location, Dedicated Instance is responsible for routing the emergency call to RedSky, an Everbridge company, for dispatch to a Public Safety Answering Point (PSAP). When a Webex App client places an emergency call, Dedicated Instance routes the call directly to RedSky using a SIP route string. This procedure sets the call routing components to route emergency calls from the Webex App to the RedSkyHorizon™ Mobility services.

Note: Dedicated Instance uses a predefined the SIP Trunk, route group, and route list to reach the RedSky cloud services.

Procedure

1. In UC Manager Admin, navigate to Call Routing > SIP Route Pattern.
2. Add a new route string based on the RedSky HELD URI. The standard RedSky URL is <https://api.wxc.e911cloud.com/>, which makes the SIP Route String `*wxc.e911cloud.com`.

In the IPv4 field, add the *wxc.e911cloud.com and select the xUS-<DC>-e911-RedSky-Trk as the SIP Trunk that has been preconfigured to reach the RedSky services. Select a partition for the route string that is reachable by the Webex App clients.

3. Click Save.
4. In UC Manager Admin, navigate to 'Device->Trunk', click **Find**, and then select the xUS-<DC>-e911-RedSky-Trk.
5. Scroll down to the normalization script. This section should be pre-populated with a script name, parameter, and a placeholder parameter value. Replace the placeholder value with the RedSky E911HeldOrgId.

Note: All calls from Dedicated Instance must have the HELD organization ID included in the SIP headers. The LUA Script on the SIP trunk inserts the header to ensure proper treatment by RedSky.

6. Click Save.

Configuring Service Profile in Unified CM for RedSky Integration

The Webex App clients must get its configuration from the UC Manager to enable the HELD+ location updates. A UC Manager administrator must configure the required parameters in a service profile and assign the service profile to the Webex App clients.

Procedure

1. In UC Manager Admin, navigate to User Management > User Settings > Service Profile.
2. Select the service profile that the Webex App uses for configuration. In many cases, there are multiple service profiles that you must update.
3. Navigate to the **Emergency Calling** section.
4. Select the **Enable National Emergency Calling** check box, and then populate the following settings: (You can find most of the values in the RedSky Horizon Mobility portal.)

Parameter	Description
Organization ID	32-character alphanumeric string provided by RedSky.
Secret	16-character alphanumeric string provided by RedSky.
Location URL	https://api.wxc.e911cloud.com/ (default)
Emergency Numbers	911, 933 (default)

5. Click Save.
6. Configure the RedSky settings on any other service profiles that require location updates to RedSky.

Testing Nomadic E911 Service and Address Verification

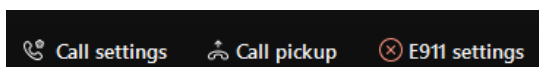
After you add the UC service profile parameters and restart the Webex App, the app displays an icon indicating the current association of the client to a defined address. The E911 status is either a check or an "X". If the Webex App cannot determine the user's location, then the client prompts the user to define an address.

Cisco does not recommend calling 911 to verify the calling party's address. Instead, all address verification calls should use the 933 pattern. 933 calls route to RedSky the same way as 911 calls, but instead of reaching a PSAP dispatch center, the call is directed to an IVR that reads back the calling party number and the address of record for the number.

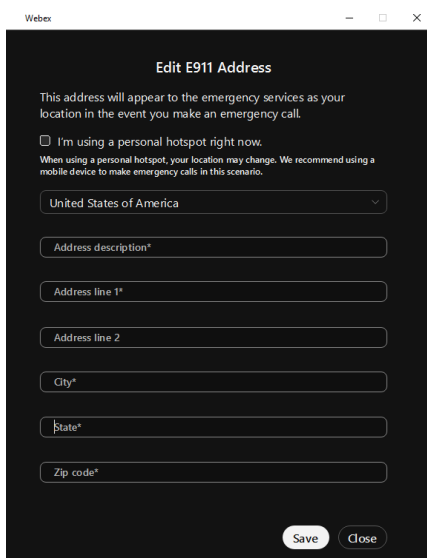
Warning: When performing this testing on premises, Cisco recommends defining the location address and the infrastructure devices (switches, access points or IP subnet) prior to launching the Webex App. The on-premises infrastructure devices and their location must be defined in RedSky. See the section "Configuring RedSky Horizon Mobility for on-premises Devices" for information about configuration locations and associating infrastructure to the locations in the RedSky Horizon Mobility administration portal.

Procedure

1. When the client starts, the "E911 Settings" icon is an "X".



If you are in a location not previously defined or on the corporate network that has not been administratively defined, then the Webex App will pop up windows asking the current address to be defined.

A screenshot of the 'Edit E911 Address' dialog box. The title is 'Edit E911 Address'. Below the title is a note: 'This address will appear to the emergency services as your location in the event you make an emergency call.' There is a checkbox labeled 'I'm using a personal hotspot right now.' with a warning below it: 'When using a personal hotspot, your location may change. We recommend using a mobile device to make emergency calls in this scenario.' Below this is a dropdown menu showing 'United States of America'. Then there are several text input fields: 'Address description*', 'Address line 1*', 'Address line 2', 'City*', 'State*', and 'Zip code*'. At the bottom right are 'Save' and 'Close' buttons.

2. Define the current address of your location. You must include the address description, the street address line 1, city, state, and zip code.
3. Click **Save**. If the address is valid, a message appears in the lower left corner indicating that the save operation is successfully. If the address is invalid, verify the address and try saving again.
4. If the address was successfully saved in Step 3, access the Webex phone services tab and dial "933".
After dialing 933, the verification service answers the call.
5. Verify that the number and address are the same as the ones set by the client in Step 2.

Determining On-Premises and Off-Premises Devices

This section provides information about handling on-premises and off-premises devices. Cisco recommends that a Dedicated Instance administrator define all dispatchable addresses for on-premises locations. So, at a minimum, an administrator must define the IPSubnets of both the wireless voice IP subnet and the data IP subnet. The global definition of wireless voice and data IPSubnets ensures that the administrator is the authoritative source of addresses for emergency services when employees are on-premises. Although global subnets are not going to provide the accuracy that most customers need, setting global IP subnets ensures that when a user and their client are on premises, the administrator controls the address. You can find more information about configuring infrastructure and dispatchable locations in the “Configuring On-Premises Locations” section.

Any device that is not on the enterprise network, as described above, is considered off-premises. In any off-premises location, the client is prompted to enter their emergency dispatch location. The request for location typically occurs after the user stops moving and is stationary for approximately five minutes. The Webex App populates the address with the last defined address, but if the address is no longer current, the user should update the address to the current location. If the user does not set the current location, then any calls to 911 are routed to the Emergency Call Relay Center (ECRC) where a live agent asks the caller for their current location.

Configuring RedSky Horizon Mobility for On-Premises Devices

The process of designing and implementing a wire map for accurate location identification of users for emergency calling purposes requires extensive planning to identify, classify and ultimately deploy an emergency calling solution. Trying to provide design guidance for a well-designed wire map in this document is not possible due to the number of considerations that must be considered. With that understanding, this document provides guidance to help an administrator provide basic on-premises awareness for nomadic users by configuring IP subnets on a per building basis.

When the Webex App is configured to use the native location awareness feature, then all location setting/association is done within the Webex App. This includes situations where nomadic users are on-premises. In this scenario, Cisco Emergency Responder (CER) does not perform any location tracking services nor does it handle the emergency call when placed from the HELD/HELD+ enabled client.

Procedure

	Command or Action	Purpose
Step 1	Identify dispatch locations.	Identifies areas of a building that you will name as dispatchable locations.
Step 2	Define dispatch addresses and locations.	Defines the buildings and locations inside the building that are used for dispatch.
Step 3	Add infrastructure and associate to a location.	Inserts “network infrastructure to’ and “associate to” locations. Infrastructure is IP subnets.

	Command or Action	Purpose
Step 4	Verify device-to-infrastructure mappings.	Verifies that a device maps to the desired location when stationary and after moving.

Identifying Dispatch Locations

Although the term “dispatch location” can represent a building, a floor of a building, a quadrant, or a cubicle the dispatch location that is used for this configuration is the entire building. More detailed dispatchable locations can be defined using the same method that we describe here, but for ease of understanding, a “multiple buildings” scenario is used in this configuration example.

There are two parts of a dispatchable location that you must consider when identifying a dispatchable location. The first is the address of the building and the other is a location inside the building. The address of a building is the actual street address assigned to the building during the construction process. Each building should have a unique address assigned to it. Within each building, there must be at least one “location”. A location inside a building provides the additional details that is used to further identify an area of a building. A location inside a building can be the floor, a specific room, or the building.

In this configuration there is one location inside each building that represents the entire building.

Defining the Dispatchable Address and Location

After identifying the buildings that you want to use for emergency services dispatch, you must define the buildings so that the emergency services unit knows the address and any additional details about the location of the caller inside the building. In this example, the additional details are the entire building as the location inside the building.

Procedure

1. In RedSky Horizon Mobility, navigate to **Configuration > Locations**.
2. Select **Add Building**.
3. Give a name to represent the location and the street address. The name of a building should always provide enough detail to identify which building you’re identifying.

	Building Name	Address
▼	SJC20	725 Alder Dr, Milpitas, CA 95035

For this example, we’re using the building name “SJC20” to represent building 20 on Cisco’s San Jose campus, with a street address of 725 Alder Drive. Click **Save**.

4. After saving the building, you must add at least one location to the building. A location within a building can be of arbitrary size. Using a “location” inside a building allows you to define an entire floor or an office as the location. After expanding the building name, click Add Location. Since this example uses the entire building as the dispatch location, the location description is as follows:

Edit Location

CLOSE

*Name

SJC20

Phone Number

Location Information

Building 20

Note: The phone number in a location definition is not the call back number nor is it the Emergency Location Identification Number (ELIN). This number is used to associate a specific calling party to the location. If the location represents a large area (like a floor), then leave the phone number blank.

- Click **Save**.
- Repeat steps 1 – 5 for each building that should be defined. When you finish, you should have a list of buildings that looks like this:

	Building Name	Address
▶	SJC20	725 Alder Dr, Milpitas, CA 95035
▶	SJC21	771 Alder Dr, Milpitas, CA 95035
▶	SJC22	821 Alder Dr, Milpitas, CA 95035

	Building Name	Address	
▼	SJC20	725 Alder Dr, Milpitas, CA 95035	
Locations			
	Location Name	Info	Phone Number
	Building 20	Building 20	(408) 555-1000

When you complete this step, you have created a dispatchable location.

A phone number associated with the location is not required, but you define a phone number, then that number must be unique and will be matched to the location if the calling party matches the phone number of the location.

Adding Infrastructure and Associates to a Location

After adding buildings and locations, an administrator must define the infrastructure that is used to identify a user's physical location. The term "Infrastructure" can represent a switch or switch port, an access point, or an IP subnet. Since wired connections can be directly terminated and mapped to a physical location, a wired connection can be very specific to the location of the emergency call.

Similarly, an access point (AP) includes a physical range to the signal, which cannot provide a location as specific to a desk or an office, but it can provide a radius of certainty for the location of the emergency call. Finally, an IP subnet is a very broad resolution for an emergency caller's location but can be used to identify the building that issued the IP address via DHCP.

There are many factors you should consider when determining the infrastructure device to use for location tracking. In this configuration example, we will use an IP subnet to identify the building that an emergency call was placed from. Since most customers use non-public IP addresses for their IP telephony deployments, the private IP address must be paired with a public IP address to ensure proper account association as well as addresses that the administrator identifies as on-premises addresses. For a typical deployment, you should use two private IP ranges. One for the voice VLAN and one for the data VLAN.

Procedure

1. In the RedSky administration portal, navigate to **Configuration > Network Discovery**. The network discovery options are MAC, LLDP, BSSID, and IP Ranges.
2. Select the **IP Ranges** tab.
3. To correctly identify network IP addresses that a company uses, an administrator must define a private IP range and a trusted IP range. Click **Add IP Range Mapping**. Add a Range Start address and a Range End address. The start and end addresses should match the address range of the DHCP scope of the building. Although the start and end values do not need to follow conventional IPv4 or IPv6 subnet definitions, it is advisable to match the DHCP scope. Next, select the building and location that you want to source the IP subnet from.

Continuing the example above, the DHCP scope for the data VLAN in building 20 is 10.160.1.0 to 10.160.1.255. The IP range mapping should look like this:

Range Start	Range End	Location	Description
10.160.1.0	10.160.1.255	Building 20 725 Alder Dr, Milpitas, CA 95035	

4. Create additional ranges for voice VLAN and IPv6 ranges.
5. Define the company's public IP addresses so that RedSky can verify the private source addresses of a company's devices. Slide the toggle to **Trusted IP Range**. The administrator should communicate with their IT staff that manages the firewall/NAT connections to their Internet provider. If that information is not readily available, you can use a source IP reflector service (like <https://www.whatismyip.com/>). Add both the IPv4 addresses and IPv6 addresses to the trusted range. Click **Save**.

After completing this configuration, any Webex App that comes on premises should be successfully associated to the correct building based on the building's DHCP scope.

Verifying Device to Infrastructure Mappings

After completing the previous procedure, any Webex App that has been enabled for HELD+ operation in UCM should now report on-premises information to RedSky. The next step is to verify that the Webex client is correctly associated to the right location in RedSky.

The best way to verify the location of the Webex client is to use RedSky's 933 service. The RedSky Horizon Mobility service allows callers to call 933 to verify their address. A 933 call will be answered by the RedSky Address Verification IVR. The IVR will read back the calling party number, as well as the current dispatchable street address of the caller. The 933 service is available to both on-premises and off-premises callers.

From the Webex App client, place a call to 933. After verifying the calling party number and the location address, hang up the call.

If the address is not correctly repeated, you can find additional information about the location request in RedSky's administration portal on the **Monitoring > Held Devices** page. After finding the device that is incorrectly reporting its location, click on the vertical ellipses and select **View HELD+ Request** to get additional information on matching criteria to the location. Adjust the IP address ranges, as needed, to ensure a proper location map.

Document history

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

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.