MiVOICE BUSINESS
EMERGENCY SERVICES

911 and E911 Emergency Services

911 is the number dialed by someone in NA who requires emergency assistance.

In Europe and other locations around the world, the number(s) dialed is different. For example, in the UK, callers can dial either 999 or 112.

In NA, emergency calls are answered by a Public Safety Answering Point (PSAP) call-taker who is trained to determine who placed the call, from where the call was placed, and to dispatch the appropriate emergency service personnel to the exact location of the caller.

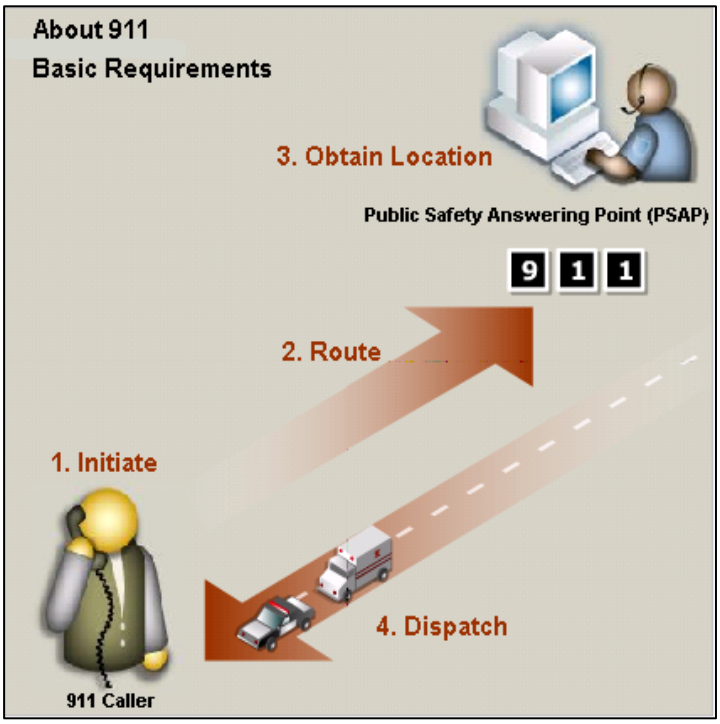
The PSAP is an Emergency Services Call Center trained to receive emergency 911 calls, and is typically operated by a combination of the local police, fire department, and ambulance services.

Governments and enterprises are required to address residential and multiline telephone system emergency call handling with efficiency and accuracy. Enhanced 911, or E911, addresses these concerns.

The basic requirements needed to comply with E911 legislation is the ability to:

- Initiate an emergency 911 call.
- Route emergency 911 calls automatically to a PSAP.
- Obtain the caller's exact location and a callback telephone number.
- Acknowledge the 911 call and dispatch the appropriate emergency services personnel to the exact location of the 911 caller.

The following sections discuss how emergency calls are handled in a residential environment and then discuss how emergency calls are handled in a MiVoice Business environment.

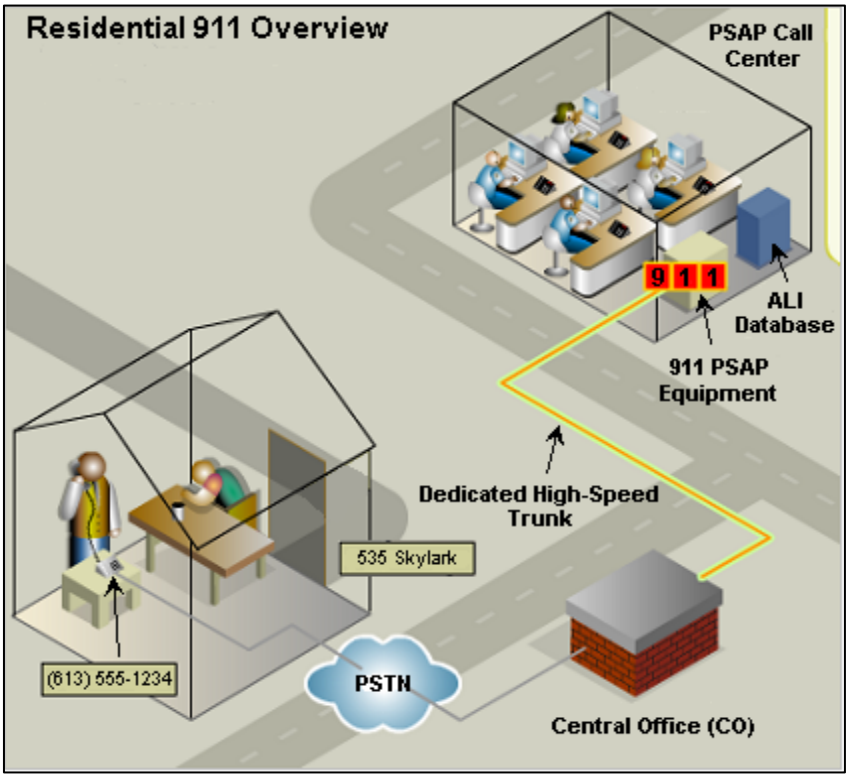


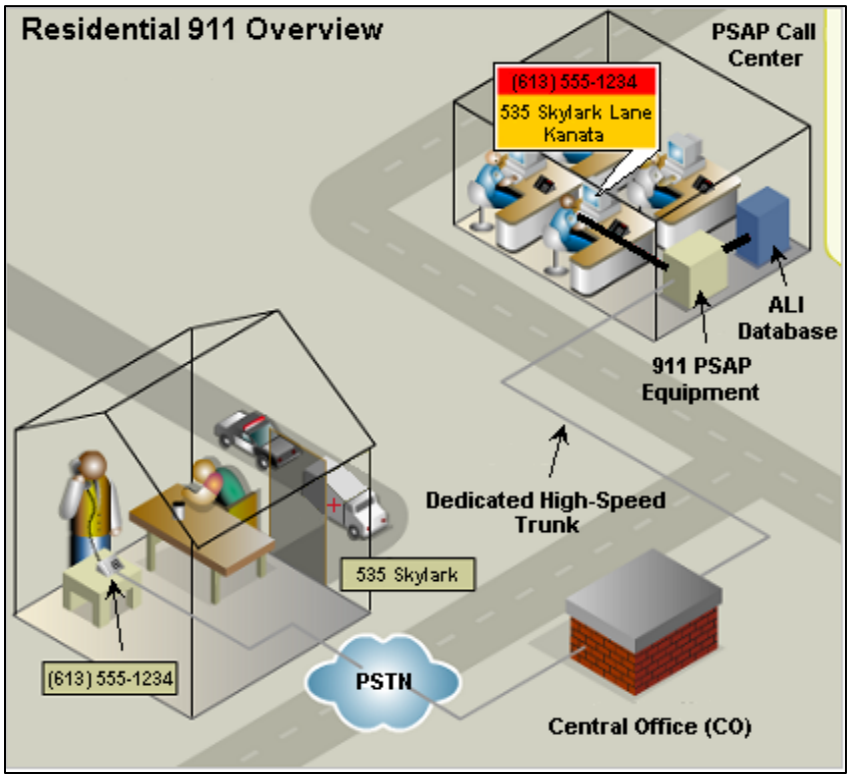
Basic 911 Requirements

Residential 911

In a residential or single-line small business environment, E911 provides the PSAP with the address of the telephone from where a 911 call originates. For example:

- An emergency occurs at 535 Skylark Lane in the city of Kanata. A caller at (613) 555-1234 places a 911 emergency call.
- When the caller dials 911, the emergency call routes over the caller's PSTN line to the CO.
- The CO detects the 911 call and automatically routes the 911 call information over a dedicated high-speed PSAP trunk to the PSAP.
- As the 911 call-taker receives the call, the PSAP automatically sends the caller's Automatic Number Identification (ANI) information to the Automatic Location Information (ALI) database to retrieve detailed information on the exact location of the caller.
- The ALI database returns the exact location of the caller back to the 911 call-taker's screen.
- The 911 call-taker can now dispatch the appropriate emergency services personnel to 535 Skylark Lane in Kanata based on the location information retrieved from the PSAP ALI database.

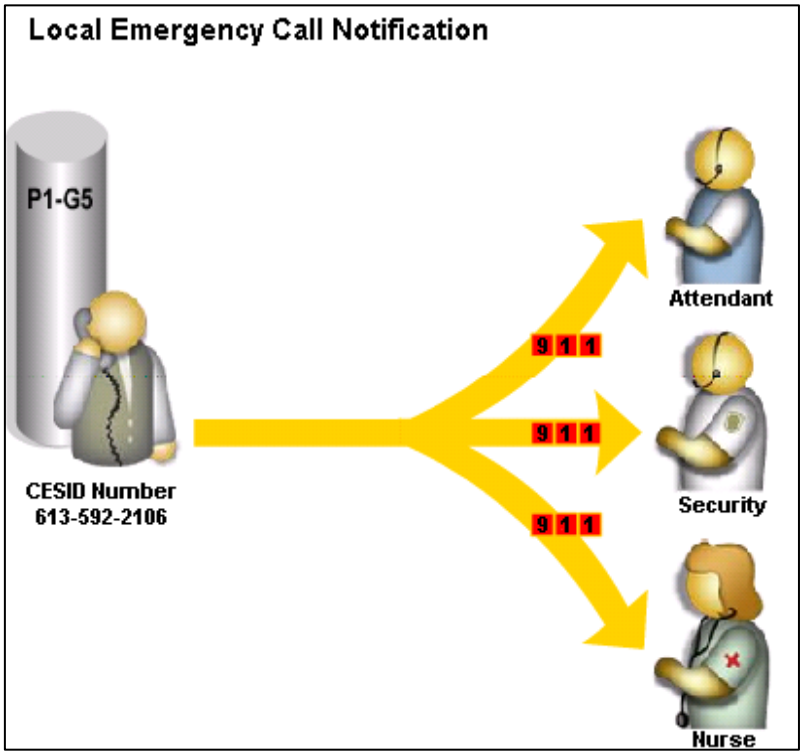




All of the above functions work well when the single point of connection to the CO is a relatively small establishment. Large facilities can have an individual dial 911 and they could be on the second floor, in the warehouse, etc.

Local Emergency Call Notification

The Local Emergency Call Notification feature allows you to program the system to send an emergency call notification to one or more attendant consoles or display phones when an emergency number is dialed.



A designated attendant or display set user can select a softkey button or dial a feature access code to view the following Emergency Call Notification details:

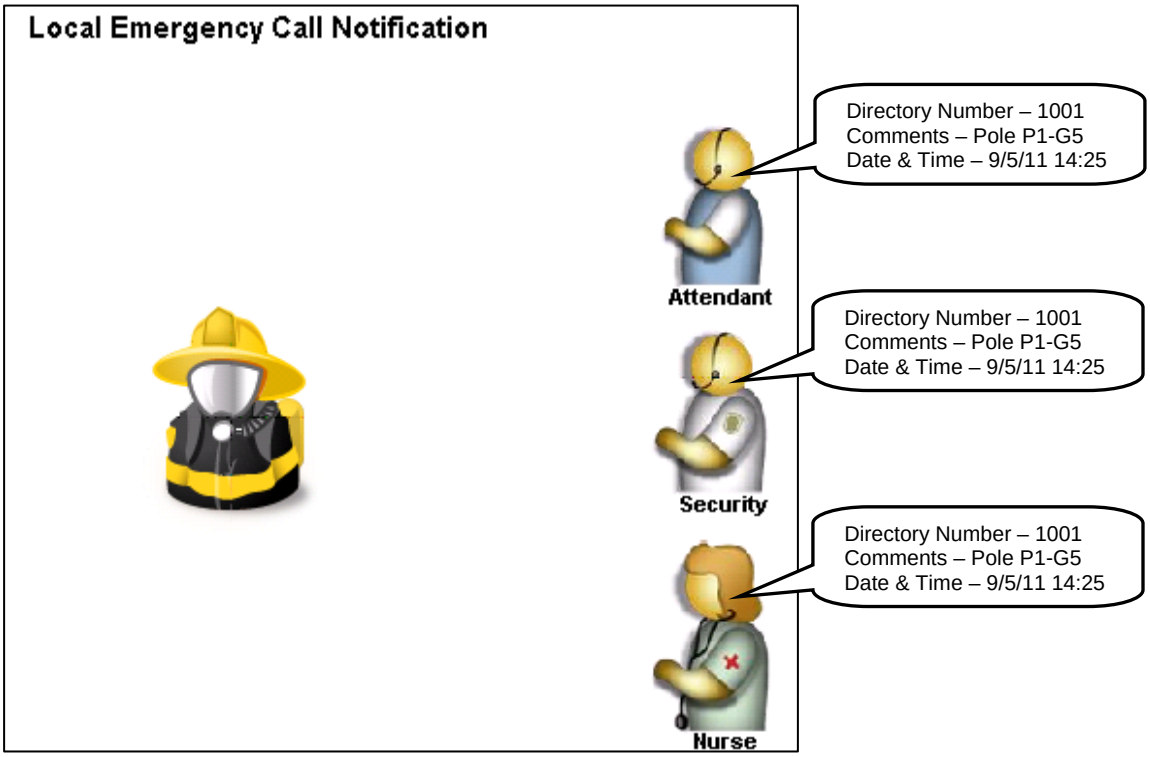
- The caller's DN.
- Special instructions that are programmed for the DN in the Comments field of the CESID Assignment form. If the comments field for an IP phone is blank, the system displays the name of the emergency caller on the attendant console or display set. If the comments field is blank for an ONS CLASS/CLIP phone, the system displays No Data.

Note

CESIDs are discussed later.

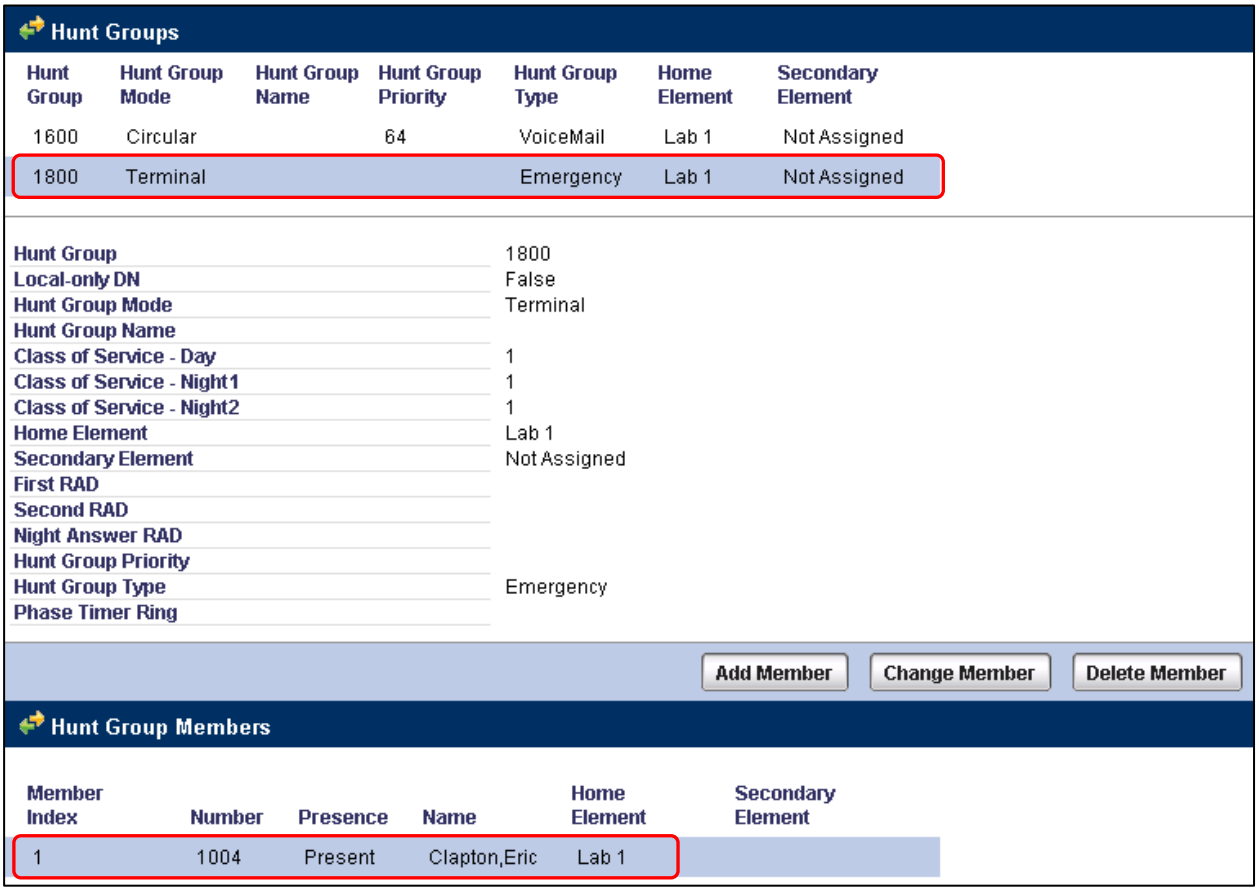
- The date and time of the call.

When emergency service personnel arrive on the scene, a person familiar with the building layout can direct fire, police, and ambulance personnel to the exact location of the caller.



Programming

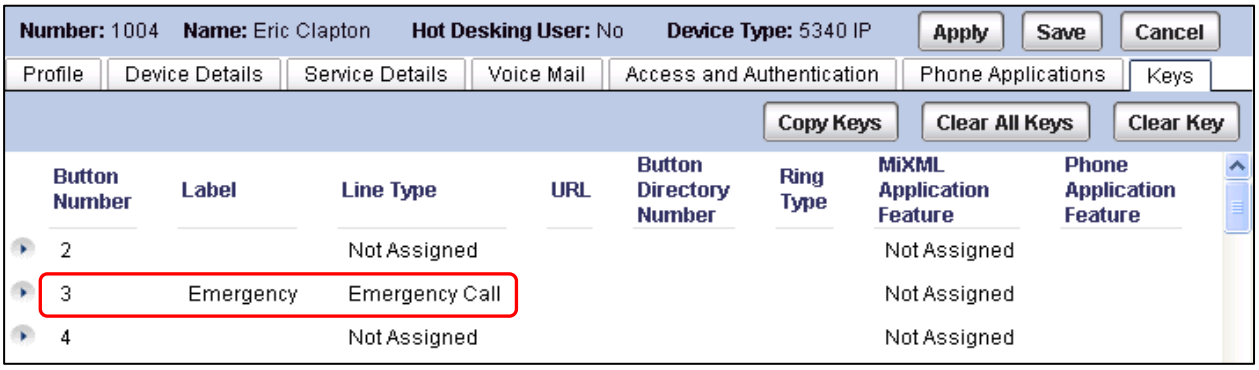
To program local emergency call notification, create a hunt group with the Hunt Group Type being Emergency. Add the required members to the hunt group.



Note

Devices that are added to an Emergency Hunt Group cannot also be Hot Desk Enabled. The Hot Desk Softkey is removed as soon as you place the device into the group.

Program an Emergency Call Notification Feature Key on the set.



Note

In the COSs for the phones and attendant console that will be alerted on an emergency call:

- Set Emergency Call Notification - Audio to Yes
- Set Emergency Call Notification - Visual to Yes

Emergency Services Description

With Emergency Services support, when an emergency number is dialed, a Customer Emergency Services ID (CESID) is sent from the system to the Public Safety Answering Point (PSAP). The CESID is used as a key in the Automatic Location Information (ALI) database. The ALI database displays the precise location of the caller, as well as emergency services information identifying the proper medical, fire, or law enforcement agency for the location.

Caution

It is important that you communicate all CESID changes to the ALI database!

Different state or provincial regulations may govern the CESID requirements at your location. Some require a unique CESID for every telephone, and others allow shared CESID if the telephone users are within sight of one another. One dialable directory number is required for each CESID.

The network environment must have all L2 switches configured for Cisco Discovery Protocol (CDP), Spanning Tree Protocol (STP), or both. The system performs automatic CESID updating for IP devices that are moved to a known location. CESID Logs and CESID Alarms record all CESID-related activity on the system.

Appropriate trunk availability must be maintained for emergency services calls.

Any ARS string can be flagged as an Emergency Services number. Commonly used numbers are 911 and 999. Ensure all combinations of the Emergency Services number are programmed appropriately in ARS. For example, if the Emergency Services number is 911 and some users may dial a leading digit (9) to access an outgoing line before dialing 911, program both 911 and 9-911.

The Emergency Services feature consists of the following elements:

- CESID Support. This is required. Sending alarms as Local Notification of emergency calls to an attendant console or a display set, where an attendant or set user can view alarm details and clear alarms.
- Sending emergency response notification to a Mitel Emergency Response Adviser.

Emergency Services – CESID Support Description

When a caller makes an emergency call, the CESID provides location information for a phone extension on a private network. The information can help direct emergency crews to a caller's location.

CESIDs are public network Listed Directory Numbers (LDNs) that you obtain from a local carrier. You can assign a CESID to:

- Each DN on your network using the CESID Assignment form.
- A device, using the L2 to CESID Mapping form.
- A network zone, using the Network Zones form. Zones are discussed in the Bandwidth Management module.
- The whole system, using the Default CESID form.

When an emergency call is made, the system sends the CESID of the extension out to the PSTN. The CESID is used by the CO to route the call to the local PSAP and then by the PSAP to call up information such as the address, building, floor, area, and callback number. MiVoice Business's CESID support complies with Emergency Services regulations, such as the FCC's Enhanced 911 standards requiring PBXs to support CESIDs.

CESIDs can be manually or automatically updated to maintain current CESID information in the system.

CESIDs and their assigned location information are stored in an ALI database.

CESIDs are not dialable numbers and the data contained in them is only used for outbound Emergency calls. CESID numbers are never displayed to a 3rd party during a routine call.

Note

Different state or provincial regulations may govern the CESID requirements at your location. Some require a unique CESID for every telephone, and others allow the sharing of CESIDs if the telephone users are within sight of one another. One dialable call back number is required for each CESID.

Coordinating CESIDs with the ALI Database

The CESID sent to the PSAP to identify the location of the emergency caller must be the same number that resides in the Automatic Location Information (ALI) database for that location.

The ALI database is independent of MiVoice Business and may reside at the local PSAP, at the CO, or at an independent location. It is essential that CESID numbers and the ALI database remain synchronized when moves, adds, and changes take place. Any changes made to a user's location or data associated with a CESID must be communicated to the ALI database administrator. Ensure that local changes affecting ALI information are kept from going into service until the ALI database has been updated. The System Administrator must ensure that CESID related changes are communicated to the ALI database.

CESID Conditions

- The CESID must be a valid public network 7 or 12 digit Listed Directory Number.

Caution

Starting with MCD Release 6.0, CESIDs up to 12 digits in length are supported. This may have safety implications in networks of older releases that only support 10-digit CESIDs. If you plan to use the longer CESIDs, upgrade the entire network to support the longer CESIDs first.

The same scenario applies to resilient devices. Both the primary and secondary MiVoice Business instances should be upgraded to avoid mismatched CESID lengths under failover/failback conditions.

- A minimum of one L2 connectivity detection protocol, either STP or CDP, must be uniformly and consistently configured on all the L2 switches that the devices are connected to. The administrator must define the same protocol of choice for each MiVoice Business in the network.
- CESID tagging is only supported on ISDN PRI trunks from standalone systems or from within MSDN, which includes systems networked using IP trunks. If there are transit systems between the caller and the outgoing ISDN trunk, the CESID is propagated through the network to the PSAP. This is for MSDN networks only. Sites without ISDN capability should route emergency calls to an attendant or security.
- If ISDN is programmed to block calling number ID, it will ignore this and send the calling number for emergency service calls.
- CESIDs are not associated with location independent entities such as ACD agents and regular Hot Desk users. If an ACD agent or regular Hot Desk user makes an emergency services call, the CESID associated with the originating set is sent.
- For EHDUs logged on to private trunks, the CESID associated with the user's mobile DN is sent.

  For EHDUs logged on to public trunks, the external party's public number is sent as the CESID.

  For EHDUs is logged in over public trunks that provide no calling line identify, the EHDU configured external number is sent as the CESID.

  For EHDUs logged in internally, the CESID associated with the originating set is sent.
- COR and Interconnect Restrictions remain in effect for emergency services calls. Specific users may be restricted from accessing the designated Emergency Services number.
- SMDR output and HCI events are changed in the event of an emergency services call; the prime DN of the originating station is output.

Automatic CESID Updating

- Automatic CESID updating is not supported on hubs where multiple devices report connectivity to the same L2 port, or on L2 switches that do not have CDP or STP enabled. The system detects and logs this condition upon device registration.
- The MiVoice Business portion of the Mitel Emergency Services solution does not support handling of special circumstance DNs. Some DN users have special needs. For example, a DN may be associated with a wheelchair user or with an area where dangerous chemicals are stored. The PSAP may have a record associating a user or DN with this type of special circumstance. If such a device is moved, MiVoice Business treats it like any other device move and attempts to automatically update the CESID Assignment form. This causes the PSAP database to be out of sync with MiVoice Business. To avoid this situation, the administrator should ensure that such DNs are not allowed to move.
- Automatic CESID updating does not function during a database backup or restore.
- A log is generated if the system detects a conflict between CDP and STP data.
- Automatic CESID updating should not be enabled for:
  - Devices in Teleworker mode or devices that are connected outside of the corporate firewall. 911 calls placed from such devices may report an incorrect CESID, or may be outside of the PSAP's coverage area. Devices are not compatible with the Mitel Emergency Services solution when they are operating outside the corporate network serviced by MiVoice Business. The reasons are:
    - A Teleworker device operating outside the corporate network may or may not trigger a device move
    - The system will not be able to accurately assign a CESID to such a device outside the network
    - MiVoice Business will not be able to route the 911 correctly. Note that the system will not block the Teleworker device from making 911 calls, even if they are outside the corporate network. It is not recommended that users make 911 calls from devices operating in Teleworker mode outside the corporate firewall. It is best if the administrator change the CESID Updating state manual for Teleworker enabled devices.
  - Generic SIP phones and the 5302
  - Wireless devices

Note

Device move detection and CESID updating are not supported on non-IP devices.

Emergency Services - CESID Guidelines

- Defining default CESIDs – always define the default CESID for each MiVoice Business in the network. This will act as a last resort if no CESID is available for a particular DN when an emergency call is placed.
- 911 and CESID – for a 911 call to be compliant with FCC guidelines, the call must report a CESID to the PSAP. At a minimum, you must define a CESID for each DN in the CESID Assignment form. In order to ensure that CESIDs are updated when a device is moved and can be correctly reported to the PSAP, promptly investigate and address all CESID-related alarms. You may have to return a phone to its original location if the move was not authorized or update the CESID Assignment and/or L2 to CESID Mapping forms. Alternatively, you can populate the L2 to CESID Mapping form in advance of a device move.
- Defining the primary protocol – consider the difference between STP and CDP, and designate one as your primary protocol in the CESID Assignment form.
- Switching between CDP and STP in the network – the system may detect a false device move if the primary protocol is changed while a device is connected to an L2 switch.
- Enabling Layer 2 (L2) protocol – ensure all L2 switches in the network have the primary protocol enabled.
- New installations – in a new MiVoice Business installation scenario where no database is being restored, it is recommended that you allow the system to auto-discover the L2 Port MAC and L2 Port, as devices are registered, rather than manually entering the information. Auto-discovery ensures that the values are correct, particularly for VLANs, while manual entry can be prone to error. Once the information has been auto-discovered, you can go into the CESID Assignment form or the L2 to CESID Mapping form and enter the CESID for each entry. You may also want to go to other network drops where a phone might be moved to and allow the device to register there as well so that the ports can be auto-discovered. Note that any network drops that do not have a Mitel IP device connected to them will remain undiscovered by MiVoice Business. You can either wait for a CESID alarm to be generated when a device connects to an unknown L2 port, or you can proactively auto-discover L2 data by plugging devices into L2 ports.
- Upgrades – when you restore a database that contains accurate and complete CESID assignments, the L2 to CESID mapping for known devices will be fully and automatically discovered upon device registration. For this to happen, the CESID Assignment data must be accurate prior to the backup and upgrade.
- Backup and restore – device move detection, automatic CESID updating, and alarming do not function during a database backup or restore.
- Maintaining CESID Logs – the CESID Logs form will begin overwriting data, from the oldest to newest entries, when 5000 CESID logs have been posted.

- Replacing L2 switches – if an L2 switch is replaced in the network, MiVoice Business will recognize the event as a device move once the sets re-register through the new L2 switch. Assuming that no new L2 to CESID mappings were manually created for the new switch, the system will clear the CESID values in the CESID Assignment form and raise a CESID alarm.

  So when a switch is replaced, reprogram the CESID assignments for the sets that were connected to the replaced switch. Also, you should delete the old L2 to CESID mappings for the replaced switch, since they are no longer relevant. Alternately, you may wish to set the DNs connected to the retiring L2 switch to Manual CESID updating, as opposed to Automatic, so that the CESIDs don't get cleared.

  Another replacement scenario is that two L2 switches are swapped in the network. Again, MiVoice Business and IP devices will register this swap as device moves, even though it was the switches that were moved and not the devices. In this case, the system will automatically update the CESID Assignment for each moved device, assuming that CESID Assignment was complete prior to the swap. The problem here is that the automatic CESID updating will likely be inaccurate because the L2 swapping will cause the L2 to CESID mapping to become incorrect. For this reason, it is recommended that you delete the CESID assignments before the L2 switches are swapped, update the L2 to CESID mapping, and then the correct CESID assignments to be auto-discovered.

- Retiring an L2 switch – delete the relevant entries from the L2 to CESID mapping form.
- Physically moving a network drop – for automatic CESID updating, the system will not be able to detect when a network drop is physically moved from one location to another, assuming the L2 port connection point remains the same. Be wary of any physical port location changes, such as those done during a re-wiring project. It may happen that if a network drop is physically moved, it will move into a location serviced by a different CESID. It is the system administrator's responsibility to ensure that network drops aren't moved without permission, and to update CESIDs when they are.
- Connecting IP devices to a hub – it is recommended that devices be connected directly to an L2 switch. Avoid connecting IP devices to a hub that is, in turn, connected to an L2 switch. Apart from QoS reasons, IP devices connected directly to a hub will all report the same L2 Port MAC/Port, and the system will not be able to automatically update the CESID for any devices registering to that hub.
- Swapping Ethernet cables on an L2 switch – it is recommended that you do not swap Ethernet cables on L2 switches, such as when troubleshooting a malfunctioning port. The system will see this switch as a device move. The device will report a new L2 connectivity point, even though it was not physically moved. Depending on the configuration, this could result in an automatic CESID update with the wrong CESID, a CESID alarm, or the deletion of the device's CESID. If you must swap Ethernet cables on an L2 switch, be aware of the effect this will have on device detection and CESID assignment.
- Addressing CESID alarms and logs – if a device is moved and the system is unable to assign a CESID to the device at its new location, the system will raise an alarm and log the problem. Monitor the system alarms for such an event, and when it occurs, use the logs, the CESID Assignment form, the L2 to CESID Mapping, and/or the Device Connectivity forms to determine the nature of the problem. Once the problem is understood, you should update the CESID Assignment or L2 to CESID Mapping form. This will ensure that the device has the correct CESID and will clear the alarm once all CESIDs have been assigned.

- Resilient-environment considerations – when a CESID alarm or log indicates a CESID assignment problem has occurred due to a device move in a resilient environment, you must at the very least update the L2 to CESID Mapping form on the primary controller. You should also add/update the same entry on the secondary controller; otherwise, a CESID alarm will be raised again if the device fails to the secondary.
- Resilient Clustered Hot Desking environment considerations – when you change a virtual CESID Assignment for a Registration DN in a Hot Desking environment, based on a device move detection or CESID-related alarm, the Mobile DN user must log out and log back in to the Hot Desk enabled set.
- Resilient environment, mixed cluster – in a case where the primary is a Release 5.x controller, and the secondary is a 4.x controller, automatic CESID updating/alarming and device move detection will not occur for a device that has been moved while it is in service on its secondary controller. When the device fails back to the Release 5.x primary controller, the move will be detected and CESID assignment and alarms will be updated.
- Set firmware considerations – automatic CESID updating/alarming and device move detection will not work unless the sets have the appropriate firmware load. This may be done through a LOAD IP DEVICE 1 to 700 command, by powering down the sets, or by a loss of connectivity with MiVoice Business for 10 minutes or more.
- Teleworkers – Mitel IP devices that are running in Teleworker mode and are connected outside the corporate network through the Mitel Standard Linux (MSL) gateway will not be blocked from making 911 calls, but an incorrect CESID may be reported.
- CDE and automatic CESID updating – it is recommended that you do not use the CDE interface to open and work in the CESID Assignment form. If the CDE interface is open to the CESID Assignment form while the system is attempting to automatically update a CESID based on a device move, the automatic update will fail.

Programming a CESID

Program a CESID for:

- Each DN in the network, or for
- Each device, or for
- Each network zone, or at least
- A default value for the whole system.

When determining the CESID for an emergency call, the system searches appropriate forms in the following order:

- For MiNet IP devices:
  - L2 to CESID Mapping form for CESIDs associated with a device
  - CESID Assignment form for CESIDs associated with a DN
  - Zone CESID field in the Network Zones form for CESIDs associated with a zone
  - Default CESID form for a default CESID associated with the whole system

- For TDM devices, non-MiNET IP/SIP devices, and devices that do not have associated zones:
  - CESID Assignment form for CESIDs associated with a DN
  - Default CESID form for a default CESID associated with the whole system
- For SIP trunks originating 911 calls, the Calling Party number is used instead of a CESID.

To program CESIDs:

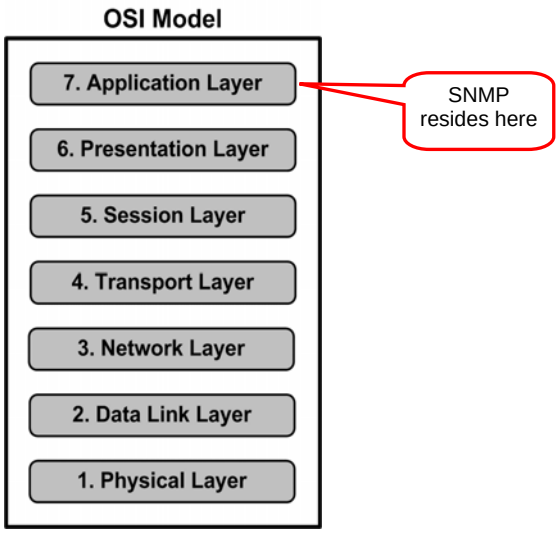
1. In the Class of Service Options form, set Display ANI/ISDN Calling Number Only to Yes.
2. Program ARS for the ISDN trunks:
   - Assign the ISDN trunks in the Trunk Attributes form.
   - Put the trunks into a trunk group, using the Trunk Groups form.
   - Assign the Trunk Group to a route in the ARS Routes form. Designate the route as an Emergency route.
   - Add an entry in the ARS Digits Dialed form for 911. Use digits dialed 911, with no digits to follow, and point it to the Emergency route. There are additional considerations if multiple emergency dialing strings are necessary for different geographic regions within a cluster. Emergency dialing strings must be COR restricted if the telephone set location is not served by the PSAP.
3. Program CESID information using one of the following:
   - In the CESID Assignment form, assign a CESID number to each DN, which can be either a registration or mobile DN. The MAC address of the Layer 2 switch port and the Layer 2 switch port identifier are detected by the system when an IP phone registers.

     You also have the option of manually assigning the MAC Address and port identifier to the Layer 2 switch ports in the L2 to CESID Mapping form.
   - In the L2 to CESID Mapping form, assign a CESID number to a device.
     - The L2 Port MAC field displays the MAC address of the Layer 2 switch port. The MAC address is detected by the system when an IP phone registers. You also can manually assign the L2 switch port MAC address during an Add operation, but not during an Edit operation.
     - The L2 Port field displays the identifier of the port. The port identifier is detected by the system when an IP phone registers. You can also manually assign the L2 switch port identifier during an Add operation, but not during an Edit operation.
     - Assign a CESID to each Layer 2 switch port.
   - In the Network Zones form, assign a Zone CESID number to each network zone. This programming is particularly important for Location Based Call Routing. Since the Network Zones is a shared form, if an emergency call is routed to a different zone, the system will still be able to retrieve the CESID information and locate the calling device using the Default Zone ID.
   - In the Default CESID form, assign a default CESID number for the whole system.

Simple Network Management Protocol (SNMP)

The Simple Network Management Protocol (SNMP) is an application layer protocol that facilitates the exchange of management information between network devices. SNMP is part of the TCP/IP protocol suite.

SNMP allows network administrators to manage network devices, monitor alarms, and pass information to other network devices that are configured to receive SNMP information.



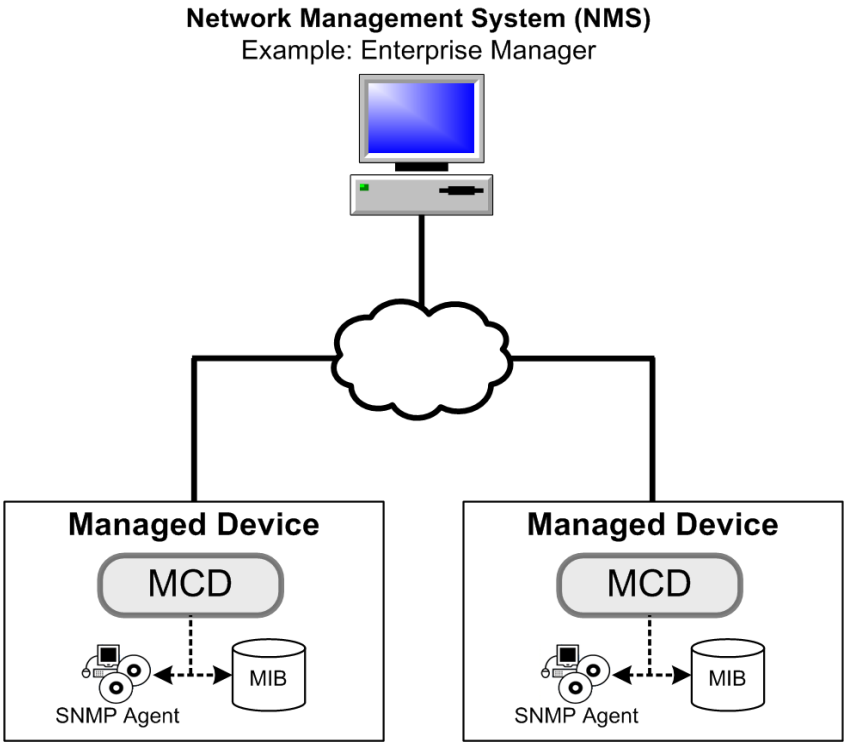
SNMP Components

An SNMP managed network consists of two basic components:

- Managed Devices
- Network Management Systems

A Managed Device is an IP network device that contains an SNMP agent and resides in a managed network. Managed devices collect and store a list of managed objects called Management Information Bases (MIBs) and make the MIB information available to Network Management Systems (NMSs) using SNMP. Managed devices, sometimes called Network Elements or Nodes, can be routers, switches and bridges, printers, or a MiVoice Business system. An Agent is a Network Management software module that resides in a Managed Device. An agent has local knowledge of MIB information and translates that information into a format compatible with SNMP.

A Network Management System executes application software that monitors and controls managed devices. Mitel Enterprise Manager is an example of an NMS that manages network nodes using SNMP.



SNMP Execution

SNMP uses five basic messages to communicate between the NMS and the SNMP agent located on a Managed Device:

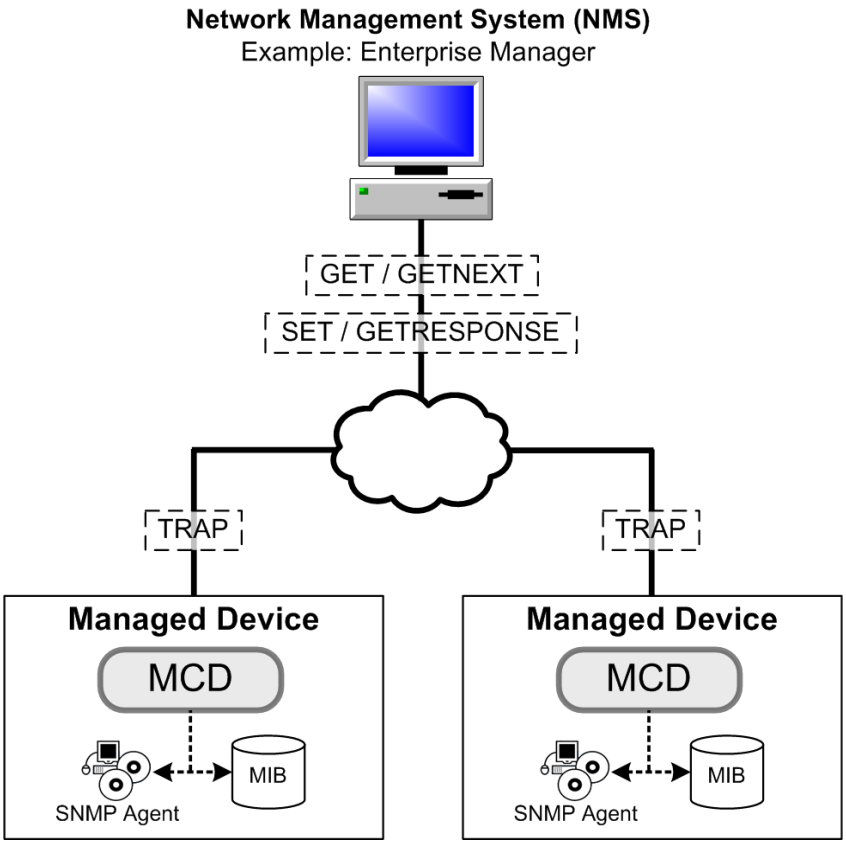
- Get
- GetNext
- GetResponse
- Set
- Trap

The Get and GetNext messages allow the NMS to request information for a specific variable on a Managed Device. Upon receiving a Get or GetNext message, the SNMP agent, running on a Managed Device, issues a GetResponse message to the NMS with either the information requested or an error indication as to why the request cannot be processed.

A Set message allows the NMS to request a change to the value of a specific managed variable. For example, when an alarm is detected on a managed device, the Set message can clear the alarm. Keep in mind if the condition that generated the alarm is not resolved, the Set message can not clear the alarm.

The SNMP agent then responds to the Set message with a GetResponse message, indicating the change has been made or an error indication as to why the change cannot be made.

The Trap message allows the SNMP agent to immediately inform the NMS of an important event on a managed device. For example, the Trap message is the only message initiated by an SNMP agent and is used by MiVoice Business to report alarms and other information to an NMS. An SNMP Trap immediately notifies an NMS when a predetermined condition occurs, instead of waiting for the NMS to request this information.



Mitel SNMP Traps

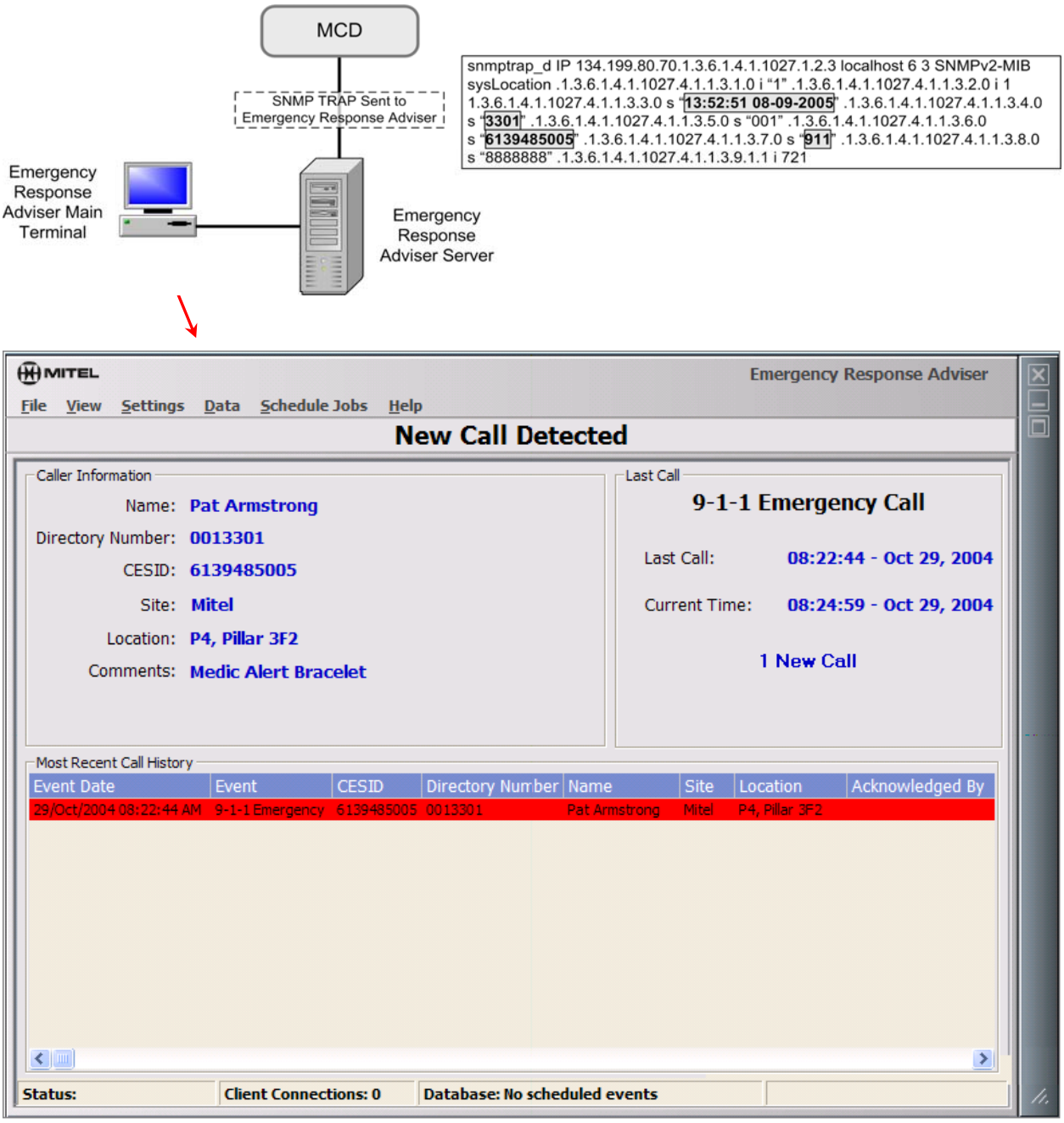
In a MiVoice Business environment, an SNMP trap allows MiVoice Business to automatically send SNMP information to an NMS or other applications that are programmed to receive the information.

For example, Mitel Emergency Response Adviser is an SNMP trap-driven software application that monitors and manages emergency calls. It waits for an appropriate SNMP Trap sent from MiVoice Business and acts on it. When Emergency Response Adviser receives an SNMP trap, it compares the trapped information with information programmed in its database. If a match occurs, Emergency Response Adviser logs the emergency call and automatically displays information about the emergency call and the caller on a client PC.

MiVoice Business must be programmed to send an SNMP trap to Emergency Response Adviser when a caller dials an emergency number.

An example of a Mitel SNMP trap sent to Emergency Response Adviser may contain the following information:

- Time and Date = 13:52:51 08-09-2005
- Directory Number (DN) = 3301
- CESID Number = 6139485005
- The Call Type = 911

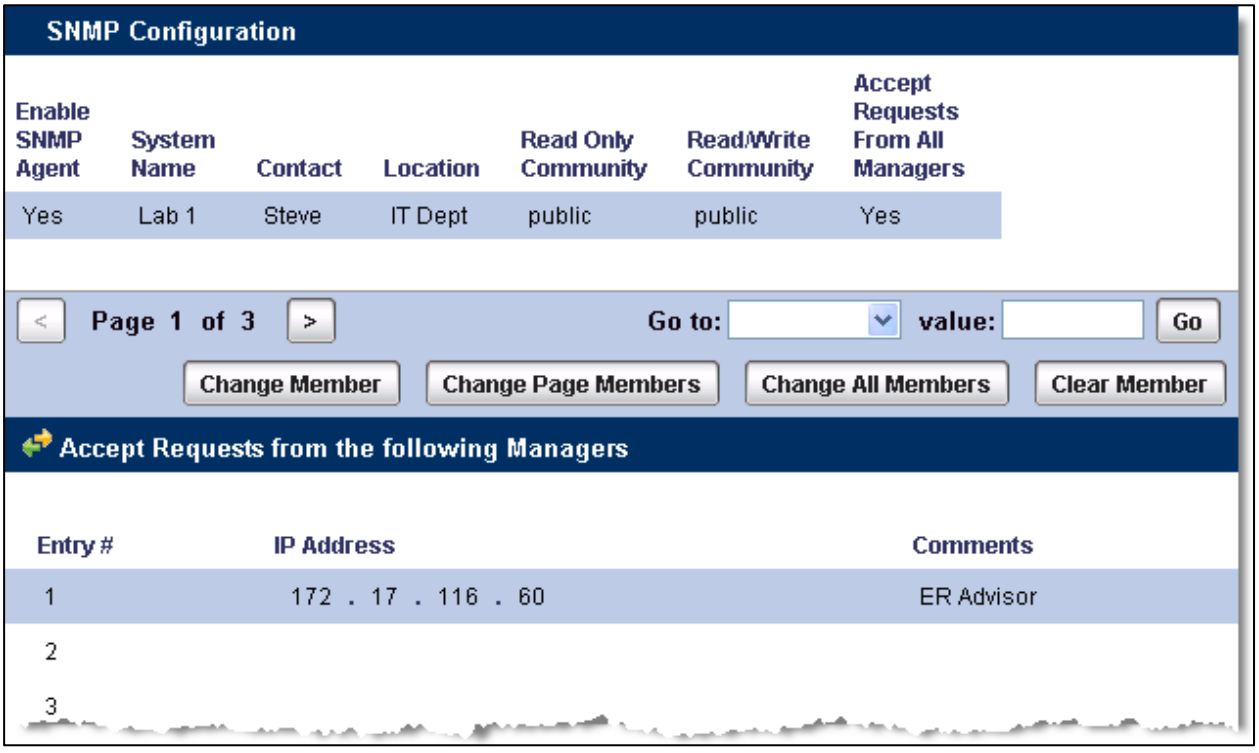

MCD
SNMP TRAP Sent to Emergency Response Adviser
snmptrap_d IP 134.199.80.70.1.3.6.1.4.1.1027.1.2.3 localhost 6 3 SNMPv2-MIB sysLocation .1.3.6.1.4.1.1027.4.1.1.3.1.0 i "1" .1.3.6.1.4.1.1027.4.1.1.3.2.0 i 1 1.3.6.1.4.1.1027.4.1.1.3.3.0 s "13:52:51 08-09-2005" .1.3.6.1.4.1.1027.4.1.1.3.4.0 s "3301" .1.3.6.1.4.1.1027.4.1.1.3.5.0 s "001" .1.3.6.1.4.1.1027.4.1.1.3.6.0 s "6139485005" .1.3.6.1.4.1.1027.4.1.1.3.7.0 s "911" .1.3.6.1.4.1.1027.4.1.1.3.8.0 s "8888888" .1.3.6.1.4.1.1027.4.1.1.3.9.1.1 i 721
Emergency Response Adviser Main Terminal
Emergency Response Adviser Server
MITEL
Emergency Response Adviser
File View Settings Data Schedule Jobs Help
New Call Detected
Caller Information
Name: Pat Armstrong
Directory Number: 0013301
CESID: 6139485005
Site: Mitel
Location: P4, Pillar 3F2
Comments: Medic Alert Bracelet
Last Call
9-1-1 Emergency Call
Last Call: 08:22:44 - Oct 29, 2004
Current Time: 08:24:59 - Oct 29, 2004
1 New Call
Most Recent Call History
Event Date | Event | CESID | Directory Number | Name | Site | Location | Acknowledged By
29/Oct/2004 08:22:44 AM | 9-1-1 Emergency | 6139485005 | 0013301 | Pat Armstrong | Mitel | P4, Pillar 3F2
Status:
Client Connections: 0
Database: No scheduled events

Programming SNMP

Use the SNMP Configuration form to provide configuration settings that control the functional behavior of SNMP agents.

To enable an SNMP agent:

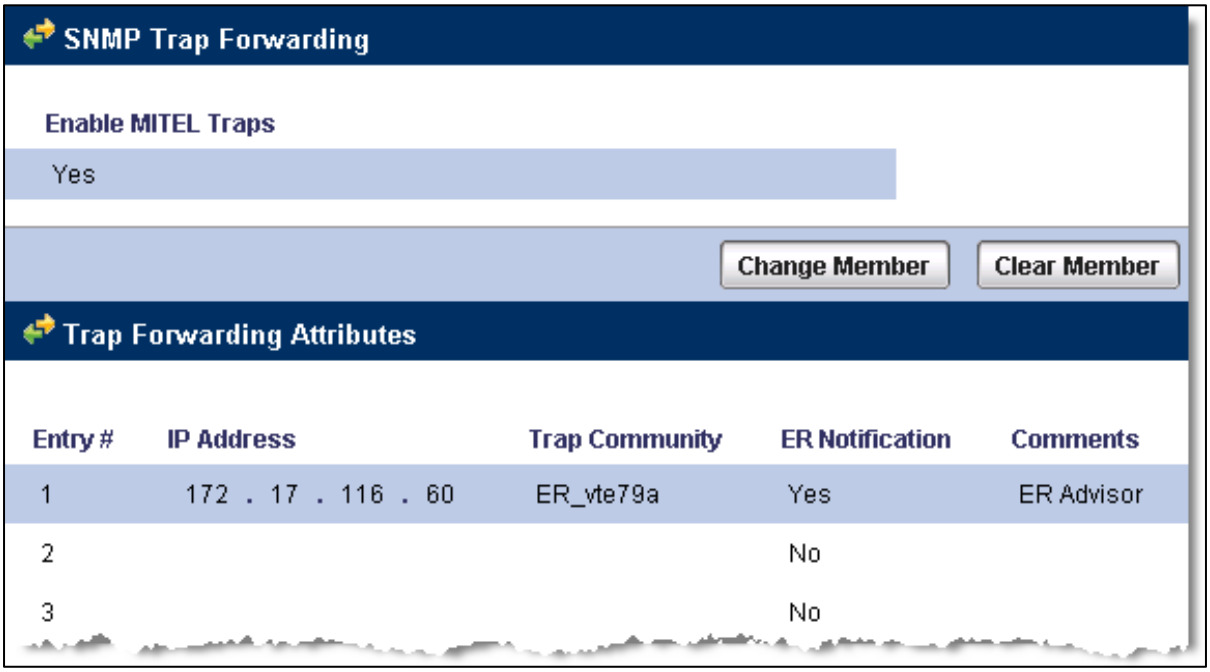
- Set the Enable an SNMP Agent field to Yes.
- Verify or enter the MiVoice Business system name.
- Enter optional contact and location information.
- Enter the Read/Write community names of the SNMP agent. The default value is Public. For example, the text entered in these fields is inserted into the SNMP Community String, or message, and is passed between an SNMP agent and a NMS. The entries in these fields must match those of the SNMP agent or communication between the SNMP devices will fail. Contact your network administrator to validate these entries.
- Enter a value in the Accept Requests From All Managers field. Select Yes to indicate the SNMP agent will respond to all SNMP Manager requests. The default value is Yes. Select No to indicate only SNMP Managers with IP addresses programmed in the Accept Requests from the following Managers field.
- If you select No in the Accept Requests From All Managers field, enter the IP address of each SNMP managed device. In the Comment field, give the managed device a name for easy reference.



SNMP Trap Forwarding Form

Use the SNMP Trap Forwarding form to program trap configuration settings to enable easy identification of trap message destinations.

- Enable Mitel Traps – select Yes to send Mitel traps to specific SNMP managers. Selecting No, which is the default, indicates that no trap messages will be dispatched. After you enable or disable Mitel traps, there is a 100-second delay before the setting takes effect.
- Trap Forwarding Attributes – enter the IP address of each SNMP manager who may receive trap messages. Up to 10 entries.
  - Trap Community – enter the Trap Community Name of the corresponding SNMP Manager. Up to 20 characters.
  - ER Notification – enter Yes to identify the SNMP manager that receives notification. For example, Emergency Response Adviser. The default is No. Only one SNMP manager can have the ER Notification field set to Yes.
  - Comments – enter information to identify the corresponding IP address. Up to 20 characters.



Programming and Review of CESID Information

Note

STP or CDP must be activated on the Layer 2 switch.

You will:

- Program Emergency Services Management.
- View and interpret Emergency Services calls that appear on a display phone.
- View and interpret CESID Logs.

In addition to the ARS forms, you will be using the:

- Emergency Services Management > **Default CESID** form.
- Emergency Services Management > **CESID Assignment** form.
- Emergency Services Management > **L2 to CESID Mapping** form.
- Users and Devices > Group Programming > **Hunt Groups** form.
- Maintenance and Diagnostics > IP Telephone Inventory > **Device Connectivity-Moved** form.

Step	Task	Expected Result/Observation	✓
1	Program all required ARS forms to support emergency call handling. Caution must be taken if you program an actual emergency call number like 911. Verify your emergency routes are set to Route Type = Emergency.	ARS is programmed for emergency calls.	
2	Program the **Default CESID** form. • Enter a default CESID number. • Select an L2 Connectivity Protocol. • Enable Automatic CESID Updating.	The Default CESID form is programmed.	

Step	Task	Expected Result/Observation	✓
3	Program the **CESID Assignment** form. • Assign a CESID number to selected DNs. • Enter CESID location information in the CESID Comments field. **CAUTION:** This comment field does not update automatically and is only used for internal reference. • Enable Automatic CESID Updating. • Set Route Emergency Calls to Through System Only. • Print or Export a copy of the CESID Assignment form for L2 MAC address. OR • Reboot the IP sets to automatically update the L2 to CESID Mapping Form.		
4	Program the **L2 to CESID Mapping** form. If the IP sets were reset, this form should be automatically populated, otherwise you will need to manually add the MAC Address and CESID Numbers. For each L2 Port: • Add the MAC Address of the L2 Port. • Add the L2 Port Number. • Add the CESID number assigned to the L2 Port Number.	Since CESIDS have already been assigned, a reboot of the phones will fill in the L2 to CESID table automatically.	
5	In the COS Options for the sets and attendant console that will be alerted on an emergency call: • Set Emergency Call Notification - Audio to Yes • Set Emergency Call Notification - Visual to Yes	The specified devices will provide both audio and visual indications of an emergency call.	
6	Program the **Hunt Groups** form. • Create a new Hunt Group as an Emergency Group Type. • Add members to the Emergency Hunt Group. Do not place the Attendant Console in the Emergency Hunt Group.		
7	Program an Emergency Call Notification Key on a display phone who is a member of the Emergency Hunt Group.		

Step	Task	Expected Result/Observation	✓
8	Move an IP phone to a new L2 port. • Verify that the IP phone moved to the new L2 MAC address and port as shown in the **CESID Logs** form. • Verify the new CESID number in the **CESID Assignment** form.		
9	Verify that the IP phone moved to the new L2 MAC address and port in the **Device Connectivity** form.		
10	Return the IP sets to their original ports.		
11	Delete the Emergency Hunt Group.		

Local Emergency Calls

Programming Emergency Calls Using ARS (NA Only)

You will be using the following forms, in this order:

- Call Routing > Automatic Route Selection (ARS) > **ARS Routes** form.
- Call Routing > Automatic Route Selection (ARS) > **ARS Digits Dialed** form.

Caution

Always allow all desktop devices to dial emergency numbers. The COR Group Number used for the Emergency Routes must not contain any COR Numbers.

Define Route Number for 911

Step	Task	Expected Result	✓
1	In the **ARS Routes** form, double-click on an available Route Number; Route 2. **NOTE:** It is best practice to use the same number as the COR Group Number that will be used, and that COR Group Number must NOT contain any COR Numbers.	The ARS Routes change window opens.	
2	In the ARS Routes change window: • Select SIP Trunk from the Routing Medium drop-down menu. • Select the SIP Peer Profile to be used. • Enter a COR Group Number that contains no COR Numbers. • Enter a Digit Modification Number that absorbs no digits; Digit Modification Number 1. • Leave the Digits Before Outpulsing field blank. • Select Emergency from the Route Type drop-down menu. Click Save.	The data is displayed in the ARS Routes form.	

Define Route Number for 9-911

It is quite possible that a phone user might attempt to dial the leading 9 to get an outside line. This programming will alleviate that problem.

Step	Task	Expected Result	✓
3	In the ARS Routes form, double-click on an available Route Number; Route 3. **NOTE:** It is best practice to use the same number as the COR Group Number that will be used, and that COR Group Number must NOT contain any COR Numbers.	The ARS Routes change window opens.	
4	In the ARS Routes change window: • Select SIP Trunk from the Routing Medium drop-down menu. • Select the SIP Peer Profile to be used. • Enter the COR Group Number that contains no COR Numbers. • Enter the previously programmed Digit Modification Number that absorbs one digit; Digit Modification Number 2. • Leave the Digits Before Outpulsing filed blank. • Select Emergency from the Route Type drop-down menu.	The data is entered, saved, and displayed in the ARS Routes form.	

Route Call Based on Digits Dialed

Step	Task	Expected Result	✓
5	In the **ARS Digits Dialed** form, add the following: • 911, absorbing no digits. Select the route created in the previous step for 911 calls. • 9-911, absorbing one digit. Select the route created in the previous step for 9911 calls. Digits to Follow must be zero.	911 and 9911 digit strings are added. 9911 is added just in case an emergency caller tries to dial a 9 to make an external call.	

Programming Emergency Calls Using ARS (EMEA Only)

You will be using the following forms, in this order:

- Call Routing > Automatic Route Selection (ARS) > **ARS Routes** form.
- Call Routing > Automatic Route Selection (ARS) > **ARS Digits Dialed** form.

Caution

Always allow all desktop devices to dial emergency numbers. The COR Group Number used for the emergency routes must not contain any COR numbers.

Define Route Number for 999 and 112

Step	Task	Expected Result	✓
1	In the **ARS Routes** form, double-click on an available Route Number; Route 2. **NOTE:** It is best practice to use the same number as the COR Group Number that will be used, and that COR Group Number must NOT contain any COR Numbers.	The ARS Routes change window opens.	
2	In the ARS Routes change window: • Select SIP Trunk from the Routing Medium drop-down menu. • Enter the COR Group Number that contains no COR Numbers. • Enter a Digit Modification Number that absorbs no digits; Digit Modification Number 1. • Leave the Digits Before Outpulsing field blank. • Select Emergency from the Route Type drop-down menu.	The data is displayed in the ARS Routes form.	

Define Route Number for 9-999 and 9-112

Step	Task	Expected Result	✓
3	In the ARS Routes form, double-click on an available Route Number; Route 3. **NOTE:** It is best practice to use the same number as the COR Group Number that will be used, and that COR Group Number must NOT contain any COR Numbers.	The ARS Routes change window opens.	
4	In the ARS Routes change window: • Select SIP Trunk from the Routing Medium drop-down menu. • Enter the COR Group Number that contains no COR Numbers. • Enter the previously programmed Digit Modification Number that absorbs one digit; Digit Modification Number 2. • Leave the Digits Before Outpulsing filed blank. • Select Emergency from the Route Type drop-down menu.	The data is entered, saved, and displayed in the ARS Routes form.	

Route Call Based on Digits Dialed

Step	Task	Expected Result	✓
5	In the **ARS Digits Dialed** form, add the following: • 999, absorbing no digits. Select the route created in the previous step for 999 calls. • 9-999, absorbing one digit. Select the route created in the previous step for 9999 calls. • 112, absorbing no digits. Select the route created in the previous step for 999 calls. • 9-112, absorbing one digit. Select the route created in the previous step for 9999 calls. Digits to Follow must be zero.	999 and 9999 digit strings are added. 9999 is added just in case an emergency caller tries to dial a 9 to make an external call.	

Hot Desk Emergency Services

Hot Desk Users are assigned DNs and User PINs through the Multiline IP Sets form or User and Services Configuration form.

When a user logs in to a Hot Desk Set, the system associates the user's DN, COS/COR settings, display preferences, and button programming with the set.

The system, however, continues to use the Customer Emergency Services ID (CESID) programmed for the set's registration DN. For example, if someone makes an emergency call from a Hot Desk Set, the system sends the CESID associated with the Hot Desk Set regardless of which profile (set or user) is active on the phone. If the set's registration DN is not available, the system sends the default CESID.

For networked Hot Desking, Location Based Routing (LBR) can be used to identify the location of a Hot Desk User calling from across the network. For example, LBR allows you to program the system to route emergency calls to services local to the device from which the user dials.

EHDU Emergency Services

When a user logs into a Hot Desk Set, the system associates the user's settings, such as DN, COS/COR settings, display preferences, and button programming, with the set.

For EHDUs logged on to Private Trunks, the system uses the CESID associated with the user's mobile DN.

For EHDUs logged on to Public Trunks, the system uses the external party's public number as the CESID.

For EHDUs logged on to Public Trunks that provide no CLID, the EHDU's configured external number is used as the CESID.

For EHDUs logged in internally, the CESID associated with the originating set is used.

Reference

CESIDs are covered in the MiVoice Business Networking, Clustering, and Resiliency I&M course.

For local notification in SMDR logs and at Attendant Consoles, the system displays the DN and name of the active profile, if available. If a Hot Desk User is logged in, the user's DN and name are displayed.

Caution

Emergency calls should not be made from an EHDU device since the call cannot be guaranteed to contain the correct location information. Mitel assumes no legal, financial, or personal responsibility for users or persons performing such actions.

Emergency Services for SIP Phones and Trunks

911 Emergency Services (NA Only)

Generic SIP phones support 911 emergency services and can be assigned a Customer Emergency Services ID (CESID) number. Moves are not automatically reflected in the CESID table. The table must be updated manually.

Emergency Support for Generic SIP Phones – provides:

- CESID when a generic SIP phone makes an emergency call.
- An SNMP event is generated to the Emergency Response Advisor when a generic SIP phone makes an emergency call. The CESID number in the SNMP event must be the default CESID number or a programmed CESID number for the generic SIP phone.

Emergency Services - Location Notification is also supported on Generic SIP phones.

SIP Trunks support 911 emergency services. The SIP Service Provider can be chosen as the outgoing emergency route. The Caller's CESID information must be programmed.