MiVoice Connect

RAY BAUM'S General Overview and Solution Deployment Guide

Release 19.2 SP2

November, 2021

Mitel®

NOTICE

The information contained in this document is believed to be accurate in all respects but is not warranted by Mitel Networks™ Corporation (MITEL®). Mitel makes no warranty of any kind with regards to this material, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. The information is subject to change without notice and should not be construed in any way as a commitment by Mitel or any of its affiliates or subsidiaries. Mitel and its affiliates and subsidiaries assume no responsibility for any errors or omissions in this document. Revisions of this document or new editions of it may be issued to incorporate such changes.

TRADEMARKS

Contents

Kari's Law and RAY BAUM'S Act

In August 2019, the United States Federal Communications Commission (FCC) adopted rules for implementing two federal laws that strengthen emergency calling; Kari's Law and Section 506 of RAY BAUM'S Act.

Kari's law requires that users must be able to dial 911 emergency calls directly without having to dial any prefix or access code, such as the number 9.

RAY BAUM'S Act requires that Multi-Line Telephone Systems (MLTS) must ensure that a "dispatchable location" is conveyed with 911 emergency calls to dispatch centers, regardless of the technological platform used. There are multiple compliance date requirements. In general, the federal rules are forward-looking and apply only with respect to MLTS that are installed after February 16, 2020.

Details about these laws are available at the following link:

https://www.fcc.gov/mlts-911-requirements

FAQ about RAY BAUM can be found at the following link. https://www.fcc.gov/files/mltsfaqspdf.

Introduction of MIVC Support for section 506 of RAY BAUM'S Act and Kari´s Law

MiVoice Connect has always been able to implement direct 911 emergency dialing. Similarly, sending a dispatchable location by Site is standard for on-premises and fixed devices (although some companies might need to evaluate whether additional granularity is required, such as, the floor level, room number, and so on.). This location information is sent as a Caller Emergency Service ID (CESID) through the telephone carrier, which delivers location information to the Public Safety Answering Point (PSAP) based on the calling number.

Section 506 of RAY BAUM'S Act (hereafter referred to as "RAY BAUM" for simplification) has additional requirements to deliver a dispatchable location for on-premises non-fixed devices and off-premises devices. According to the FCC, this location information should be automated if technically feasible, a location based on end-user manual update, or the best available location that can be obtained from any available technology or combination of technologies at reasonable cost.

For non-fixed and off-premises devices, MiVoice Connect systems, beginning with Release 19.2 SP2 can deliver a dispatchable location by integrating with third-party companies known as Next Generation 911 emergency service providers (NG911). Depending on the customer requirements, the CESID can be mapped to the phone's location using the IP address range, MAC address, or updated directly by the user into an application. The NG911 service providers also offer other features such as email and SMS notification to other individuals when an 911 emergency call is made.

MIVC - RAY BAUM High Level Architecture

Before making any changes, customers should spend some time planning how they will implement their solution to meet RAY BAUM'S Act. The option selected depend on the type of deployment in place, such as:

- Size of the physical location site.
- Deployment is purely on-premises.
- Deployment includes off-premises endpoints.

Depending on the solution, the customer might:

- Need not upgrade, but rather use existing CESID mappings to allow for automatic move detection of IP phones.
- Need to upgrade to get the new CESID mappings.
- Need to upgrade to get the new CESID mappings and will be required to integrate with a third-party vendor.

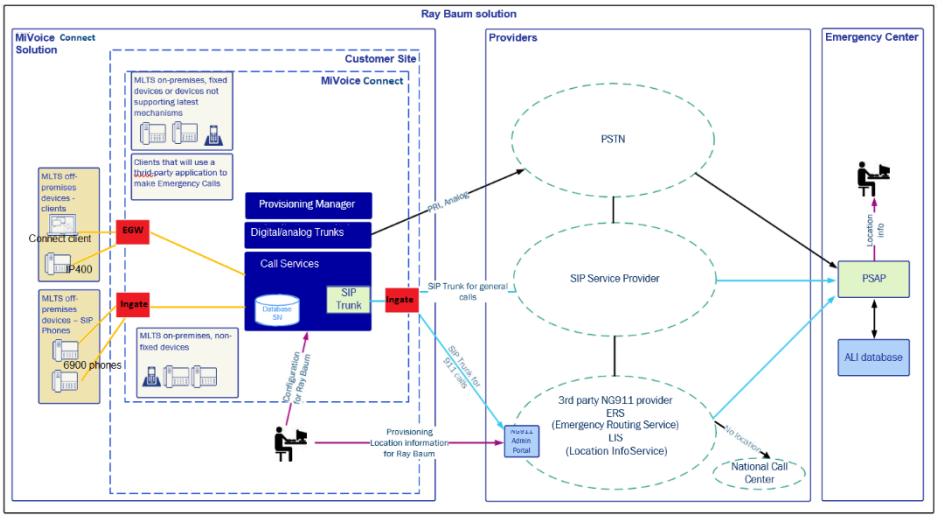
To help illustrate the options, a customer with a large physical deployment that will require more than one dispatchable location. For example, a single floor of a large building might require four dispatchable locations, one to cover each corner:

1. Customer has only on-premises IP4xx and/or 69xx and/or DECT devices. In this situation, the customer can order the required number of CESIDs (four in above example) from their service provider and use the existing IP range and/or L2 CESID mapping features available on MiVoice Connect system without the need for any upgrade. Enabling these features provides a dynamic location update if the device is moved by the user within the premises.
2. If the customer adds MiVC Connect Client softphones on laptops or mobile phones or any kind of remote Teleworkers to their solution, the customer must upgrade and integrate with a Mitel-verified third-party vendor.

The solution required for third-party NG911 vendor integration will be discussed further in this document; expect for the *RAY BAUM Different Deployment Method Visualization* section, which describes using the RAY BAUM feature without integrating NG911 vendors.

The following figure illustrates a high-level veiw of the MiVoice Connect RAY BAUM architecture:

Figure 1 : MiVC system onsite - RAY BAUM high-level architecture



The MiVoice Connect RAY BAUM solution is composed of the following components described in the sections below.

- NG911 Service Provider

- Edge Gateway
- Ingate SIParator
- MiVoice Connect

NG911 Service Provider

The third-party Next Generation of 911 (NG911) emergency call service provider enables entities. MiVoice Connect supports integrating with two service providers in USA; RedSky and Intrado. Based on the availability, ease of use, feature set, and cost, the customer can select from these options and execute a commercial agreement with the NG911 service provider.

Edge Gateway

Edge Gateway is used for enabling Teleworker support for IP 400-Series phones and Connect Client.

Ingate SIParator

- Acts as Session Border Controller (SBC) and enables SIP trunking to/from the NG911 service provider.
- Enables Teleworker support for 6900-Series phones. (In pipeline for 2021 release).

MiVoice Connect

The following are the major network elements of MiVoice Connect:

- Provisioning interface
- Call servers
- SIP Peer for Ingate
- Trunking nodes for PSTN or SIP trunks

MiVoice Connect enables the following features for RAY BAUM conformance:

- Location information by wire-map or by HTTP Enabled location discovery (HELD).
- DID and calling party number (CPN) substitution per device (or location) that can make 911 emergency calls.
- SIP peer profile dedicated to signaling with NG911 vendors, which helps in vendor integrations.
- SIP device capabilities for devices that provide location information.
- Emergency number dialing and routing calls based on trunks configured.

The SIParator is commonly used as the Session Border Controller (SBC) between MiVoice Connect and the third-party NG911 service provider in the solution.

A SIP trunk is set up between MiVoice Connect and Ingate; and between Ingate and the third-party NG911 service provider.

MiVoice Connect contains emergency location identification information for devices that are used with the RAY BAUM'S Act solution.

In the third-party NG911 service provider system, a portal is used to set up the information required to the solution to work properly. The information required depends on the provider. However, some information is mandatory, irrespective of the service provider; for example civic address, valid DID for callback calls (a 10-digit number), valid DID number, extension number, or alternate identification of a device or a user.

The devices supported with MiVoice Connect are IP 400-Series phones, 6900-Series phones, and Connect Client.

Requirements for MIVC - RAY BAUM Integration

MiVoice Connect Requirements

The following are the minimum MiVoice Connect requirements for RAY BAUM integration:

- A MiVoice Connect system with software version 19.2 SP2.
- A minimum of one SIP trunk routes is required for the RAY BAUM solution.
- Device licenses.

Ingate SIParator/Firewall

The following are the minimum Ingate requirements for RAY BAUM integration:

Note: It is recommended to use Ingate for RAY BAUM deployment. However, customers can still use RAY BAUM without Ingate or third-party vendor (Redsky); however they will not be able to use SRTP without Ingate.

- Minimum one Ingate SIParator/Firewall version 6.3.3.
- SIP trunks connection to NG911 service providers.
  Note: A minimum of two SIP trunk connections is recommended for redundancy.
- Ingate SIParator/Firewall licenses.
- (Optional) Multiple trunk group license from Ingate based on deployment use-case.

Third-Party NG911 Emergency Services Requirements

When there are edge gateway devices and softphones, it is mandatory for the channel partner/customer to have an agreement with one of the Next Generation 911 (NG911) service providers that are validated with the MiVoice Connect solution.

Note: If you do not have edge gateway devices and softphones, then it is not mandatory to have an agreement with the NG911 service providers.

Table 1: MiVoice Connect NG911 requirements

Requirement	Description
Locations	The number of locations required to satisfy RAY BAUM'S law.
Users/Devices	For the MiVoice Connect solution, this will include all users and devices associated with users who can make emergency calls (for example, IP device only, lobby phone, and so on).
HELD Clients	These are the number of users/devices that will provide Geolocation (currently, provided only by connect client).
NG911 Application Clients	The number of users/devices that will require the NG911 application (for example, third-party soft clients such as X Lite).
Notification Clients	The number of notification recipients required for the MiVoice Connect solution to satisfy Kari's Law.

Description of MIVC RAY BAUM Support

Introduction

MiVoice Connect implements functions to support the emergency services according to the RAY BAUM'S Act. The MiVoice Connect system must be configured properly to achieve the functionality required by the law. With the latest 911 design, the CESID might be decoupled from the callback number. The decoupling is not always essential; for example, when the customer continues to use the externally obtained DID number as CESID (DID will act as both CESID and callback number). However, decoupling is required when MIVC is integrated with third-party vendors. Therefore, MiVoice Connect, when integrated with third-party vendors (or when RAY BAUM support flag enabled in MiVoice Connect), will derive CESID and callback number (also referred to as calling party number) in an independent manner from DID or Caller ID.

The specific functions to support emergency service in North America are as follows:

- Identify and configure device capabilities.
- Wire-map creation and maintenance.
- Set up SIP trunks, SIP trunk profiles, and routes for user groups.
- (Optional) Third-party NG911 vendor integration.

How the Integration Works

Non-Fixed Devices

A non-fixed device is a device that the end-user can move from one endpoint to another without assistance.

Collecting Data

The data presented to PSAP basically involves two components; location-related data and the callback number. Location information is identified based on either CESID or Geolocation.

For non-fixed devices, the MiVoice Connect internal logic will check for Geo-location, MAC address, and IP address provided by the device. Additional information can be added in the MiVoice Connect database to complement the information received from the device. The additional information must be added in the system by the system administrator.

During an emergency call, the caller location and the CPN number are determined based on the information presented by the endpoint and any of the additional information configured in MiVoice Connect.

MiVoice Connect uses the following priority order for deriving the location information during an emergency call:

- Geolocation – provided by HELD enabled devices
- IP address to CESID mapping
- L2 to CESID mapping
- Switch CESID
- Site CESID
- Empty/No CESID (must not be used as it is not sufficient to satisfy the RAY BAUM law).

MiVoice Connect uses the following priority order for deriving CPN (callback number) during an emergency call:

The callback number presented for RAY BAUM implementation will be the closest DID for the actual caller. The closest DID is derived using the following priority order:

- User's caller ID.
- User’s DID for premise users only.
- Callback number configured in the IP/MAC address map.
- Front desk/Receptionist DID of building (as default trunk level callback number).

Note: MiVoice Connect provides a mechanism to allow customers to configure callback numbers using all the above-mentioned methods. Each method uses a different input. However, what is configured in each method can have an impact on where the callback can go. MiVoice Connect will suggest how to configure each method, what can be configured as callback, and what numbers can cause issues and in which scenario.

The following are the suggestions for callback number configuration:

1. Users’ caller ID in the User’s page

   The caller ID can be a personal mobile phone number or a personal landline number.

   If a user uses a personal phone number or a personal DID that is not linked to the current PBX, then callback will work fine for the user who is logged in to that phone. However, in case of an emergency, anybody can use any phone available in that situation. Therefore, if someone else uses the extension to dial the 911 emergency call in the absence of others in the premises, then in case of a call disconnect, the callback does not go to the relevant caller, rather it will go to the individual who might be anywhere outside. But this case can be properly addressed if specific office-related DID is configured. Therefore, the administrator must check the current configuration and identify whether any problematic scenarios are possible. If there are any, use the MiVoice Connect option to turn off this method for deriving the callback number in Connect Director by accessing **Administrator** > **Telephones** > **IP Phone Address Map** page and enabling the **Ignore CID/DID for Callback** option.
2. User’s DID in the User’s page

   The DID can only be from the DID list configured for the PBX. Therefore, if this option is used, the callback can reach the actual extension. There are no issues with this configuration but for the drawback that not all users will have DID mapped to them. MiVoice Connect provides an option to turn off this method for deriving the callback number by accessing **Administrator** > **Telephones** > **IP Phone Address Map** page and enabling the **Ignore CID/DID for Callback** option.
3. IP/MAC address mapping

   Existing IP address map does not contain the callback configuration. However, as part of the RAY BAUM implementation, this will be added. This is the suggested preferred method, as it is an easy-to-configure and easy-to-maintain option.

   Note: MiVoice Connect uses MAC address to identify teleworker users to send their CESIDs to the NG911 service provider.
4. Front desk/Receptionist DID of building (as default trunk level callback number).

   For the third-party vendor SIP trunk, an externally dialable number of the front desk/ receptionist can be set. This will act as the default callback if the other options are not available. This option is suitable when the common location is always active and can serve all the users in the site.

Sending Data to the NG911 Service Provider

After MiVoice Connect has collected the information from the device side, it checks which provider is used, and it builds the information to be sent in the SIP trunk, including the appropriate SIP headers required by the provider.

After that, the call is sent to Ingate, which will transparently pass through the supported SIP Headers to the NG911 service provider.

To conclude the process, the NG911 service provider will validate the information received and will take the appropriate action. If the data is accurate, the call is sent directly to the PSAP (emergency center). If the information is not accurate, then the call is redirected to the National Call Center for further triage.

Note: The call to the National Call Center entails an extra cost for the customer.

Fixed Devices

Fixed device is a device that cannot be moved to another place in the enterprise without assistance from a professional installer or network manager, such as analog phones.

Collecting Data

For fixed devices, as no information is provided by the device, the MiVoice Connect internal logic will check for information in the emergency location database. This information must be added in the system by the system administrator.

MiVoice Connect uses the emergency location Information in the following order of priority:

- CESID assigned to switch port
- Switch CESID
- Site CESID
- Empty/No CESID (must not be used as it is not sufficient to satisfy the RAY BAUM law).

Note: The Callback or CPN derivation will have the same procedure as that for non-fixed devices.

Sending Data to the NG911 Service Provider

After MiVoice Connect has collected the information from the device side, it checks which provider is used and it builds the information to be sent in the SIP trunk; including the appropriate SIP headers required by the provider.

After that, the call is sent to Ingate, which will transparently pass through the supported SIP Headers to the NG911 service provider

To conclude the process, the NG911 service provider will validate the information received and will take the appropriate action. If the data is accurate, the call is sent directly to the PSAP (emergency center). If the information is not accurate, then the call is redirected to the National Call Center for further triage.

Note: The call to the National Call Center entails an extra cost for the customer.

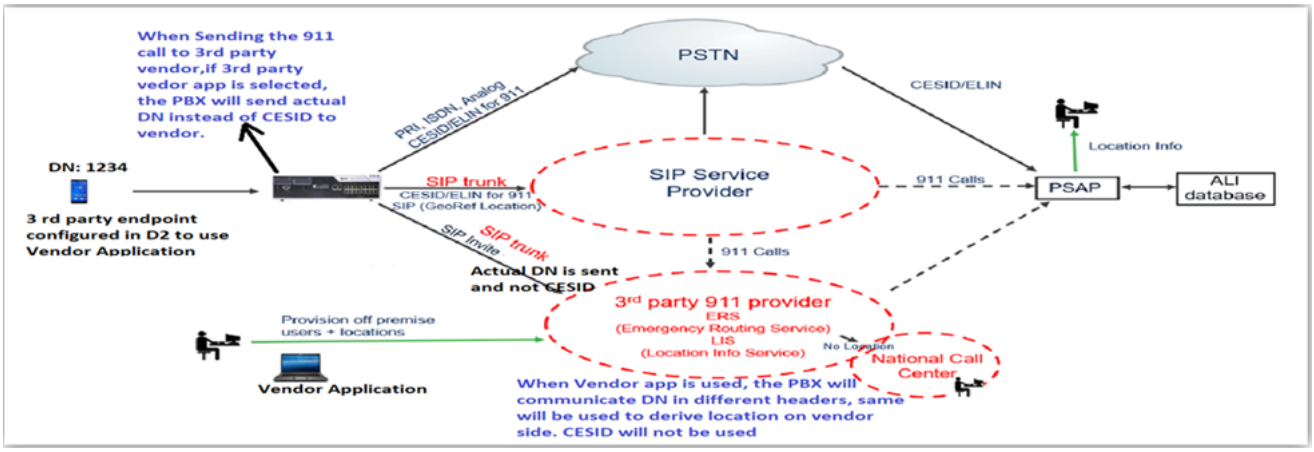
Third-Party Devices

The third-party clients might not provide IP/MAC address information when an emergency call is used. Therefore, it is not possible for MiVoice Connect to provide granular location information. MiVoice Connect can use only switch-level or site-level location information. Therefore, if the third-party application requires more granular and individual location information, they can use the NG911 vendor application. With the vendor application, no location information is maintained or mapped in MiVoice Connect and it is present in the vendor database. Instead of sending the location information, MiVoice Connect will send the extension number as the key to the location information service (LIS) database. Using the extension number, the LIS will send the proper location to PSAP.

Note:

- Using the vendor application, the individual user can directly update the location information dynamically on the vendor LIS.
- For systems using On-Net Dialing (OND) prefixes, while configuring the emergency 911 vendor application, do not add a hyphen in the extension while configuring the device user IDs. For example, if the extension is 53000-50712, enter 5300050712 in the **Device User ID** field.

Figure 2 : MiVoice Connect Deployment



MIVC Location ID Definition

The location ID is a reference/identification used to identify a device or several devices in MiVoice Connect. It is sent as a key to identify location records with the NG911 service provider.

The location ID states the “location identity” of a specific physical place in order to determine a building, a campus, a site, a room, suite, or radio cell reference.

The location ID can be set up depending of the granularity required by the customer’s setup.

In this example, the customer has two buildings. Building one is composed of three stories and building two has only one.

Building one has a location ID for each floor and the third floor contains three rooms, each of them with a location ID.

Building two has location IDs defined by department, each of which has one location ID. The location IDs defined here are nothing but a CESID/emergency location identification number (ELIN).

A location ID supports only digits and the + character.

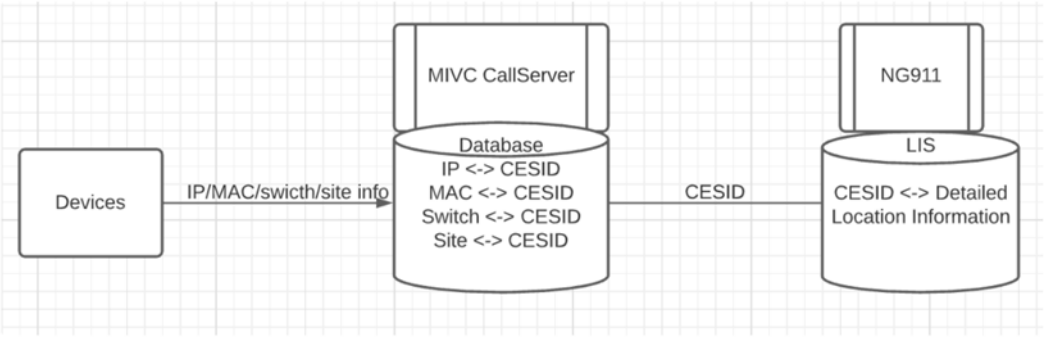
The same CESID identified here will configured as an alternate ID in the NG911 vendor portal and also in the MIVC configuration database.

After a CESID is defined in the MiVoice Connect config database, the CESID can be associated with IP addresses/subnets, MAC addresses, switch, and site. MiVoice Connect provides the following mapping mechanism to associate the CESID (location ID) with a device.

- IP address to CESID mapping - Allows a device in a given IP address range to be associated with a CESID (by associating the IP address range to a zone, and assigning a CESID to the zone). This option requires that the IP address ranges are sufficiently segmented to provide sufficient granularity to satisfy RAY BAUM requirements. This is the preferred method of associating a CESID with a device because, it is based on the physical connection rather than on a logical one.
- L2 (MAC) to CESID mapping - Associates a device based on its MAC address to a given CESID. This is the preferred method for teleworker physical phones because IP addresses keep changing in teleworker mode.
- CESID Assignment - Allows a device to be assigned a CESID directly.
  Note: For analog phones, a specific phone can be assigned a CESID.
- Switch to CESID mapping - Associates the MiVoice Connect Switch serving area to a CESID. As with IP to CESID mapping, this requires careful segregation of devices in the same area that is to be served by the same MiVoice Connect switch.
- Site to CESID mapping - Associates the MiVoice Connect site to a CESID. All the devices in the site will have the same CESID and therefore, the same dispatchable location. While using this option, it is important to understand that one dispatchable location might be enough to conform to RAY BAUM.

The flow of location information from the MiVoice Connect device to NG911 vendor can be illustrated as follows:

Figure 3 : Location information flow



Devices that support HTTP Enabled location discovery (HELD) will send their location ID directly to the NG911 service provider, sent through MiVoice Connect. However, the location ID is not required to be programmed on MiVoice Connect. This is required for soft phones only.

Devices must be programmed to support the NG911 service provider sending the CESID/ELIN directly. However, the location ID need not be programmed on MiVoice Connect.

Note: Currently, there are no such devices in MiVoice Connect.

Devices that support the NG911 service provider's application will update the location based on the NG911 service provider application itself, and will not need any location ID programmed on MiVoice Connect. Any third-party clients used by the customer will fall into this category. The administrator is required to configure only if the extension is used on the third-party client or on MiVoice Connect native devices.

Note: The MiVoice Connect system administrator has the responsibility to provide accurate information about the correct location for a device.

The DECT device location is identified by the base station IP address. Therefore, note that all DECT handsets of that base station will have the same dispatchable location and must be deployed with this information in mind.

MiVoice Connect Emergency Configuration

As explained in the preceding section, MiVoice Connect is configured to:

- Derive CESID or location ID
- Derive the callback number
- Provide utility operation support for system administration.

As part of above mentioned configuration, MiVoice Connect will implement the following provisioning support.

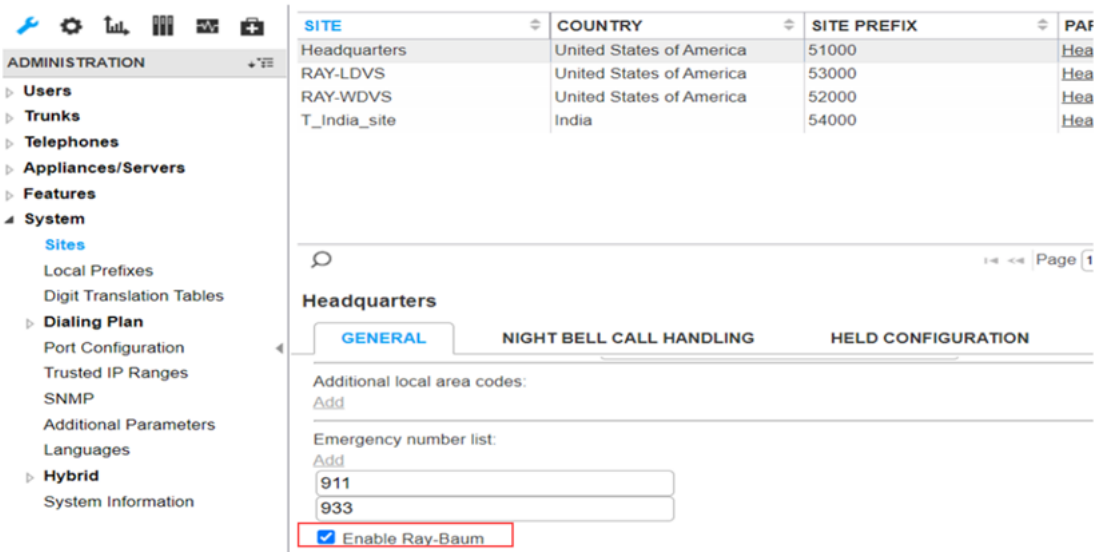
- Enable or disable RAY BAUM feature for a site.
- For teleworker phones, MiVoice Connect will ensure that the **IP Phone Address Map** page will have MAC-address-based entries.
- Allow the administrator to configure the type of SIP third-party (Intrado or RedSky) server and related parameters.
- Extend the assignment of the analog phones to have CESID assignment also.
- Provide an option for a callback number to be configured in the **IP Phone Address Map** page.
- Provide an option to ignore the caller ID/DID for a user in the **IP Phone Address Map** page.
- Allow the user to use vendor application for location information.
- Allow the user to configure phone flags related to location change and HTTP enabled location discovery (HELD) usage.
- Alter the validation of the CESID.
- Allow the user to configure SIP profile parameters for vendor trunks.
- Ignore the caller ID/DID as CESID for US site.
- Utility interface to import and export **IP Phone Address Map** page data.

Enable or Disable RAY BAUM Feature for a Site

To enable/disable RAY BAUM feature for a site:

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **System** > **Sites**. The **Sites** page opens.
3. Select the site to enable the **Enable RAY BAUM** option.
4. To enable/disable RAY BAUM, in the **General** tab, select/clear the **Enable RAY BAUM** option.
   Note: After you clear the **Enable RAY BAUM** option, a reboot of the servers and switches will be required for the change to take effect.
5. Click **Save**.

Figure 4 : Enable/Disable RAY BAUM

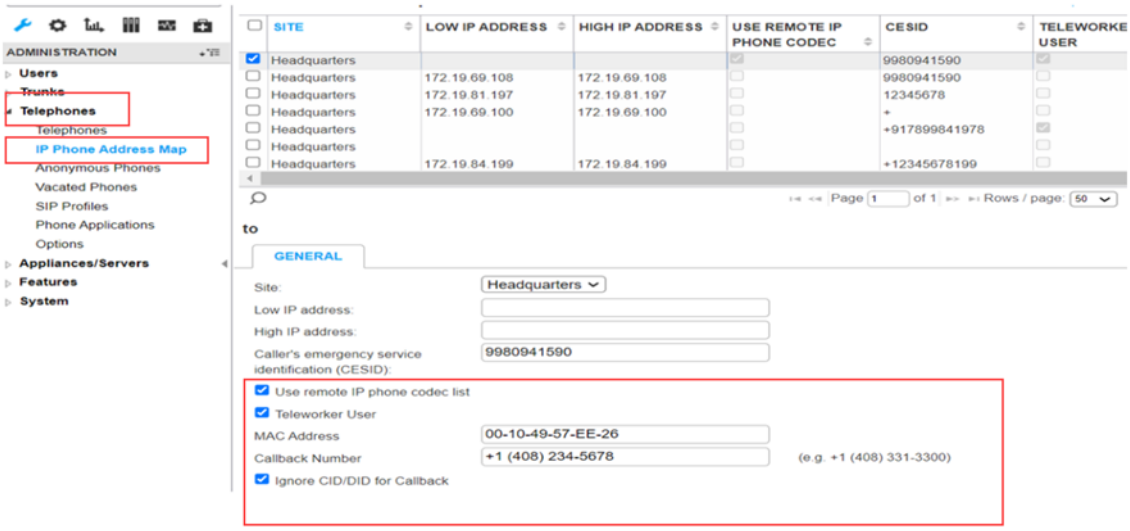


MAC-Based Entries in the IP Phone Address Map Page

To add MAC-based entries in the **IP Phone Address Map** page:

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Telephones** > **IP Phone Address Map**. The **IP Phone Address Map** page opens.
3. To add a new MAC address for mapping for IP phones, click **New**.
4. In the **General** tab, enter the MAC address in the **MAC Address** field and add other relevant information.
5. Click **Save**.

Figure 5 : IP Phone Address Map Page

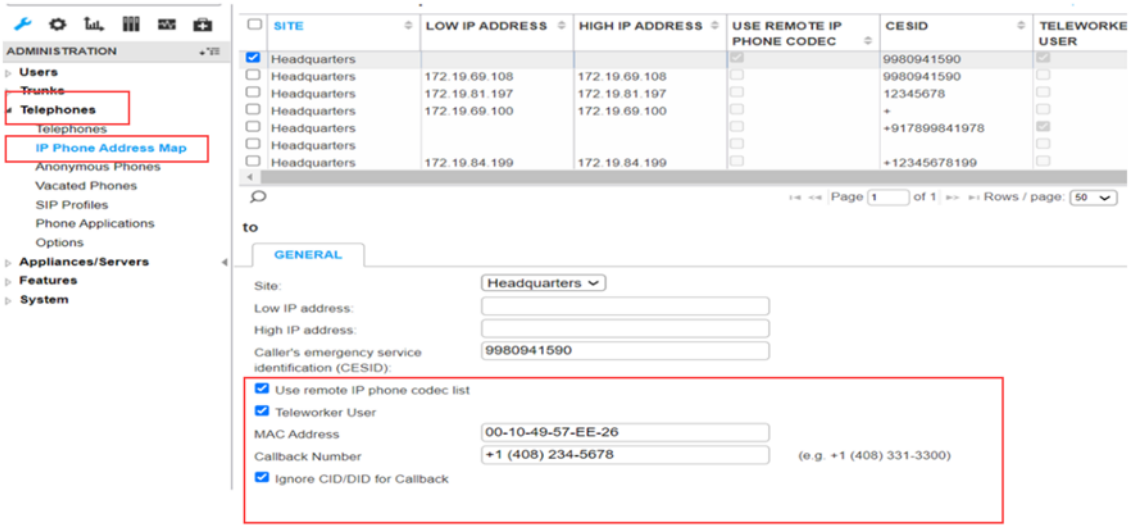


Configuring the Callback Number

To configure the callback number in the **IP Phone Address Map** page:

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Telephones** > **IP Phone Address Map**. The **IP Phone Address Map** page opens.
3. To add the callback number, select entry to update, then enter the callback number in the **Callback Number** field.
4. Click **Save**.

Figure 6 : Configuring the callback number

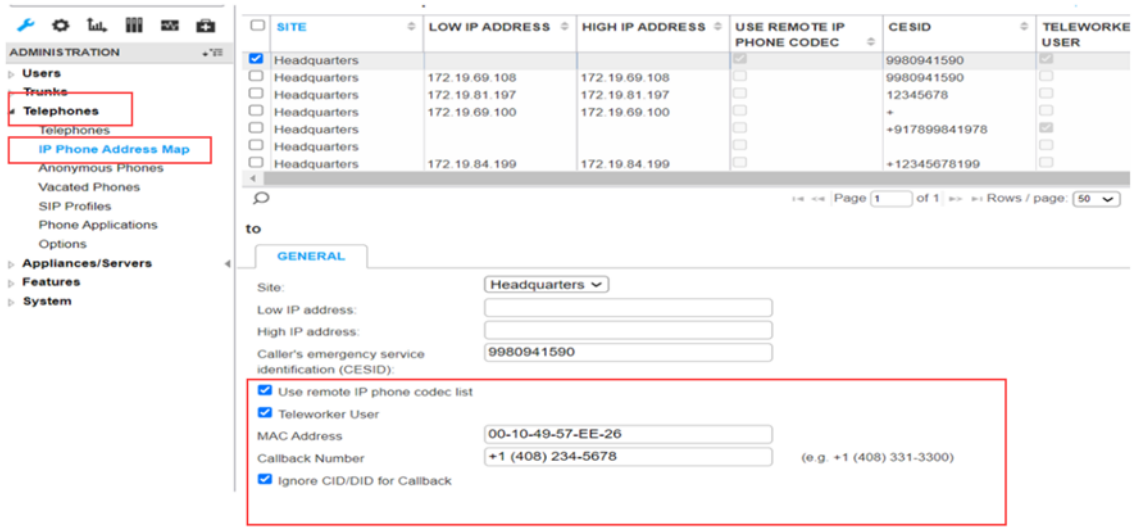


Ignoring Caller ID/DID for a User

To ignore the caller ID/DID for a user in the **IP Phone Address Map** page:

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Telephones** > **IP Phone Address Map**. The **IP Phone Address Map** page opens.
3. Select the entry to update or click **New** to add a new entry for IP-based or MAC-based address.
4. To enable ignore CID/DID for callback, in the **General** tab, select the **Ignore CID/DID for Callback** option.
5. Click **Save**.

Figure 7 : Ignoring caller ID/DID



Configuring the Third-Party Vendor

To configure the third-party vendor (Intrado or RedSky) and related parameters:

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **System** > **Sites**. The **Sites** page opens.
3. Select the site where the **Enable RAY BAUM** option is enabled.
4. To configure the third-party vendor, in the **HELD Configuration** tab, complete the fields as described in Sites Page: Parameters on the HELD Configuration Tab. See HELD Configuration tab for more details.
5. Click **Save**.

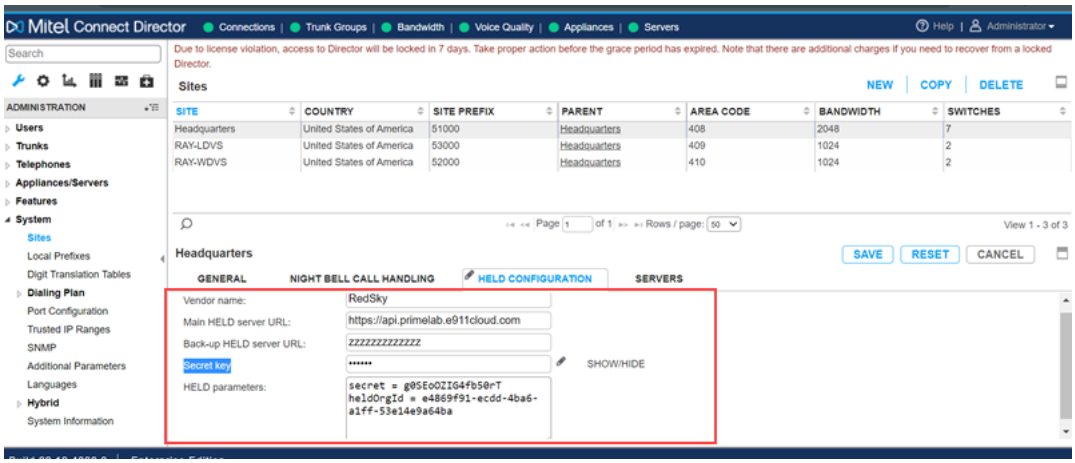
Table 2: Sites Page: Parameters on the HELD Configuration Tab

Parameter	Description
Vendor Name	The third-party vendor (Intrado or RedSky) enables retrieving the location during emergency calls. The third-party vendor enables you to retrieve the location indirectly through a Location URI provided by the vendor's location information service (LIS).
Main HELD Server URL	The address of the third-party vendor's main LIS server. Example: https://api.primelab.e911cloud.com
Back-up HELD Server URL	The address of the third-party vendor's backup LIS server. Example: https://api.primelab.e911cloud.com
Secret Key	Enter the secret key obtained from the third-party vendor. **Note**: • Click the **SHOW/HIDE** option alternatively to view or hide the secret key. • Secret Key is a mandatory parameter. Contact RedSky vendor for the secret key.

Parameter	Description

HELD Parameters	The HTTPS enabled location discovery (HELD) parameters for a specific third-party vendor.
	Note: The administrator can specify any number of vendor-specific parameters in this field in the following format:
	`key1=value1`
	`key1=value2`
	`...`
	`keyN=valueN`
	Note:
	The heldOrgID parameter is mandatory. Contact RedSky vendor for the heldOrgID parameter information.

Figure 8 : HELD Configuration tab

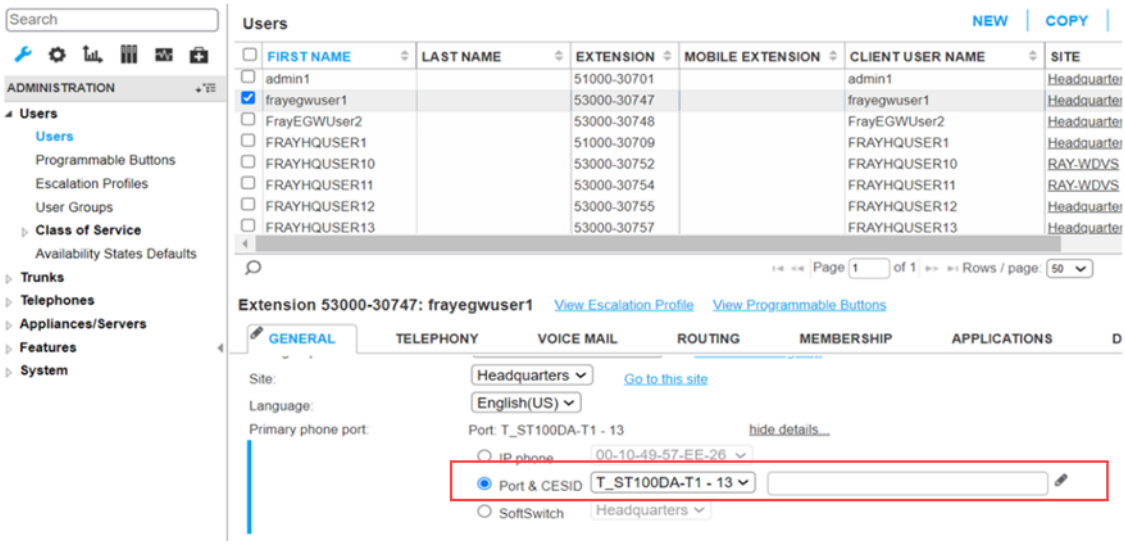


Extend Analog Phones Assignment to have CESID Assignment

To extend the analog phones assignment to have CESID assignment:

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Users** > **Users**. The **Users** page opens.
3. To extend the analog phones assignment to have CESID assignment, in the **General** tab, select the **Port & CESID** option.
4. Enter the CESID for the analog port. See CESID assignment for analog phones
5. Click **Save**.

Figure 9 : CESID assignment for analog phones

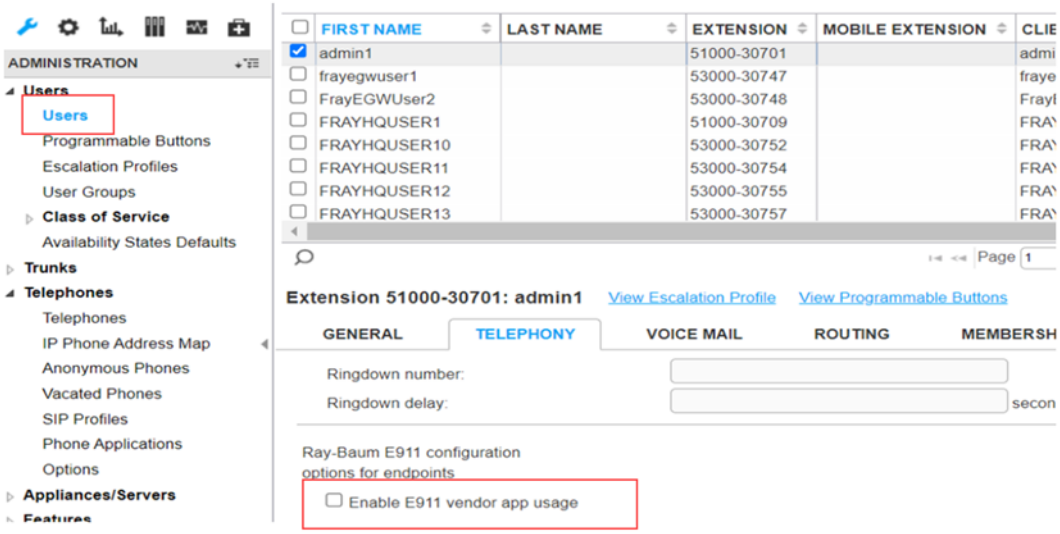


Using the Vendor Application for Location Information

To allow the user to use the vendor application for location information:

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Users** > **Users**. The **Users** page opens.
3. To use the vendor in the **Telephony** tab, select the **Enable E911 vendor app usage** option.
4. Click **Save**.

Figure 10 : Enable E911 Vendor



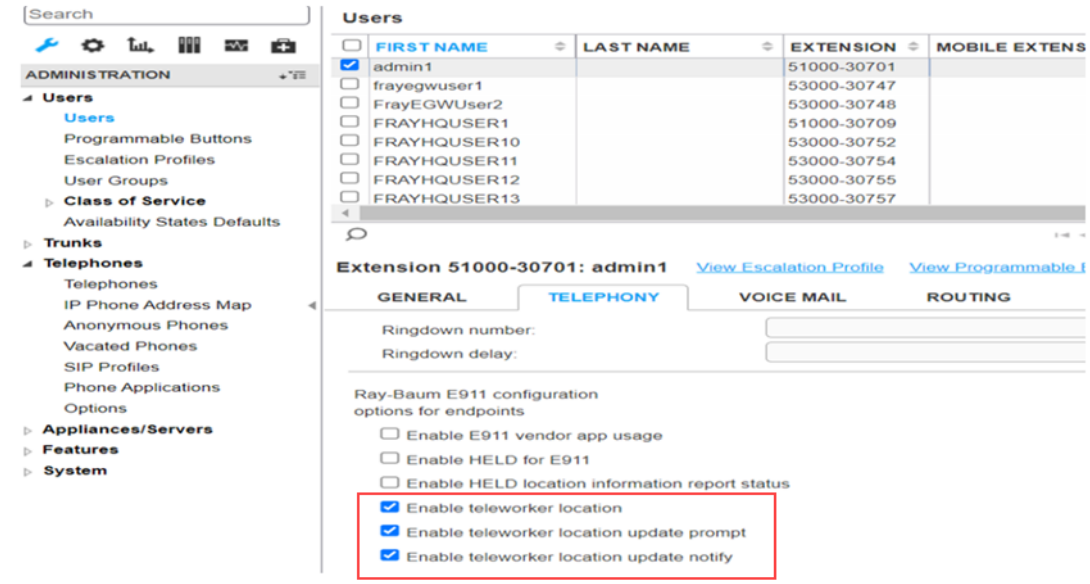
Configuring Phone Flags Related to Location Change

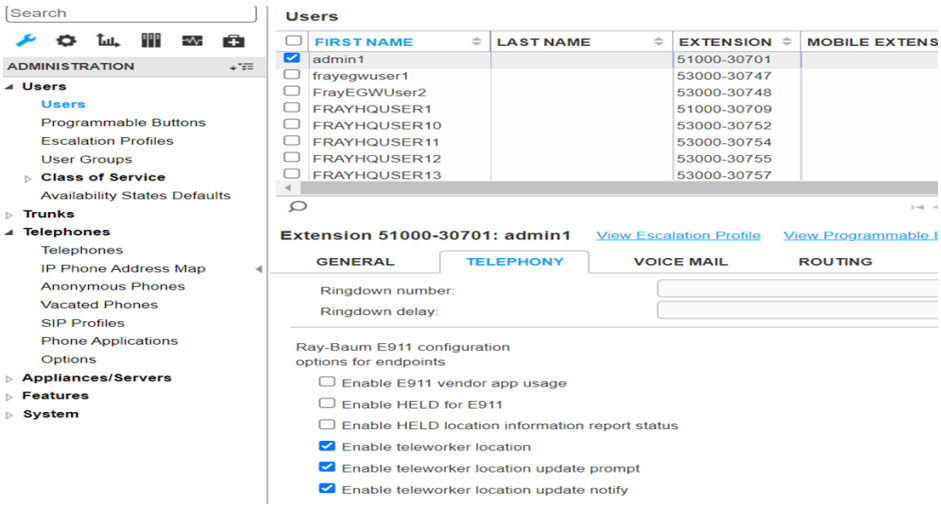
To allow the user to configure Phone flags related to location change and HELD usage:

Note: This section is applicable only for teleworker phones.

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Users** > **Users**. The **Users** page opens.
3. In the **Telephony** tab, select the following options:
   - **Enable teleworker location**
   - **Enable teleworker location update prompt**
   - **Enable teleworker location update notify**
4. Click **Save**.

Figure 11 : Enabling teleworker options





Altering the Validation of the CESID

CESID is the 10-digit number, optionally starting with the + character allowed.

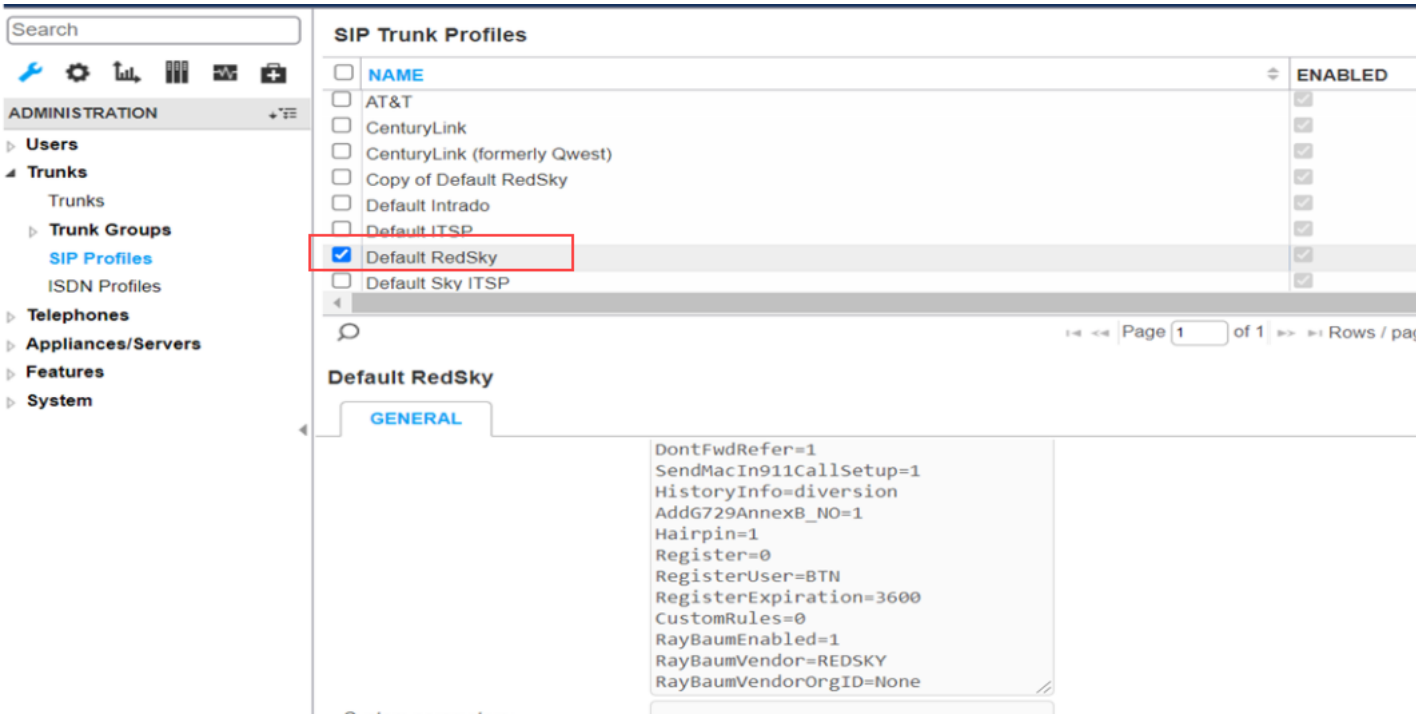
Existing entries present in the config database remains unchanged; and will have no impact on them.

Configuring SIP Profile parameters for Vendor Trunks

To allow the user to configure SIP profile parameters for vendor trunks:

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Trunks** > **SIP Profiles**. The **SIP Trunk Profiles** page opens.
3. In the **SIP Trunk Profiles** page, select the vendor. For example, **Default RedSky**.
4. Using the **Copy** option to copy this profile.
5. In the **General Tab** > **Custom Parameters** field, add the following parameters:
   - RayBaumVendorOrgID=<>(Org ID)
     Note: The Org ID must be obtained from the vendor (Intrado or RedSky).
   - RayBaumDefaultCallback=+(callback number)
     Note: The callback number is the front desk/Receptionist DID of building (as default trunk level callback number).
6. Click **Save**.

Figure 12 : Third-party SIP profiles

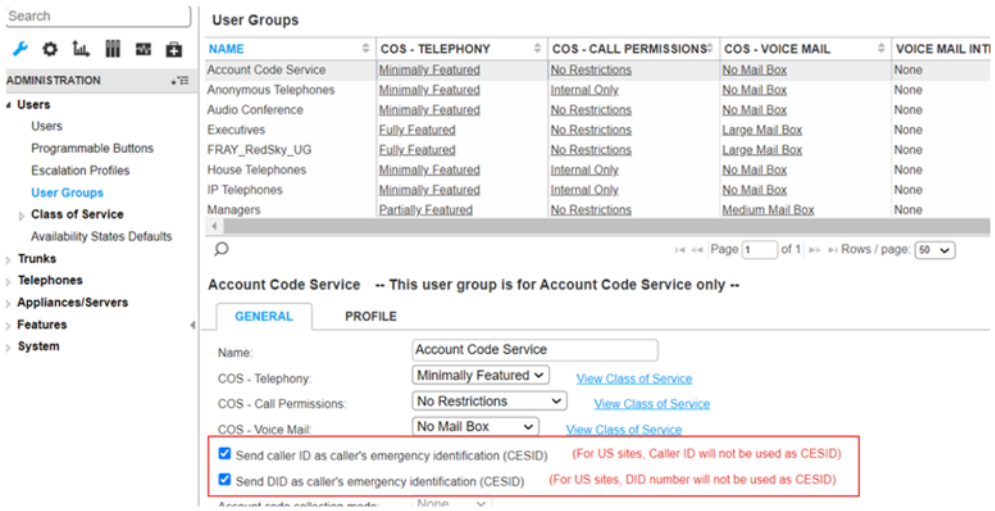


Ignoring Caller ID/DID as CESID for US Sites

To ignore the caller ID/DID as CESID for a US site:

1. Launch Connect Director.
2. In the navigation pane, click **Administration** > **Users** > **User Groups**. The **User Groups** page opens.
3. In the **General** tab, select the following options to ignore the caller ID/DID as CESID for a US site:
   - **Send caller ID as caller's emergency identification (CESID)**
   - **Send DID as caller's emergency identification (CESID)**
4. Enter the CESID for the analog port.
5. Click **Save**.

Figure 13 : Ignoring Caller ID/DID



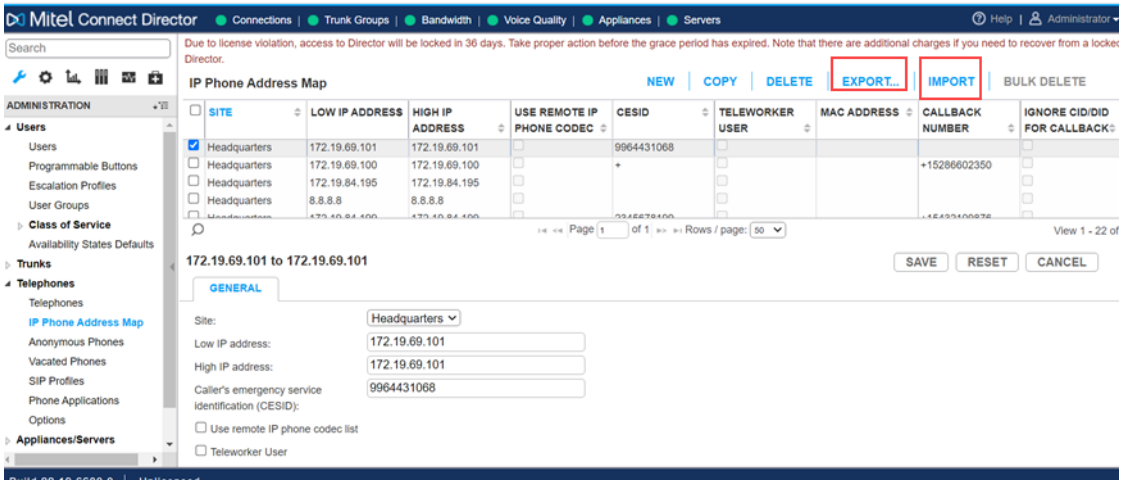
Exporting and Importing IP Phone Address Map Data

To export the IP phone address map information, follow the steps provided in the *Exporting the IP Phone Address Map* section in the *MiVoice Connect System Administration Guide* located at https://www.mitel.com/document-center/business-phone-systems/mivoice-connect/mivoice-connect-platform

To import the IP phone address map information, follow the steps provided in the *Importing the IP Phone Address Map* section in the *MiVoice Connect System Administration Guide* located at https://www.mitel.com/document-center/business-phone-systems/mivoice-connect/mivoice-connect-platform

See Exporting and Importing IP Phone Address Map for more details.

Figure 14 : Exporting and Importing IP Phone Address Map



Solution: MIVC Device RAY BAUM Support Summary

The following table shows a list of devices that support RAY BAUM and the options they have for supporting RAY BAUM. The later sections provide details about how to program each option.

Table 3: MiVC Device RAY BAUM Support

Device	On-Premise	Off-Premise (Teleworker)
IP4xx SIP/MGCP	IP Address to CESID mapping	L2 (MAC) to CESID mapping
69xx SIP	IP Address to CESID mapping	L2 (MAC) to CESID mapping
Generic SIP Device **Note**: Mitel must certify the solution with any Generic SIP Device.	Geo-Location NG911-provided applications	NA
Multi cell DECT	IP Address to CESID mapping	NA
MIVC Connect Client Soft phone	Geo Location	Geo Location
Analog	CESID Assignment	NA
SIP ATA (Analog Terminal Adapters)	IP Address to CESID mapping	NA
Third-Party Soft Client	Third-party Vendor application	NA

MIVC Solution Architecture High level - RAY BAUM

The MiVoice Connect solution for RAY BAUM is composed of different devices, Mitel applications, and third-party devices or applications.

The MiVoice Connect system is capable of supporting different implementations to identify the site from which an emergency call is made. However, Mitel certifies only devices and applications that are validated with MiVoice Connect and can work properly with the Next Generation 911 (NG911) service providers.

Devices

For RAY BAUM, the MiVoice Connect system has support for fixed and non-fixed devices.

The following are the fixed devices in MiVoice Connect:

- Analog - ATS
- Analog devices connected through SIP ATA or SIP-to-analog gateway

The following are non-fixed devices in MiVoice Connect:

- SIP - Mitel Phones (69XX and IP4xx)
- MGCP phones
- SIP – Third-Party (3PP) phones
- SIP – Mitel 5364 phones
- SIP DECT
- SIP – ATA
- Traditional DECT
- IP DECT
- Softphone - Connect Client

Devices off-premises (Remote users – Teleworker)

Note: Teleworker support for 6900-Series phones is currently not supported; and is planned for future release.

- SIP - Mitel Phones (6900-Series and IP 400-Series)
- Softphone- Connect Client

MIVC Functions with RAY BAUM Support

MiVoice Connect supports various functions that might be used to make 911 emergency calls. The supported MiVoice Connect functions are:

- Workgroup extensions
- Hunt group extensions
- Auto-registered anonymous extension
- Teleworker extensions
- SCA – Shared Call Appearance
- ECC agents

Mitel Applications with RAY BAUM Support

The following Mitel applications support RAY BAUM:

- MIVC Connect Client
- Connect Client sales force extensions

Mitel Applications with no RAY BAUM Support

The following Mitel applications do not currently support RAY BAUM:

- Mitel Revolution
- Mitel Connect Mobility Router (CMR) clients (use mobile phone native dialer for emergency calls)

Third-Party Applications

The following third-party applications supported using NG911 vendor application

- X Lite

Advanced Applications

The following advanced applications need to use an NG911 vendor for location detection during emergency calls:

- Skype for Business
- MIVC Connect Client
- Connect Client Chrome plugins
- Connect Client Salesforce Extensions

Devices Emergency Services Setup

Each type of device supported by MiVoice Connect has a different capability regarding emergency services (for example, different possibilities of how to set it up depends on the use case). The goal of setting the devices correctly is to provide the most accurate and precise location information when an emergency call is made.

For non-fixed devices such as, SIP desk phones, SIP-DECT devices, IP DECT, WiFi phones, and SIP softphones (Connect Client), MiVoice Connect can obtain information during the call setup. Some of the devices requires preconfiguration for example, HTTP enabled location discovery (HELD) setup in MIVC Connect Client, while others such as, MAC address in the SIP phone for teleworker use cases do not require this.

For fixed devices, the setup must be preconfigured manually.

Note: MiVoice Connect can identify any device using a directory number setup (extension number), regardless of whether the device is a fixed or non- fixed device. However, the directory number setup is recommended only for third-party applications and devices using the NG911 vendor application.

- Non-Fixed Devices (Hardware Devices)
- Non-Fixed Devices (Softphones/Clients)
- Fixed Devices (Legacy Devices)

Non-Fixed Devices (Hardware Devices)

SIP Phones Setup (Mitel IP4xx and 6900-Series)

Dynamic Setup

- IP address

  An IP address can be used to identify in which ip_domain the SIP phone is located.

  MiVoice Connect will check whether the IP address is available when the invite is received and take the appropriate action. If an entry for the IP address or subnet and respective location ID is set up in the MiVoice Connect IP address configuration, then MiVoice Connect transmits the corresponding location ID to the 911 service provider.
- MAC address

  The SIP phones (Mitel IP4xx and 6900-Series) transmit the MAC in the following field in the **SIP invite: sip_instance="<urn:uuid … MACaddr>**

  MiVoice Connect will check whether the MAC address is available when the invite is received and will take the appropriate action. If an entry for the MAC address and respective location ID is set up in the MiVoice Connect config database, then MiVoice Connect transmits the corresponding location ID to the 911 service provider.

  A MAC address can be used to differentiate two or more SIP phones, for example in a Teleworker case, when the user has a forking extension with two SIP phones, one at the office and another at home.

  Currently, MiVoice Connect uses the MAC-address-based mechanism only for teleworker-based phones

Note: MGCP-based phones also use the same mechanism as SIP phones.

SIP and Third-Party SIP Phones

SIP-DECT, Multi cell IP-DECT, Single Cell IP-DECT, SIP ATA (Analog Terminal Adapters), and third-party SIP phone devices use the same mechanism as that used by SIP phones.

Non-Fixed Devices (Softphones/Clients)

MIVC Connect Client (Softphones)

The MIVC connect client uses HTTP-enabled location discovery (HELD) to provide dynamic location information. In this setup, the GeoLocation and GeoLocation Routing Header will be sent from the client with a reference only in the SIP invite. MiVoice Connect will transparently pass through the supported SIP headers to the NG911 service provider. Along with transparently passing the Geolocation headers, the only responsibility MiVoice Connect handles with-regard-to Connect Client is to maintain HELD-related configuration parameters. Only these configuration parameters will be used by Connect Client to connect and get information from the NG911 vendors.

Fixed Devices (Legacy Devices)

ATS – Analog Phone Static Setup

Directory Number in the Emergency Location Database

The analog phone directory number can be manually set up in the MiVoice Connect emergency location database. The CESID can be assigned by the administrator while setting up the directory number for the analog phone. Alternately, the administrator can assign CESID for the specific analog port to which the analog phone is connected.

MiVoice Connect will check whether there is information related to analog phone available in the config database when the call is initiated and will take the appropriate action. If an entry for the directory number and respective location ID is set up in the MiVoice Connect config database, then MiVoice Connect transmits the corresponding location ID to the NG911 service provider.

Alarms, Events/Notifications and Logs

The MiVoice Connect events and notification mechanism for emergency calls is the same as the existing one.

Events/Notifications in MiVoice Connect

MiVoice Connect provides an emergency notification application for notifying specific users when emergency calls are made. You can use this application to configure notifications when emergency calls are made. See the Mitel Emergency Notification Server User Guide for more information.

SIP Phones Notification

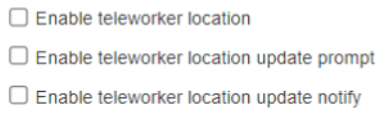
Whenever a teleworker phone changes location, the phone will identify it and give a pop-up indication to the user about this. It is the responsibility of the teleworker user to update the new location information in the third-party vendor database with the help of the system administrator. If this is not done, the 911 emergency call might give incorrect location information to the PSAP. Because the phones request the user to update the location information, these intimations will be logged in the persistent logs of MiVoice Connect. This information can be used for audit purposes later to determine whether the location was not updated by the end-user even after the phones requested for this.

The Mitel SIP phones (IP 400-Series and 6900-Series) running the latest firmware version send notifications to the user when a SIP phone is moved from one location to another. In this situation, the SIP phone will send a notification to MiVoice Connect, and MiVoice Connect adds that information to the messages log in the file named `EmergencyLocationUpdateInfo`.

This will be present in the standard log location of the controlling servers. These files will not be deleted automatically based on log file archive configuration; administrators can delete these log files manually only if they are no longer required for further auditing.

This notification and logging features can be enabled or disabled by the system administrator by configuring the following parameters in the MiVoice Connect Director by accessing the **Administration** > **Users** > **Users**> **Telephony** tab.

Figure 15 : Enabling teleworker location



If the options in Enabling teleworker location are enabled, wheneverthere is a location change in the teleworker phone, the end-user will be prompted by a pop-up alert. This process information will also be reported to call managers through SIPNOTIFYmessages. The call managers will log the event in the persistent log file (`EmergencyLocationUpdateInfo`). Logging the event might be required for legal auditing. Because the phone log is temporary and the vendor is not in Mitel's control,a single point of audit for MiVoice Connect solutionhelps resolve any complaints.

By default, these options are enabled on the phone side and MiVoice Connect side for US customers and disabled on MiVoice Connect side for non-US users.

For more information, see the *Telephony Tab* section in the *MiVoice Connect System Administration Guide* located at https://www.mitel.com/document-center/business-phone-systems/mivoice-connect/mivoice-connect-platform.

MIVC Integration with NG911 Service Provider – Deployment Setup

This section explains the deployment setup between MiVoice Connect and the NG911 service provider.

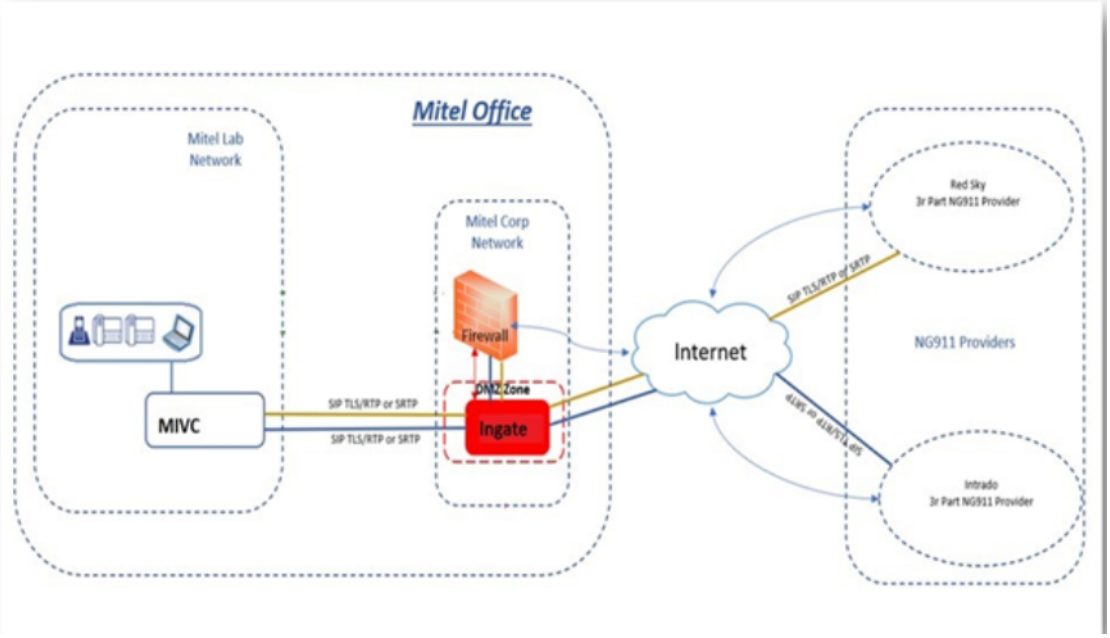
The scenario illustrated in MIVC integration with a third-party vendor on page 27 shows only one service node/site for the sake of simplicity; however, multiple Service Nodes/sites can be deployed in the same manner.

Note: You can integrate only one vendor per site.

MIVC Integration with Third-Party Vendor Using an Ingate SIParator

The architectural view in MIVC integration with a third-party vendor shows the most basic setup between MiVoice Connect and the NG911 service provider. A SIP trunk is set up between one MiVoice Connect system and another, and the Ingate has SIP trunks towards the NG911 service provider gateways.

Figure 16 : MIVC integration with a third-party vendor



For information about configuring Ingate, see the following documents:

- SIP Trunking Configuration Guide for Ingate Solutions
- SIP Trunking Configuration - Ingate

MiVoice Connect does not support voice SRTP on the trunk side by itself. Therefore, to use voice-over SRTP with third-party vendor, you must set up the MiVoice Connect system using the following steps. In this case, the connection between MiVoice Connect and Ingate will be normal User Datagram Protocol (UDP) and that between Ingate and third-party vendor will be on SRTP.

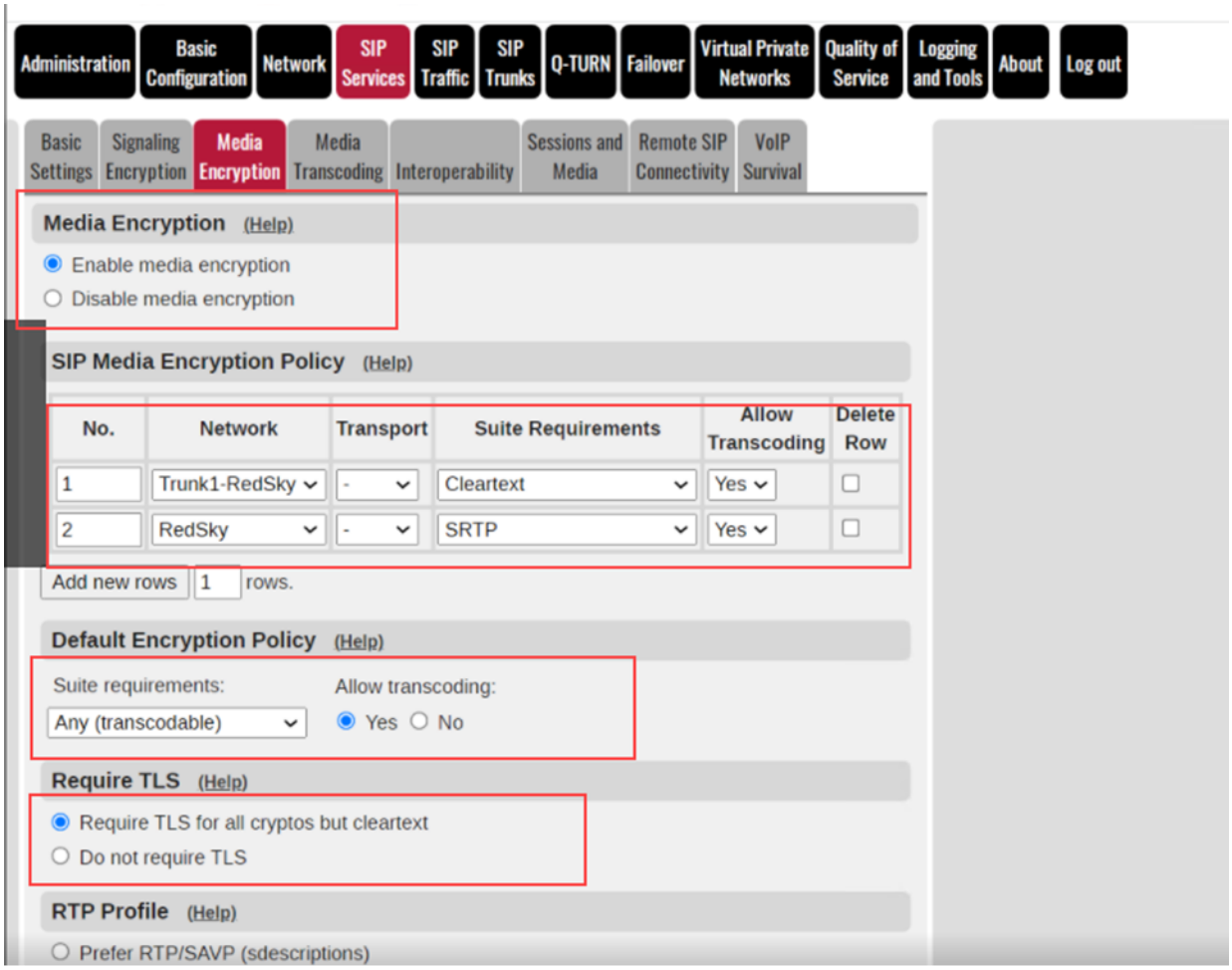
Note: Currently, TLS is supported only by RedSky and Intrado do not support TLS.

Between MiVoice Connect to Ingate, configure the trunk to use with SRTP disabled. On INGATE, you must configure the trunk to use SRTP irrespective of what is used in the previous leg.

Following is a sample with Twilio as the ITSP:

1. Enable Media Encryption module in SIP Services.

   Figure 17 : Enable media encryption

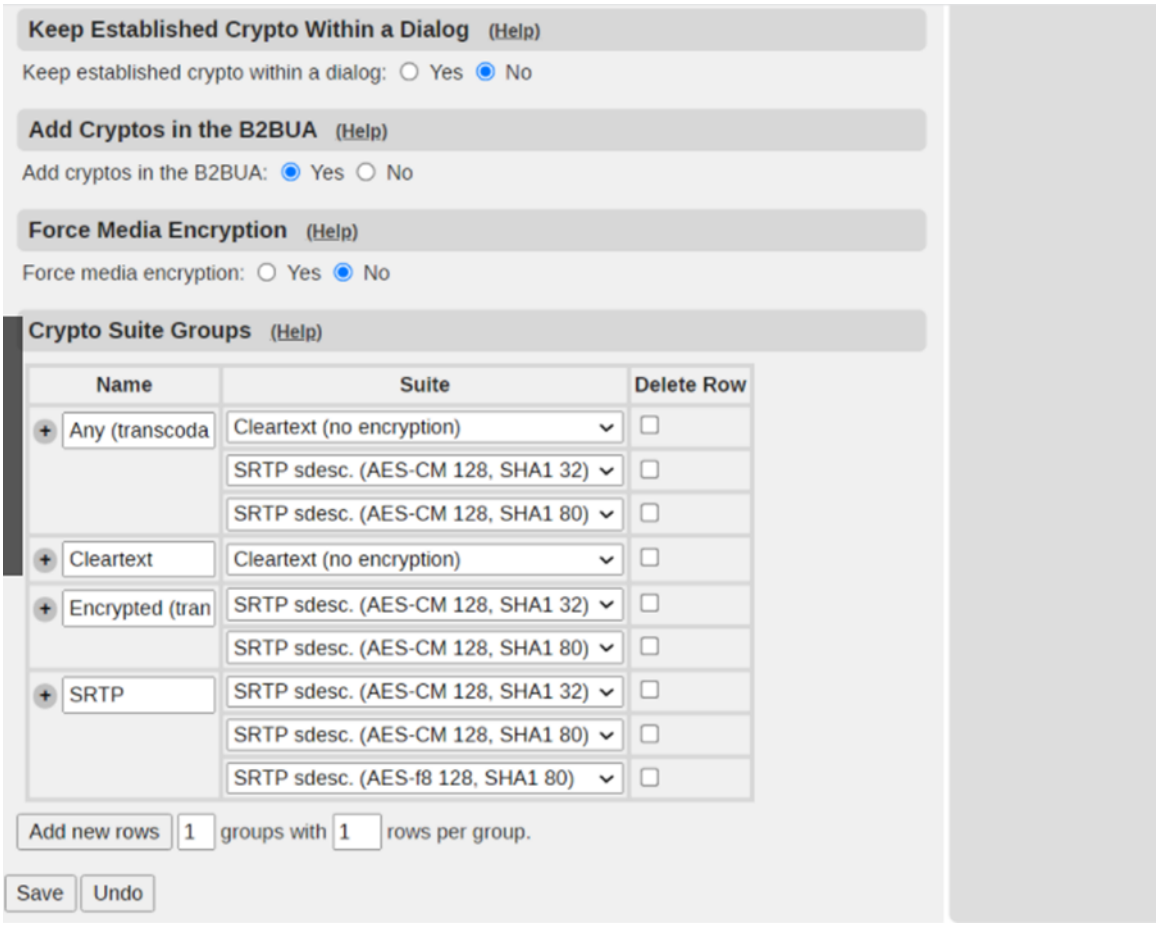


To enable media encryption:

a. Add a policy for your carrier (for example, Trunk1-RedSky) to enforce SRTP suite.
b. Add a policy for your vTrunks to enforce no-encryption (Cleartext) suite.
c. Enable transcoding on both policies.
d. Configure the required TLS option based on the encryption requirement on carrier side. If you want the carrier side to enforce TLS with media encryption, select **Require TLS for all cryptos but cleartext**. If not, then select the **Do not require TLS** option.
e. Define a default encryption policy for other networks that are not included in the previous policy. Select the option that better fits the case. For example, under **Default Encryption Policy** > **Suite requirements**, select **Any (transcodable)** as shown in MIVC integration with a third-party vendor.

2. Review the suites to confirm that they include what you need and make any modifications if required .

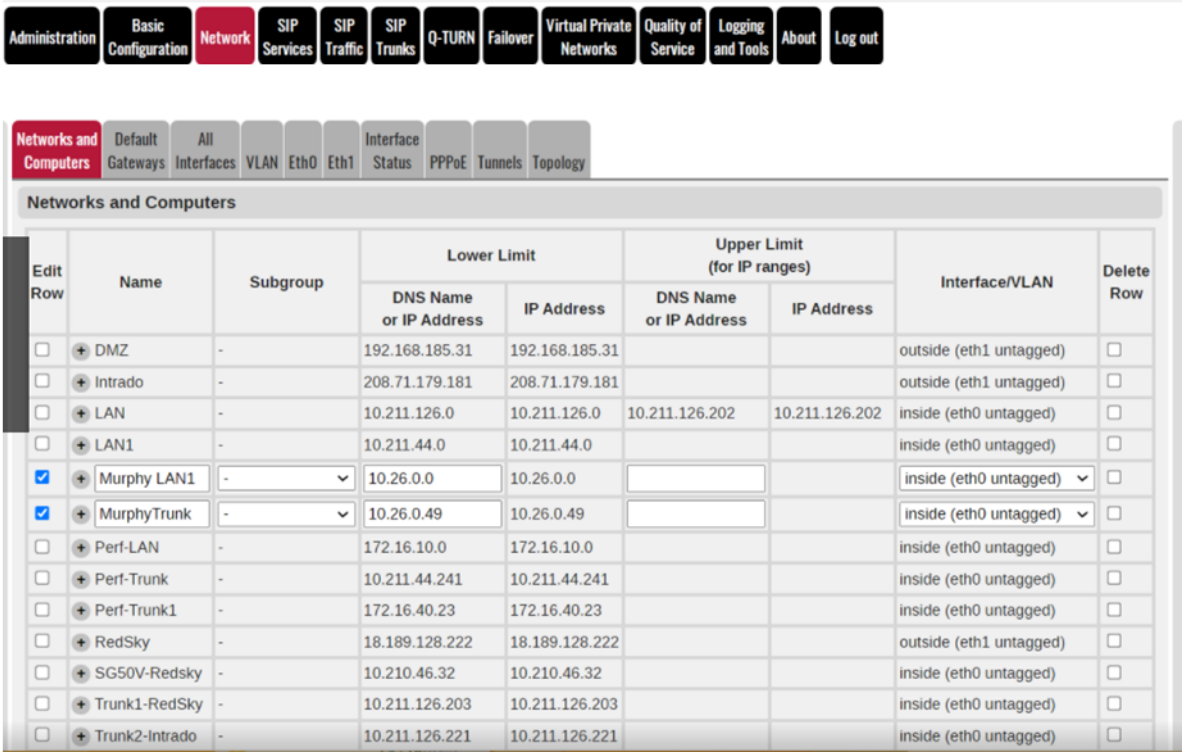
Figure 18 : Reviewing the Suites



3. Leave all the other fields with the default values.
   Note: Ensure that the network names you select include all media/signaling IP addresses for your ITSP as well as vTrunks.

Default Values illustrates an example.

Figure 19 : Default Values



Note: The media negotiation between Ingate and the third-party vendor (Redsky) will follow the policies already defined in the **Media Encryption** page.

MIVC Integration to Support RAY BAUM - Deployment Setup

This section provides information about MiVoice Connect integration to support RAY BAUM in a deployment setup that uses the conventional trunk provider (not NG911 service provider) deployment setup.

As mentioned earlier, if the customer has only on-premises IP4xx and/or 69xx devices and/or Dect phones, the customer can purchase the required number of CESIDs from their service provider which can identify all the dispatchable locations. If only one CESID is required (as for a single floor or a small office space), then you can use the existing IP range and/or L2 CESID mapping features available in MiVoice Connect and you need not upgrade the features. If more than one CESID is required, and the cost for the CESIDs is not more than the cost of integrating with NG911 vendor, then you can use any existing trunks and upgrade MiVoice Connect to the latest version to comply with RAY BAUM. If only one CESID is required, then to use the existing IP range and/or L2 CESID mapping features available in MiVoice Connect, do the following:

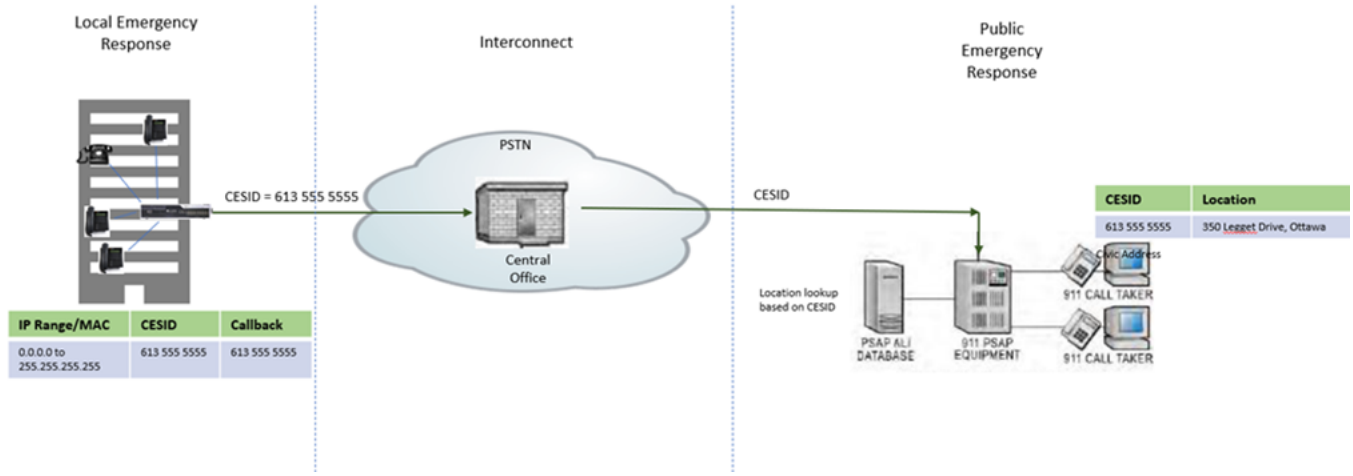
1. If not already obtained, then get the required CESID numbers from the NG911 service provider.
2. If the CESID obtained is a new one, then update the IP address map to match the new CESID to location mapping.
3. Enable the **Enable RAY BAUM** option in the **Sites** page. For information about enabling the **Enable RAY BAUM** option, see Enable or Disable RAY BAUM Feature for a Site on page 13.
4. Integrate the trunks with the site and configure them correctly.
5. Add the new RayBaumEnabled SIP profile parameter and set it to 1 for enabling the RAY BAUM feature. For example, RayBaumEnabled=1. For more information, see the *SIP Trunk Profiles Provided by Mitel* section in the *MiVoice Connect System Administration Guide*.

RAY BAUM Different Deployment Method Visualization

To summarize, following are the three major deployment models possible for RAY BAUM based on the type of devices the PBX host:

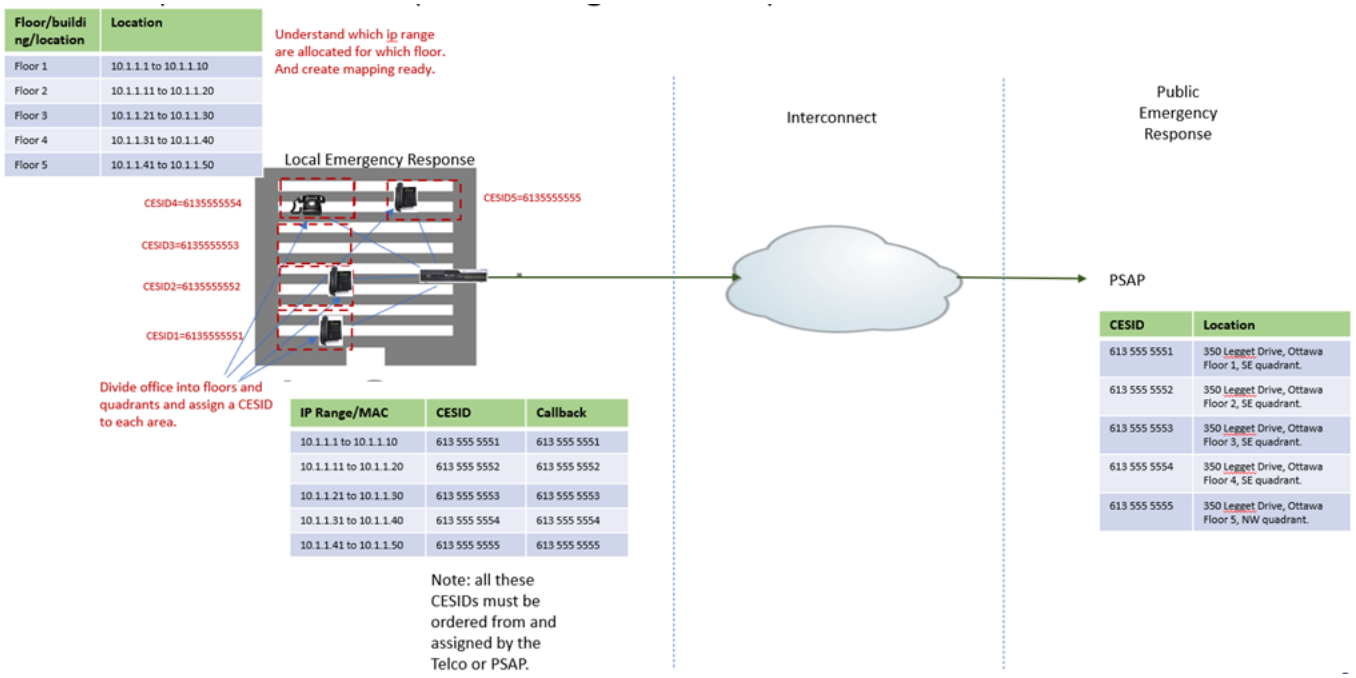
- Office with single floor and single building – single dispatchable location. For more information, see Office with single floor and single building.

Figure 20 : Office with single floor and single building



- Multiple floors/multiple buildings (no Connect Clients or teleworkers) – multiple on-premises only dispatchable locations. For more information, see Multiple floor/multiple building - no softphone clients or teleworkers

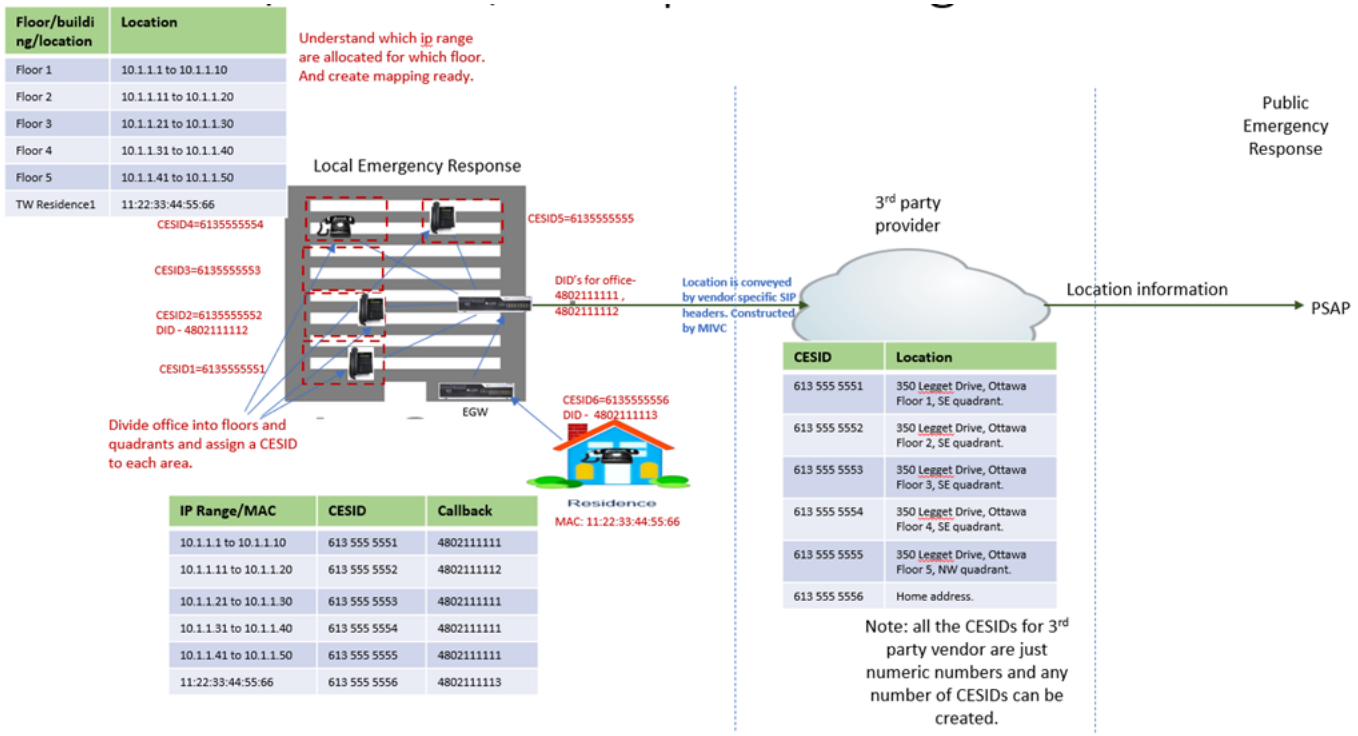
Figure 21 : Multiple floor/multiple building - no softphone clients or teleworkers



- Multiple floors/multiple buildings (with teleworker and/or with Connect Client and/or third-party soft phones) – multiple off-premises and on-premises dispatchable locations. This deployment model is further sub-divided into:

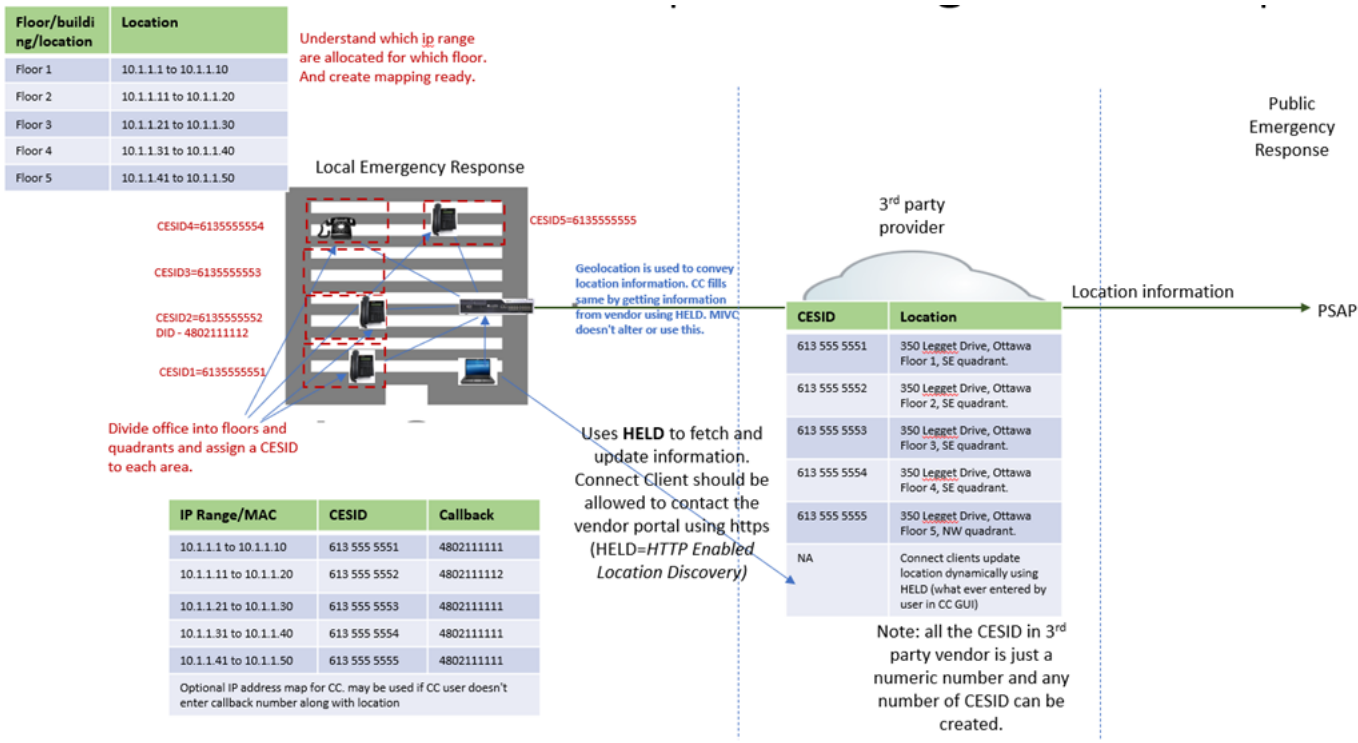
- Multiple floors/multiple buildings – with teleworkers. For more information, see Multiple floor/multiple building - with teleworkers.

Figure 22 : Multiple floor/multiple building - with teleworkers



- Multiple floors/multiple buildings – with Connect Client. For more information, see Multiple floor/multiple building – with softphone.

Figure 23 : Multiple floor/multiple building – with softphone

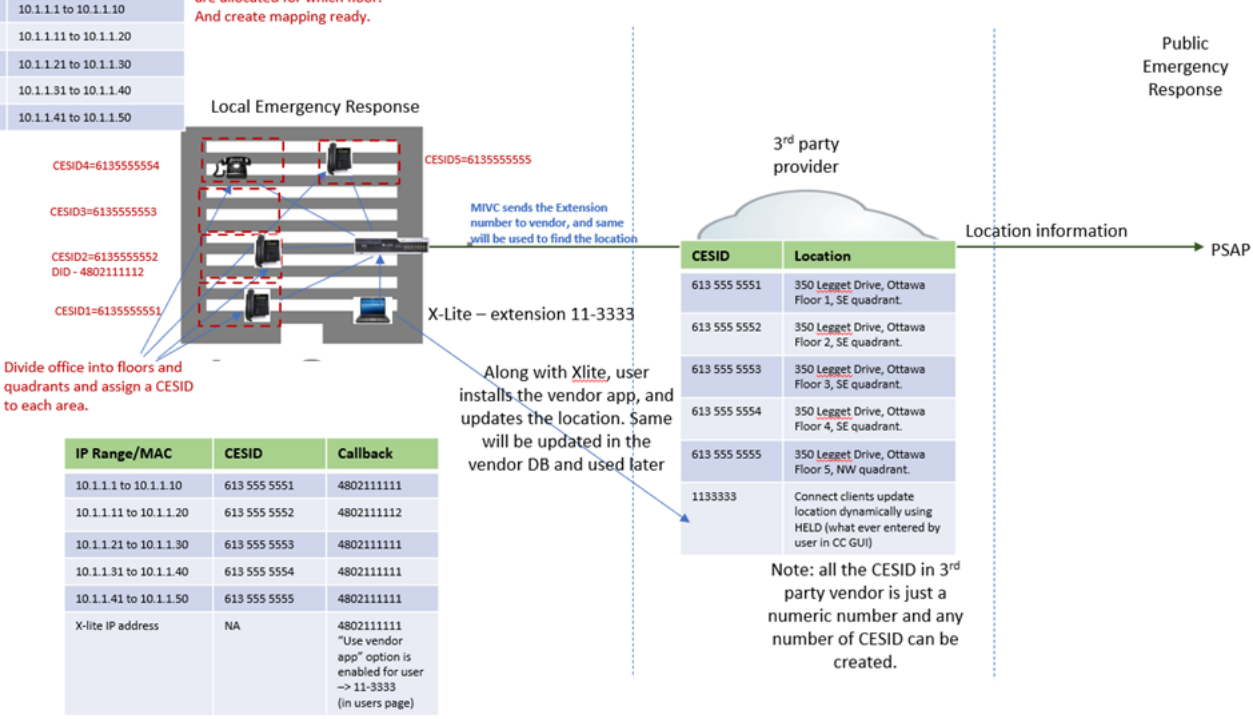


- Multiple floors/multiple buildings – third-party clients (vendor apps). For more information, see Multiple floor/multiple building – third-party clients.

Figure 24 : Multiple floor/multiple building – third-party clients

Floor/building/location	Location
Floor 1	10.1.1.1 to 10.1.1.10
Floor 2	10.1.1.11 to 10.1.1.20
Floor 3	10.1.1.21 to 10.1.1.30
Floor 4	10.1.1.31 to 10.1.1.40
Floor 5	10.1.1.41 to 10.1.1.50

Understand which ip range are allocated for which floor. And create mapping ready.



CESID	Location
613 555 5551	350 Legget Drive, Ottawa Floor 1, SE quadrant.
613 555 5552	350 Legget Drive, Ottawa Floor 2, SE quadrant.
613 555 5553	350 Legget Drive, Ottawa Floor 3, SE quadrant.
613 555 5554	350 Legget Drive, Ottawa Floor 4, SE quadrant.
613 555 5555	350 Legget Drive, Ottawa Floor 5, NW quadrant.
1133333	Connect clients update location dynamically using HELD (what ever entered by user in CC GUI)

Note: all the CESID in 3rd party vendor is just a numeric number and any number of CESID can be created.

IP Range/MAC	CESID	Callback
10.1.1.1 to 10.1.1.10	613 555 5551	4802111111
10.1.1.11 to 10.1.1.20	613 555 5552	4802111112
10.1.1.21 to 10.1.1.30	613 555 5553	4802111111
10.1.1.31 to 10.1.1.40	613 555 5554	4802111111
10.1.1.41 to 10.1.1.50	613 555 5555	4802111111
X-lite IP address	NA	4802111111 "Use vendor app" option is enabled for user --> 11-3333 (in users page)

Limitations of RAY BAUM

- Mobile phones – Mobile phones are not part of the MiVoice Connect solution with RAY BAUM as they use the native phone function to provide the location services information during an emergency call.
- MiVoice Connect does not support more than one NG911 service provider per site.

Acronyms, Abbreviations, and Glossary

- **ELIN** - Emergency Location Identification Number also known as CESID.
- **LIS** - Location Information Service
- **ERS** - Emergency outing Services.
- **CID** - Caller ID
- **CESID** - Caller's Emergency Service Identification
- **MAC** - Media Access Control
- **SRTP** - Secure Real-time Transport Protocol
- **CPN** - Calling Party Number
- **EON** - Emergency On-Site Notification
- **E911** - Enhanced 911
- **FQDN** - Fully Qualified Domain Name
- **Fixed devices** - Fixed device is a device that cannot be moved to another place in the enterprise without assistance from a professional installer or network manager.
- **L2** - Layer 2
- **L3** - Layer 3 of the Open OSI model
- **MLTS**- Multi Line Telephone System. Equivalent to a PBX, but is the nomenclature used in the RAY BAUM'S Act.
- **NG911** – Next Generation 911
- **Non-fixed devices** – A non-fixed device is a device that the end user can move from one endpoint to another without assistance.
- **SBC**– Session Border Controller
- **SIP** - Session Initiation Protocol
- **TLS** - Transport Layer Security
- **TCP** - Transmission Control Protocol
- **HELD**– HTTP-enabled location discovery
- **UDP**– User Datagram Protocol