InnoMedia

EMS Administration Guide

Version 2.5.4

May 31, 2018

Table of Contents

1 Preparing to Install the EMS

This document contains important safety information you should know before working with the EMS Use the following guidelines to ensure your own personal safety and to help protect your EMS from potential damage.

1.1 IMPORTANT SAFETY INSTRUCTIONS

Warning This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents

Only trained and qualified personnel should be allowed to install, replace, or service this equipment.

To avoid electric shock, do not connect safety extra-low voltage (SELV) circuits to telephone-network voltage (TNV) circuits. LAN ports contain SELV circuits, and WAN ports contain TNV circuits. Some LAN and WAN ports both use RJ-45 connectors. Use caution when connecting cables. Statement 1021

Warning Before working on a system that has an on/off switch, turn OFF the power and unplug the power cord.

Warning This unit is intended for installation in restricted access areas. A restricted access area is where access can only be gained by service personnel through the use of a special tool, lock and key, or other means of security, and is controlled by the authority responsible for the location.

Warning This product relies on the building's installation for short-circuit (overcurrent) protection. Ensure that a fuse or circuit breaker no larger than 120 VAC, 15A U.S. (240 VAC, 10A international) is used on the phase conductors (all current-carrying conductors).

Warning This equipment must be grounded. Never defeat the ground conductor or operate the equipment in the absence of a suitably installed ground conductor. Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available.

Warning Do not work on the system or connect or disconnect cables during periods of lightning activity.

Warning Before working on equipment that is connected to power lines, remove jewelry (including rings, necklaces, and watches). Metal objects will heat up when connected to power and ground and can cause serious burns or weld the metal object to the terminals.

Warning The safety cover is an integral part of the product. Do not operate the unit without the safety cover installed. Operating the unit without the cover in place will invalidate the safety approvals and pose a risk of fire and electrical hazards.

Warning Enclosure cover serves three important functions: they prevent exposure to hazardous voltages and currents inside the chassis; they contain electromagnetic interference (EMI) that might disrupt other equipment; and they direct the flow of cooling air through the chassis. Do not operate the system unless all covers are in place.

Warning Ultimate disposal of this product should be handled according to all nation laws and regulations.

Warning To prevent bodily injury when mounting or servicing this unit in a rack, you must take special precautions to ensure that the system remains stable. The following guidelines are provided to ensure your safety:

- This unit should be mounted at the bottom of the rack if it is the only unit in the rack.
- When mounting this unit in a partially filled rack, load the rack from the bottom to the top with the heaviest component at the bottom of the rack.
- If the rack is provided with stabilizing devices, install the stabilizers before mounting or servicing the unit in the rack.

1.2 Safety Guidelines

This equipment is intended to be installed by qualified Service Person. The socket outlet will be connected to shall be verified as having protective earthing on the equipment.

To reduce the risk of bodily injury, electrical shock, fire, and damage to the equipment, observe the following precautions.

1.2.1 General Precautions

Observe the following general precautions for using and working with your system:

Opening or removing covers might expose you to electrical shock. Components inside these compartments should be serviced only by an authorized service technician.

- If any of the following conditions occur, unplug the product from the electrical outlet and replace the part or contact your authorized service provider:
  - The power cable, extension cord, or plug is damaged.
  - An object has fallen into the product.
  - The product does not operate correctly when you follow the operating instructions.
  - The product has been exposed to water.
  - The product has been dropped or damaged.
  - The product does not operate correctly when you follow the operating instructions.
- Keep your system components away from radiators and heat sources. Also, do not block cooling vents.
- Do not spill food or liquids on your system components, and never operate the product in a wet environment.
- Do not push any objects into the openings of your system components. Doing so can cause fire or electric shock by shorting out interior components.
- Allow the product to cool before removing covers or touching internal components.
- Use the correct external power source. Operate the product only from the type of power source indicated on the electrical ratings label. If you are not sure of the type of power source required, consult your service representative or local power company.
- Use only approved power cables. If you have not been provided with a power cable for any AC-powered option intended for your system, purchase a power cable that is approved for use in your country. The power cable must be rated for the product and for the voltage and current marked on the product's electrical ratings label. The voltage and current rating of the cable should be greater than the ratings marked on the product.
- To help prevent electric shock, plug the system components and peripheral power cables into properly grounded electrical outlets. These cables are equipped with three-prong plugs to help ensure proper grounding. Do not use adapter plugs or remove the grounding prong from a cable. If you must use an extension cord, use a three-wire cord with properly grounded plugs.
- Observe extension cord and power strip ratings. Make sure that the total ampere rating of all products plugged into the extension cord or power strip does not exceed 80 percent of the extension cord or power strip ampere ratings limit.

- To help protect your system components from sudden, transient increases and decreases in electrical power, use a surge suppressor, line conditioner, or uninterruptible power supply (UPS).
- Position cables and power cords carefully; route cables and the power cord and plug so that they cannot be stepped on or tripped over. Be sure that nothing rests on your system components' cables or power cord.
- Do not modify power cables or plugs. Consult a licensed electrician or your power company for site modifications. Always follow your local or national wiring rules.

1.2.2 Protecting Against Electrostatic Discharge

Static electricity can harm delicate components inside the Content Engine. To prevent static damage, discharge static electricity from your body before you touch any of your system's electronic components. You can do so by touching an unpainted metal surface on the chassis.

You can also take the following steps to prevent damage from electrostatic discharge (ESD):

- When unpacking a static-sensitive component from its shipping carton, do not remove the component from the antistatic packing material until you are ready to install the component in your system. Just before unwrapping the antistatic packaging, be sure to discharge static electricity from your body.
- When transporting a sensitive component, first place it in an antistatic container or packaging.
- Handle all sensitive components in a static-safe area. If possible, use antistatic floor pads and workbench pads.

2 Overview

InnoMedia Element Management System (EMS) is a feature-rich, highly scalable, and highly reliable VoIP device network element management system. It is an ideal solution for streamlining the myriad configuration and management tasks associated with the deployment, operation, and maintenance of Voice-over-IP CPE (Customer Premise Equipment) devices. The EMS is designed with the following objectives: To provide effective element management with flexible Device **Auto-Provisioning** and reliable remote **Device Management** to VoIP service providers.

- To work with devices using various provisioning protocols and configuration file formats.
- To support service providers that require hierarchical or regional partitioning of device classes, as well as scheduled provisioning with reliable provisioning history logs.
- To work with devices operating in various customer premises environments where SOHO router/ NAT may be deployed.
- To work with a multitude of ISP's where SNMP filtering may be taking place.
- To have a reliable fail-over mechanism required by commercial VoIP services.
- To be scalable to meet growing business needs.

With these objectives in mind, InnoMedia EMS offers the following features and capabilities:

Device Management:

- As a VoIP device element management system:
    - Provides a network view of device distribution
    - Allows MIB configuration
    - Provides event, alarm, and fault management
- As a vehicle to access remote devices (which may be behind SOHO routers) with:
    - SNMP, Telnet, and Web access (even for devices behind a NAT firewall)

- Device Status Monitoring, Line Diagnostics, and Performance Analysis:
    - Provides device On-line/Off-line/Registration status monitoring, call statistics and VoIP metrics collection, and performance analysis
    - Ability to perform remote GR909 tests on devices supporting this feature which allows support personnel to diagnose RJ11 port problems such as foreign or hazardous voltages on the RJ11 telephone line, unintended device off-hook, REN overload, and resistive fault

Device Auto-Provisioning:

- Provisioning protocols: Support TFTP, HTTP, and HTTP with security
- Configuration file formats: INI (tag="value"), XML, Column Separated Value (tag:value), and TLV
- Device initiated or server scheduled provisioning
- Provisioning history records

System Architecture: Hierarchical, reliable, and scalable, and Geographically Redundant:

- It allows devices to be hierarchically structured with layered regions and multiple device types. The hierarchical structure can be used for flexible device query and device provisioning with multiple inheritances.
- It is highly reliable with active-standby failover redundancy for High Availability (HA). The HA algorithm randomly determines which server is active Master after system power-up. Upon failure of the active server, the standby server will assume the Mastership role and will not relinquish it, if the previously active server does not come back online within 5 minutes.
- With a distributed architecture, it is highly scalable by allowing multiple instances for all its components to be deployed in multiple servers, thus providing the system with the ability to scale up linearly for mass device deployment as well as enhanced system redundancy.
- The EMS's Geographical redundancy feature allows operators to host two systems, each in different geographical locations. This provides the flexibility to deliver services even when the operational system is not available, or becomes unreachable for any reason, including a natural disaster. Please see "Appendix A. Geographical Redundancy Design" for further details of the design of the Geographical redundancy feature.

Furthermore, the InnoMedia EMS provides a web-based and customizable dashboard interface, allowing the system administrator to have a quick overview of the whole system's statistical data and to query individual device status and current configuration information.

The InnoMedia's EMS requires the client devices to have an embedded EMS gateway module which has the ability to send heartbeat messages to the EMS, relay SNMP requests forwarded from EMS to its local SNMP module, and also relay TCP packets between the device and the EMS gateway.

3 Launching the EMS GUI

The Element Management System (EMS) provides a graphical, secure, web-based interface that allows system administrators to manage the client devices, such as InnoMedia MTAs, and ESBCs. This section will show you how to log into the EMS's web-based GUI.

NOTE: Depending on the license purchased and components installed, you will have access to the Device Management, or Auto-Provisioning, or both components of the EMS.

3.1 Before You Begin

Before you can work with the EMS, you must have the following:

- A web browser loaded on your machine, such as Internet Explorer 7.0 or higher, Firefox 3.6 or higher, or Google Chrome.
- Access to the Internet or the network that hosts the EMS server machine.

You must also know the IP address or the name of your EMS host. This information is used to access the web page that contains the links to the GUI system utilities. This web address can be expressed as:

http://<IP address or Domain name of EMS>/ems/

or https://<IP address or Domain name of EMS>/ems/ (for systems configured with secured access)

An example of this web address could be:

http://10.10.10.1/ems/

3.2 Logging In

1. Start your web browser, such as Microsoft Internet Explorer or Firefox, from your computer and enter the web address of the EMS. The Login screen appears.

NOTE: If your web browser has the pop-up blocker enabled, please allow pop-ups for the EMS web Site.

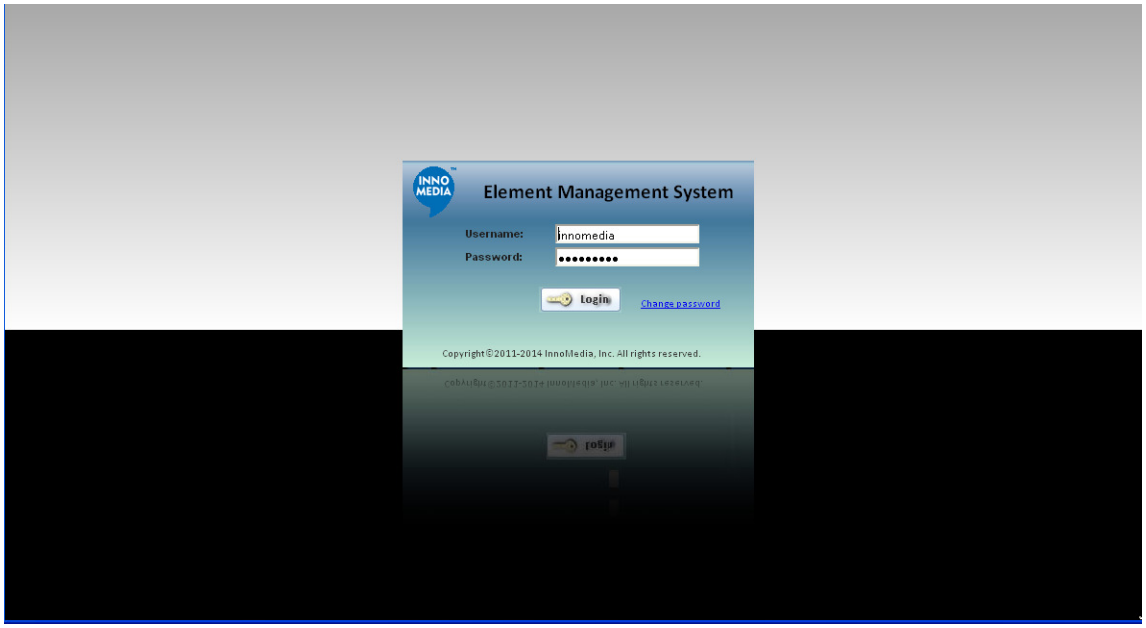


Figure 3.1

2. Enter your username and password, and then click the Login button.

NOTE: If this is a newly installed system, please use the default username and password to login. The default username and password is "innomedia". For security reason, InnoMedia recommends you to change the username and password after initially logging in.

3. (Optional) Click either Enterprise Session Border Controller or VoIP Device to enter the Device Management main page if asked.

Figure 3.2. Selecting Device Category

3.3 Password Change

Users can change their password by clicking “Change password” which is near the “Login” button on the login screen.

Users will be prompted with the following password change screen where they are prompted to enter existing password and enter new password. After entering and changing password successfully, the system will direct the user to the main login screen again.

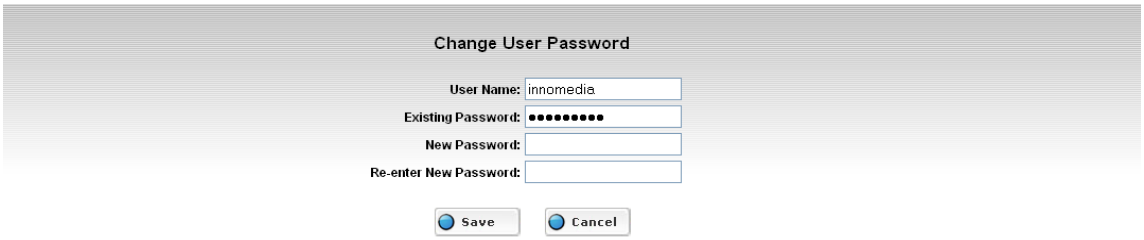


Figure 3.3

There is a time limit (as set by the EMS administrator) when the password will expire. Users who go beyond this time limit, will be prompted with the password change warning screen for up to 30 days..

Figure 3.4

If the password is not changed within the 30 day grace period, then the user's password will expire and they will get the following message the next time they attempt to login, and will be requested to contact the administrator who will then need to reset the users password and notify the user.

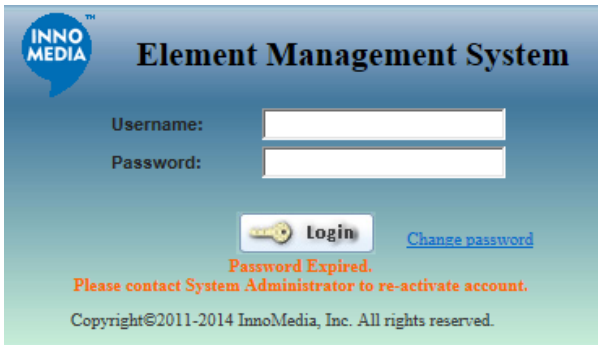


Figure 3.5

3.4 Logging Out

To log out EMS GUI, Click the  icon to complete the log out.

4 Administrator Account Management

The Administrator Account Management interface allows the system manager to configure the administrator groups, user accounts, and web GUI menu. Each administrator will be assigned to an administrator group with different group access rights.

NOTES:

The Administrator Account Management interface is only accessible to the system manager with all the access rights. A system manager account is created by the EMS system as a default.

All administrators need to have their unique user names and passwords for using the EMS web-based GUI interface.

To access the Administrator Configuration Page, follow these steps:

1. Login to the EMS GUI with your user name and password.

2. Click the System Administration icon. 

4.1 Add, Edit and Delete Account and Group Information

4.1.1 Administrator Group Configuration

The EMS allows multiple users to login to the system. In order to give them a user administrator access rights, you need to add them to the Admin User Group. To do so, make sure you are logging in as Administrator or a profile on the system which has Admin rights.

4.1.2 Access Administrator Groups Screen

1. Click the System Administration icon. 

2. Select [Group] tab.

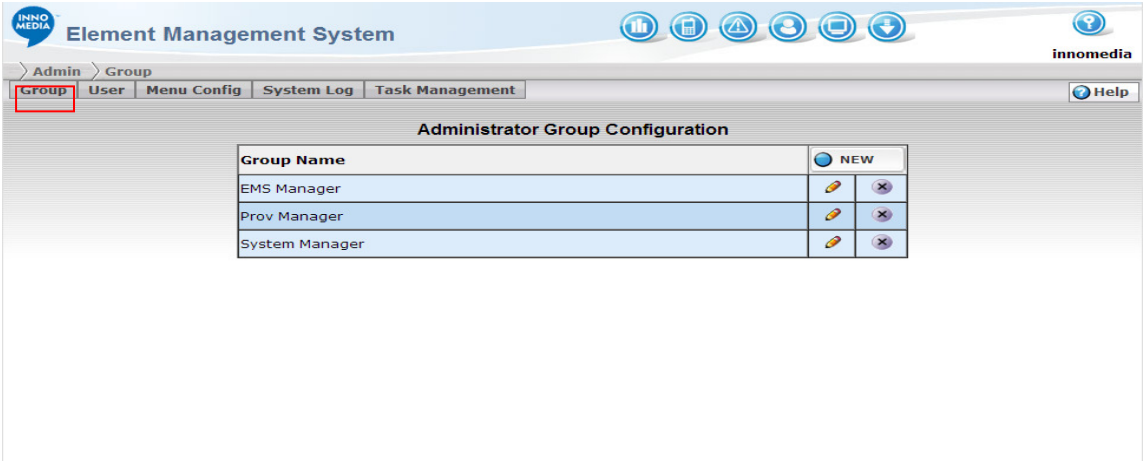


Figure 4.1. Administrator Group Configuration

4.1.3 Adding Administrator Groups

1. Click the Group tab on the System Administration Screen.
2. Click NEW  to add a new Administrator Group.

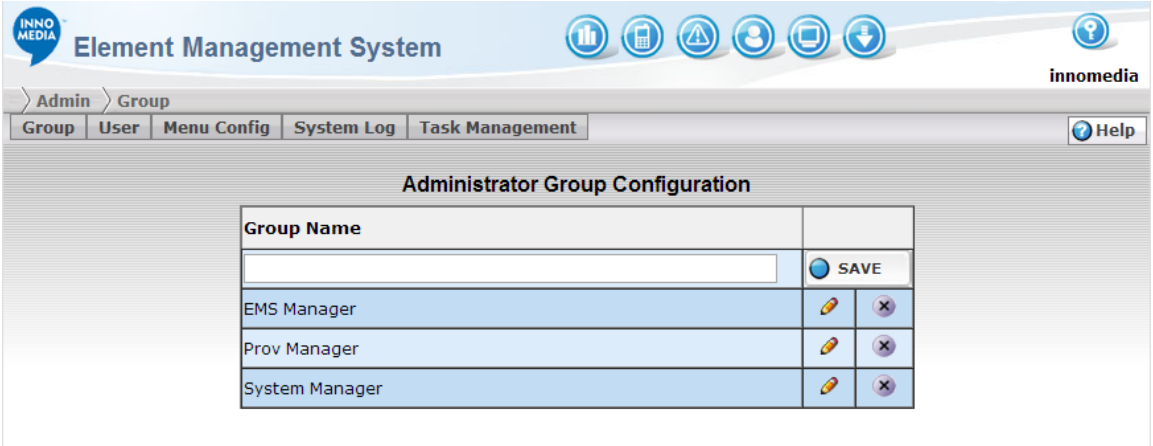


Figure 4.2. Administrator Group Configuration

3. Enter the group name in the Group Name field.
4. Click the SAVE button  to submit the new entry.
5. Follow the instruction described in Administrator Group Configuration on page 21 to configure the group access rights.

4.1.4 Editing Administrator Groups

1. Click the  button of the Administrator Group. The Page Access Permission screen appears.

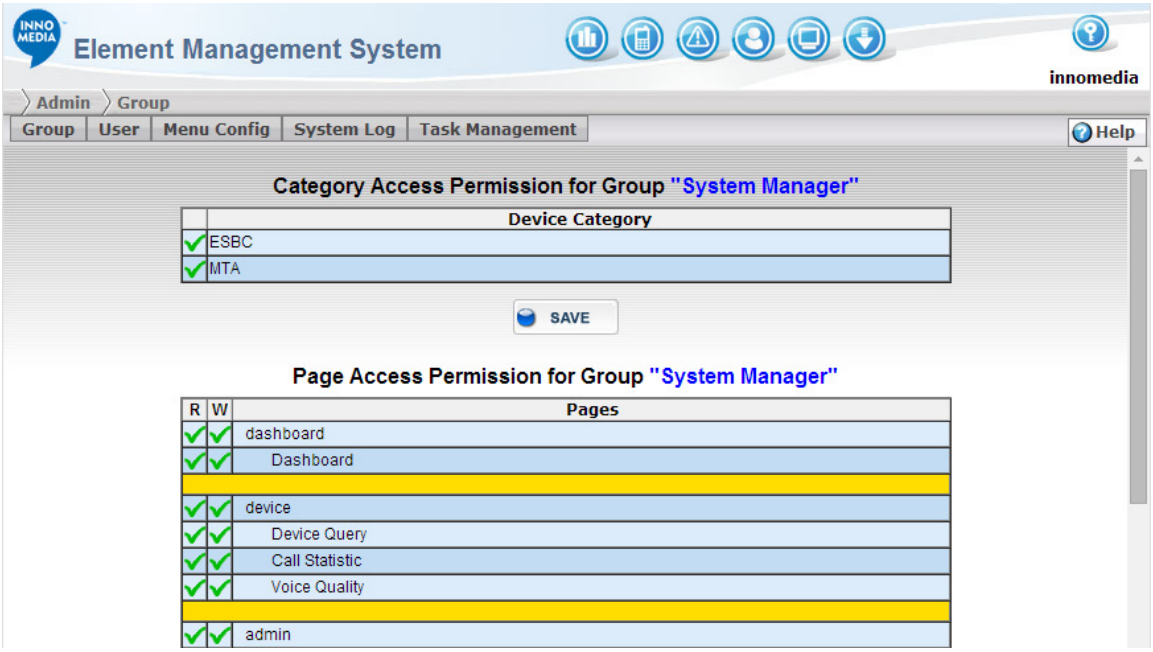


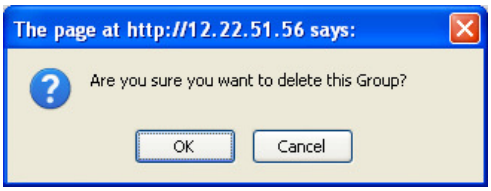
Figure 4.3. Administrator Group Configuration

2. Edit the Page Access permission by clicking on the R (read permission) and W (write permission) fields.
3. Click the SAVE button 

to submit your changes.

4.1.5 Deleting Administrator Groups

1. Click the button to the right of the Administrator Group record. A dialog box appears with the following message:



2. Click OK to remove the Administrator Group from the table list.

4.2 Administrator User Configuration

All administrators must be assigned to a user group and have a unique user name and password for accessing the EMS web-based GUI interface.

This section describes how to access the Administrator Configuration screen and configure administrator accounts.

NOTE: The system manager account was created by the EMS system by default. It has all the privileges to access the EMS web-based GUI.

4.2.1 Accessing Administrator User Configuration Screen

To access the Administrator User Configuration screen, follow these steps:

1. Login to the EMS GUI with your user name and password.
2. Click the Admin icon. 
3. Select [User] tab. Administrator User Configuration screen appears.

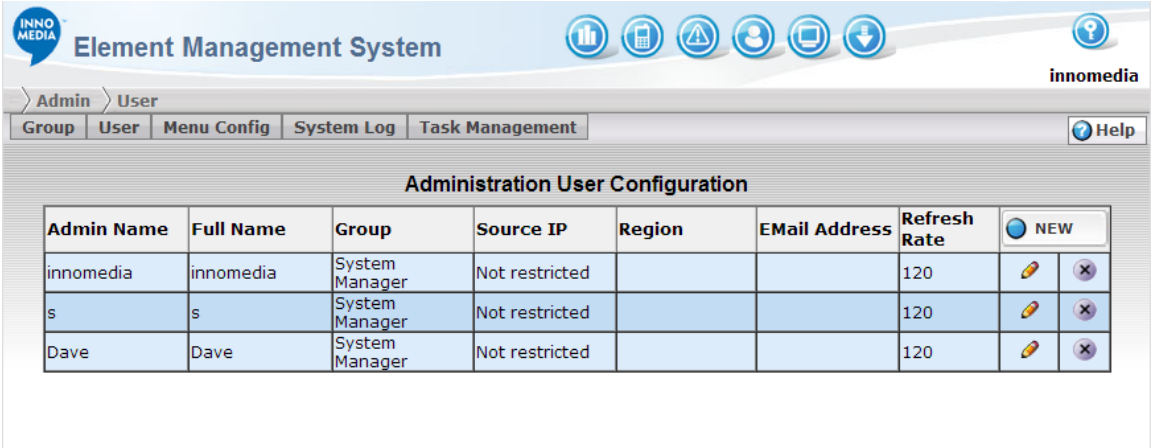


Figure 4.4. Administrator User Configuration

4.2.2 Adding an Administrator Account

To add an administrator account, follow these steps:

1. Click the NEW button.  The Admin Detail Information Screen appears.
2. Fill in the fields then click. 

Field Description

Field	Description
Admin Name	Login ID of the administrator for accessing the EMS web-based interface. It has to be unique. Please use combination of letters {a-z}, {A-Z}, digit {0-9}, and characters from {!@#$%&*()_-} Admin Name should not exceed 38 characters. **NOTE:** Login ID is case sensitive.
Password	Password is the security passphrase for accessing the EMS GUI. Please use combination of letters {a-z}, {A-Z}, digit {0-9}, and characters from {!@#$%&*()_-} Password should not exceed 38 characters. **NOTE:** Password is case sensitive.
Confirm Password	Re-enter the password for confirmation.

Full Name	Full name of the administrator
Group	The administrator Group that the administrator belongs to
Email Address	E-mail address of the Administrator (optional).
Refresh Rate	The interval for life data update
Last Password Update	The date that the password was updated last time
Password Expired after	How long the current password will expire.
Source IP Address	If specified, the user can only access the web GUI from the assigned source IP address (optional).
Region	The regions that the administrator has the access rights to (optional). If you have configured the Region Rights for this administrator, the allowed regions will show in the field. **NOTE:** The configuration on the Region Rights screen will override the information entered in this field.

4.2.3 Editing an Administrator Account

To edit an existing administrator account, follow these steps:

1. Click the  button to the right of the administrator account record. The Admin Detail Information screen appears.

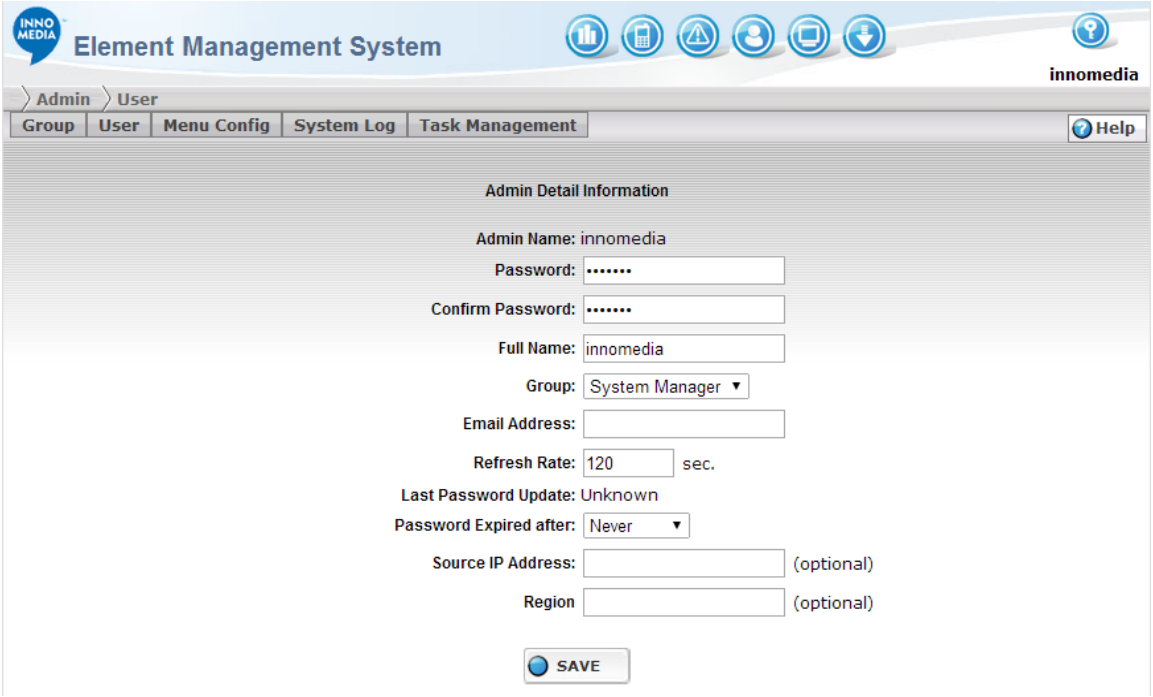


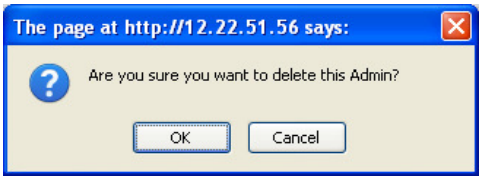
Figure 4.5. Administrator Detail Configuration

2. Make your changes
3. Click the Save button  to submit your changes.

4.2.4 Delete an Administrator Account

To delete an administrator account, follow these steps:

1. Click the button of the administrator account record. A dialog box appears with the following message:



2. Click [OK] to remove the administrator account from the table list.

4.3 System Log

System Log screen allows the system administrator to manage log records. All activities including any inserts, updates, deletes and login/logout will be recorded in the database. This section describes how to access the System Log screen, search and delete log records.

4.3.1 Accessing the System Log Screen

To access the System Log screen, follow these steps:

1. Click Admin icon. 
2. Select [System Log] tab.

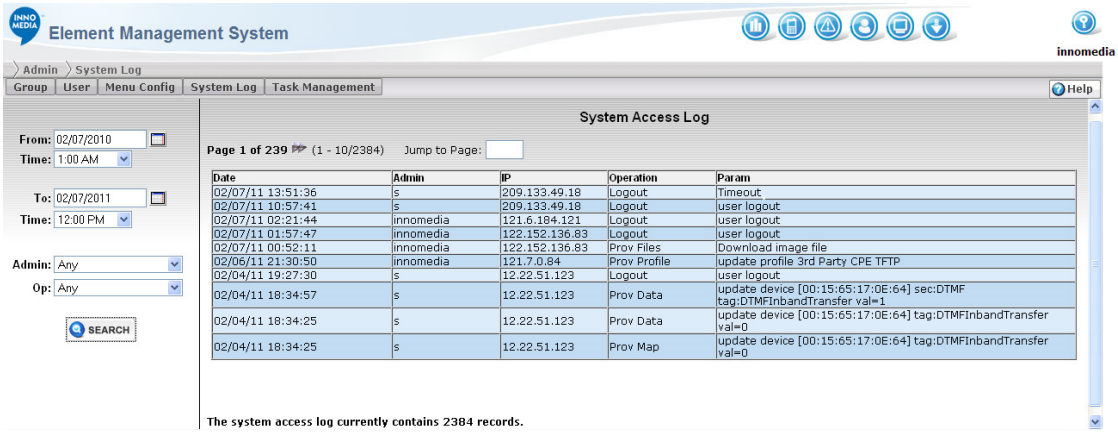


Figure 4.6. System Access Log

Log Table Field Description

Field	Description
Date:	The time when the log was generated.
Admin	The Administrator that triggered this log.
IP	The IP address of where the Administrator accessed the system from.
Operation	The operation type of the log.

Param	Extra information for the operation.

4.3.2 Searching for Log Records

To search the log records, follow these steps:

1. Specify the search criteria in the left panel
2. Click the Search button. 

The search result will be displayed in the right panel

Field	Description
From: Time:	The search starting date time. You can either enter the date in the field or select it by clicking the Calendar.
To: Time:	The search ending date time. You can either enter the date in the field or select it by clicking the Calendar.
Admin	The log that is related to certain system administrator.
Op	The operation type performed such as Login/Logout and adding device etc.

4.3.3 Routine Maintenance

The system is designed to perform some routine maintenance tasks once a week in the background. During this time, there may a slight delay of up to 10 seconds when using Web GUI. In addition, the System Log may indicate some extraneous errors such as “license expired’ which can be ignored.

5 EMS System Configuration

The Server Configuration interface provides the access to:

- Global Setting
- Service Management
- Database Management
- Device Import
- SNMP MIB Management
- Region Management
- Device Type Management
- Wiki Page
- Revision

5.1 Global Parameter Setting

This section describes how to access the Global Parameter Setting screen as well as how to configure the global parameter settings.

5.1.1 Accessing the Global Parameter Setting Screen

To access the Global Parameter Setting screen, follow these steps:

1. Click the System icon.
2. Click the Global tab.

Figure 5.1. System Configuration

5.1.2 Configuring the Global Parameter Settings

To configure the global parameter settings, follow these steps:

1. Click the Parameters tab on the left panel.

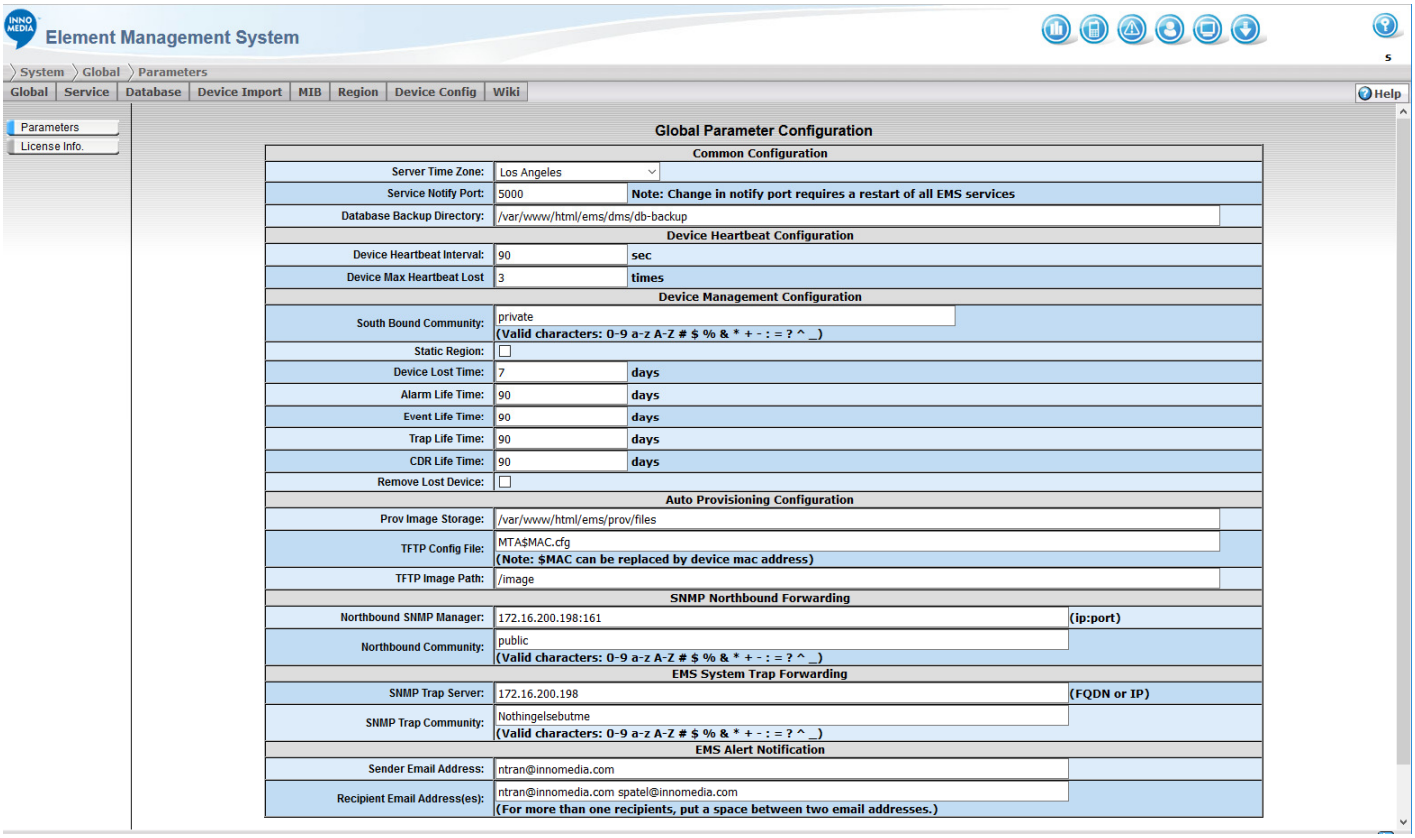


Figure 5.2. Global Parameter Configuration

2. Fill in the fields on the Global Parameter Setting screen.
3. And click the Save button  to update the change.

The following Table describes the fields in the Global Parameter Settings:

Field	Description
Server Time Zone	Set the time zone for Local time string conversion.
Service Notify Port	A TCP port for WEB server communication communicates with local or remote EMS service routines. **Note:** If an update is made to "Service Notify Port", all EMS services will need to be restarted

Database Backup Directory:	This is where the system will store the Backup copy of the Database when you use the Scheduled Database Backup under the DB Backup Tab under Database
Device Heartbeat Configuration	
Device Heartbeat Interval	The transmission rate in second for heartbeats on all devices. EMS detects the device Heartbeat to know the device is online or not. Device should be sending Heartbeat as frequently as defined in this field. If EMS misses several consecutive device Heartbeats as defined in the Device Maximum Heartbeat lost field, then the device will be designated as being offline. NOTE: System capacity can be affected if the heartbeat interval is too short. System capacity is based on a typical heartbeat interval of 90 sec.
Device Max Heartbeat Lost	The maximum number of heartbeats a device can miss before its status becomes offline.
Device Management Configuration	
South Bound Community	Default SNMP community for EMS to access any device that is under its management. Device may have its own SNMP community secret.
Static Region	If checked, device region only learns device information from database, instead of learning it from device heartbeat messages.
Device Lost Time	Days the device has stopped sending heartbeat messages before it is designated as being Lost. If device stops sending heartbeat (or not able to reach EMS) after specified days will be designated as a lost device. A lost device will be shown on the device list as a gray icon.
Alarm Life Time	Days of history Alarm messages are kept in EMS database. Alarm messages of age older than specified days will be deleted from database.
Event Life Time	Days of history Event messages are kept in EMS database. Event messages of age older than specified days will be deleted from database.
Trap Life Time	Days of history Trap messages are kept in EMS database. Trap message of age older than specified days will be deleted from database.
CDR Life Time	Days of history CDR records are kept in EMS database. CDR records of age older than specified days will be deleted from database.

Remove Lost Device	Remove device from database if the device has been designated as Lost. EMS can still learn device information if device starts sending heartbeats again and the static regions not checked.
Embedded Telnet Client:	When enabled, this will use the Embedded Telnet Client, instead of the PC Telnet Client requesting to connect to desired device.
Auto Provisioning Configuration	
Prov Image Storage	Directory in Master server to store uploaded image file for provisioning download.
TFTP Config File	Pattern of device configuration file for TFTP. Since TFTP protocol cannot indicate the source of the device which downloads the file, the device identity must embedded in the file name. This field can have multiple patterns separated by vertical bar (¦). Macro $MAC can be replaced by device MAC Address. Acceptable MAC address format includes xx:xx:xx:xx:xx xx_xx_xx_xx_xx_xx and xxxxxxxxxxxx
TFTP Image Path	TFTP file will match directory prefix indicating it is an image file. Image Path can have multiple patterns separated by vertical bar (¦).
SNMP Northbound Forwarding	
Northbound SNMP Manager:	IP address of the SNMP Server you want to forward SNMP Messages to.
Northbound Community*	The SNMP Community name of the Northbound Server. Max length is 128 characters and acceptable characters are - 0-9 a-z A-Z # $ % & * + - : = ? ^ and _.
EMS System Trap Forwarding	
SNMP Trap Server	IP address or FQDN of the external SNMP Manager that will manage the EMS' Traps eg when HA failover takes place and nodes are switched.
SNMP Trap Community*	The SNMP Community name of the external SNMP Manager. Max length is 128 characters and acceptable characters are - 0-9 a-z A-Z # $ % & * + - : = ? ^ and _.
EMS Alert Notification	
Sender Email Address:	Enter the sender's email address for the From field of the notification email

Recipient Email Address(es):	Enter one or more recipient email addresses with space in between for multiple email addresses. Do not exceed 128 characters.

Note: Characters will be auto-corrected if using keyboard, but using mouse copy/paste will show a pop-up Error after trying to save any invalid characters.

5.1.3 License Information

The License Information screen allows the system administrator to view the details of the system license information. The information that appears on this page cannot be changed.

5.1.3.1 Accessing the License Information Screen

1. Login to the EMS GUI with your user name and password.
2. Click the System icon.
3. Select [Global] tab.
4. Select License Info. On the left panel.

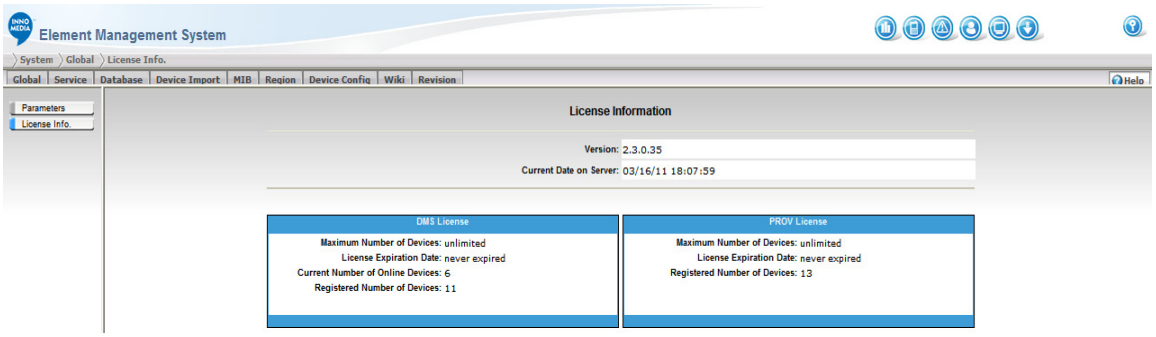


Figure 5.3. EMS License Information

The following table describes the fields used in License Info. page:

Field	Description
Version	Current EMS version number installed
Current Date on Server	Local Date time information of the license server
Maximum Number of	The maximum active devices allowed to be handled by this system.

Devices	
License Expiration Date	The date that the license expires.
Current Number of Online Devices	Current number of devices which are online.
Registered Number of Devices	Number of devices that are currently registered to EMS. It includes all online, offline, and lost devices.

5.2 EMS Server configuration

EMS is a distributed system. EMS can be distributed to different hosts with very few limitations. Distributing services to multiple hosts not only provides a system with load balancing and high availability, but also allows the system to linearly scale up for mass device deployment.

All the hosts on the EMS are defined based on their IP addresses along with their unique alias names. Alias names are used and referred to by the EMS in the system. This provides great flexibility when the deployment environment has to be changed. For example, the administrator needs to move services from one host to another. The only configuration he/she has to redo is to change the IP address of the host. With a simple change, all services will be able to communicate with the new host immediately.

NOTE: IP addresses and alias names on the EMS have to be unique throughout the whole system.

5.2.1 Service Limitation

Some limitations apply when creating an EMS service.

- Only one MDB (master DB) allowed in the whole EMS system.
- Only one instance of each type of service per host is allowed. e.g. It is not possible to have two proxies run on the same host.

5.2.2 Service Configuration

5.2.2.1 Accessing the Service Configuration Screen

To access the Service Configuration screen, follow these steps:

1. Login to the EMS GUI with your user name and password.
2. Click the  icon.

3. Select [Service] tab
4. Select [Config] tab on the left panel

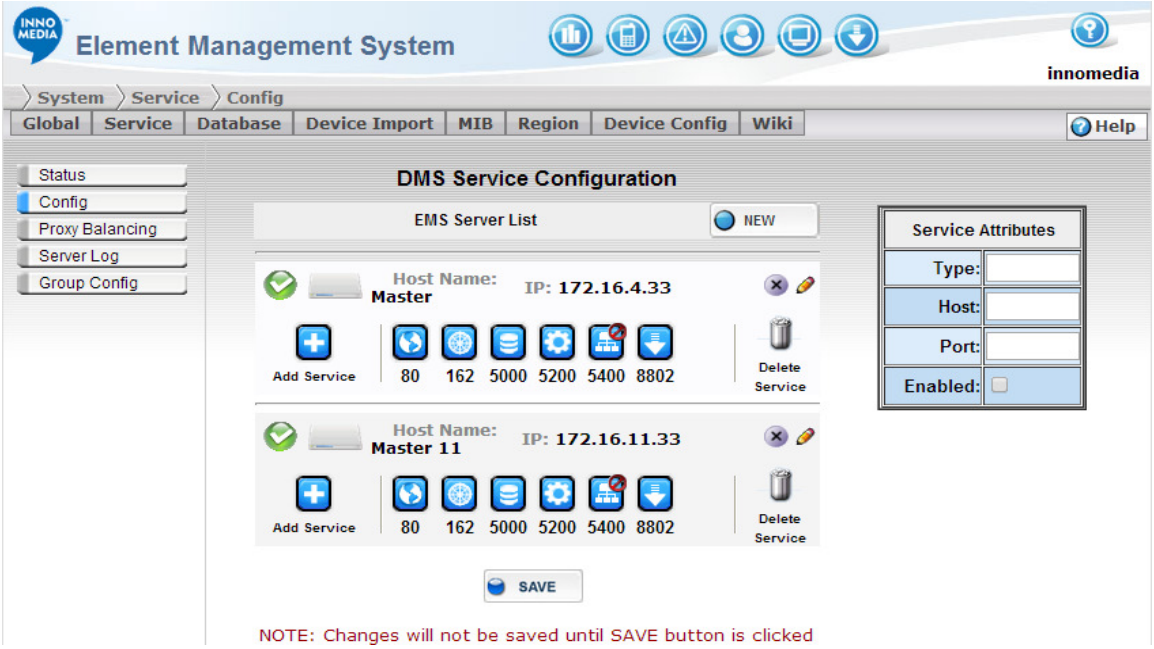


Figure 5.4. EMS Service Configuration

5.2.2.2 Adding Hosts and services

To add a host and services to the host, follow these steps:

1. On the Service Configuration screen, click the New button 

and Host Detail screen will pop up.

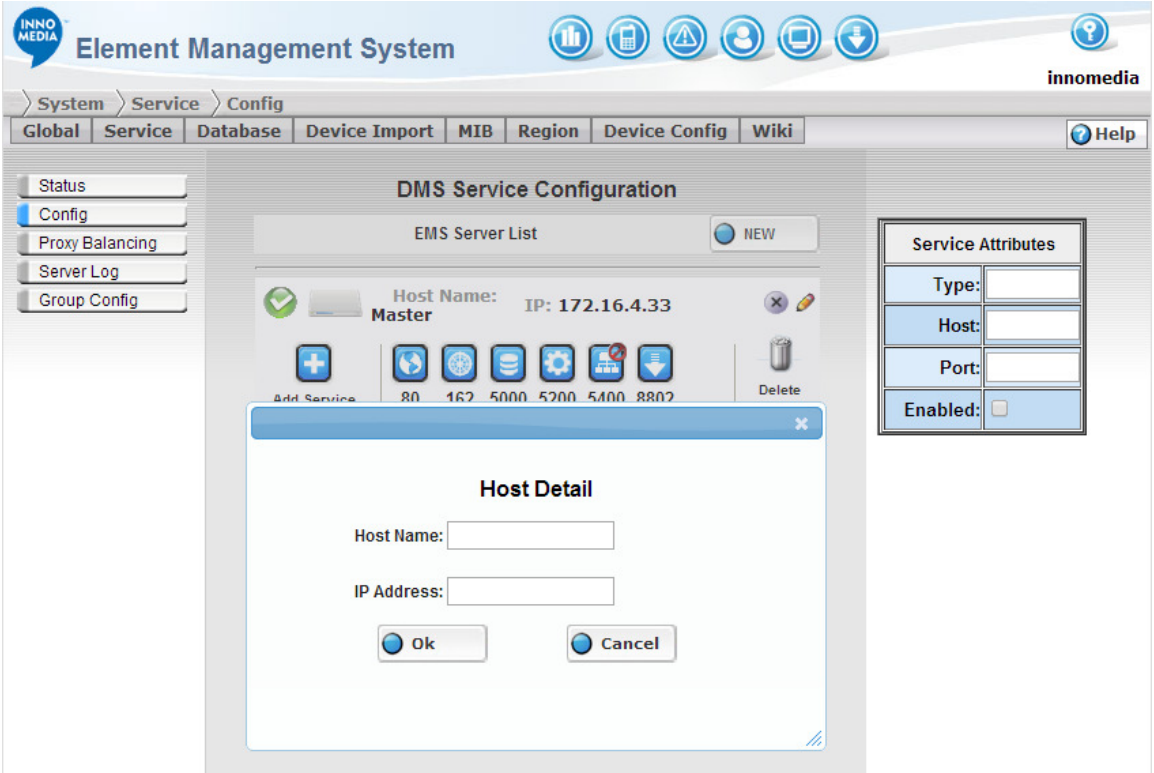


Figure 5.5. EMS Service Configuration – Host Detail Screen

2. Enter the Host Detail information in the appropriate fields. No _ (underscore) is allowed in Host name.
3. Click OK to add a new host to the host list.
4. Click the **Add Service** button and **Add Service Dialog** will pop up.

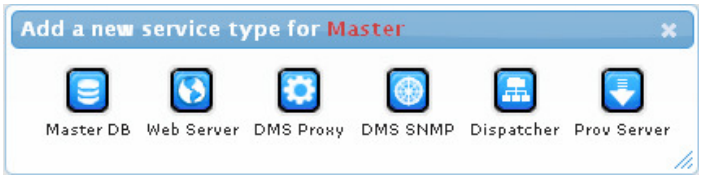


Figure 5.6. EMS Service Configuration – Add a New Service Type

5. Select a service type icon on the pop-up screen. The system will automatically assign a port number to that service (you will find it right under the service icon). The Port numbers can be reconfigured on the Service Attribute fields to the right of the screen. The port number used by each service on the same host must be unique (see Editing Hosts and Service Attribute section).
6. Repeat step 3 to 5 if more hosts and services are required.

7. Click Save button 

to submit your changes.

5.2.2.3 Editing Hosts and Service Attribute

Editing Host Info

To edit a host, follow these steps:

1. Click the Edit button () on top right of host row and **Edit Host Dialog** will pop up.

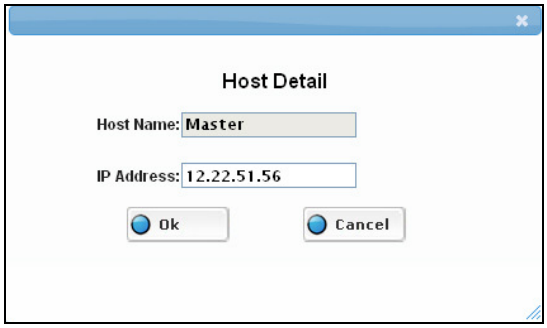


Figure 5.7. EMS Service Configuration – Editing Host Information

2. Edit the fields in the pop-up window.
3. Click OK to close the screen.
4. Click Save on the bottom of host list page to submit your changes.

Enabling/Disabling a Host

To Enable/Disable a host, follow these steps:

1. Click the Enable/Disable on top left of host row to toggle the host enable/disabled  icon. indicates host is enabled;  icon indicates host is disabled.
2. Click Save on the bottom host list page to submit your changes.

Deleting a Host

To delete a host, follow these steps:

1. Click the Delete button  on top right of host row.
2. A “Delete Host” dialog pop-up, Click [OK] to remove the host from host list.
3. Click Save on the bottom host list page to submit your changes.

Editing Service attribute

To edit the service attribute, follow these steps:

1. Select a service from the host box. The service attribute information appears on the Service Attribute fields to the right.
2. Edit the fields. The service attribute fields allow you to reconfigure the port number, and enable/disable the service. The Host name and Type field is not editable.
3. Click Save on the bottom host list page to submit your changes.

5.2.2.4 Delete a Service

To delete a service, follow these steps:

1. Select a service from the host box.
2. Click the **Delete Service** button on the right of host box
3. Click Save on the host list page to submit your changes.

You can also simply click a service and drag it to the trash-can to delete a service.

5.3 Service Status

The Service Status screen allows the system administrator to see an overview of the current status of each host and services. This is a view only page.

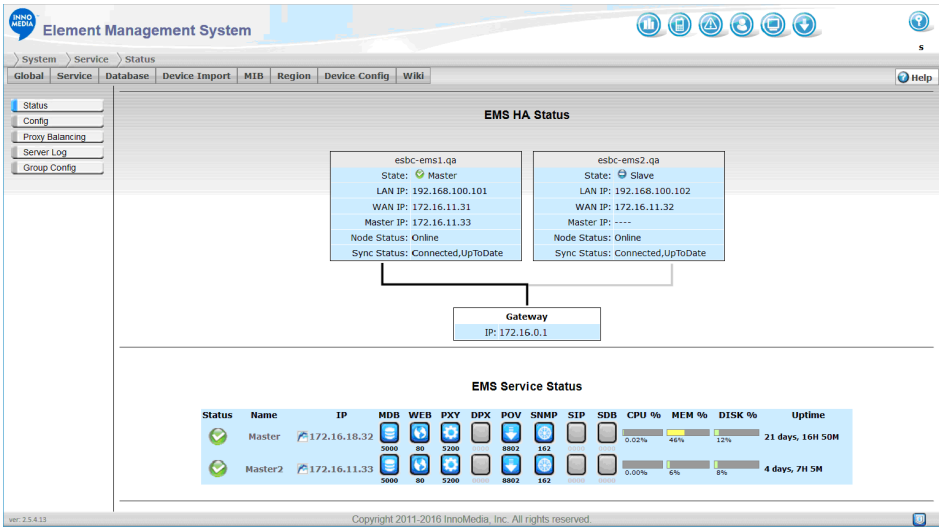


Figure 5.8. EMS HA Status

Note: If system is configured with FQDN for System Host Name, then the Master and Slave units will display appropriate FQDN for the servers instead of DMSHA1 and DMSHA2 which are default host names.

Service status page will refresh automatically. The refresh rate is defined on the Administration User Configuration screen (for more information, see Administrator User Configuration on page 22.

The following table describes each field on the screen:

Field	Description
Status	The green check on left of each host indicates the hosts up and running. The red cross indicates the hosts are down and may require special attention. The blue bar indicates the host is disabled.
Name	The Host's Alias Name. Click to open Host Detail page.
	Click to open Host Detail page.
IP	IP Address of the host. Click to open Host Detail page.
Node Status	Shows Online or Offline
Sync Status	This represents [Connection State, Disk State] **Connection State:** • Connected (Connection is established – Normal state) • WFConnection (This node is waiting for peer node to become visible on the network) • SyncSource (Data synchronization is currently running. This node is the synchronization target (Master)) • SyncTarget (Data synchronization is currently running. This node is the synchronization source (Slave)) • StandAlone (No network configuration is available) **Disk State:** • Diskless (Problem with attaching to disk device) • Inconsistent (Data is inconsistent ie not accessible or useful)

	• Outdated (Data is consistent but outdated) • Unknown (No network connection is available) • Consistent (Consistent data without connection) • UpToDate (Normal state, and data is consistent)
MDB WEB PXY DPX POV SNMP SIP SDB	Service run on this host. Gray icon indicate the service is not configured in this host
CPU	CPU usage percentage.
MEM	Memory usage percentage.
DISK	Disk storage usage percentage. Note: Does not include /boot partition
Uptime	Host up time since boot up

5.3.1 Accessing the Service Status Screen

To access the Service Status screen, follow these steps:

1. Click the System icon. 
2. Select the [Service] Tab.
3. Select [Status] on the left panel.

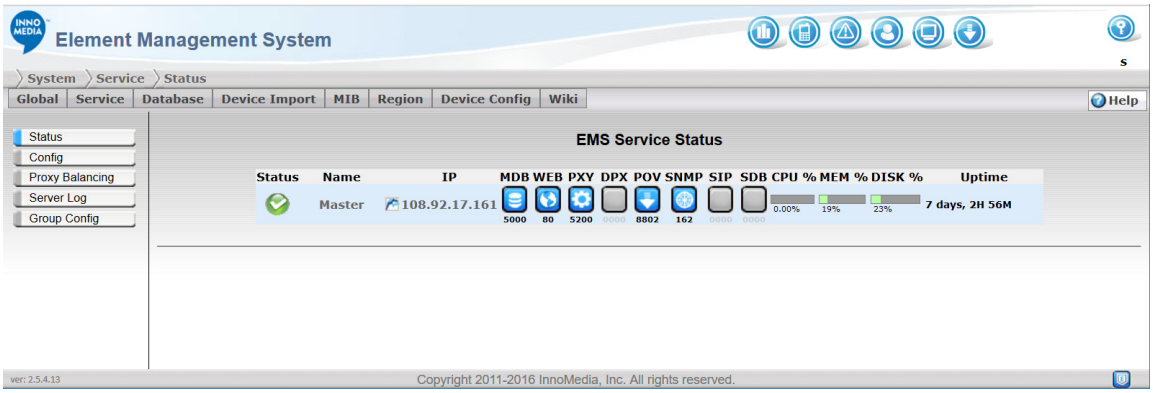


Figure 5.9. EMS Service Status Screen for non-HA system

5.3.2 Check Host Detail

Clicking the Host Name or IP address will link to Host Detail page.

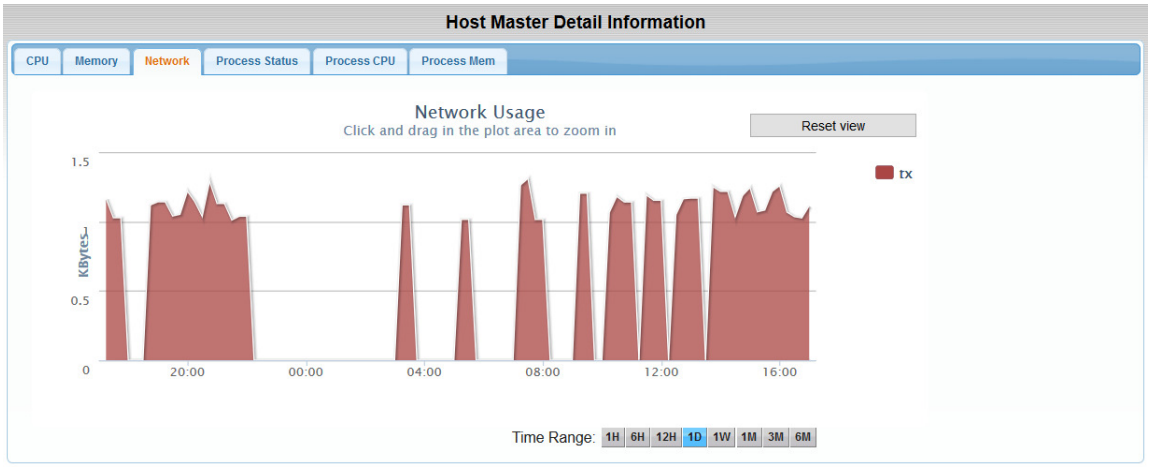
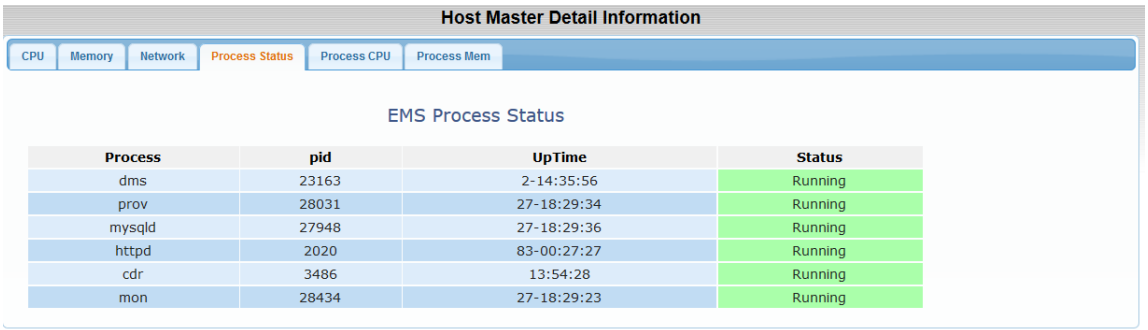


Figure 5.10 EMS Master Detail Information – Network Usage



Process	pid	UpTime	Status
dms	23163	2-14:35:56	Running
prov	28031	27-18:29:34	Running
mysqld	27948	27-18:29:36	Running
httpd	2020	83-00:27:27	Running
cdr	3486	13:54:28	Running
mon	28434	27-18:29:23	Running

Figure 5.11 EMS Master Detail Information – Process Status

Host Detail Page provides a history view of **CPU**, **Memory**, **Network, Process Status**, **Process CPU** and **Process Memory** usage.

- Click each tab to show a **history chart** of specific resource usage.
- Click the **Time Range** button at bottom right to zoom in/zoom out the history chart.
- **Click and drag** on the plot area to zoom in a selected range of the history chart.
- Click the **"Reset View"** button to zoom history chart back to selected time range.

5.4 Exporting Database

The Database Export screen allows the system administrator to retrieve the EMS database content into a SQL file for download. SQL file can be imported into another EMS system or can be a backup for the current system.

5.4.1 Accessing Database Export Screen

To access the Database Export screen, follow these steps:

1. Click System icon.
2. Select [Database] tab.
3. Select [DB Export] on the left panel.

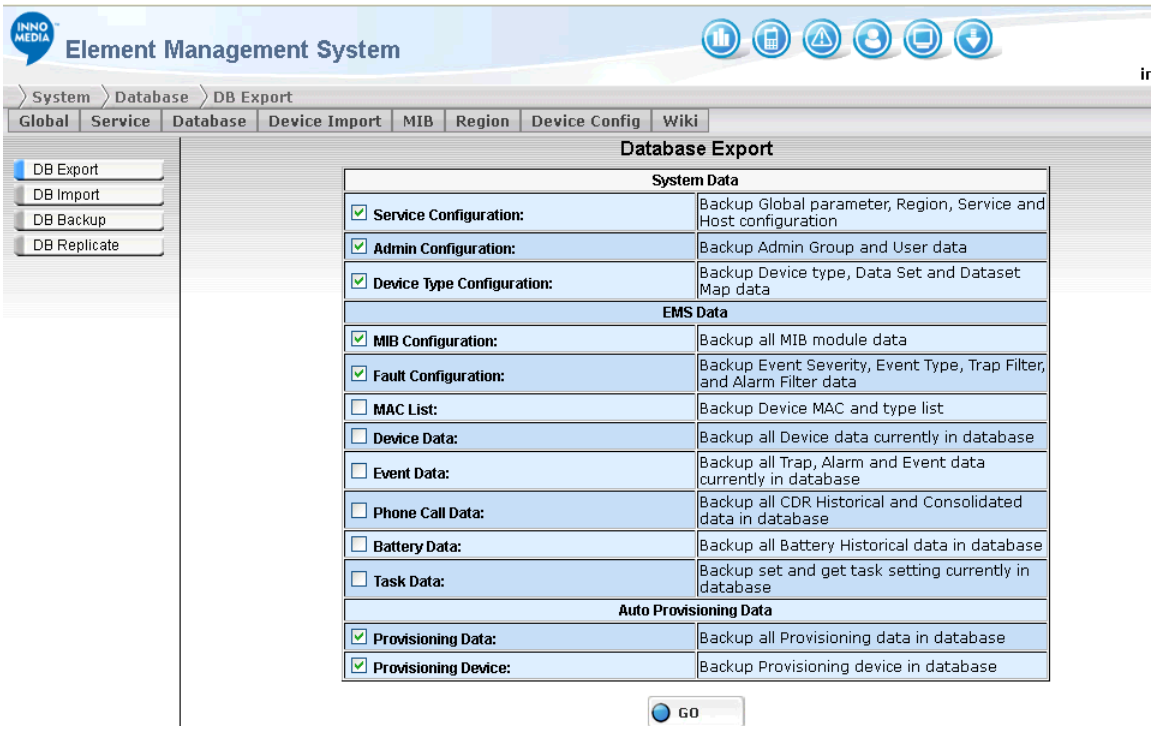


Figure 5.12. Database Export

5.4.2 Selecting Tables for Export

Table is classified into two major categories: System table and Device Table. System Table is common setting for EMS system, like global parameter, user, region etc. Device Table contains device related data. Device Table may grow rapidly since the table size is proportional to the number of devices. System tables grow slower in

comparison to device tables. System data usually is more critical. Data in system tables is usually manually entered by operators, whereas device data can be automatically learned in real time.

Category	Table
System Data	
Service Configuration	Backup Global parameter, Region, Service and Host configuration
Admin Configuration	Backup Admin Group and User data
Device Type Configuration	Backup Device type, Data Set and Dataset Map data
EMS Data	
MIB Configuration	Backup all MIB module data
Fault Configuration	Backup Event Severity, Event Type, Trap Filter, and Alarm Filter data
MAC List	Backup Device MAC and type list
Device Data	Backup all Device data currently in database
Event Data	Backup all Trap, Alarm and Event data currently in database
Phone Call Data	Backup all CDR Historical and Consolidated data in database
Battery Data	Backup all Battery Historical data in database
Task Data	Backup set and get task setting currently in database
Auto Provisioning Data	
Provision Data	Backup all Provisioning data in database
Provision Device	Backup Provisioned devices in database

5.4.3 Exporting Data

To export the data, follow these steps:

1. Check the categories that need be exported.
2. Click the Go button. 

3. A popup window appears and asks for the file name. Input the file name then click “Ok”.

5.5 Importing Database

The backup database files are saved in .sql format. In case of an equipment failure or disaster, the backup file can be used to restore the EMS database.

5.5.1 Accessing Database Import screen

To access the Database Import screen, follow these steps:

1. Click System icon
2. Select [Database] tab
3. Select [DB Import] on the left panel

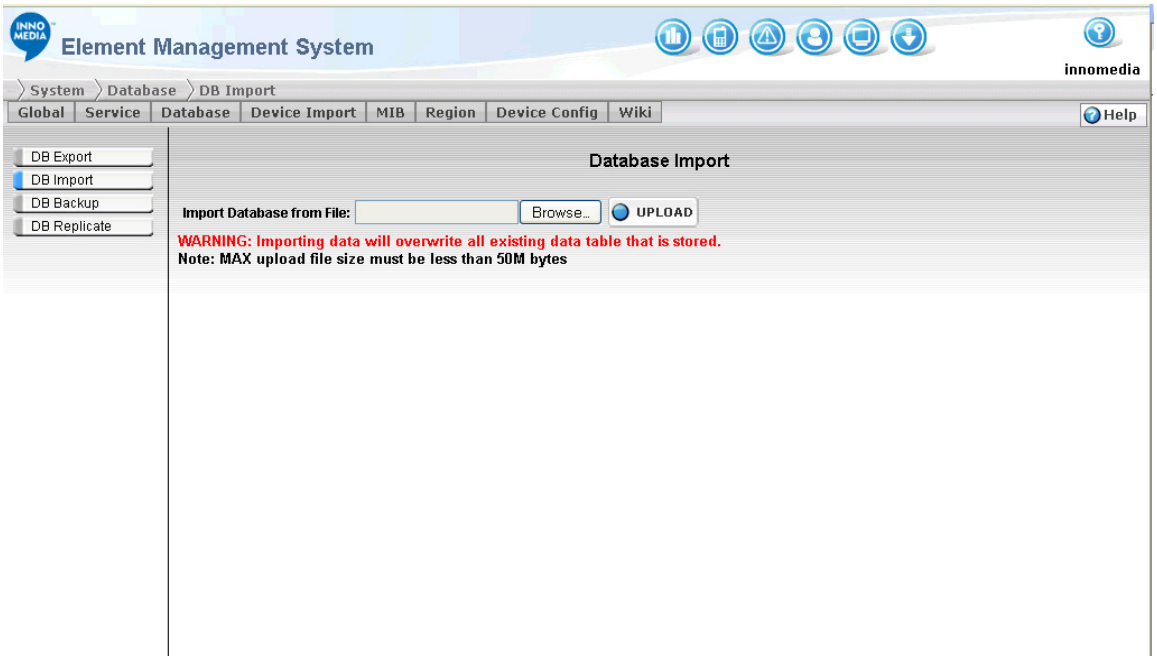


Figure 5.13. Database Import Screen

5.5.2 Importing Database

1. Click the [Browse] button, a file open dialog will popup.
2. Select a previous EMS backup file. Click [Open].
3. Click Upload button.

Note 1: Upload backup file will overwrite all existing data without warning!

Note 2: Uploading backup file has size limit. The limit depends on the web host php server setting. The allowed maximum file size is noted on the last line of page.

5.6 Scheduling Database Backup

The Database Backup screen allows the system administrator to schedule the database backup time periodically, specify backup data, download, and restore the database from the backup files.

5.6.1 Accessing the Database Backup Screen

1. Click System icon
2. Select [Database] tab
3. Select [DB Backup]

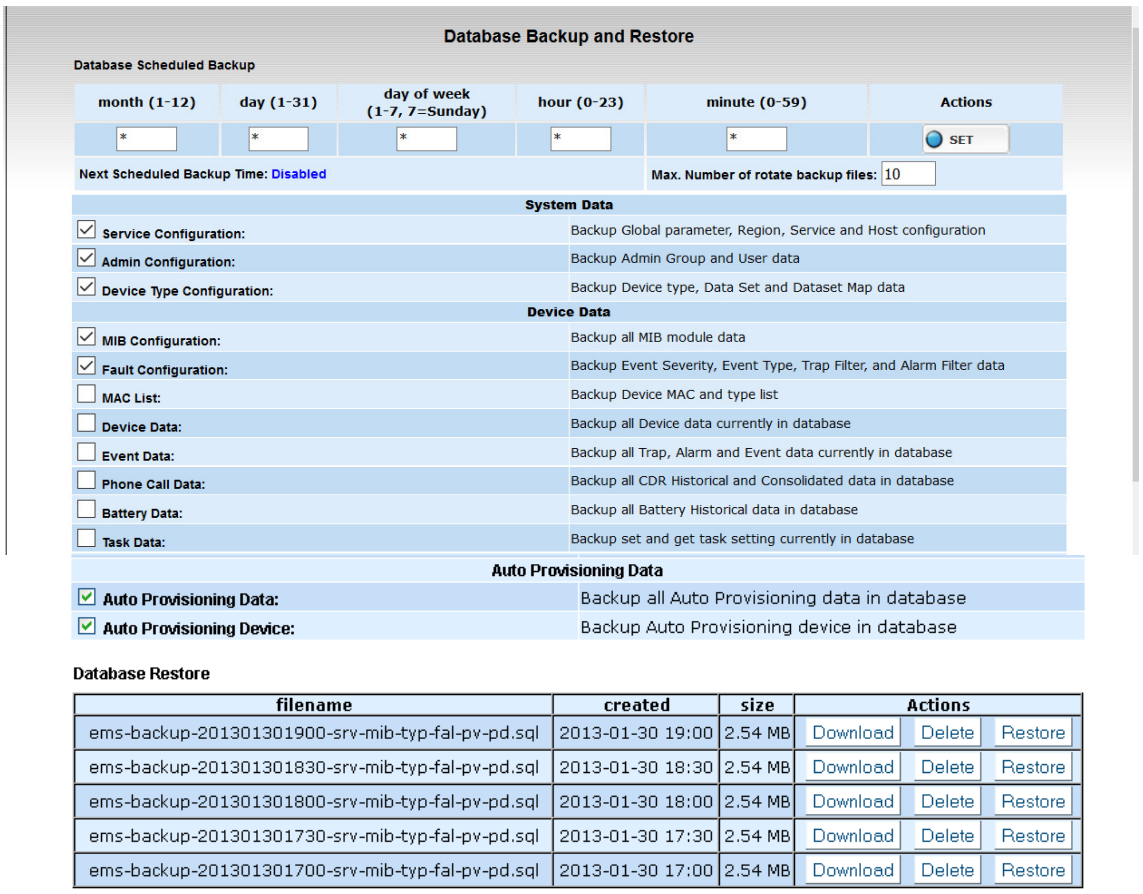


Figure 5.14. Database Backup and Restore Screen

5.6.2 Scheduling Database Backup

5.6.2.1 Cron Syntax

EMS uses UNIX **Cron Syntax** for backup schedule definition.

```
*    *    *   *   *
|    |    |   |   |
|    |    |   |   +------ minute (0-59)
|    |    |   +------- hour(0-23)
|    |    +--------- day of week (1 - 7) (Sunday=7)
|    +----------- day of month (1 - 31)
+------------- month (1 - 12)
```

The value field can have a * or a list of elements separated by commas. An element is either a number in the ranges shown above or two numbers in the range separated by a hyphen (meaning an inclusive range).

e.g.

“*” in hour field specifies 'every hour'

Lists can be in the form, 1,2,3 (meaning 1 and 2 and 3) or 1-3 (also meaning 1 and 2 and 3).

Cron also supports 'step' values (or call repeat pattern). A value of */2 in the day field would mean the command runs every two days and likewise, */5 in the hours field would mean the command runs every 5 hours.

Example 1: Current time is 7:00. You have entered “*/3” in the hour time field. So, the scheduled backup time will be 0:00, 3:00, 6:00, 9:00, 12:00, 15:00, 18:00, and 21:00. The next backup time will be 9:00.

Example 2: Current time is 7:00. You have entered “*/3” in the hour time field and “*/ 30” in the minute time field. So, the scheduled backup tome will be 0:00, 3:30, 6:30, 9:30, 12:30, 15:30, 18:30, and 21:30. The next backup time will be 9:30.

5.6.2.2 Scheduling Database Backup

To configure the database scheduled backup values, follow these steps:

1. Specify the values in the month, day, day of week, hour or minute time fields.
2. Specify the Maximum Number of backup files you would like to save in the database in the Max. Number of rotate backup files field. Once the backup files reach the maximum setting, the old files will be removed from the system.
3. Check the data to be backed up
4. Click the Set button at upper right of page.

5.6.3 Disabling Scheduled Backup

To disable the scheduled backup, enter '*' in all the time fields.

5.6.4 Restoring Database

The backup database files are saved in .sql format. In case of an equipment failure or disaster, the backup file can be retrieved. To prevent the backup files being removed from the database when it reaches its maximum setting, you can choose to download the files to your local drive. You can also delete the unwanted files from the backup server by clicking the Delete button.

To Restore a previous data file, click the [Restore] button on the right of backup file list.

5.6.5 Downloading Database File

You can download the database backup file from EMS server to local disk.

1. Click [Download] button on the right of backup file.
2. A file save dialog will pop up. Enter the local file name and click [Open] to save the file.

5.6.6 Deleting Database File

You can delete the old database backup file from EMS server:

1. Click [Delete] button on the right of backup file.
2. A confirm dialog pop up with message:

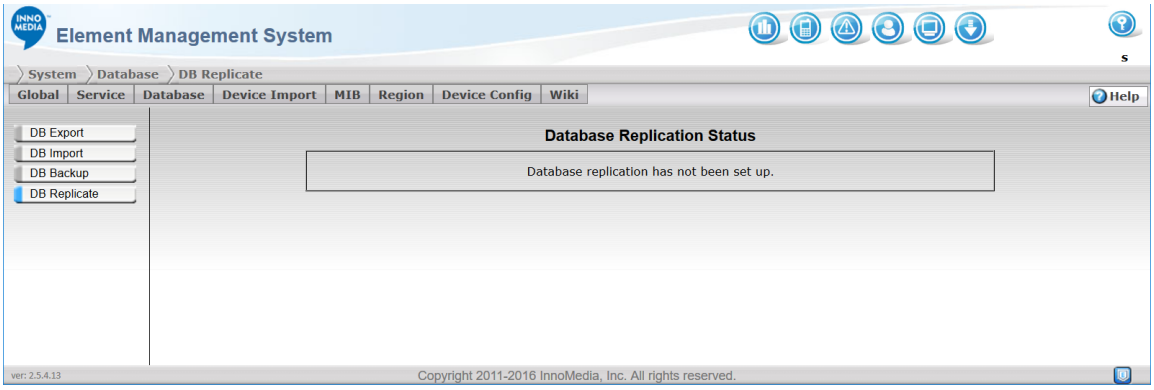
Confirm to delete this backup?

3. Click [Ok] to delete the database file.

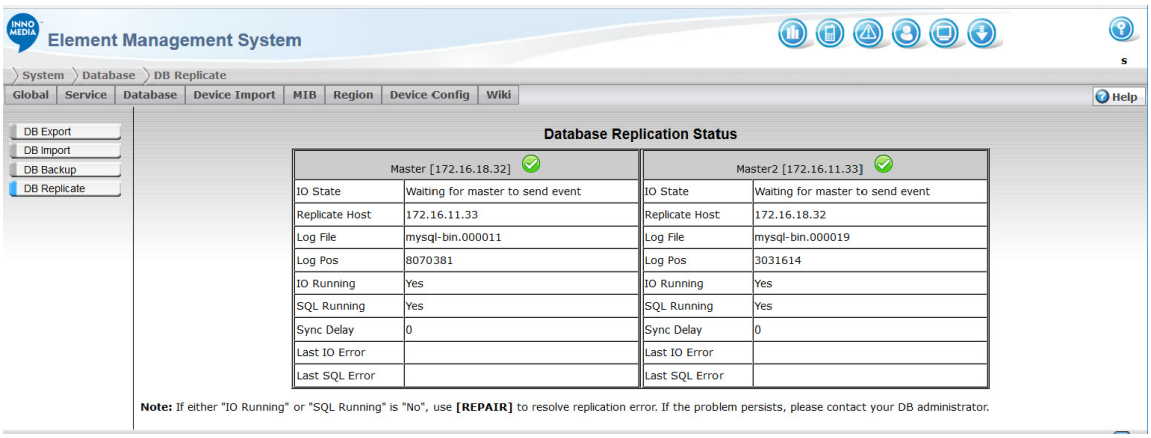
5.7 Database Replicate

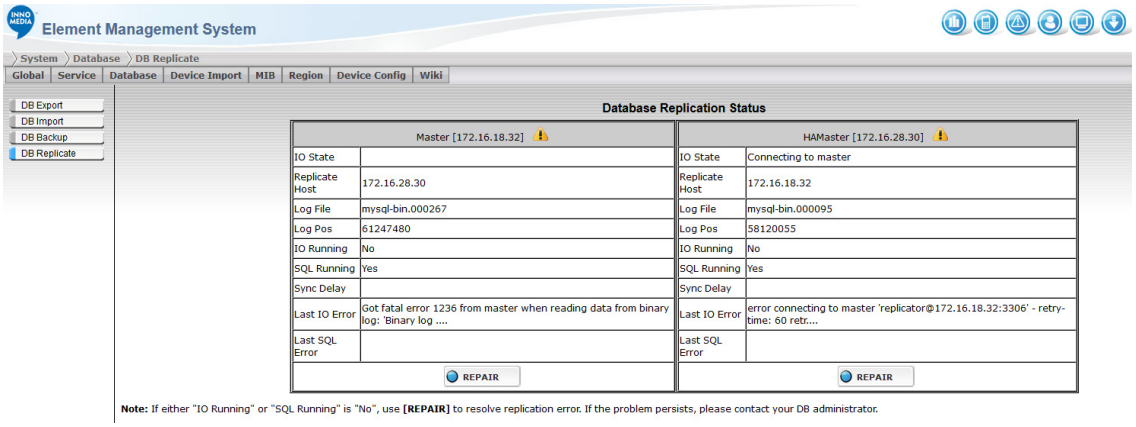
It is important to show if the DB replication in a Geographical Redundant system is running in a normal state or not, and whether further actions are necessary by the operator to restore it back to the normal operating state.

Non-Geographical Redundant System will show the following screen since it does not have any other remote system DB to update.



In a Geographical Redundant system, the DB operation state for both systems will be shown. If the "IO Running" or "SQL Running" are not operating normally, then "No" status will be shown and a **[REPAIR]** option will be provided at the bottom of the screen. Use the **[REPAIR]** option to restore the DB to a normal operational state, and if the problem persists, then notify your DB administrator (or contact InnoMedia) for further support and assistance.





Field	Description
IO State	Shows a description of the current status of the Slave.
Replicate Host	Shows the server IP that the current server is replicating.
Log File	Shows the filename of the file currently being used by the master to record the events that have made changes to the database.
Log Pos	Shows the current read position of the log file.
IO Running	Connects to the Master, and reads the events from the Master's log file. States Yes when DB replication is running Normally.
SQL Running	Executes the events from the log file to update the local database. States Yes when DB replication is running Normally.
Sync Delay	Shows the number of seconds the Slave's database is behind the Master's. It will show 0 or a positive number if the slave is running normally.
Last IO Error	Shows the Error condition when IO Running is 'No'. Synchronization will stop when there is an error.
Last SQL Error	Shows the Error condition when SQL Running is 'No'. Synchronization will stop when there is an error.

5.8 Device Import

There are two ways for EMS to get the device information - One is through the device register message; the other is by importing the device information from a file. This section describes how to access the Device Import screen and also how to import device information from a file.

NOTE: EMS only imports the device MAC address.

This is an optional feature and may only be used when adding devices manually.

5.8.1 Accessing the Device Import Screen

1. Click the System icon. 
2. Select [Device Import] tab

Figure 5.15. Device Import Screen

5.8.2 Importing Device Information from File

To import device information from file, follow these steps:

1. Select the **Import Device MAC From File** radio box.
2. Select the target file from your local file system by clicking the Browse button or enter the directory in the field.

NOTE: the EMS only imports the device MAC Address. The target file must be a .txt file with Enter/Return after each entry,

3. Click the Go button. 

5.8.3 Adding Single Device

To add a single device, follow these steps:

1. Select the **Add One Device** radio box.
2. Enter the device Mac address in the MAC field.
3. Click the Go button. 

5.8.4 Deleting MAC not on the List

This is an option to clean up the old MAC list on your EMS. If you check the **Delete MAC not on List** option, any device its Mac address is not listed on the imported list will be deleted.

5.9 SNMP MIB Configuration

The MIBs are files describing the objects used by the SNMP protocol. The MIB term stands for Management Information Base. This is a text file following the ASN1 standard. MIBs are organized in hierarchy that looks like a tree. The structure of this tree follows a standard defined by RFC.

EMS uses SNMP Get and SNMP Set to retrieve and alter device information. The MIB module contains the variables used to configure or administer the device to be managed. The MIB module defines the Object ID (OID) and each variable. Loading MIB module to EMS allows the administrator to set and select proper OID for device information gathering and configuration. This section describes how to load MIB modules and build MIB trees.

5.9.1 MIB Module Configuration

Since each MIB module has a dependency, the appropriate module must be loaded to the EMS first. MIB module configuration screen has an order field that indicates the load order. Those with smaller order numbers were loaded earlier than those with larger order numbers. This section describes how to access the MIB Module Configuration screen and edit MIB modules.

5.9.1.1 Accessing the MIB Module Configuration Screen

To access the MIB Module Configuration screen, follow these steps:

1. Click the System icon. 
2. Select [MIB] tab.
3. Select [Modules] from the left panel.

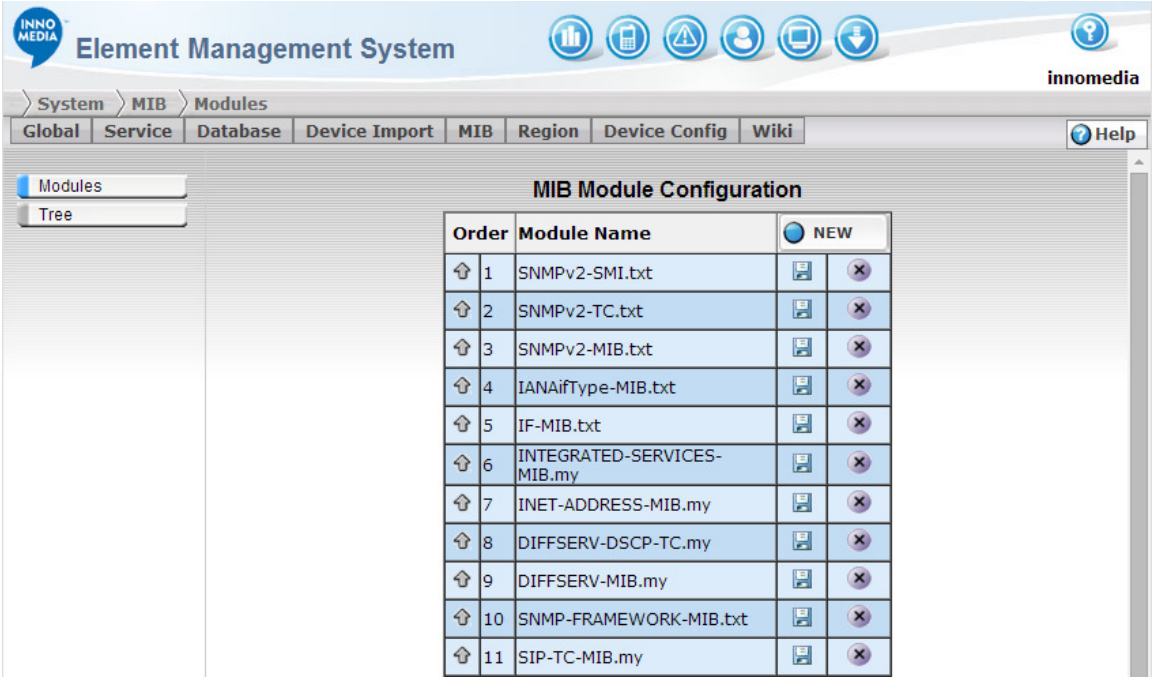


Figure 5.16. MIB Module Configuration Screen

5.9.1.2 Adding MIB Modules

This section describes how to add a MIB module. To add a MIB module, follow these steps:

1. Click the New button  on the MIB Module Configuration screen, the MIB Module Loader screen appears.

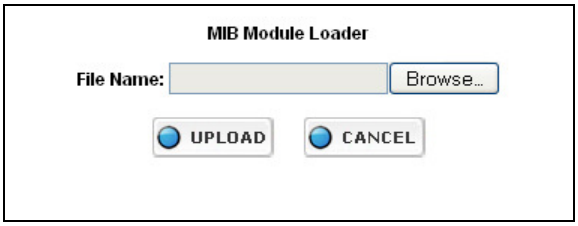


Figure 5.17. MIB Module Loader

2. Enter the directory of the MIB file in the field or click the Browse button to locate the file.

3. Click UPLOAD to upload the MIB file. The new uploaded MIB module should show on the bottom of the module list.

5.9.1.3 Saving MIB Modules

You can download any MIB module that already exists in the EMS system. To download a MIB module, follow these steps:

1. Click the Save button ( ) and the Save file dialog will popup.
2. Select Save file and then click [OK] to save the module.

5.9.1.4 Deleting MIB Modules

This section describes how to delete a MIB module. To delete a MIB module, follow these steps:

1. Click the Delete button at the right of the module record.
2. A dialog box appears with the following message:

   Are you sure you want to delete this module?

3. Click [OK] to remove the module from the module list.

5.9.1.5 Changing the Module Order

Since each MIB module has dependency, the appropriate module must be loaded to the EMS first. The order of MIB module loaded must be correct before the build process. Otherwise the build process may fail.

To change the order of the modules listed on the screen, click the **Up Arrow** button next to the module to move it up one level at a time.

5.9.1.6 Building Module Tree

MIB modules need to be compiled before they can be shown as a tree on the MIB Tree Viewer Screen.

To compile MIB modules, follow these steps:

1. Load the required modules and adjust the module order.
2. Click the BUILD button to build the MIB tree. A dialog box appears with the following message: MIB Tree Build Successfully

NOTE: If the loader fails to build a module tree (because of syntax error or missing module), error message will popup. You will need to correct the MIB module or adjust the module order and then build it again.

3. Click OK to close the window

5.9.2 MIB Tree Viewer

MIB Tree Viewer consists of two panels - The MIB Tree panel (on the left) and the MIB Object Definition panel (on the right). In the MIB Tree panel, the system administrator can either choose to display the tree in tree view or in module view. The tree view displays the MIB tree from the OID root as defined in RFC. It gives you the real location of each module on the MIB tree. The screen on the right is the MIB Object Definition panel. It displays the MIB object definition details.

5.9.2.1 Accessing the MIB Tree Viewer Screen

To access the MIB Tree Viewer screen, follow these steps:

1. Click the System icon.
2. Select [MIB] tab
3. Select [Tree] from the left panel

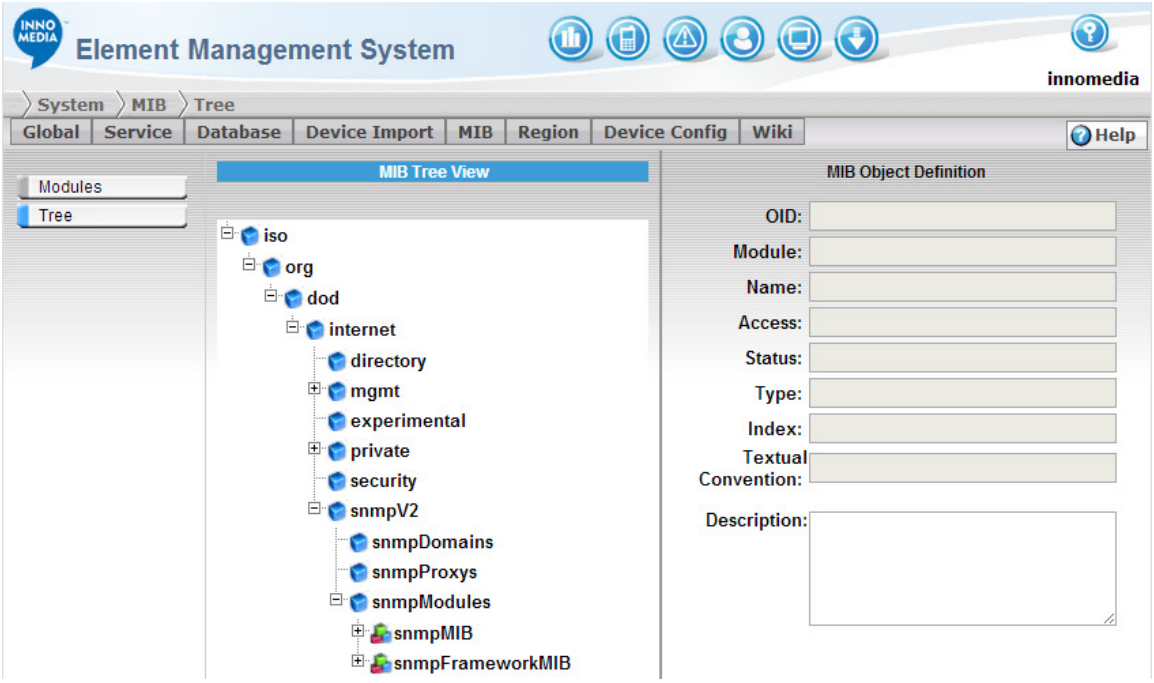


Figure 5.18. MIB Tree Screen

5.9.2.2 Expand/Collapse MIB Tree

Click ⊞ to expand a tree node,

Click ⊟ to collapse a tree node,

5.9.2.3 Check MIB Object Definition

To view a MIB object definition, click a node in the left **Tree View** panel. The definition of the selected MIB object displays in the right **MIB Object Definition** panel.

5.10 Region Management

Regions represent a geographic grouping or a logical grouping of devices. Administrators are allowed to access the device information in their allowed regions only. Each administrator can be assigned with individual region access rights. This section describes how to configure the region table and region access rights on the EMS Region Configuration pages.

5.10.1 **Region Table**

Region table organizes all the regions and sub regions in hierarchy for easy management. This section describes how to access the Region Table screen and configure regions.

By default, the region table tree is expanded. You can click the expanded button to the left of the region name to hide its sub-regions.

5.10.1.1 Accessing Region Table Screen

To access the Region Table screen, follow these steps:

1. Click the System icon. 
2. Select [Region] tab.
3. Select [Table] from the left panel.

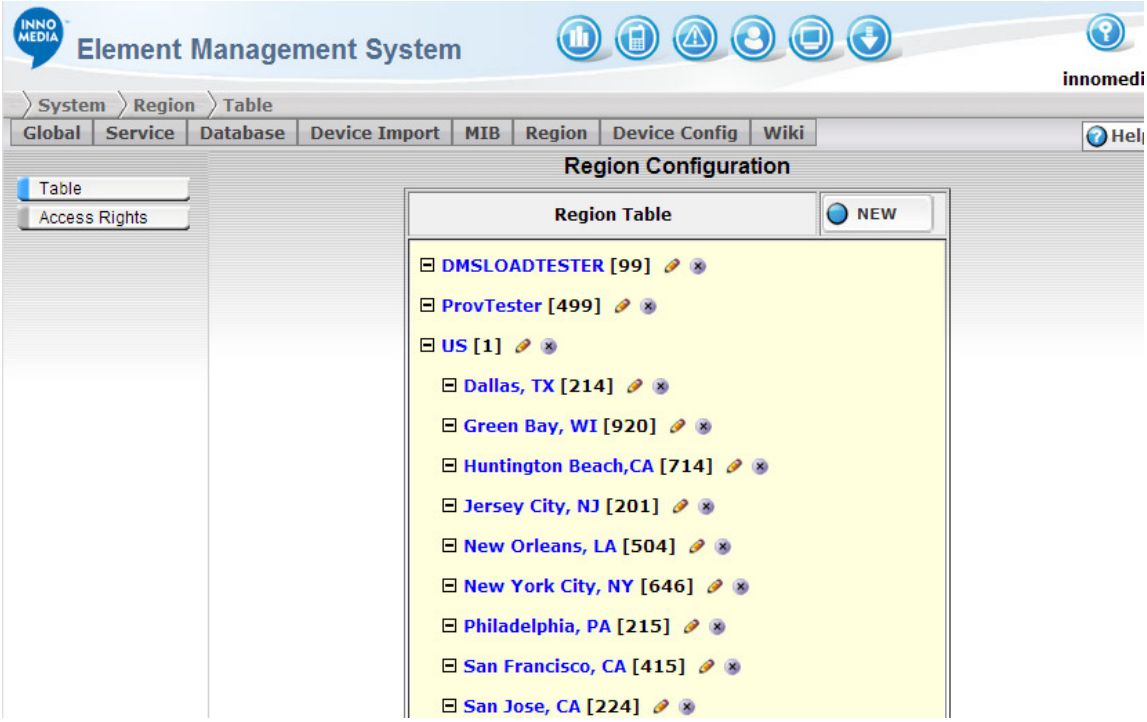


Figure 5.19. Region Configuration Screen

5.10.1.2 Adding Regions

To add a region, follow these steps:

1. Click the New button, The Edit Region screen appears.
2. Fill in the fields.
3. Click Save to add the new region to the table.

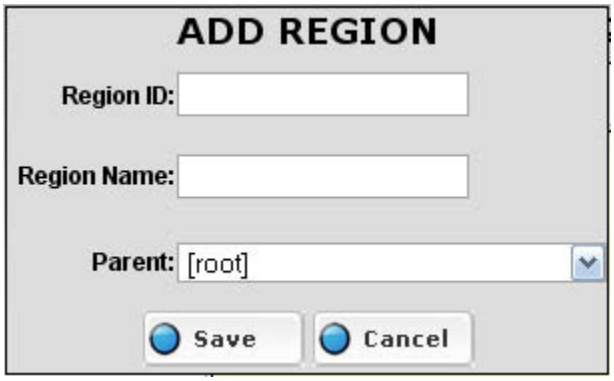


Figure 5.20. Add Region Screen

The following table describes the fields in Edit Region screen:

Field	Description
Region ID	Identifier of the region. It must be a unique number. Region ID is not hierarchical and not related to its parent Region ID.
Region Name	The Name of the region. NOTE Region name can be reused in different parent root but not in the same region.
Parent	This is the upper level of the region. Select [root] from the drop-down manual to add a new parent region or select an existing region to add a subregion underneath it.

5.10.1.3 Editing Regions

To edit a region, follow these steps:

1. Click the Edit button of the region. The Edit Region screen appears.
2. Make your changes. Refer to Adding Regions for field description.
3. Click Save to save your changes

Figure 5.21. Edit Region Screen

5.10.1.4 Deleting Regions

To delete a region, follow these steps:

1. Click the Delete button( ) to the right of the region.
2. Click [Ok] on the pop-up warning screen to confirm delete action.

NOTE: The system does not allow deletion of a region that contains subregions. To remove such regions, remove all the subregions first, and then remove the root or region.

5.10.2 **Region Rights**

The Region Rights Configuration screen allows the system administrator to configure the region access rights for each administrator user account. Each account can be granted access to multiple regions. This section describes how to access the Region Right Configuration screen as well as how to configure the access rights for each individual user.

5.10.2.1 Accessing Region Right Configuration Screen

To access the Region Right Configuration screen, follow these steps:

1. Click the System icon.
2. Select [Region] tab
3. Select [Access Right] from the left panel

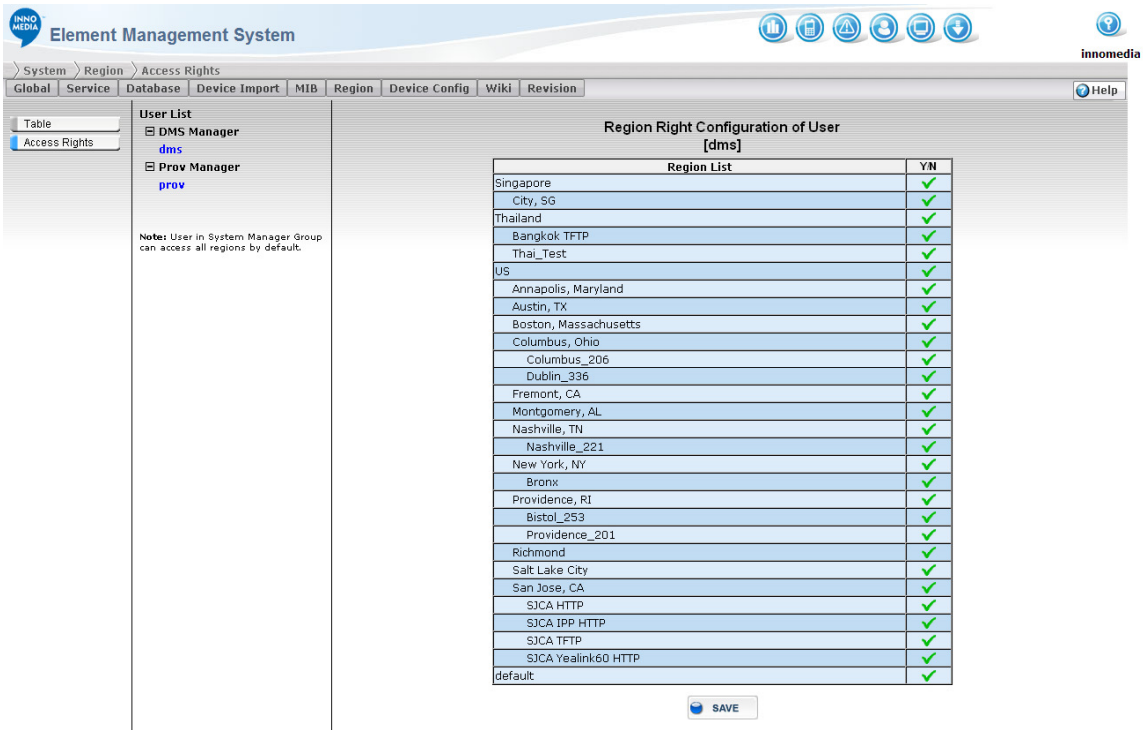


Figure 5.22. Region Right Configuration Screen

5.10.2.2 Configuring Region Right for Users

Region Right Configuration screen consists of two panels:

The left panel contains a user group list and the right panel displays the region right configuration table of selected user.

5.10.2.3 Change User Right

To make changes on the configuration, follow these steps:

1. Select a user from the left panel by clicking on the user name. User list is organized by the group. You may click on the ⊞ button to hide the users or the ⊟ button to display all the users in that group. The Region Right Configuration for the user appears in the right panel.
2. Click on the Y/N field to the right of each region to allow or disallow the access right. The green tick mark ✓ means the user is allowed to access the device information in this region. The red cross mark ✗ means the user is not allowed to access the device information in this region. Please note that if you allow the parent regions, the user will also be allowed to access the entire sub region underneath it.
3. Click the SAVE button to submit your changes.
4. Click OK on the successfully updated pop-up screen.

NOTE: The regions granted to the administrator will show in the Region field on the Administrator Detail screen

5.11 Device Type Configuration

This section describes how to configure:

- Device MIB Groups
- MIB Group Access
- Device Types

5.11.1 MIB Group Access Right

MIB Group Access Configuration screen allows the system administrator to configure the MIB group access right based on the individual user group. This section describes how to access the MIB Group Access Configuration screen as well as how to configure MIB group access right. Un-granted MIB Group will not display on the tab of **Device Info** page.

5.11.1.1 Accessing MIB Group Access Configuration Screen

To access the MIB Group Access Configuration screen, follow these steps:

1. Click the System icon.
2. Select [Device Config] tab
3. Select [MIB Group Access]

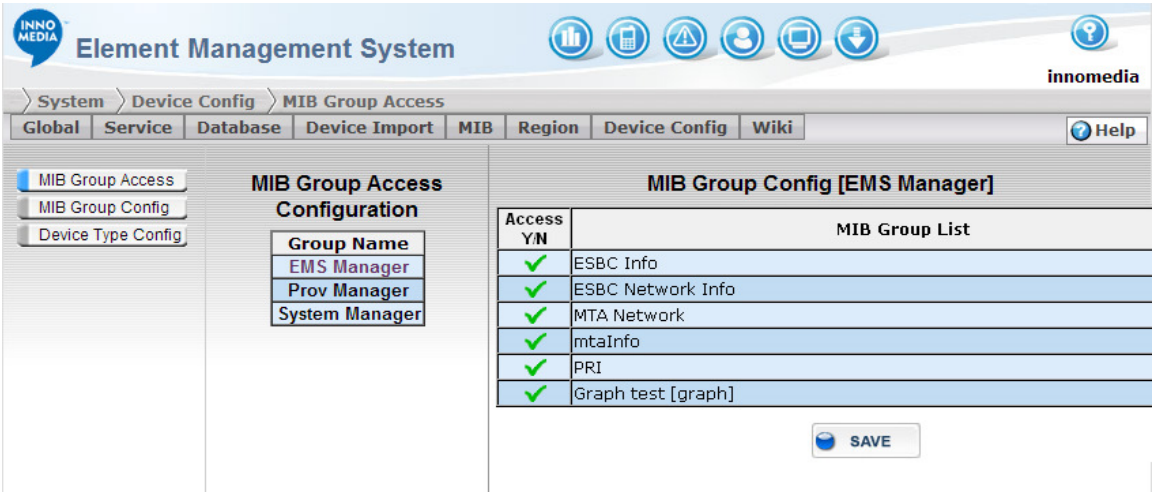


Figure 5.23. MIB Group Access Configuration Screen

5.11.1.2 Configuring MIB Group Access Right

The MIB Group Access Configuration screen consists of two panels:

- The left panel contains a user group list, and
- The right panel contains the MIB group access configuration information for the selected user group.

To change the configuration for the user group, follow these steps:

1. Select a user group from the left panel. The MIB group access right configuration appears in the right panel.
2. Click the Access Y/N field to the left of each MIB group to allow or disallow the access. The green mark (✓) means the user group is allowed to access the MIB group. The red cross mark (✗) means the user group is not allowed to access the MIB group information.
3. Click the SAVE button to submit your changes.
4. Click OK on the successfully updated pop-up screen.

NOTE: The MIB Group Access Right granted to the system administrator will appear as a click-able tab on the device information screen that contains MIB group information.

5.11.2 **MIB Group Configuration**

In the EMS system, OID's are grouped into different MIB groups and assigned to various device types to help user to easy locate useful MIB values. These MIB Group are predefined and available for your quick query and setting on the Device Detail screen.

The MIB OID data can also be viewed graphically by setting up Graph MIB Groups on the MIB Group configuration screen. Please note that only the system administrators who have the MIB group access right can view the graph data on the Device Detail screen.

5.11.2.1 Accessing to the MIB Group Configuration Screen

To access to the MIB Group Configuration screen, follow these steps:

1. Click System icon.
2. Select [Device Config] tab.
3. Select [MIB Group Config] from the left side panel.

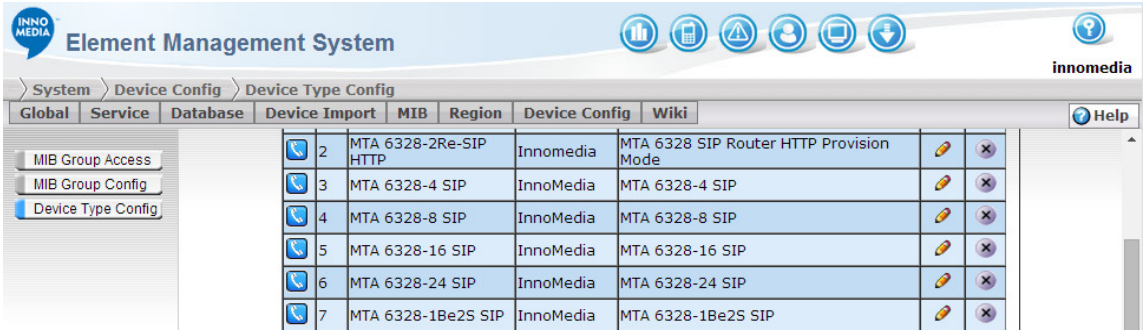


Figure 5.24. Device MIB Group Configuration Screen

5.11.2.2 Adding Data MIB Groups

To add a new data MIB Group, follow these steps:

1. Click the NEW button NEW, a new entry row appears.

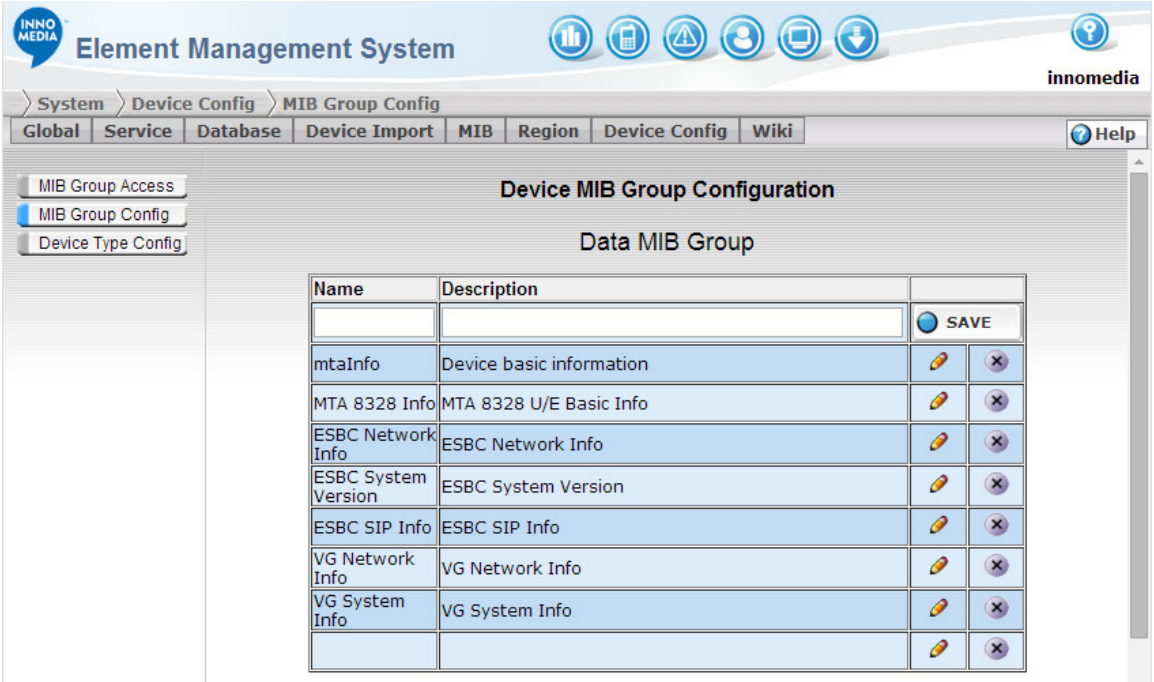


Figure 5.25. Adding Data MIP Group

2. Fill in the fields.
3. Click the SAVE button  on the right to submit the new group and enter the MIB Group Configuration screen. Follow the Edit instruction below to configure the MIB Group data set list.

Data MIB Group Table - Field Description

Field	Description
Name	Name of the data MIB group. This name will be used for the device type configuration. Please only use the alphanumeric characters to prevent system error.
Description	A text description about this MIB Group.

5.11.2.3 Editing Data MIB Groups

To edit an existing MIB Group, follow these steps:

1. Click the Edit button  of the MIB Group. The MIB Group Configuration screen appears.
2. Fill in the fields. For field description, see the table in Adding Data MIB Groups.

5.11.2.4 Delete Data MIB Groups

1. To delete a Graph MIB Group from the table list, follow these steps:
2. Click the Delete button ( ) of the MIB Group on the table list. A dialog box appears to confirm the action.
3. Click [OK] to confirm the delete action.

5.11.3 **Device Type List**

Devices are grouped together based on their various types for SNMP configurations. This section describes how to add, edit, and delete device types.

Device Type List will not be affected by the View Category control. View Category is configured in each Device Type Detail.

5.11.3.1 Accessing the Device Type List Screen

To access the Device Type List screen, follow these steps:

1. Click the System icon.
2. Select [Device Config] tab.
3. Select [Device Type Config] from the left panel.

Figure 5.26. Device Type List Configuration

5.11.3.2 Adding New Device Types

To add a new device type, follow these steps:

1. Click the NEW button NEW on the top right of screen to add a new entry row at the top of the device type table list.
2. Fill in the fields.
3. Click the SAVE button SAVE to submit your new entry and enter the Device Type Configuration screen.

Field	Description

CAT	Show the View Category of this type. for Voice Device and for Session Boarder Controller device.
ID	Device type identification number. **NOTE:** Please make sure your devices are also configured with the appropriate type ID in the device's configuration file.
Name	Name of the device type. It is a major device reference in the EMS.
Vendor	The vendor of device.
Description	Text description of the device type. "Clone From:" an existing device or Create New device type.

5.11.3.3 Editing Device Types

To edit a device type, follow these steps:

Click the Edit button next to the device type record. Device Type Configuration screen appears. Follow the instruction of Device Type Configuration screen (see Device Type Configuration on page 641) and click Save to submit your change.

5.11.3.4 Delete Device Type

To delete a device type, follow these steps:

1. Click the Delete button next to the device type record. A dialog box appears with the following message:

   Are you sure you want to delete this type?

2. Click [OK] to remove the device type from the table list.

5.11.4 **Device Type Configuration**

Device Type Configuration Screen provides an interface to configure MIB objects for different types of device. MIB objects used in this screen are important to EMS operations. EMS uses these MIB objects to trigger device command or query device attributes.

Device Type Configuration
MTA 6328-2Re-SIP HTTP

Name: MTA 6328-2Re-SIP HTTP
Vendor: Innomedia
Description: MTA 6328 SIP Router HTTP Provision Mode
Category: (•) Device ( ) Embedded Session Border Controller
Has Battery: [ ]
Has Cable Modem: [ ]
Has PRI: [ ]

Command OID Set

Reset: .1.3.6.1.4.1.3354.1.3.1.1.8.1
Re-Provision: .1.3.6.1.4.1.3354.1.3.1.1.8.52
Connect Request: .1.3.6.1.4.1.3354.1.3.1.1.8.50
HB Redirect Request: .1.3.6.1.4.1.3354.1.3.1.1.8.51
User ID: .1.3.6.1.4.1.3354.1.3.1.1.9.1.1.11
Local IP: .1.3.6.1.4.1.3354.1.3.1.1.5.3
FQDN:

Enrollment OIDs

Enrollment Notify:
Enrollment MAC:
Enrollment Version:
Enrollment Type:
Enrollment Region:
Enrollment Correlation Id:

DMS Encryption

DMS Encryption Key:
Key Derivation Func: InnoMedia

Others

Extra Device Info Page: dmsinfo.ssi

SAVE

Device MIB Group		ADD
MTA Network	MTA Network Info	
Graph test [graph]	test	

Figure 5.27. Device Type Configuration Screen

The following table describes the fields shown on the Device Type Configuration screen:

Field	Description
Name	Name of the device type. Type name is a major reference ID in the EMS.
Vendor	The vendor of device.
Description	A brief description of the device type.
Category	This identifies the type of device – that is, if the device is MTA or Embedded Session Border Controller (ESBC).
Has Battery	Check if this type of device has battery.
Has Cable Modem	Check if this type of device has embedded cable modem.
Has PRI	Check if this type of device has embedded PRI interface.
Command OID Set	Set of OID that EMS needs to perform operation to device by SNMP.
Enrollment OIDs	(Optional) If device using direct SNMP message only (without EMS tunnel), here is the set of OID for EMS capture the enrollment information from device
EMS Encryption Key	A secret key to decipher decrypted data sent from devices. (Optional, Only use when device using encrypted mode)
Key Derivation Func	Select InnoMedia from the drop-down menu for InnoMedia CPEs or select PBKDF2-sha1 for the third party CPEs. (Optional, Only use when device using encrypted mode)
Extra Device Info Page	Enter file name dmsinfo.ssi in the field for InnoMedia CPEs. This is a web page on device that grants access to EMS without needing a login. This page usually shows the overview status of device.

5.11.4.1 Select OID for Device Type

To set the Command OID or Enrollment OID, follow these steps:

1. Type the OID in numeric form, or click the OID pick icon to the right of the data entry fields to bring up the MIB tree browser. Expand the MIB tree and find the OID for the command, then click the OK button.
2. Click the SAVE button SAVE to save your new OID configuration.

NOTE: Make sure you click the Save button before going to other pages or selecting different device type. Changes will not take effect if you do not click the Save button.

Pick an OID

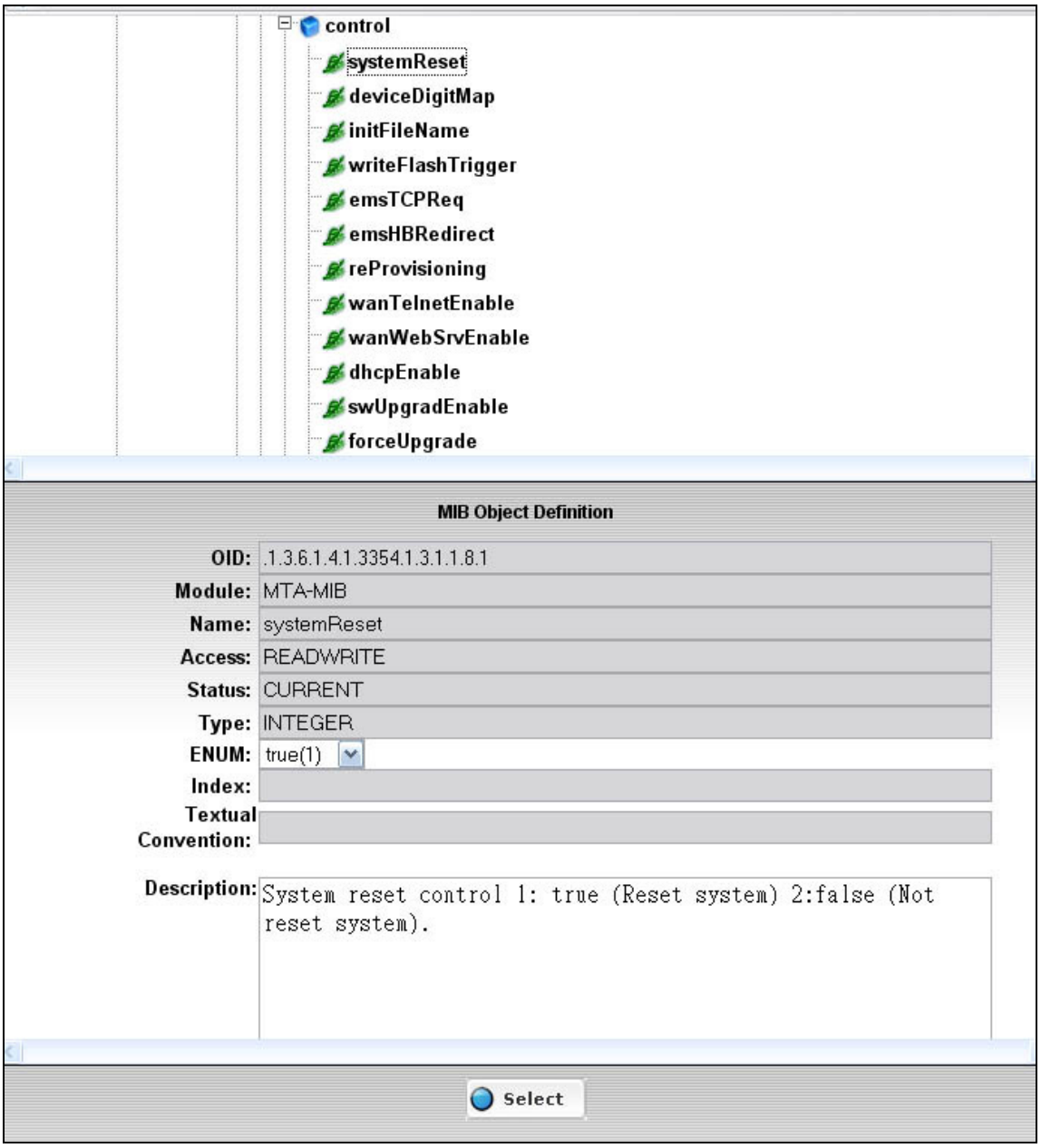


Figure 5.28. OID Picker

5.11.5 **Device MIB Group Configuration**

5.11.5.1 Add MIB Group

To add a MIB Group, follow these steps:

1. Click the ADD button on the MIB Group list.
2. Select a data set from the drop down menu.
3. Click the SAVE button 

to add the MIB Group to the table list.

5.11.5.2 Delete MIB Group

To delete a MIB Group from device type, follow these steps:

1. Click the Delete button  next to the MIB Group entry. A dialog box appears with the following message:

   Are you sure you want to delete this MIB Group?

2. Click [OK] to remove the data set from the list.

6 Device Management

EMS provides a network wide view of devices and their current status via a user friendly web-based GUI for centralized device management. There is a drill-down view of that provides direct access to device screen where the system administrator can perform some management tasks via Telnet, web access, or SNMP. Device Management provides the following features:

- Device Query
- Call Statistic
- Voice Quality Analyze

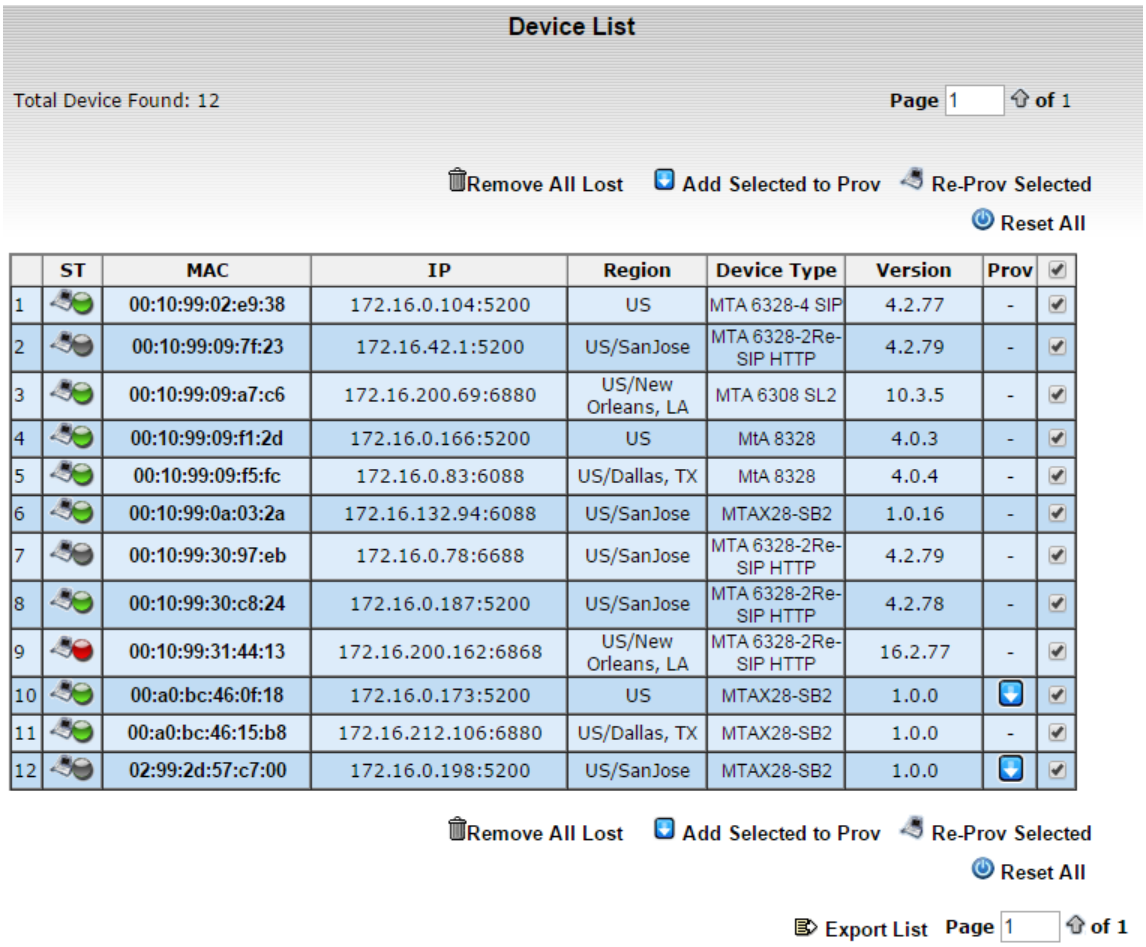
6.1 Device Query

Device Query screen allows the system administrator to search for devices by their MAC addresses, IP addresses, device type, device status, region, and User ID in their granted regions. Also, the system administrator can view the detailed device information; connect to the device, and reset or re-provision devices via the Device Query screen. This section describes how to access the Device Query screen and perform the above tasks.

6.1.1 Accessing Device Query Screen

To access the Device Query screen, follow these steps:

1. Click the Device icon.
2. Select the "Device Query" tab



	ST	MAC	IP	Region	Device Type	Version	Prov	
1		00:10:99:02:e9:38	172.16.0.104:5200	US	MTA 6328-4 SIP	4.2.77	-	
2		00:10:99:09:7f:23	172.16.42.1:5200	US/SanJose	MTA 6328-2Re-SIP HTTP	4.2.79	-	
3		00:10:99:09:a7:c6	172.16.200.69:6880	US/New Orleans, LA	MTA 6308 SL2	10.3.5	-	
4		00:10:99:09:f1:2d	172.16.0.166:5200	US	MtA 8328	4.0.3	-	
5		00:10:99:09:f5:fc	172.16.0.83:6088	US/Dallas, TX	MtA 8328	4.0.4	-	
6		00:10:99:0a:03:2a	172.16.132.94:6088	US/SanJose	MTAX28-SB2	1.0.16	-	
7		00:10:99:30:97:eb	172.16.0.78:6688	US/SanJose	MTA 6328-2Re-SIP HTTP	4.2.79	-	
8		00:10:99:30:c8:24	172.16.0.187:5200	US/SanJose	MTA 6328-2Re-SIP HTTP	4.2.78	-	
9		00:10:99:31:44:13	172.16.200.162:6868	US/New Orleans, LA	MTA 6328-2Re-SIP HTTP	16.2.77	-	
10		00:a0:bc:46:0f:18	172.16.0.173:5200	US	MTAX28-SB2	1.0.0		
11		00:a0:bc:46:15:b8	172.16.212.106:6880	US/Dallas, TX	MTAX28-SB2	1.0.0	-	
12		02:99:2d:57:c7:00	172.16.0.198:5200	US/SanJose	MTAX28-SB2	1.0.0		

Figure 6.1. Device Query Screen

6.1.2 Querying Devices

The administrators can query devices by their MAC addresses, IP addresses, device types, device status, assigned regions, firmware versions and user IDs.

NOTE: System Administrators are only allowed to query devices in their own granted regions.

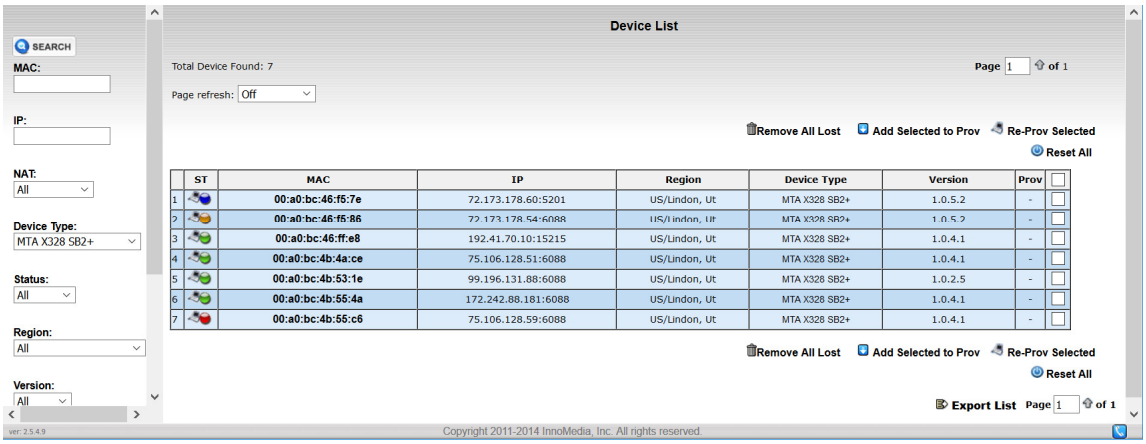
To query a device, follow these steps:

1. Enter your search or filter criteria in the search fields in the left panel.
2. Click the Search button. Devices that matched the search criteria are displayed in the right panel.

Field	Description
MAC	The MAC address of the device. It is OK to enter only the first few digits of the MAC address. The system will match the entered digits in the field and list the searched result in the right panel.
IP	The IP address of the Device
NAT	Indicates if the device is behind a NAT router or not, or if it has a public IP address.
Device Type	Type of the device. The available device types can be found in the drop-down listbox. The device types are defined on Device Type List screen (see Device Type List on page 63).
Status	The current status (i.e., All, Off-line, On-line, or Lost) of the device.
Region	Device's assigned region
Version	Device's firmware version
User ID	Device's user ID (or phone number)
Record Per Page	The number of records you would like to see per page. The default setting is 100.

6.1.3 Device List

On the upper-left corner, you will find the total number of devices found by the system (that match the search filter). The number of records displayed on the screen will depend on what you have specified in the Record per Page field. If the found records are more than the number you specified, you can either enter the page number in the field and click the Go To button, or just simply click the double arrow button for next or previous page.



The following table describes the fields on the Device List screen:

Field	Description
Page Refresh	Page will refresh at the selected refresh rate and the **default is 1 min**. Page refresh can be selected to be: Off, 10 sec, 30 sec, 1 min, 5 mins, 10 mins, 30 mins.
ST	Device current status.. In addition to Online and Offline status, certain devices having capability to report device "lost registration" and "line disabled" status to EMS. Green icon ( ) indicates Device is Online and Registered. Red icon ( ) indicates Device is Offline. Blue icon ( ) indicates Device is Online, and Registered, but line is disabled. Orange icon ( ) indicates Device is Online but lost Registration with the SIP server Gray icon ( ) indicates Device is lost (off line for more than 7 days or the max lost day defined in global parameter page). In a multiport device, since only the status of the device is represented, the OnLine-Registration failure status will take precedence over Online but having a line disabled status. Clicking the Status (ST) icon will popup a Device detail information page.

MAC	The MAC address of the device.
IP	The IP address of the device.
Region	The device assigned region name.
Device Type	Type of the device.
Version	The current firmware version loaded to the device
Prov	Indicates whether this device under EMS provision control.
Check Box	Click to select all devices in the list, click again to deselect all selected devices in the list.

There are several buttons on both top and bottom of the device list:

Button	Description
Remove All Lost	Removes all the Lost devices from the query. If the device sends a heartbeat again, the unit will be entered back into the list.
Add Selected to Prov	Add selected Device to Provision list
Delete Selected	Delete selected Devices
Re-Prov Selected	Send Re-Provision to selected Devices
Reset All	Send Reset to selected Devices

6.1.4 Device Information

Clicking the Device Status (ST) icon will take you to the device detail information screen. Device information screen provides specific device detail information. From this screen, the system administrator can either Telnet to the device or connect to the device web-based GUI interface to change the device settings. Also, the administrator can reset or re-provision the device by simply clicking the RESET or RE-PROV button, even while the device is behind a NAT firewall.

Please note that the information bar may contain different tabs that depend on what MIB Group Access right was granted to the current system administrator. However, the device type, Location Information, Event Information and Trap Information are default tabs.

6.1.4.1 Accessing Device Information Screen

1. Select Device icon. 
2. Select “Device Query” tab
3. Click “ST” icon of a selected device.

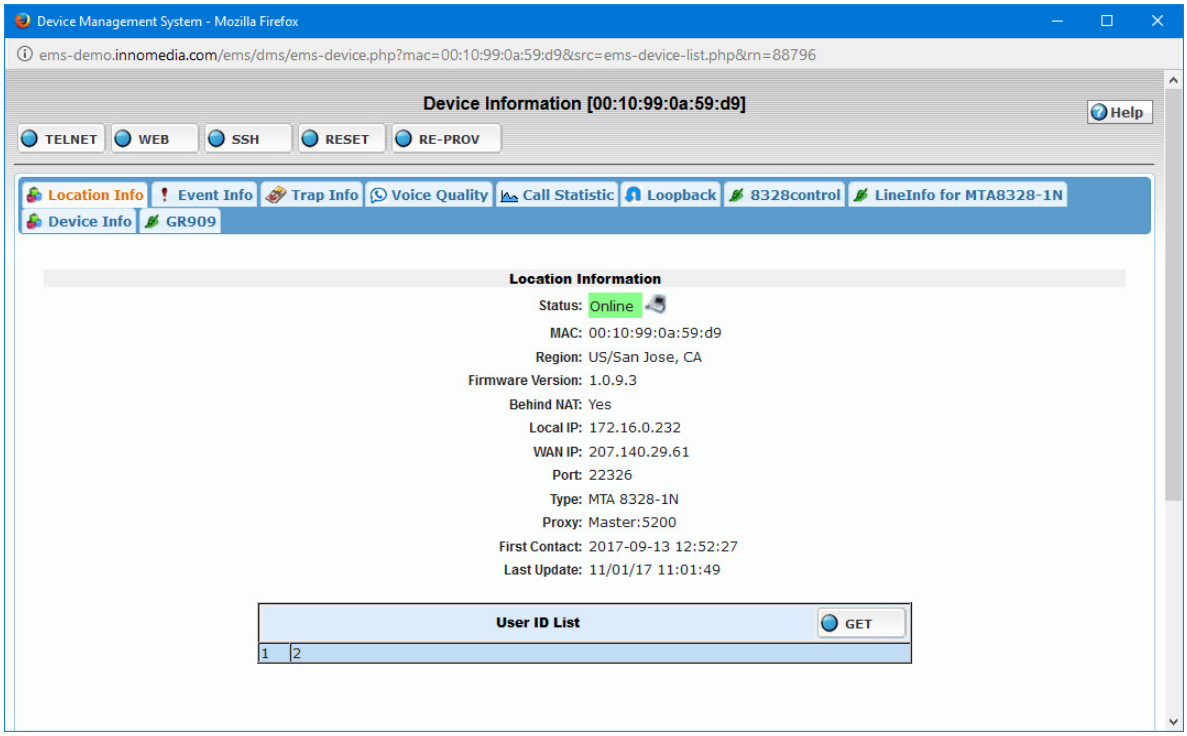


Figure 6.2. Device Information Screen

Device Info page includes the following features:

- TELNET: Open Telnet window to the device. This function is not available on certain devices eg ESBC
- WEB: Open Web browser to the device web interface.
- SSH: Open SSH window to the device. The device needs to support SSH and the browser needs to have the SSH client eg WinSCP
- RESET: Send reset command to the device.
- RE-PROV: Send re-provision command to the device.
- Location Info tab: basic information of this device collected by EMS.

NOTE: For ESBC devices managed via the EMS, since the EMS servers are considered to be secure and trusted device management entities in the operator's network, the EMS only requires a valid ESBC user account id to access the ESBC device.

NOTE: If EMS system is configured and accessed via host name, then the device also needs to support it.

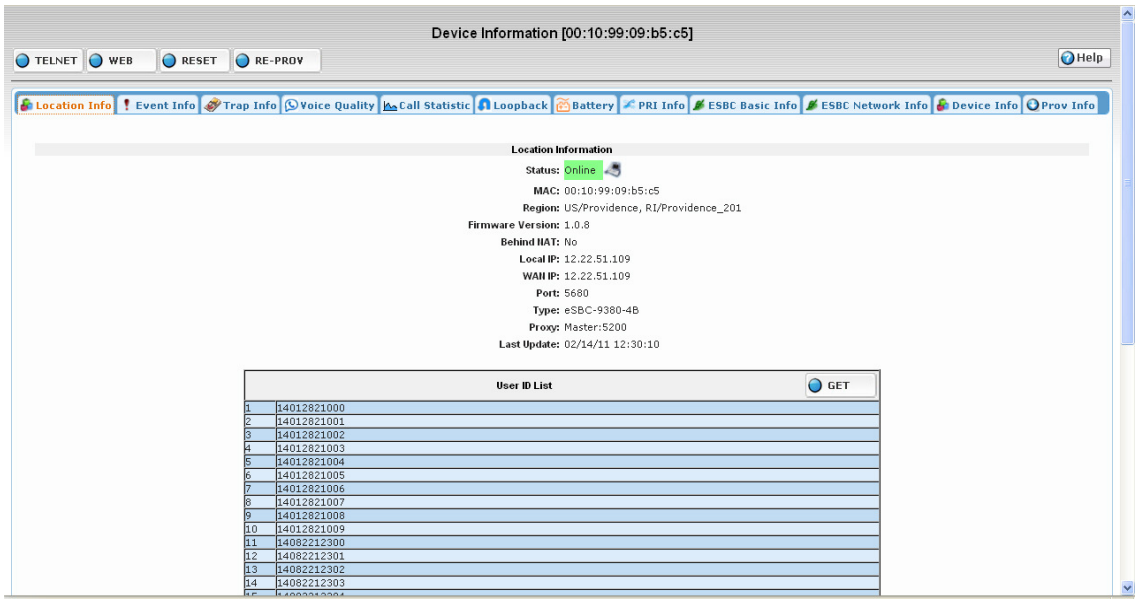


Figure 6.3. Location Information Screen

Location Information shows the current register status of the device.

Field	Description
Status	The current status of the device Typically, it will show - Online - Offline For devices supporting Registration Status, it will also show the following depending on the device status: Online-LineDisabled Online-RegFailed
MAC	The Mac address of the device
Region	The device assigned region name
Firmware Version	The device loaded firmware version

Behind NAT	If the Local IP is not equal to the WAN IP, the Behind NAT will be true.
Local IP	Is the IP address assigned to the device
WAN IP	If the device is installed behind a NAT/Firewall, it is the IP address of the NAT/firewall. If the device is on the public Internet, it is the IP address of the device.
Port	If the device is installed behind a NAT/Firewall, it is the external port on the NAT/firewall that opens for public access. If the device is on public internet, it is the port number of the device.
Type	Is the Device type. Different type of device may use different set of SNMP data set.
Proxy	The proxy server that the device connects to.
First Contact	First Time the EMS received a packet from this Device is recorded
Last Update	Time that the information on the page was updated.

User ID List

User ID list displays the User ID (or Phone number) assigned for the device. When a device is connected to the EMS, the user ID can be displayed by clicking the GET button. The last time the GET button was clicked, the EMS stored the information for this device into the database, and every time from here on, it will display these user ID's for this device until GET is clicked again and a new value is received. To update the User ID list, click the Get button on the top right of User ID List.

- Event Info tab, Event message relate to this device.

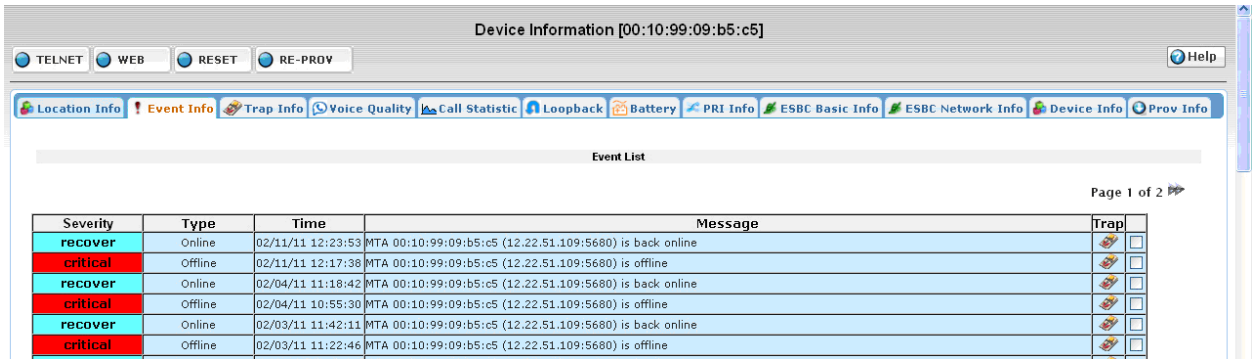


Figure 6.4. Event List Screen

Event Information shows all events related to this device. The system administrator can trace back to the original trap message that causes this event.

Field	Description
Severity	Event severity level
Type	Event Type
Time	Is the timestamp when the event was generated
Message	Event message
Trap	Click the trap icon to show the original trap message.
Select All	Click to select all the event records on the current page.
Delete Selected	Deletes selected records. To delete event from the database, click the check box on the right of the event record, and then click the DELETE SELECTED button at the bottom-right corner of the screen.

- Trap Info tab, Trap messages generated by this device.

Figure 6.5. Trap List Screen

Trap information screen shows all trap messages related to the device. Only the traps that caused the events will be recorded and stored in the database. The system administrator can see the detailed information related to the traps that include the trap OID, time, and the message sent with the trap. To delete a trap or multiple traps, check the option box of the trap/traps and click Delete Selected at the

bottom-right of the screen. To delete all the traps at once, click Select All at the bottom-right of the screen, and then click Delete Selected.

Field	Description
OID	Trap OID that generates this trap
Time	When was the trap generated
Message	Value of the trap message
Select All	Click to select all the trap records on the current page.
Delete Selected	Deletes selected records. To delete trap from the database, click the check box on the right of the trap record, and then click the DELETE SELECTED button at the bottom-right corner of the screen.

- Voice Quality tab, Voice quality analysis for this device.

Device Voice Quality screen shows the history of the device voice quality parameters over time.

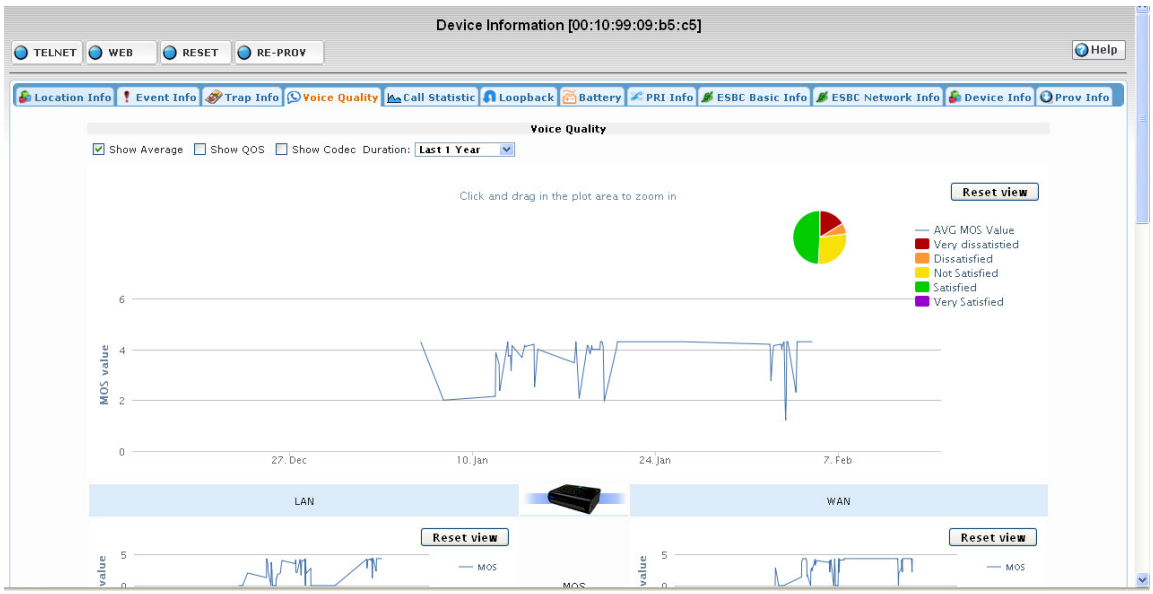


Figure 6.6. Voice Quality Screen (Example for ESBC)

Note: Both LAN and WAN statistics available for ESBC, and WAN statistics only for MTA

Voice Quality Parameter

Administrator can change the “Duration” box to zoom in/out the history chart.

Administrator also can use a mouse click and drag on the history chart to select and zoom into the selected period of time.

Check “Show Codec” to display voice quality parameter of different codec.

CDR List

All calls that are within the selected time frame will list in the CDR-List.

Clicking individual CDR records will show CDR detail on the panel right of CDR list.

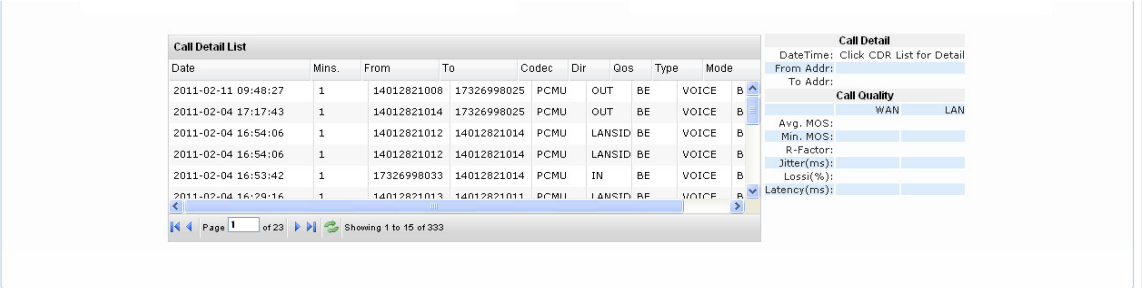


Figure 6.7. Call Detail List Screen

- Call Statistic tab, Call statistics for this device.

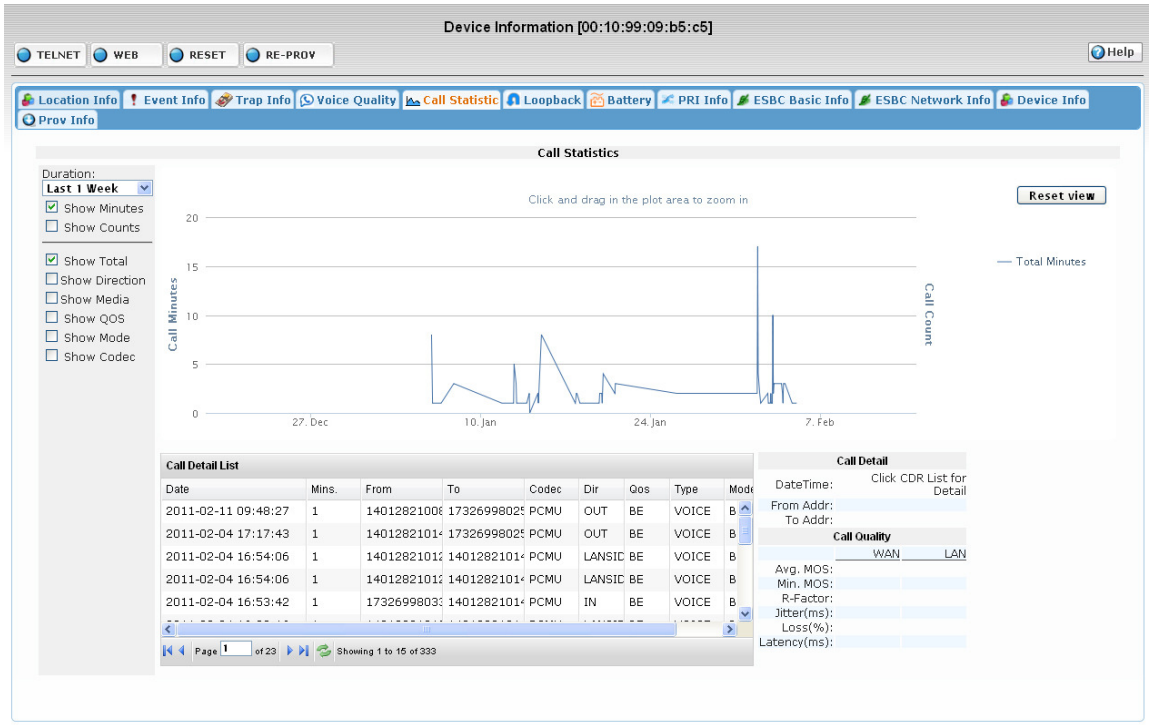


Figure 6.8. Call Statistics Screen

Call Statistics screen shows history of call minutes and call count during a selected time range.

Device Call Statistics

Administrator can change the “Duration” box to zoom in/out the history chart.

Administrator also can use a mouse click and drag on the history chart to select and zoom into the selected period of time.

Check “Show Minutes” to display call minutes during a selected time range.

Check “Show Count” to display call count during a selected time range.

Check “Show Total” to display sum of call statistics during a selected time range.

Check “Show Codec” to display call statistics based on different CODEC during a selected time range.

CDR List

All calls that are within the selected time-frame will be listed in the CDR-List.

Clicking on individual CDR records will show CDR detail on the panel right of CDR list.

- Loopback tab, Voice Quality Loop back test utility.

Device Loopback test utility evaluates the device voice quality by creating a phone call from EMS to device. The Device must support SIP loopback to perform this operation. EMS tester sends a RTP stream to device and records the loop-back RTP data. Then EMS calculates the RTP data by PESQ. EMS also collects the voice quality parameters by RTCP and show the quality parameters history during the test call.

NOTE: Loopback test only applicable for devices that are outside of firewall or NAT, and can be accessed from public Internet.

User ID List

EMS needs to know the User ID (or phone number) first before the test procedure. If the User ID is not correct at the discovery or not up to date, click the GET button to refresh the User ID.

Start Test

Select Codec type and "Testing Mode" and click the GO button next to the User ID to start the test. The test may take 30 to 40 seconds. **NOTE:** Test won't run if matching codec is not selected

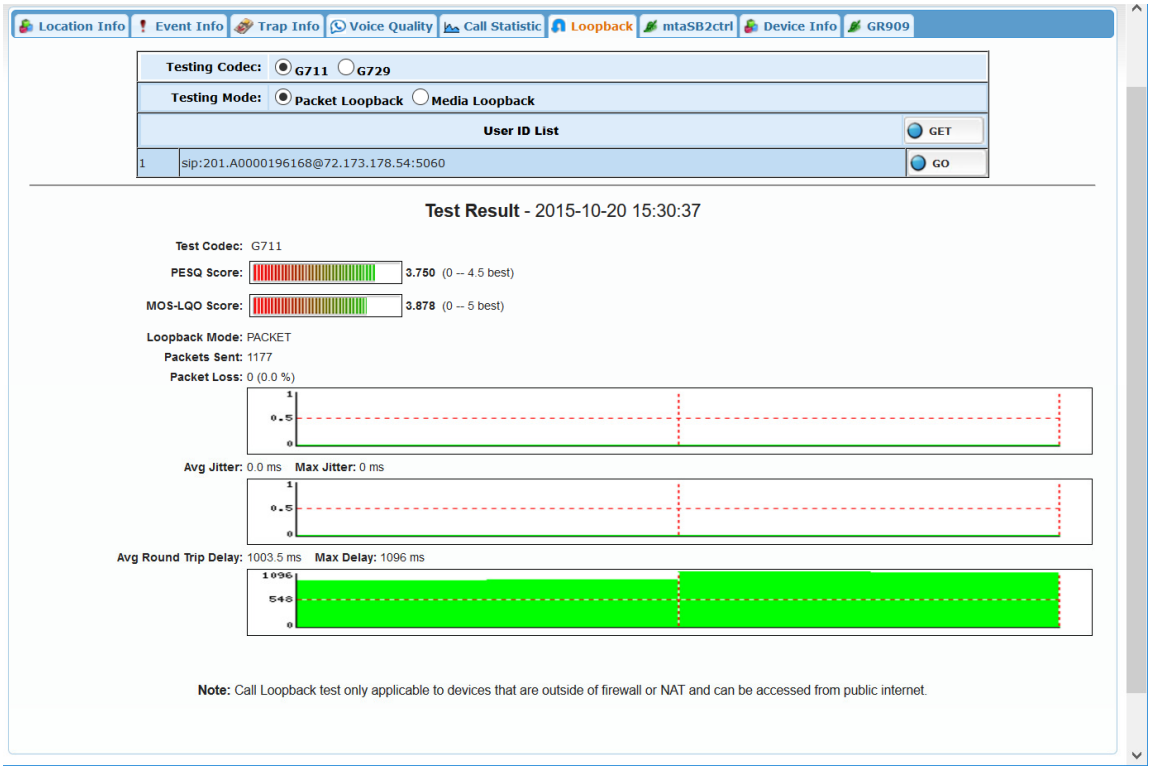


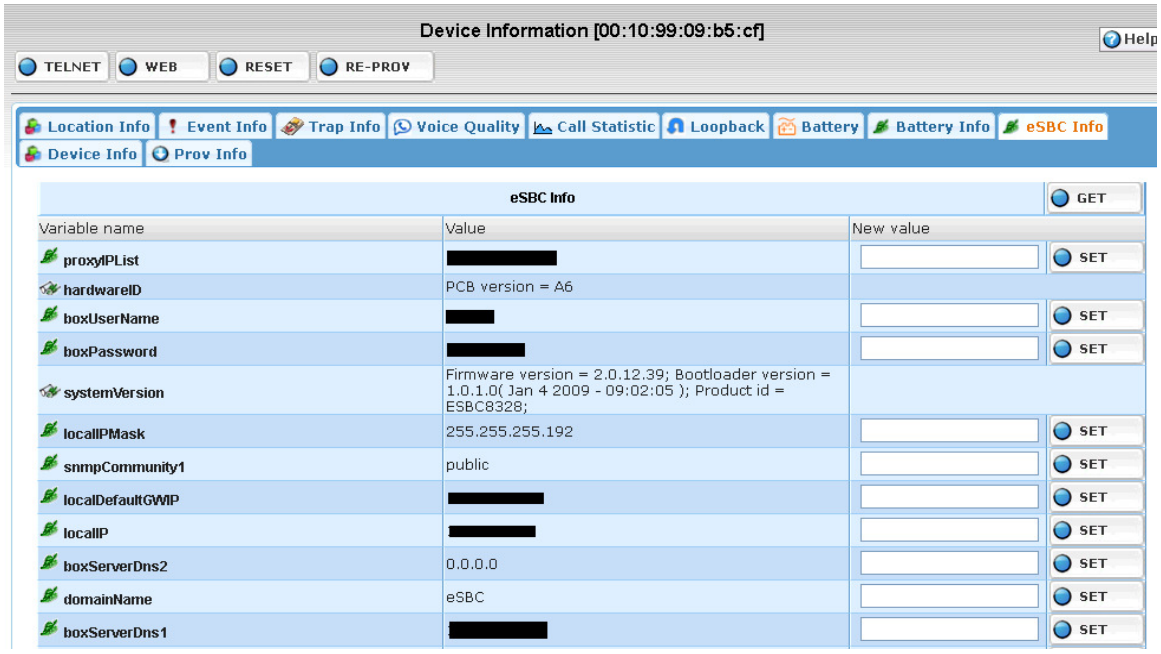
Figure 6.9. Loopback Screen

Test Result – Date/Time

Field	Description
Test Codec	Codec used for testing
PESQ Score	The final PESQ score of the test call
MOS LQO Score	This provides a MOS Listening Quality Score
Loopback Mode	This shows the selection of type of looback that was used in the test call ie “packet loopback” or “media loopback”
Packet Sent	Total number of packets send to device
Packet Loss	Percentage of packets lost
Avg Jitter	Average Jitter in milliseconds.
Avg Round Trip Delay	Average Round trip delay in milliseconds

- MIB Data Group tab, MIB Data Group assigned to this device type.

  Each MIB Data Group assign to device type will have a tab on device info page. The name of type is same as the title of MIB Data group. These are not always going to be present. It is created by the Administrator. The ESBC Info Tab or MTA Info Tab are examples. Please see below for an example.



Click the MIB Data Group to open the MIB Data page.

MIB Data page shows a list of MIB variable pre-set in the MIB Data group.

Field	Description
Variable name	The name of OID
Value	Value of MIB variable from device. If EMS can not get the data from device, it will show as "unknown"
New Value	Put the new value in the input box for setting the MIB variable
Set	Click to set the new value to MIB variable

Refresh Data

Click the top right Get button can reload the MIB data from device in real-time.

Set Data

Use the following steps to set data to device.

NOTE: Data set by SNMP usually device does not keep it permanently

1. Put new value into "New value" input box
2. Click Set button next to the input box to submit the update to device.

- MIB Graph Group tab, MIB Graph Group assigned to this device type.

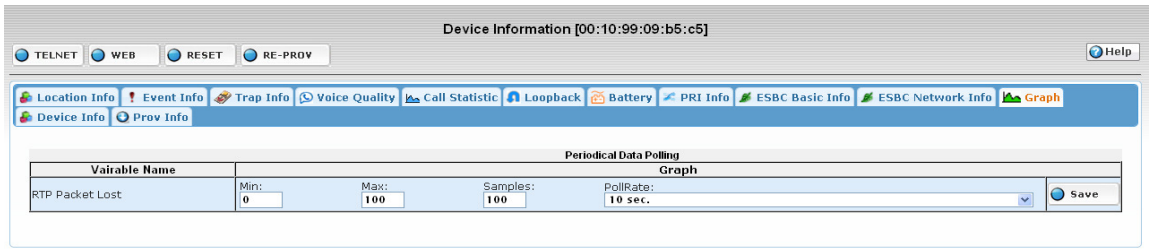


Figure 6.10. MIB Graph Group Screen

MIB Graph Group allows the system administrator to set the periodical polling targets and set the polling range to display the data in graphical format.

NOTE: Only numerical MIB variable can be polled

Field	Description
Variable name	Polled MIB variable name
Graph	History chart of value change
Edit	Enable and Edit the polling parameters
Delete	Disable the variable polling

Start polling

Since polling is a resource intensive process, the polling variables have to be enabled individually on each device. By default all polling variables are disabled. To start polling, follow the steps:

Click the Edit button next to the MIB variable.

Fill the field setting in the row.

Click OK to submit the update.

Field	Description
Variable name	Polled MIB variable name
Min/Max	Sets the possible range of poll
Samples	Number of the samples kept in the database.

Polling Rate	Polling interval in seconds.

Stop polling

Click the button next to the polled variable to stop the polling.

- Device Info tab, Remote summary web page of this device.

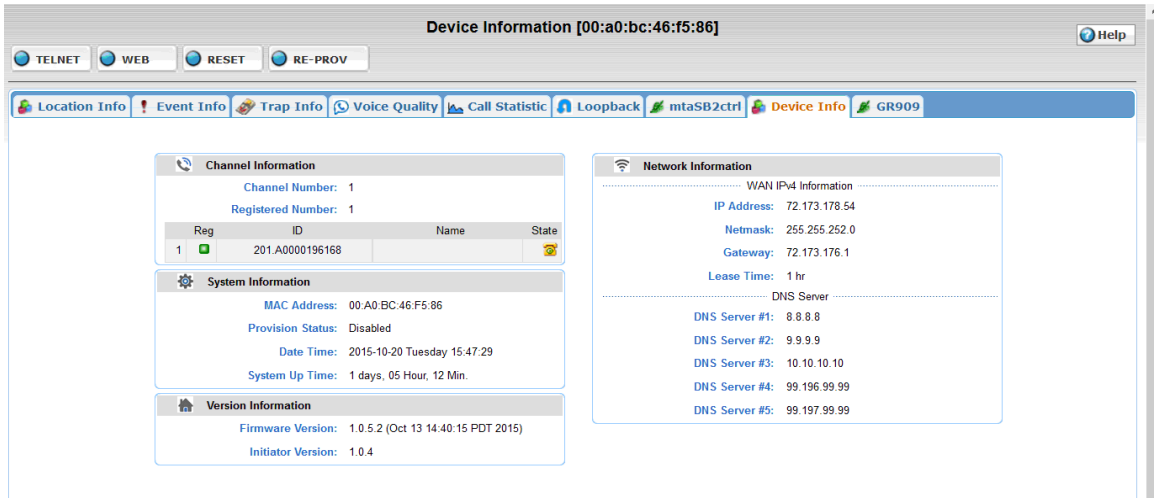
Device Info page is a short cut for EMS to directly access a predefined web page on device. Since the page is on device, device must be online to retrieve the info page. The info page URL is defined in the Device Type Configuration Screen; in a field call “Extra Device Info Page”. InnoMedia device usually use “dmsinfo.ssi”.

NOTE: The ESBC page is different then the MTA page, so you should expect to see major differences.

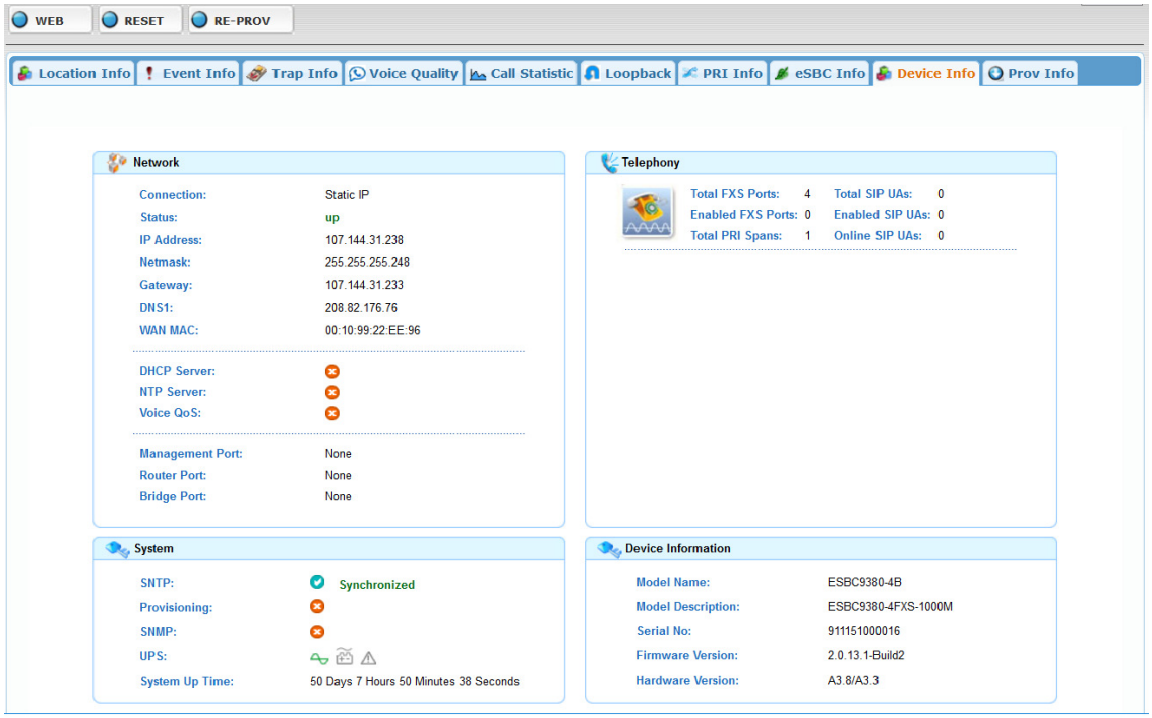
Access Device Info Page

Click Device Icon. Select “Device Query” tab. Select a device by click the status icon Select “Device Info” tab.

A particular MTA “Device Info” screen example:



A particular ESBC “Device Info” screen example:



- Prov Info tab, Provision configuration of this device (if available).
    1. Provisioning allows you to configure the unit with options every time it is brought online, and at a preset time span after it is first provisioned, such as firmware upgrade, and Account Setup, without having to connect to the box.
    2. It is a very powerful tool that is highly recommended, especially if you have a large number of devices to support.

Please see Provisioning Section 9.5 for a better understanding of Provisioning.

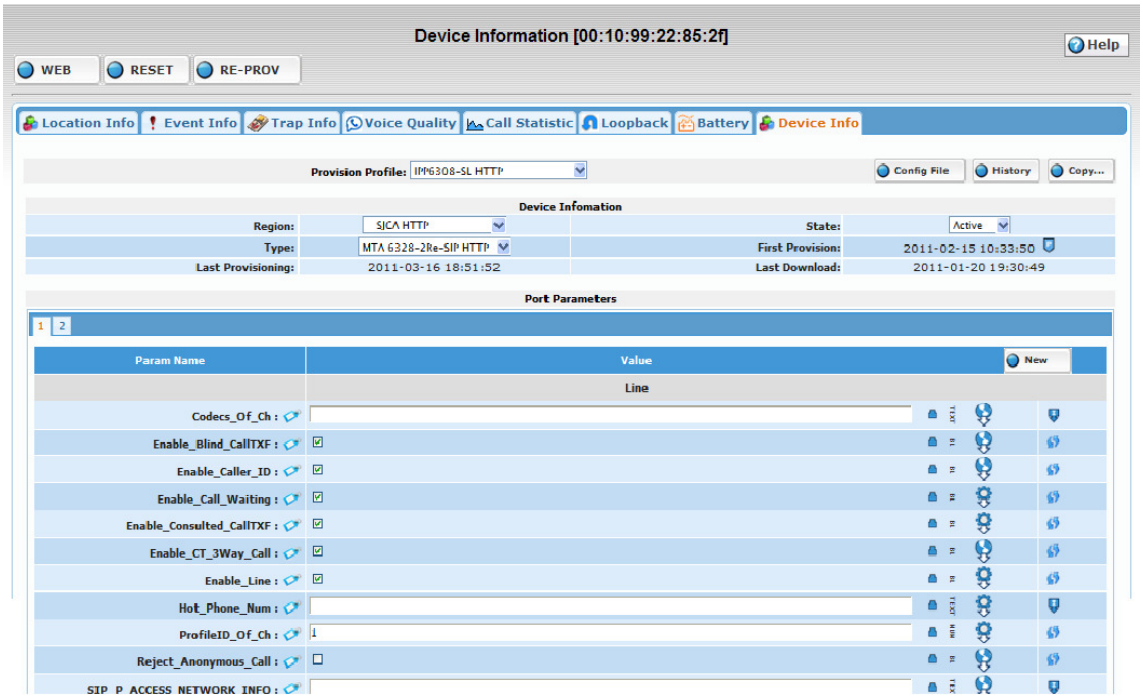


Figure 6.11. Provisioning Configuration Device Screen

- GR909 tab, GR909 testing and results (if available).

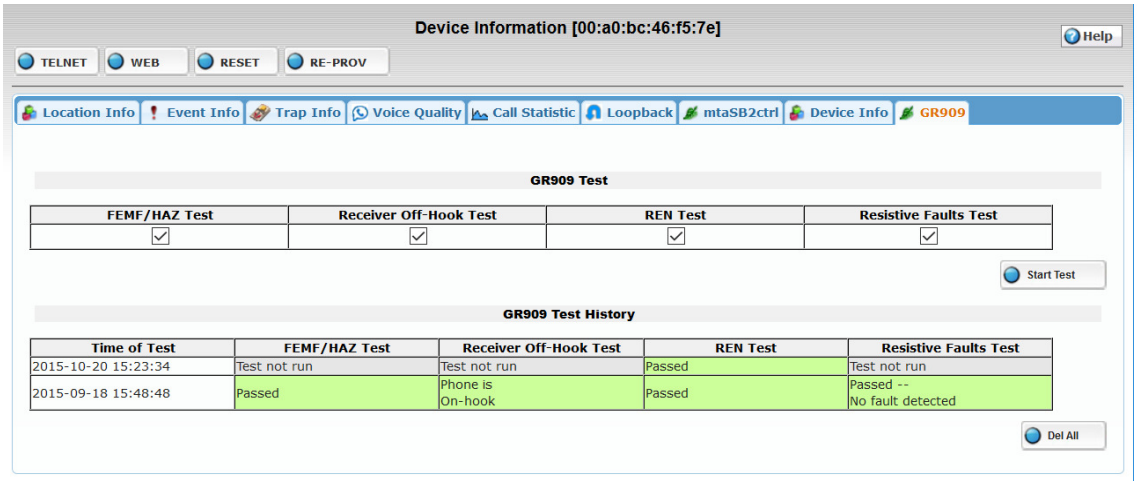
Some InnoMedia devices support GR909 functionality and the GR909 testing feature provides information relevant to the device's RJ11 connections and reports possible faults on the RJ11 ports. This is a useful tool which can be triggered from EMS and allows service provider personnel to diagnose RJ11 port problems such as foreign or hazardous voltages on the RJ11 telephone line, unintended device off-hook, REN overload, and resistive fault on end customer devices. The results are then conveyed back to EMS which keeps historical records of the GR909 tests run on that device.

i. **<u>FEMF/HAZ Testing</u>**. Foreign Electromagnetic Field Hazard ("FEMF/HAZ") testing shall test both direct current ("DC") and alternating current ("AC") voltage from outside the device between tip to ground, ring to ground, and tip to ring. Tip to ground and ring to ground testing are only available if the earth ground is connected to the device's power input ground, requiring a 3-prong adapter, and that the earth ground is connected to the DC ground. When the DC voltage exceeds 6 volts ("V") or the AC voltage exceeds 10 root mean square voltage ("Vrms"), the FEMF/HAZ test shall report the presence of foreign voltage through EMS. When the DC voltage exceeds 135V or the AC voltage exceeds 50Vrms, the FEMF HAZ test shall report the presence of hazardous voltage through EMS.

ii. **Receiver Off-Hook Testing**. The receiver off-hook testing shall measure if the phone is on-hook, off-hook, or if there is a resistive fault (a short circuit) on the telephone line. The receive off-hook test shall report the outcome of the test through EMS.

iii. **Ring Equivalence Number Testing**. The ring equivalence number ("REN") test shall measure the ringing load on the telephone line where 1REN is defined as 6930 Ohm ("Ω," a unit of electronic resistance) in series with 8µF capacitor, per FCC part 68 specifications. When REN is less than 0.175 or greater than 3.300, the REN test shall report through EMS that the REN is operating within an out of range error.

iv. **Resistive Faults Testing**. The resistive faults test shall test the resistance load between the tip and ground, ring and ground, and trip and ring. When the resistance on the resistive faults test is less than 150kΩ, the test shall report through EMS a resistive fault.



GR909 Test Results will indicate if the selected tests Passed (with indication in some cases), Failure with the cause of Failure, and also if selected test can not be performed. Tests results are also displayed with background color for better indication. For any tests not selected when clicking the Start Test button, it will state "Test not run" with grey background.

GR909 test result history is displayed in a tabular format and all the entries and be deleted when not necessary with the Del All button.

- Battery Info tab, Battery status history information for this device. **NOTE:** This feature is only available if device is capable to report battery status information to EMS

  Battery Info Screen provides the current and history view of device battery status.

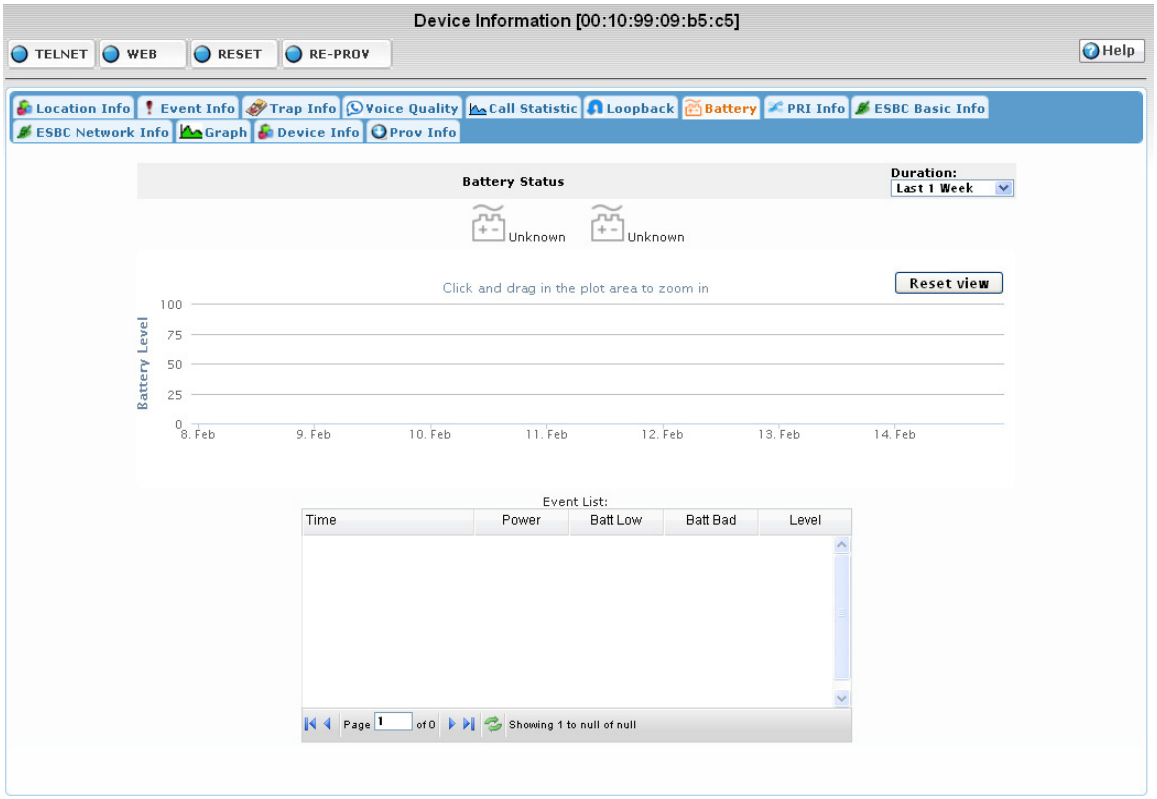


Figure 6.12. Battery Status Screen

Battery Status

Battery Status shows the current battery status. Battery status has two icons:

NOTE: If the device is offline, then the status is the last state the device reported

NOTE: This feature has not yet been implemented for ESBCs

Power Source:

-  : Device is Powered by AC now.
-  : Device is Powered by Battery now.

Battery Status:

-  : Battery is bad or missing.

- : Flashing Battery icon means battery is low.
- : Solid Battery icon means Charging Battery/Battery is Full.

Battery History

Battery History shows the Battery power level during the selected range of time. Battery History can zoom in by click and drag on the plot area. Click the "Reset View" button to zoom out to original time range setting.

Battery Event Detail

Battery Event Detail list is all battery event sent from device during the selected time range.

Field	Description
Time	Timestamp when received the event
Power	Device is powered by AC ( ) or Battery ( )
Batt Low	: Battery is normal. : Battery Low event detected.
Batt Bad	: Battery is normal. : Battery Bad event detected.
Level	Battery power level in percentage

- **PRI Tab:** PRI interface status information for this device (if available).

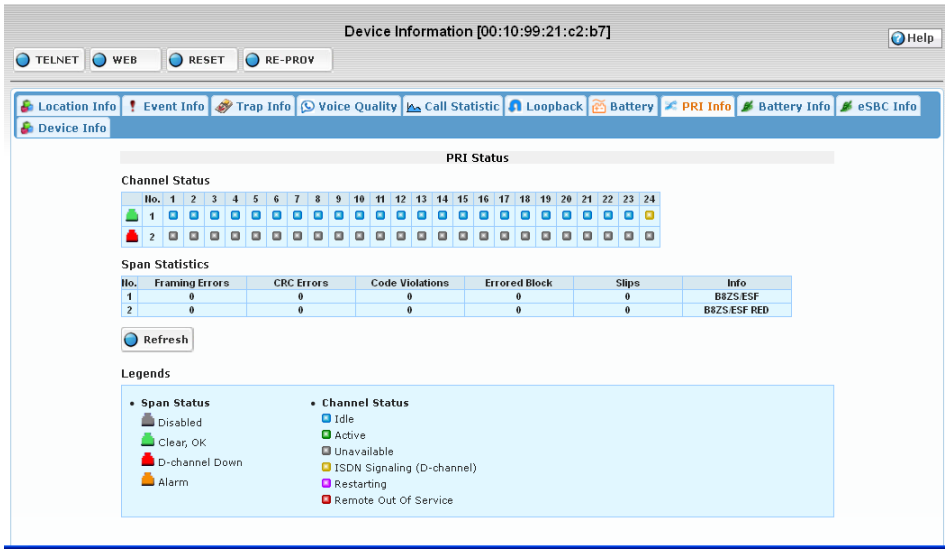


Figure 6.13. PRI Status Screen

PRI Status Screen shows the current PRI interface status of device.

Channel Status

Channel Status show the status of each Span and Channel.

Click “Refresh” Button to manually update latest status from device.

Legends

Span Status

- Disabled
- Clear, OK
- D-channel Down
- Alarm

Channel Status

- Idle
- Active
- Unavailable
- ISDN Signaling (D-channel)

6.2 Call Statistics

This screen provides graphical information on calling trends. Calls can be filtered by device, region, type and phone numbers.

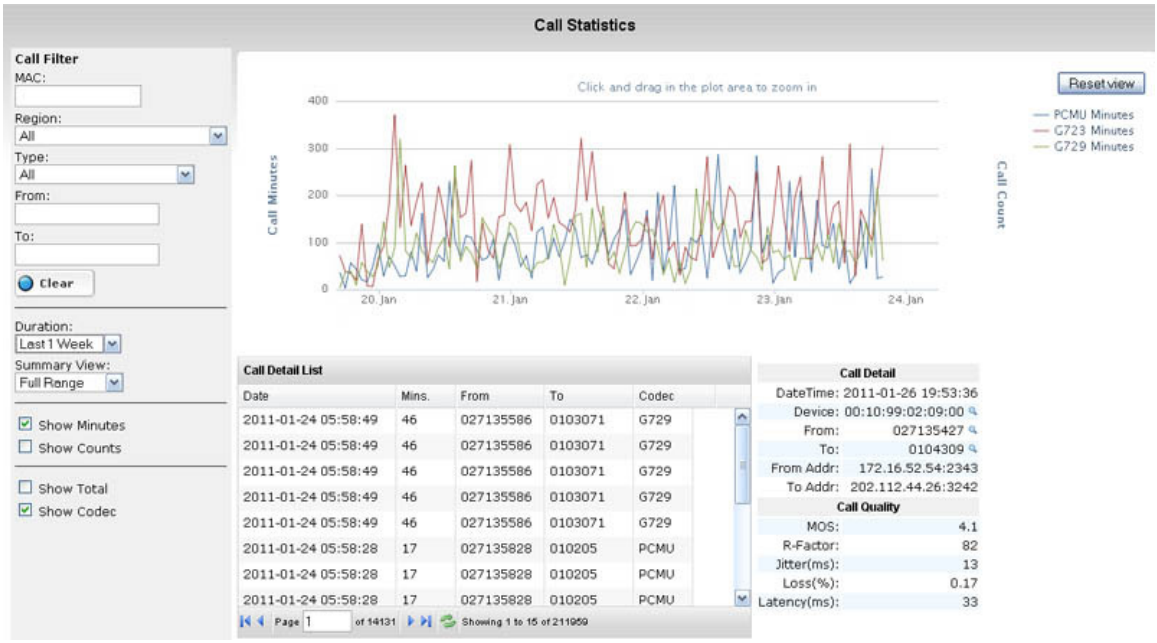


Figure 6.14. Call Statistics Screen

NOTE: this is a screen shot of VoIP Device (MTA), the ESBC will be different, and have a few more filters, such as Show Direction and Show Media, as well as the Show Total and Show Codec

It also shows individual call details. This list gives the operator data on not just important attributes associated with the call such as call time, call length, caller/callee information etc., but also, by highlighting a particular call, quality-related metrics can be seen in the lower right-hand sub-window. For this specific call, MOS, R-factor, jitter, packet loss and delay are provided and can be used to pinpoint what particular issue may have caused this particular call to experience quality problems.

6.2.1 Accessing Call Statistics Screen

To access Call Statistics Screen, follow these steps:

1. Click Device icon.
2. Select “Call Statistic” tab

6.2.2 Call Filter

Use the call filter to select or zoom into a particular section of data of interest.

Field	Description
MAC	MAC Address for device as filter.
Region	Filter devices within selected region
Type	Filter devices with selected type
From	Filter by Caller phone number.
To	Filter by Callee phone number.

"Clear" button 

clears all call filter fields.

6.2.3 Time Range Setting

Field	Description
Duration	How long of the call data to be display from now.
Summary View	**Full Range**: Display full time range from now back to date set by duration. ***By Daily Hour:*** *Consolidate call data by hours of all calls during that duration of time.* **By Week Days:** Consolidate call data by Week day of all calls during that duration of time.
Show Minutes	Show line displaying total talk minutes.
Show Counts	Show line displaying total call numbers.
Show Total	Show all lines for all CODECs
Show Codec	Show lines for individual CODECs

NOTE: below is a screen shot of VoIP Device (MTA), the ESBC will show a different view

Summary View

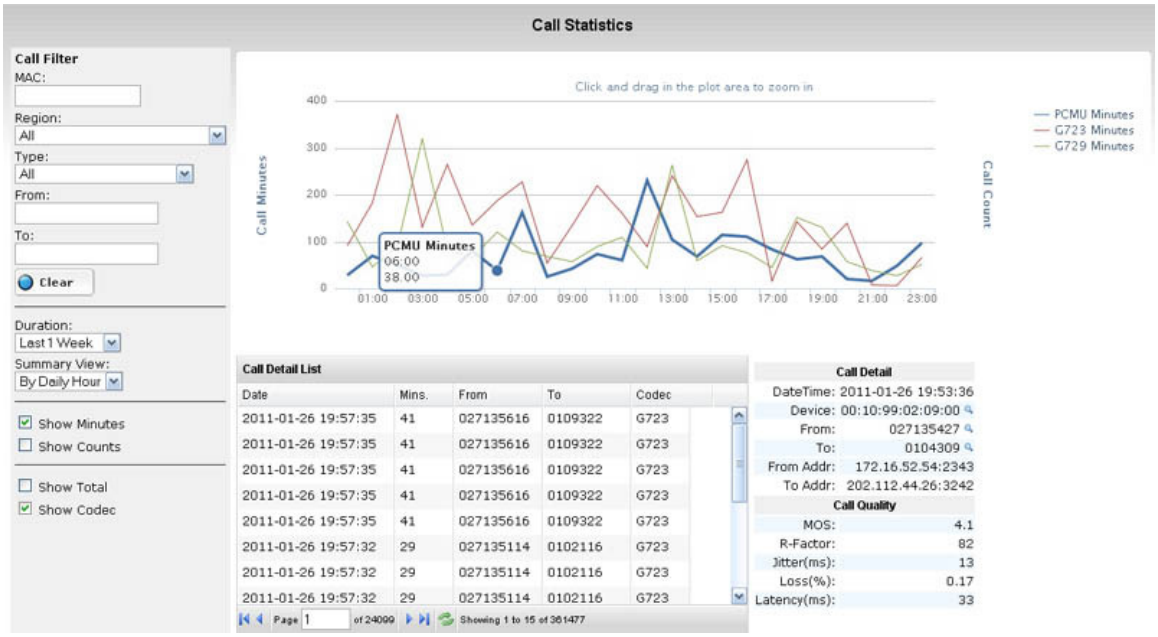


Figure 6.15. Call Statistics Screen – Summary View

6.2.4 Zoom in/Zoom out Line Chart

Click and drag on the plot area to zoom into a selected time range.

Click the “Reset View” button to zoom out to original time range.

6.2.5 Quick Filter

Click a record in the **CDR List table**, Call Detail will show on the right of CDR List table.

Click the **Device/From/To** field in the CDR Detail will apply it as a call filter automatically.

6.3 Voice Quality

Voice Quality provides different type of views to help administrator analyzes various voice quality parameters. Three different analysis types in Voice Quality Screen:

- Time View: **Time View** shows various Voice Quality parameters changing over time.
- Analysis View: **Analysis view** shows the impact of four separate quality-related variables in a single, visually informative graph.
- Summary View: **Summary view** shows Voice Quality parameters consolidated by Daily hours or week days.

6.3.1 Accessing Voice Quality Screen

To Access Voice Quality Screen, follow these steps:

1. Click Device icon .
2. Select “Voice Quality” tab.

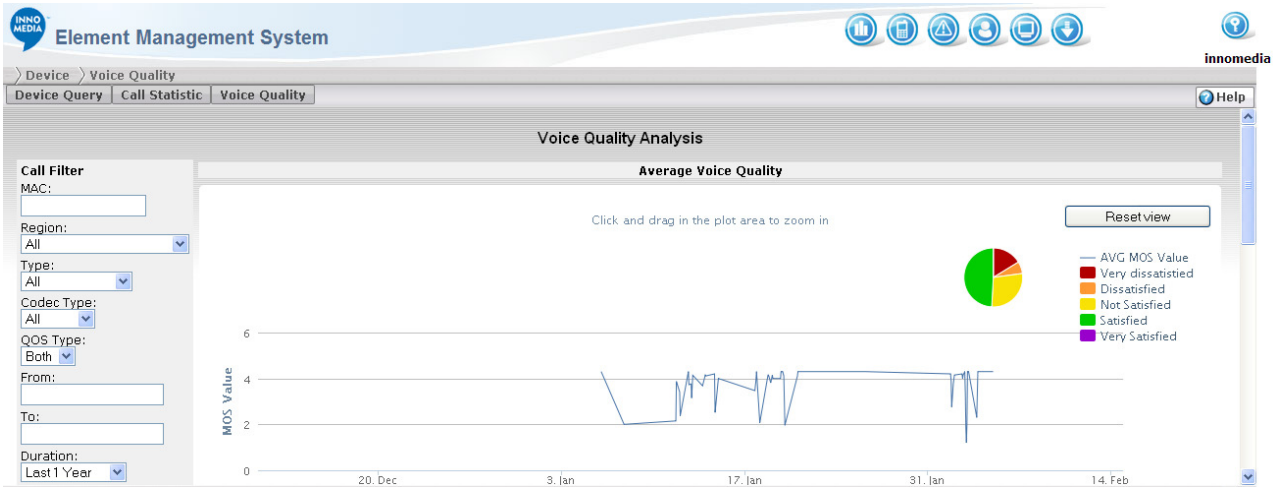


Figure 6.16. Voice Quality Analysis Screen

6.3.2 Call Filter

Use the call filter options in the left panel to select or zoom in a particular section of data of interest.

Field	Description
MAC	MAC Address for device as filter.
Region	Filter devices within selected region
Type	Filter devices with selected device type
Codec	Filter by the selected codec only
From	Filter by Caller phone number.
To	Filter by Callee phone number.
Duration	Duration of call data records to be displayed.

Click Clear button clear all call filter fields.

Quick Filter

Click a record in the CDR List table, Call Detail will show on the right of CDR List table.

Clicking the Device/From/To field in the CDR Detail will apply it as a call filter automatically.

Zoom in/Zoom out

Click and drag on the plot area to zoom into a selected time or value range. In Analyze View you can zoom in both x-axis and y-axis directions. In Time View you can only zoom in x-axis.

Click the "Reset View" button to zoom out to original time range.

6.3.3 Time View

NOTE: below is a screen shot of VoIP Device (MTA), the ESBC will show a different view

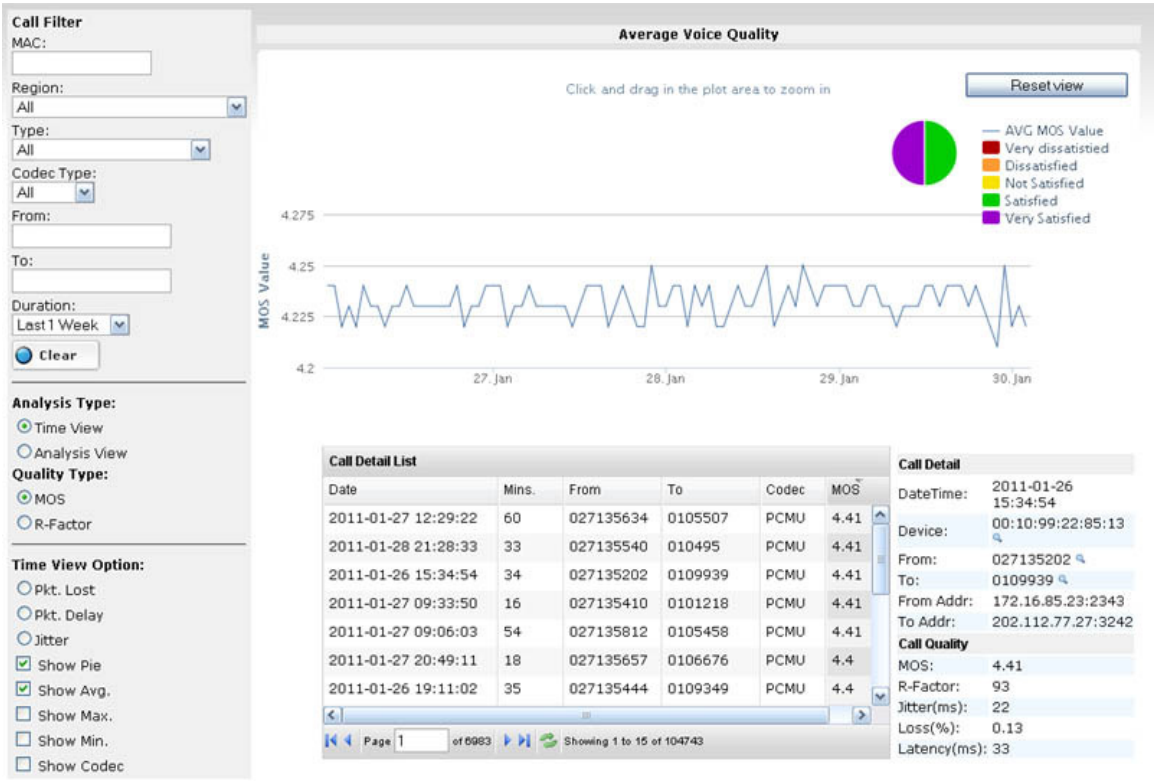


Figure 6.17. Average Voice Quality Screen

Time View Shows various Voice Quality parameters change over time.

A **pie chart** at the top right show the percentage of call quality values distributed in selected call filter and time ranges.

Click and drag in the plot area to select a time range to zoom in. Or set the **Duration** combo box to change the display time range.

Quality Type

1. **MOS**: Display MOS value over time.
2. **R-Factor**: Display R-Factor over time.
3. **Pkt. Lost**: Show Packet lost value over time.
4. **Pkt. Delay**: Show Packet delay value over time.
5. **Jitter**: Show Network jitter value over time.

Time View Options

Options	Description
Quality	Filter calls from one of the five Voice quality categories.
Show Pie	Show Voice Quality value distribution in percentage. **NOTE:** Pie view may take a little longer to display due to increased calculation time needed.
Show Avg.	Show Average Voice Quality values over time.
Show Max	Show Best Voice Quality values over time.
Show Min	Show Worst Voice Quality values over time.
Show Codec	Show various Voice Quality values by different CODEC over time.

CDR List shows all CDR records that match the call filter and selected time range.

6.3.4 Analysis View

NOTE: below is a screen shot of VoIP Device (MTA), the ESBC will show a different view

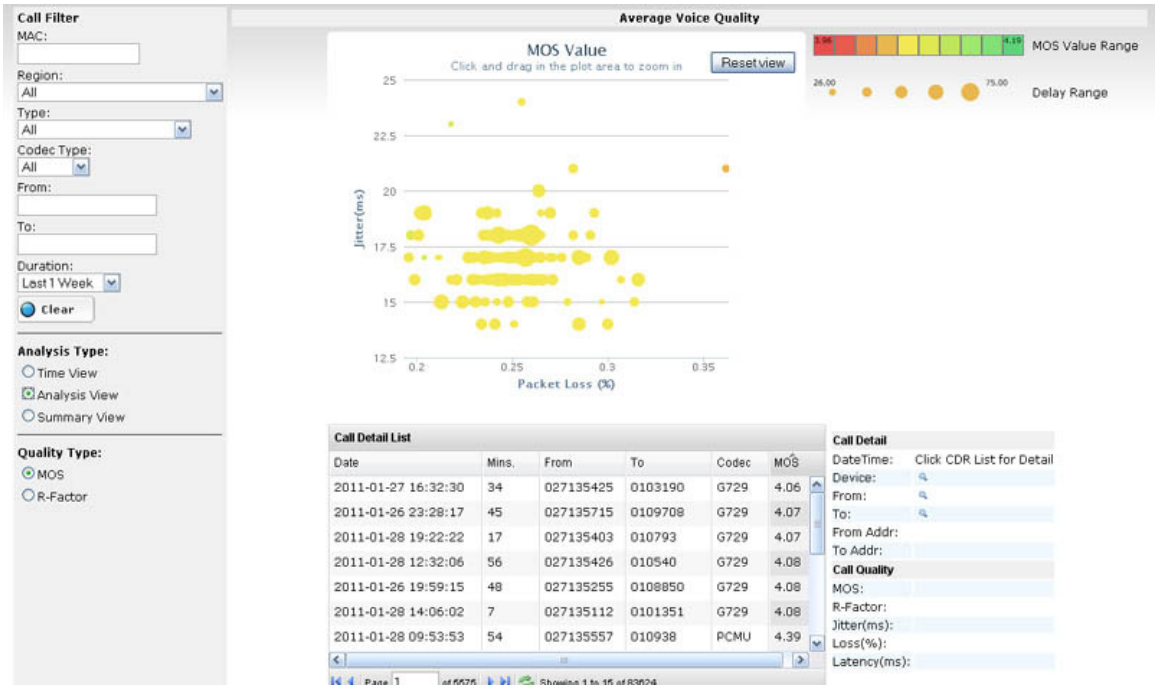


Figure 6.18. Average Voice Quality Screen – Analysis View

Analysis view is an extremely effective way of showing the impact of four separate quality-related variables in a single, visually informative graph: * Packet Loss is measured along the x-axis * Jitter is shown on the y-axis * The size of each circle represents the delay associated with that call * The color of each measurement indicates the quality of that call either in terms of MOS score or R-factor. Green indicates good quality, while red indicates poor quality.

This analysis can be viewed for the entire network, a specific region or a particular sub-region. Again, the graph is interactive in that the operator can click-and-drag to zoom into any part of the graph that may be of interest for closer analysis. By focusing on areas where any one of the four parameters shown in the graph are outside acceptable limits, the operator can get a better picture of what particular network degradations might be causing quality issues.

CDR List shows all CDR records that match the call filter and selected time range.

Quality Type

1. **MOS**: Display **MOS** value as voice quality value.
2. **R-Factor**: Display **R-Factor** value as voice quality value.

6.3.5 Summary View

NOTE: below is a screen shot of VoIP Device (MTA), the ESBC will show a different view

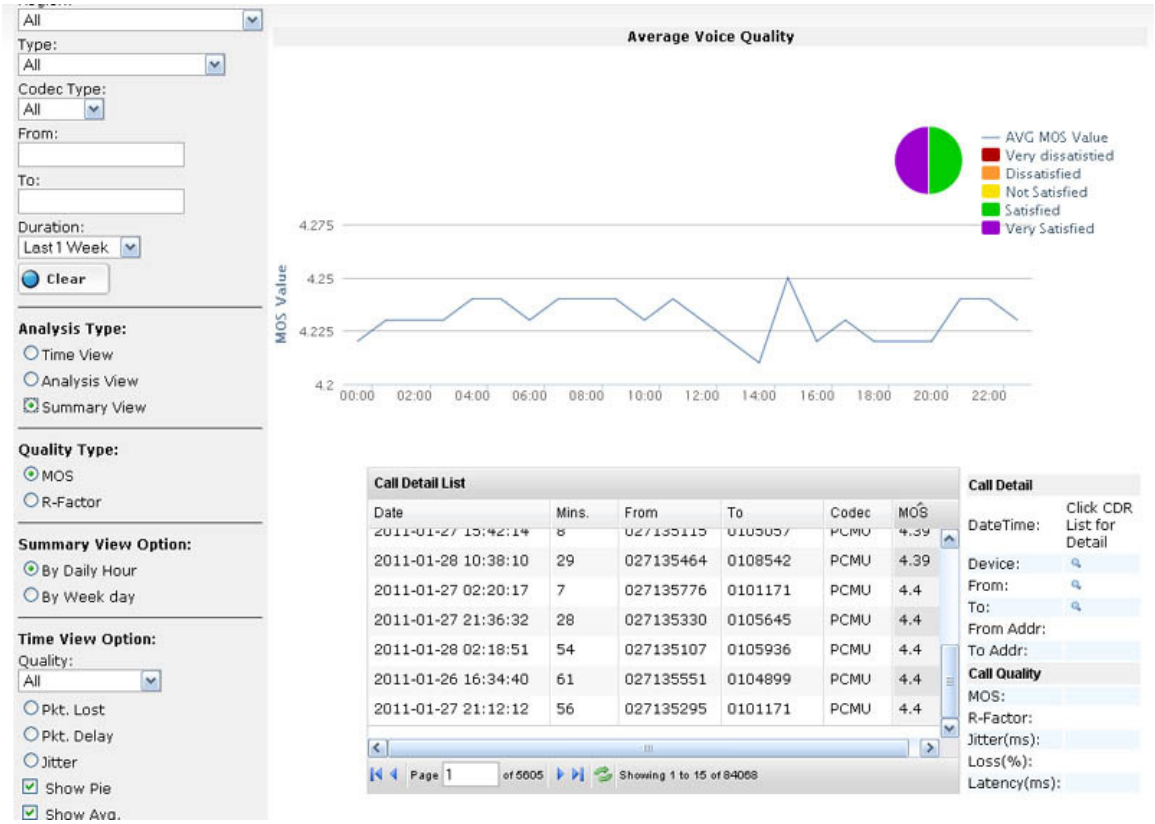


Figure 6.19. Average Voice Quality Screen – Summary View

Summary view shows Voice Quality parameters consolidated by Daily hours or week days.

Summary View Options

Summary view can use all **Time view options:**

Options	Description
By Daily Hours	Consolidate Voice Quality parameter by daily hours.
By Week Days	Consolidate Voice Quality parameter by week days.

6.3.6 Voice Quality Categories Pie Chart

Voice Quality Categories Pie Chart is available in both **Time View** and **Summary View**.

Pie Chart is only visible when **Quality Type** is MOS or R-Factor. Pie Chart is not available for Lost, Jitter and Delay options.

Click a slice of pie chart to automatically apply the selected Voice Quality Categories as **Voice Quality Filter**.

Click the pie chart again (will always show 100% after apply the Voice Quality Filter) to cancel the **Voice Quality Filter**.

7 Fault Management

The Fault Management GUI of EMS allows the system administrator to filter, view and manage traps, events, and alarms.

Trap messages from devices are filtered and translated into Events. Events will be filtered again and sent out as Alarms. Alarms will trigger actions to notify the administrator.

The SNMP trap receiver decodes the trap and sends it to the trap filter. The trap filter checks if the trap OID is defined in the Trap Filter table, if so, it stores the trap data in Trap table. It also checks if this trap should be escalated as an event. If so, the trap filter will generate an event request and send it to event filter.

The event caused by external trap will carry the trap message as the event message.

The event filtering function compares the event against the event filter rules to determine whether to generate an alarm and trigger action, such as sending out e-mails. The current filtering rules are based on the severity level, number of occurrence in a defined duration. The alarm generated assumes the same severity level as the event that triggered the alarm.

7.1 Alarm and Event Query

Alarm and Event Query GUI provides an interface for the system administrator to look up all events and alarms in the database.

7.1.1 Event Query

Event Query screen provides an interface for the system administrators to look up all events in the database within their granted regions. Events can be filtered by time, event ID, device MAC address, event type and event severity level.

7.1.1.1 Accessing Event Query Screen

1. Click the Fault icon.
2. Select “Query” tab
3. Select “Event” tab on the left panel

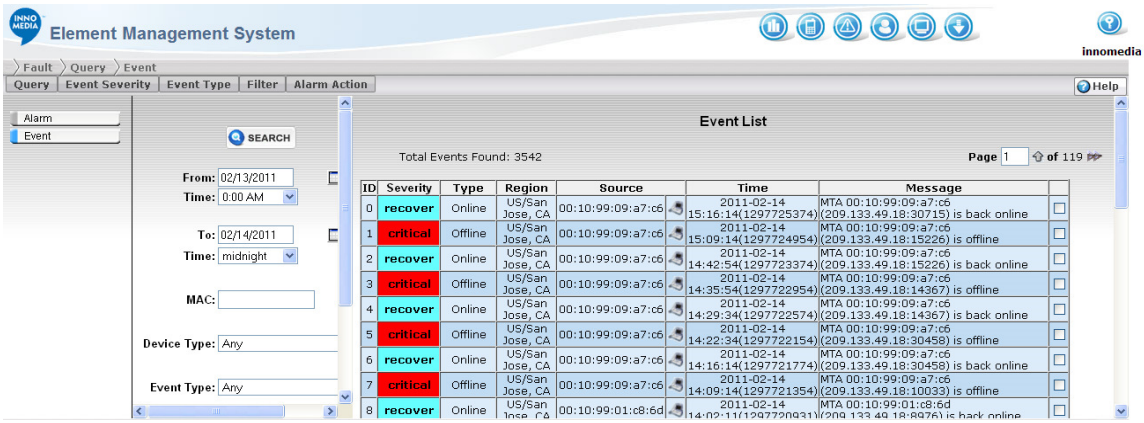


Figure 7.1. Event Query Screen

7.1.1.2 Searching for Events

System administrators can search for events by entering a time range, event ID, MAC address, device type, event type, severity level, or region in the Event Query fields on the screen. To search for events, follow these steps:

NOTE: System administrators are only allowed to search for alarms in their granted regions.

1. Enter the search criteria in the fields of left side panel
2. Click the Search button. Events that met the search criteria are shown on right panel.

Description of search fields:

Field	Description
From: Time:	Enter the search starting date in the From field or select a date by clicking the Calendar icon .
To: Time:	Enter the search ending date in the From field or select a date by clicking the Calendar icon .
Event ID	The identification number of the Event.
MAC	The MAC address of the device that caused the event.

Device Type	The type of the device. For device type definition, see Device Type screen (see page 598).
Event Type	Type of the event. For event type definition see Event Type screen (see page 97).
Severity	The event severity level. For severity level definition see Event Severity screen (see page 1046).
Regions	The region where the events occurred.

7.1.1.3 Event List

Description of Fields and Buttons on the Event List screen.

Field	Description
ID	Identification number of the event that is automatically generated by the system.
Severity	Event severity level, that is defined in Event Severity screen (see page 1046).
Type	Event Type, that is defined in Event Type screen (see page 1047).
Source	Device MAC address that caused the event. Device button  links to Device information screen.
Time	Date and Time of when the event was generated.
Message	Event message.

7.1.1.4 Delete Event Record

System administrators can delete all or selected event records. To delete event records, follow the steps:

1. Search for event recode to be deleted
2. Click “Delete All” to delete all the event records on the current page. Or click the check box on right of event record, and then click the DELETE SELECTED button at the bottom-right corner of page.

7.1.2 Alarm Query

Alarm Query screen provides an interface for the system administrators to look up all alarms in the database within their granted regions. Alarm can be filtered by time, Alarm ID, device MAC address, status, and Region.

Each Alarm has two states: New and Acked. Acked means the Alarm has been handled or acknowledged. This status helps administrator to log what alarm messages have been read.

7.1.2.1 Accessing Alarm Query Screen

1. Click the Fault icon
2. Select “Query” tab
3. Select “Alarm” tab on the left panel

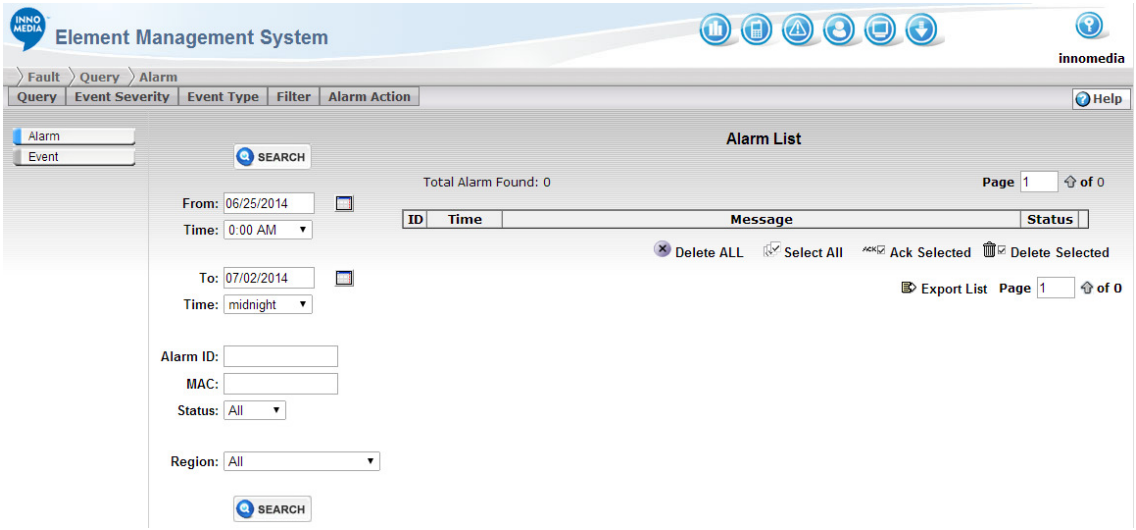


Figure 7.2. Alarm Query Screen

7.1.2.2 Searching for Alarm

Administrators can search for alarms by entering a time range, alarm ID, MAC address, device status, or region in the Alarm Query fields on the screen. To search for alarms, follow these steps:

NOTE: System administrators are only allowed to search for alarms in their granted regions.

1. Enter the search criteria in the fields of left side panel
2. Click the Search button. Alarms that met the search criteria are shown on right panel.

Description of search fields:

Field	Description
From: Time:	Enter the search starting date in the From field or select a date by clicking the Calendar icon ( ).
To: Time:	Enter the search ending date in the From field or select a date by clicking the Calendar icon ( ).

Alarm ID	The identification number of the Alarm.
MAC	The MAC address of the device that caused the alarm.
Status	The status of alarm
Regions	The region associated with the alarm.

7.1.2.3 Alarm List

Description of Fields and Buttons on the Alarm List screen.

Field	Description
ID	Identification number of the alarm that is automatically generated by the system.
Time	Date and Time of when the alarm was generated.
Message	Alarm message.
	Show associated Events. Alarm may cause by multiple instance of an alarm. Click this button to show events that trigger this alarm.

7.1.2.4 Acknowledge Alarm Record

After administrator review or handle the alarm, administrator can acknowledge the alarm been processed. To acknowledge alarm records, follow the steps:

1. Search for alarm
2. Check the check box on right of alarm record.
3. Click Ack Selected button to acknowledge selected alarm records.

7.1.2.5 Delete Alarm Record

Administrators can delete all or selected alarm records. To delete alarm records, follow the steps:

1. Search for alarm record to be deleted
2. Click Delete All button to delete all the alarm records on the current page. Or click the check box on right of alarm record, and then click the DELETE SELECTED button at the bottom-right corner of page.

7.2 Event Severity

There are 5 levels of event severity predefined on the EMS. Each level can be displayed by a user definable color. Background color and foreground color are both definable for better visual effects. The final color setting is displayed in the SEVERITY fields on the Event Severity screen.

7.2.1 Accessing the Event Severity Screen

To access the event severity screen, follow these steps:

1. Click the Fault icon.
2. Select the [Event Severity] tab.

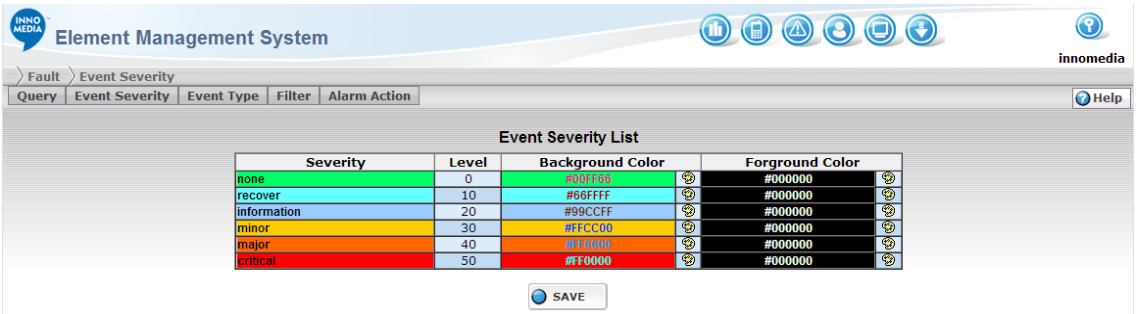


Figure 7.3. Event Severity List Screen

7.2.2 Changing Severity Colors

To change the color for different severity levels, follow these steps:

1. Click the Edit button next to the foreground or background color to make changes. A color picker pops up.
2. Click the color you prefer.
3. Repeat the same steps to change other foreground and background colors.
4. Click the SAVE button SAVE to save your new color setting.

7.3 Event Type

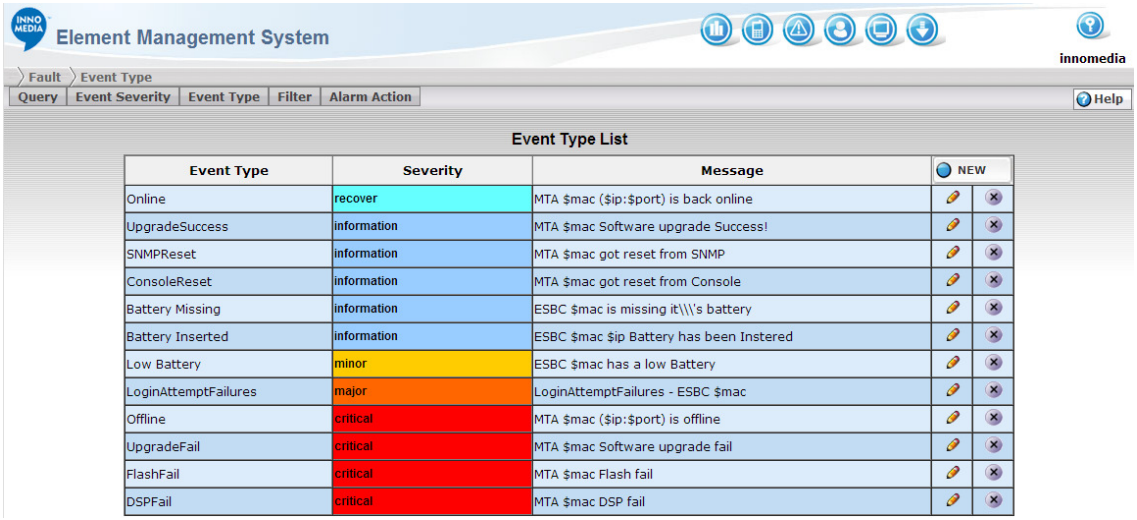
Events could be generated by a trap message from devices, or generated from the EMS itself. The trap message normally contains the information about the event type and severity level. This Event Type screen allows the

system administrator to define event types and their severity levels. To associate trap with event type, use Trap Filter to define their link.

7.3.1 Accessing the Event Type Screen

To access the Event Type screen, follow these steps:

1. Click the Fault icon.
2. Select the [Event Type] tab.



Event Type	Severity	Message
Online	recover	MTA $mac ($ip:$port) is back online
UpgradeSuccess	information	MTA $mac Software upgrade Success!
SNMPReset	information	MTA $mac got reset from SNMP
ConsoleReset	information	MTA $mac got reset from Console
Battery Missing	information	ESBC $mac is missing it\\\'s battery
Battery Inserted	information	ESBC $mac $ip Battery has been Instered
Low Battery	minor	ESBC $mac has a low Battery
LoginAttemptFailures	major	LoginAttemptFailures - ESBC $mac
Offline	critical	MTA $mac ($ip:$port) is offline
UpgradeFail	critical	MTA $mac Software upgrade fail
FlashFail	critical	MTA $mac Flash fail
DSPFail	critical	MTA $mac DSP fail

Figure 7.4. Event Type List Screen

7.3.2 Create New Event Type

To add a new event type, follow these steps:

1. Click the NEW button
2. Fill in the fields
3. Click the Save button

Here is the field description of creating an event:

Field	Description

Severity	Event severity level
Message	Text description of the event type. Predefined variables (macro) that can be used for the event message are $mac, $ip, and $port. Example: MTA $mac ($ip:$port) is offline. See Macros for Alarm Actions and Event Types on page 103 for more detailed information.

7.3.3 Edit Event Type

To edit an existing event type, follow these steps:

1. Click the Edit button next the event type you would like to change.
2. Edit the fields.
3. Click the Save button

7.3.4 Delete Event Type

To delete an existing event type,

1. Click the Delete button next the event type you would like to delete. A dialog box appears with the following message:

   Are you sure you want to delete this event type?

2. Click OK to remove the event type from list.

7.4 Trap Filter and Event Filter

Events and Traps usually indicate some major events that have been detected, but not all of the traps and events may be meaningful to EMS.

7.4.1 Trap Filter

Both devices and EMS send out traps. Traps usually indicate some major events that have been detected, such as device status changes. However, not all of the events are meaningful for EMS server to perform any task.

The trap filtering function compares the trap against the trap filter rules to determine whether to take any action. The Trap Filter screen allows the administrator to define which level of event is significant enough for EMS to have a handler to take further action. This screen provides access to the Trap Filter screen and allows system administrators to edit trap filter rules.

7.4.1.1 Accessing the Trap Filter Screen

To access the Trap Filter screen, follow these steps:

1. Click Fault icon. 
2. Select the “Filter” tab
3. Select the “Trap Filter” tab

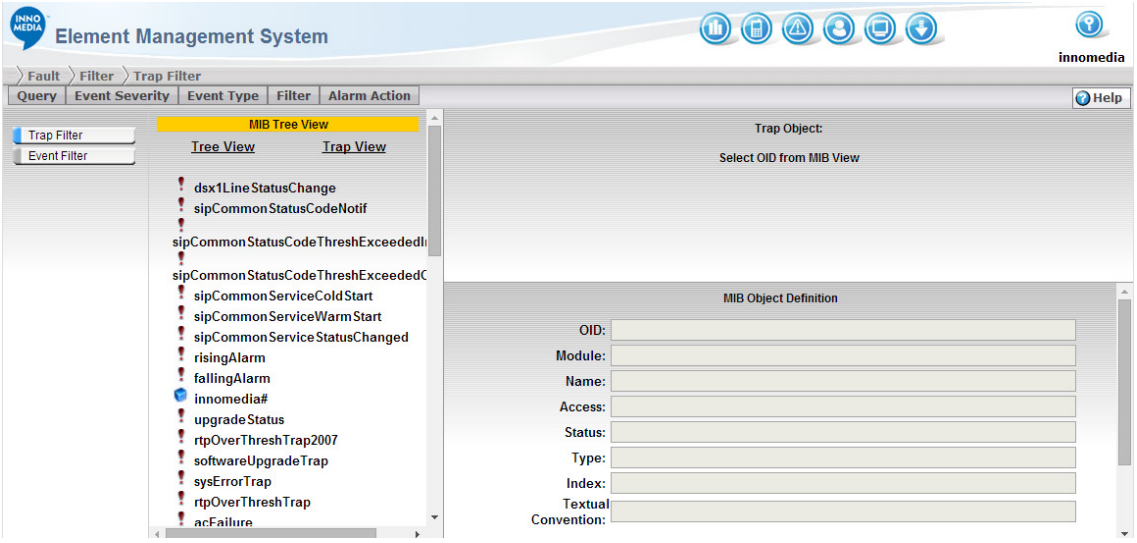


Figure 7.5. Trap Filter Screen

The Trap Filter screen consists of three panels:

1. The MIB tree browser is the one to the left. The trap OIDs can either be viewed from Tree View or Trap View.
2. A list of filter rules show in the upper-right panel.
3. The MIB object definition of the trap OID selected on the MIB tree browser will be shown in the lower-right panel.

7.4.1.2 Filter Rules

Each filter rule is a combination of a regular expression and an event type. If the trap message of the selected OID matches the regular expression, the associated event message will be generated (otherwise the trap will be dropped). One trap OID can have multiple rules mapped to different events depending on different regular expression settings.

Regular Expressions, also known as regex's, are made up of ordinary and special characters. The special characters include `$', `^', `.', `*', `+', `?', `[', `]' and `\'. Any other character used in a Regular Expression is an ordinary character. Special characters become ordinary when they are preceded by a "\".

The syntax of Regular Expressions is explained more thoroughly in the following on-line reference:

http://www.math.utah.edu/docs/info/regex_1.html.

The most commonly used symbols in regular expressions:

Symbol	Description
[ ]	Indicates a valid range. For example: [3-5]11 means 311, 411 and 511.
.	Matches any character except a new line.
{ }	Indicates a multiplier. For example: .{10} means 10 characters.
*	Indicates that the preceding regular expression can be repeated as many times as possible. For example: 011.* means 011 followed by any number of any characters.
+	Indicates that at least one match from the preceding regular expression is required. For example: 1[01]+2 does not match 12, but matches 102, 112, or any other expression that matches for 1[10]*2.
?	Indicates that zero or one match from the preceding regular expression is required. For example: 1[01]?2 matches 12, or 102, or 112 and nothing else.
\	Indicates a literal expression. For example: *69 means dialing "* 6 9".
@	This is not a special character, it is a device used in the EMS to fully specify phone numbers. The @ character appears at the end of the user portion of the SIP URI. For example: 0@ means 0 is dialed by itself. The expression, 0@ does not refer to longer phone numbers that start with 0, such as collect calls and international calls.
^	Beginning of a line.
$	End of a line.

7.4.1.3 Add Filter Rule

To add a new filter rule, follow these steps:

1. Select a TRAP OID from the MIB Tree Viewer
2. Click the New button on the Filter Rule list.

3. Enter the regular expression in Trap Message Filter, and select a event type from the pull-down menu
4. Click Save to save the rule.

7.4.1.4 Editing Filter Rules

To edit an existing filter rule, follow these steps:

1. Click the Edit button next to the filter rule.
2. Make your changes.
3. Click the Save button to save the rule.

7.4.1.5 Deleting Filter Rules

To delete a filter rule, follow these steps:

1. Click the Delete button next to the filter rule you would like to remove from the list. A dialog box appears with the following message:

   Are you sure you want to delete this Event Filter?

2. Click OK to remove the filter rule from the list.

7.4.2 Event Filter

Both devices and EMS send out traps. Traps usually indicate some major events that have been detected, such as device status changes. However, not all of the events are meaningful for the EMS server to perform any task. Events generated by the Trap Filter can be further filtered to generate alarms and take specific actions.

7.4.2.1 Accessing the Event Filter Screen

To access the Event Filter screen, follow these steps:

1. Click Fault icon.
2. Select the “Filter” tab.
3. Select the “Event Filter” tab.

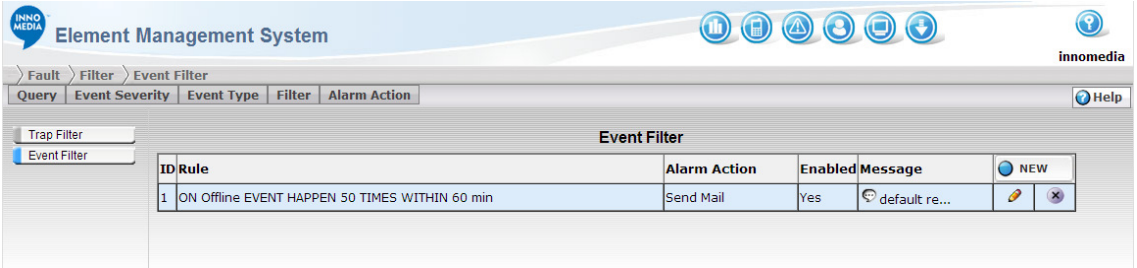


Figure 7.6. Event Filter Screen

The Event Filter screen consists of:

1. List of Event Filters.

7.4.2.2 Add Filter Rule

To add a new filter rule, follow these steps:

1. Click the New button on the Event Filter Rule list.
2. Click on Rule tab in the Rule section

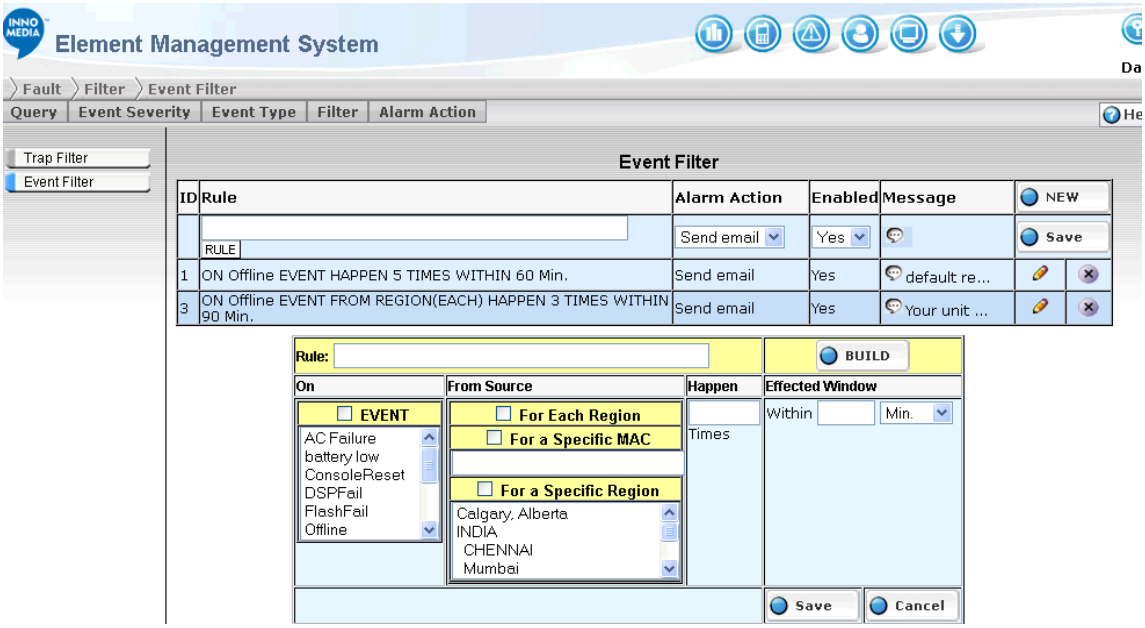
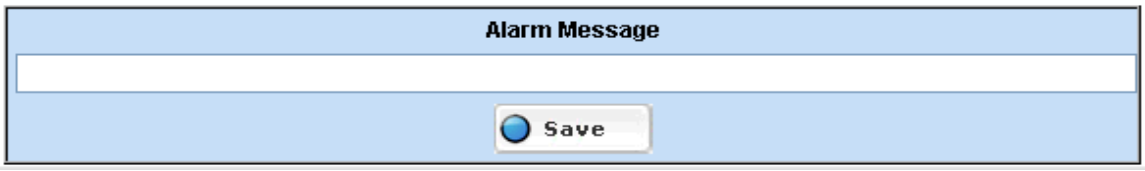


Figure 7.7. Event Filter Rule Screen

3. Click Event Check Box
4. Highlight the Event type you want to cause an Alarm for

5. Click the appropriate “From Source” you want.
6. Enter how many Times the event has to happen in the “Happen” field
7. Enter desired Within X value, and choose the pull down window for time units to use.
8. Click on Build Button to create the Rule
9. Click Save to save the rule, in the Rule Window
10. Define the Alarm Action you wish to take from the pull down window.
11. Enable or Disable the rule.



12. Edit the Message you see for this rule
13. Click Save in the Event Filter List

7.4.2.3 Editing Filter Rules

To edit an existing filter rule, follow these steps:

4. Click the Edit button next to the filter rule.
5. Make your changes.
6. Click the Save button to save the rule.

7.4.2.4 Deleting Filter Rules

To delete a filter rule, follow these steps:

3. Click the Delete button next to the filter rule you would like to remove from the list. A dialog box appears with the following message:

   Are you sure you want to delete this Rule?

4. Click OK to remove the filter rule from the list.

7.5 Alarm Action

Alarm action defines a shell script command that will be executed when an alarm has been generated. Alarm action can be taken by sending messages to the system administrator via either e-mails or page message. If the

same alarm happens for more than twenty times within ten minutes, the alarm will be suppressed. This is to prevent flooding of Alarms.

The Alarm Action screen allows the system administrator to define the notification action to be taken whenever an alarming condition requires the user's attention.

Shell script should be put in Master Database server in a predefined directory "/usr/local/dms/bin/". Only shell scripts in that predefined directory can be executed.

NOTE: The Shell script is not a part of the EMS. You need to create your own script/app to run.

Alarm Action is triggered by an Event Filter. When an event matches any entry defined in the Event Filter, the assigned Alarm action will be triggered (see Trap Filter and Event Filter on pages 106 and 109).

7.5.1 Accessing the Alarm Action Screen

To access the Alarm Action screen, follow these steps:

1. Click Fault icon.
2. Select "Alarm Action" tab.

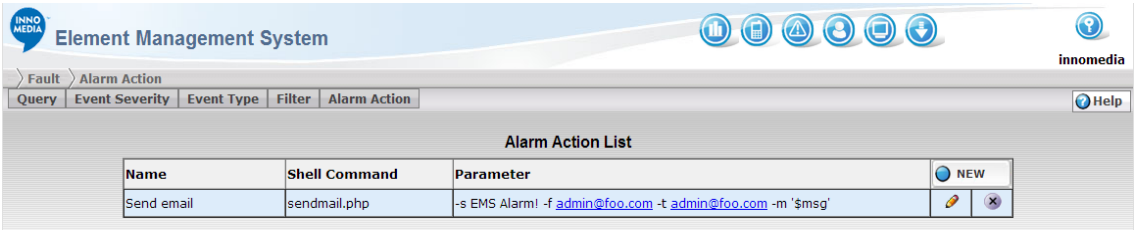


Figure 7.8. Alarm Action Screen

7.5.2 Adding Alarm Actions

To add an alarm action, follow these steps:

1. Click the New button NEW on the alarm action list. A new row adds to the table list for your new entry.
2. Fill in the fields.
3. Click the Save button SAVE to save the new entry.

Field	Description

Shell Command	Shell command executes when an alarm has been triggered. No path is allowed in command line for security reasons.
Parameter	Argument for shell command. A pre-defined variable (macro) $msg will be replaced by the alarm message that triggers this action. Refer to Macros for Alarm Actions and Event Types on page 106 for more details.

7.5.3 Editing Alarm Actions

To edit an alarm action, follow these steps:

1. Click the Edit button.
2. Make your changes.
3. Click the Save button SAVE to save your new changes.

7.5.4 Deleting Alarm Actions

To delete an alarm action, follow these steps:

1. Click the Delete button at the end of the Alarm Action entry. A dialog box appears with the following message:

   Are you sure you want to delete this action?

2. Click OK to remove the alarm action from the list.

7.6 Macros for Alarm Actions and Event Types

Example of the sendmail Alarm Action Macros:

Script	Parameter
sendmail	-s EMS Alarm! -f admin@foo.com -t admin@foo.com -m '$msg'

Where:

- -s = Subject
- -f = From

- -t = To
- -m = Message
- $msg = Message from the Alarm event you have.

Example of Event Message Macros:

Message
MTA $mac ($ip:$port) is back online
MTA $mac ip change from $oip to $ip

Where:

- $mac = MAC Address of unit
- $ip = NAT or Public IP address of unit
- $oip = Old IP address (before switching the ISP or IP Address)
- $port = NAT or Public Port

7.7 EMS Events

It is important to also have Event notification for EMS itself. Items such as system login failures, resource ultilization eg network, CPU, memory, disk, or process failures are reported via traps or system alerts to the EMS network operator

7.7.1 EMS Events Notification configuration

The following screen allows the operator to configure various elements being monitored of the EMS itself. Traps or Alert Notification can be set for each of the triggering element.

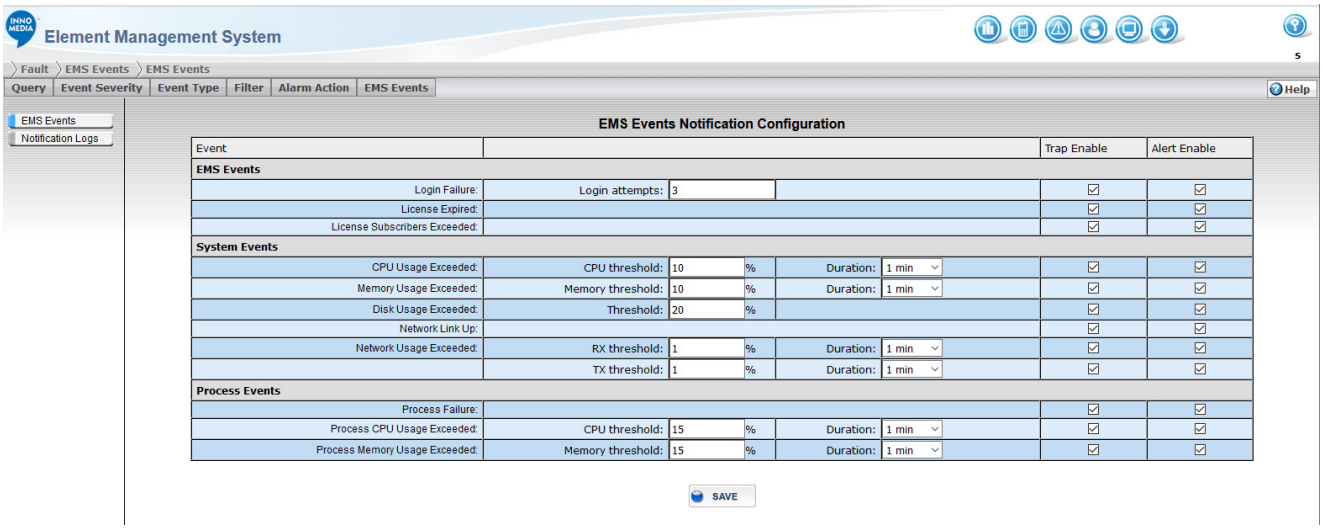


Figure 7.9. EMS Events Notification Configuration

1. **EMS Events**
    a. <u>Login Failure</u>:
        i. Tracks login failures in the web login page. If failed login attempts reaches or exceeds the specified attempts value, it will trigger a trap/alert. In addition, it will lock the account for 30 minutes, i.e. any further logins with the same username will be rejected.
        ii. The alert state will be reset after 30 minutes, and future traps/alerts will be triggered again if the same user fails to login the specified number of times.
        iii. Login attempts value must be greater than 0.
    b. <u>License Expired</u>
        i. Checks the expiry date of the DMS and PROV licenses, and triggers a trap/alert if it has expired
        ii. The trap/alert will only be sent out once, unless the proxy is restarted, such as when the server is rebooted, or even after scheduled restart by a cron job.
    c. <u>License Subscribers Exceeded</u>
        i. Checks the number of registered devices against the maximum number in the DMS and PROV licenses. If the number reaches or exceeds the maximum, a trap/alert will be sent out.
        ii. The trap/alert will only be sent out once. The alert state will be reset if the proxy restarts, or if the license maximum number of devices has changed.
2. **System Events**

a. CPU Usage or Memory Usage Exceeded
   i. Checks the system CPU and memory usage against the threshold. Triggers a trap/alert if it is exceeded over the specified duration.
   ii. The alert state will be reset if the usage falls below the threshold and the last trap/alert sent is more than 30 minutes ago.

b. Disk Usage Exceeded
   i. Checks the disk usage for the partition "/", and "/drbd" if it is present. If the threshold is exceeded, a trap/alert will be triggered.
   ii. The alert state will be reset if the usage falls below the threshold and the last trap/alert sent is more than 30 minutes ago.

c. Network Link Up
   i. Checks the network link state of the "eth0" or "em1" interface. If it changes from "down" to "up" state, a trap/alert will be triggered
   ii. The alert state will be reset if the network link state is "down

d. Network Usage Exceeded
   i. Checks the network transmit and receive bandwidth usage. If the usage exceeds the threshold over the specified duration, a trap/alert will be triggered
   ii. The alert state will be reset if the usage falls below the threshold and the last trap/alert sent is more than 30 minutes ago

3. Process Events

a. Process Failure
   i. Checks the status of the following processes: dms (dms-proxy), mysql (mysqld), cdr (collect), http (httpd), prov (prov-httpd), and mon (dms-mon). If any of these processes are not running over the last 60 seconds, a trap/alert will be triggered.
   ii. The alert state will be reset if the process is running and the last trap/alert sent is more than 30 minutes ago.

b. Process resource (CPU or Memory) Usage Exceeded
   i. Checks the CPU and memory usage of the processes listed in'*Process Failure'* event above. If the usage exceeds the threshold over the specified duration, a trap/alert will be triggered.
   ii. The alert state will be reset if the usage falls below the threshold and the last trap/alert sent is more than 30 minutes ago.

NOTE: (1) Durations to exceed the thresholds for System Events and Process Events can be selected in 1, 5, 10, 30, and 60 mins. And, threshold levels must be between 1% and 100% (inclusive).

(2) For email alert notifications, please configure "EMS Alert Notification" section of "System – Global Parameters". In addition, DNS and Sendmail services must also be set up correctly.

7.7.2 Notification Logs

EMS Notification logs will provide a Notification history of the Events that have been triggered by EMS when the thresholds or attempts set in the EMS Events have been exceeded. It will show date/time, event, and description of each notification.

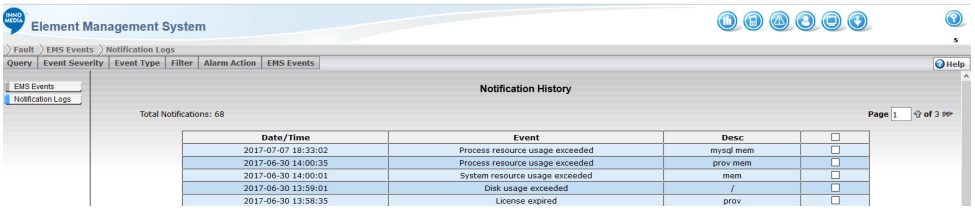


Figure 7.10. EMS Notification History Log

8 EMS Dashboard

This is a user-specific, customizable view that brings all the network-related information that a particular user may be interested in onto a single view. It allows the operator to keep their favorite set of key assessment criteria on hand at all times – even when they may be engaged in other tasks.

The dashboard is fully customizable, both in terms of content and layout. Several views are shown on the same dashboard display. These include:

- Network Map: Overall view of the number of devices in each region.
- Device Type: Shows how many device of each type are present in the network.
- Device Version: Shows how the devices are divided up by software version number.
- Device Alarms: Illustrates the alarms detected by the EMS by region.
- Device Status: How many devices are on-line/off-line within each region.
- Voice Quality: Perhaps most important with respect to call quality management, the average MOS scores for all devices in a specific region, or across all regions, can be viewed graphically over a period of time. Similar graphs can also be produced for R-factor as well.
- Call Alert: Illustrates the Voice quality related alerts detected by the EMS by region.
- Battery: Shows how many devices are running on AC or on Battery within each region.
- Talk Time: Total talk time minutes by region.

8.1 Dashboard Screen

8.1.1 Accessing Dashboard Screen

To access Dashboard Screen, click the Dashboard icon  .

Figure 8.1. Dashboard Screen

8.1.2 Adding view panel to dashboard

To Add view panel to dashboard screen, follow these steps:

1. Click the “Show Dashboard Config” tab on top left of the screen; a list of views will open.
2. Drag and Drop the selected view panel into the right side dashboard panel.

NOTE: The new panel needs to be aligned with existing panels or dragged to the top of dashboard screen before you can drop.

8.1.3 Removing view panel from dashboard

To remove a view panel from dashboard screen, follow these steps:

1. Click the button on top-right of view panel. A confirm dialog box will pop-up with message:

Remove panel xxxx Panel From Dashboard?

2. Click OK to remove the panel from dashboard.

8.1.4 Full Screen View Panel

View panel on dashboard can expand to full screen size. To expand a view panel to full screen size:

Click the button on top right of view panel.

8.1.5 Returning from Full Screen View to Normal View

Click the button on view panel will return to normal dashboard view.

8.1.6 Minimizing a View Panel

View panel on dashboard can collapse as a title bar only. To minimize a view panel:

Click the button on top right of view panel.

8.1.7 Configuring a View Panel

Each kind of view panel has some extra configurable parameters. To access the parameters configuration page, click the button on top right of view panel.

For more information, please refer to each type of view panel page.

8.2 Network Map

Network Map Screen gives an overall view of the number of devices in each region. Network Map Pie chart shows the percentage of device in each region.

Click any region slice to zoom in to the sub-region of clicked region.

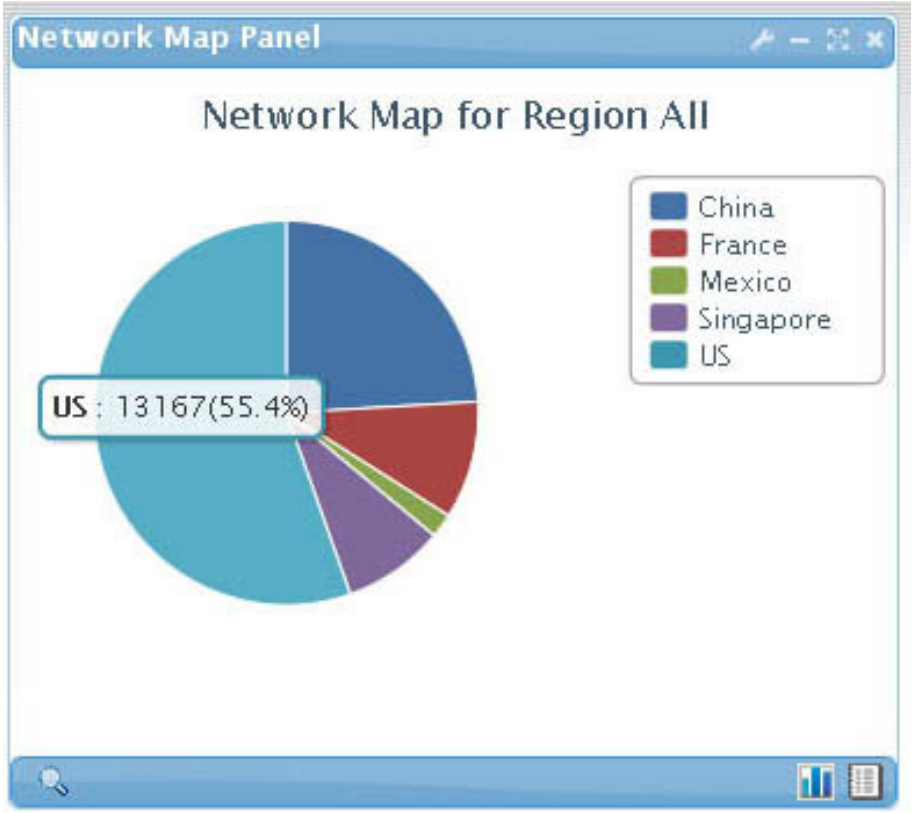


Figure 8.2. Network Map Panel

Click the button Back to go back to parent region.

Click the button to bring up list of devices of selected region.

8.2.1 Network Map Configuration

Click the configuration button to open the configuration panel:

Figure 8.3. Network Map Configuration Panel

Field	Description
Title	Panel Title
Select A Region	Set the Top view region

Click 

button to save and apply change.

Click 

button to cancel update and close configuration panel.

8.2.2 Network Map List

Click the  button to open a list of device in selected region.

Click the  button to go back to Pie Chart display.

8.3 Device Type

Device Type Screen Shows how many devices of each type are present in the network. Device Type Pie chart shows the percentage of device by each type.

Click any Device type slice of the pie chart to go to device list selected or filtered by device type.

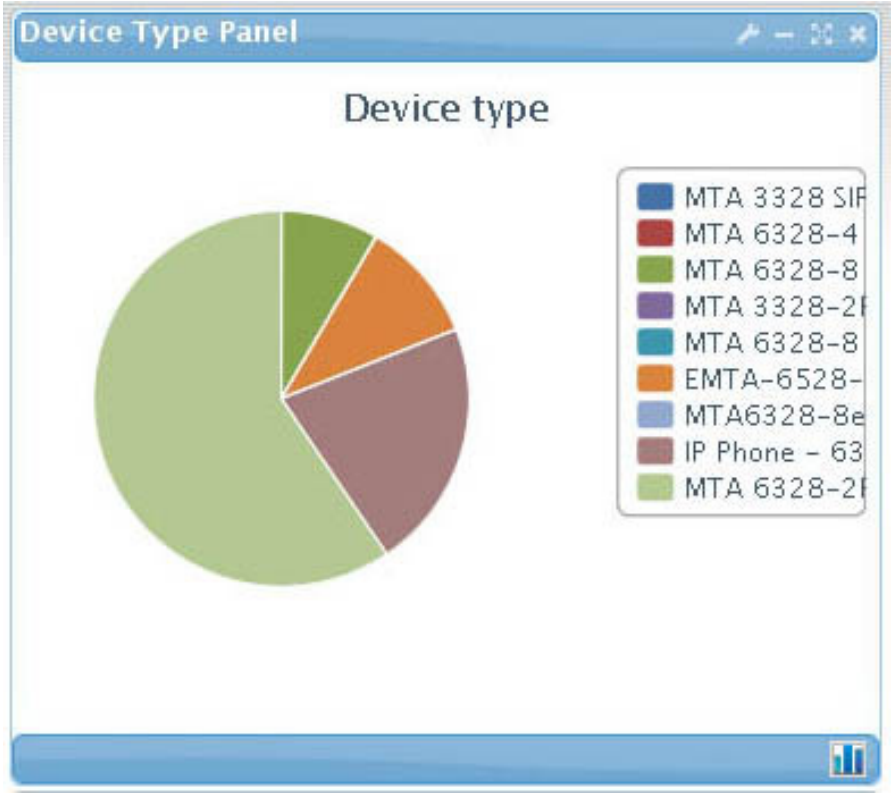


Figure 8.4. Device Type Panel

8.3.1 Device Type Configuration

Click the configuration button to open the configuration panel:

Figure 8.5. Device Type Configuration Panel

Field	Description
Title	Panel Title

Click 

button to save and apply change.

Click 

button to cancel update and close configuration panel.

8.4 Device Version

Device Version Screen Shows how many devices of each version are present in the network**.** Device Version Pie chart shows the percentage of devices by each version.

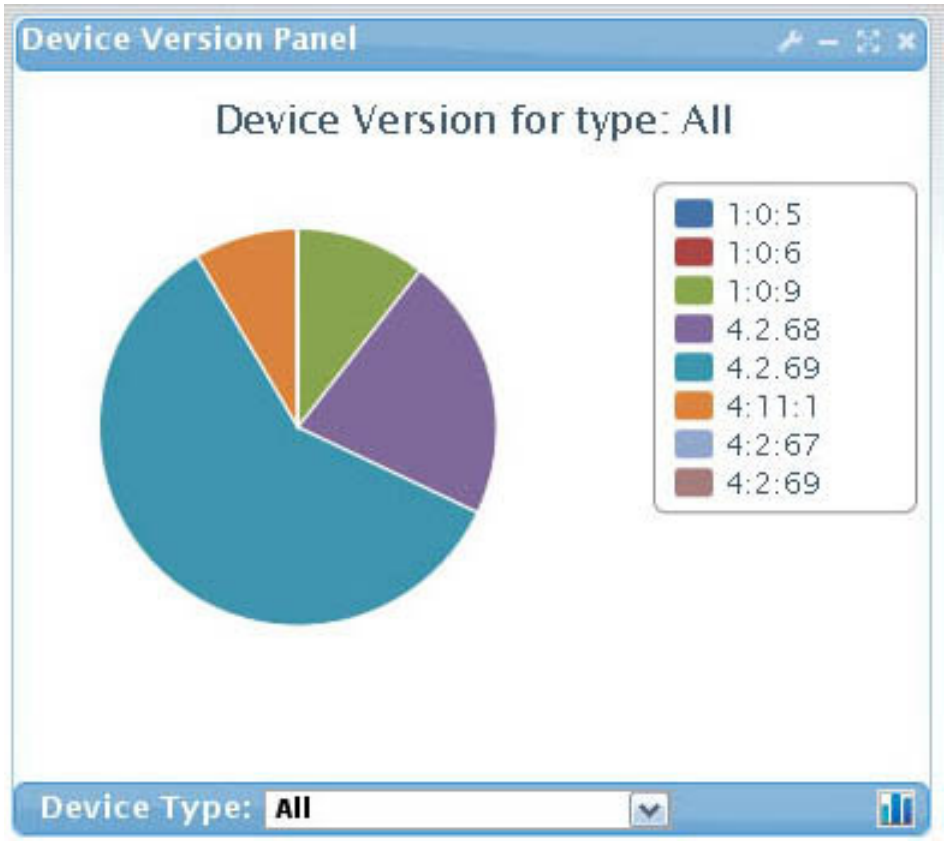


Figure 8.6. Device version Panel

8.4.1 Device Version Configuration

Click the configuration button  to open the configuration panel:

Figure 8.7. Device Version Configuration Panel

Field	Description
Title	Panel Title

Click 

button to save and apply change.

Click 

button to cancel update and close configuration panel.

8.4.2 Device Type Filter

Device Version can be filtered by a selected device type. Device Pie chart will show the percentage of different versions of this selected device type. Click the combo box on the bottom of the Device Version Panel to select a device type.

8.5 Device Alart

Device Alert Screen Shows how many alarms of each region within a specified duration are present in the network. Device Alert bar chart shows the number of alarms by each region.

Figure 8.8. Device Alert Panel

8.5.1 Region Zoom In

Click on **bar** to zoom in for alarm count for each sub-region of clicked region.

Click the Back button to go back to parent region.

Click the button to bring up Alarm/Event Query page of selected region.

8.5.2 Device Alert Configuration

Click the configuration button to open the configuration panel:

Figure 8.9. Device Alert Configuration Panel

Field	Description
Title	Panel Title
Select A Region	Set the Top view region
Severity Display	**Alarm**:Count the number of alarms during the time duration. **Event**:Count the number of events during the time duration.
Time duration	List the Alarm starting from selected time duration to now.
Refresh Rate	Panel refresh rate. Set this field to automatically refresh by assigned rate. Dashboard panel refresh rate is independent from other panels.

Click  button to save and apply change.

Click  button to cancel update and close configuration panel.

8.5.3 Device Alert List

Click the button to open an alarm/event list page.

Click the button to go back to Bar Chart display.

8.6 Device Status

Device Status Screen Shows how many devices are online or offline in the network. Device Status Bar chart shows the number of devices online/offline by each region.

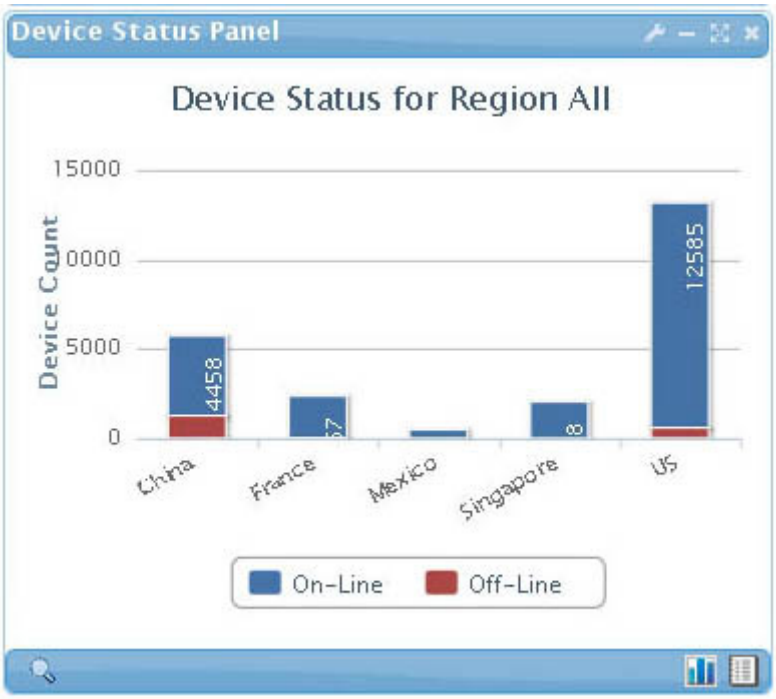


Figure 8.10. Device status Panel

Click on **bar** to go to a list of sub-region of click region.

Click the Back button to go back to parent region.

Click the button to bring up list of devices of selected region.

8.6.1 Device Status Configuration

Click the configuration button to open the configuration panel:

Figure 8.11. Device status Configuration Panel

Field	Description
Title	Panel Title
Select A Region	Set the Top view region
Refresh Rate	Panel refresh rate. Set this field to automatically refresh by assigned rate. Dashboard panel refresh rate is independent from other panels.

Click  button to save and apply change.

Click  button to cancel update and close configuration panel.

8.6.2 Device Status List

Click the  button to open a list of device in selected region.

Click the  button to go back to Bar Chart display.

8.7 Voice Quality

Voice Quality Panel shows the average MOS scores and other voice quality parameters for all devices of each region, or across all regions, over a period of time. Each region shows 5 Min, 1 Hour and 1 Day average of Voice Quality value.

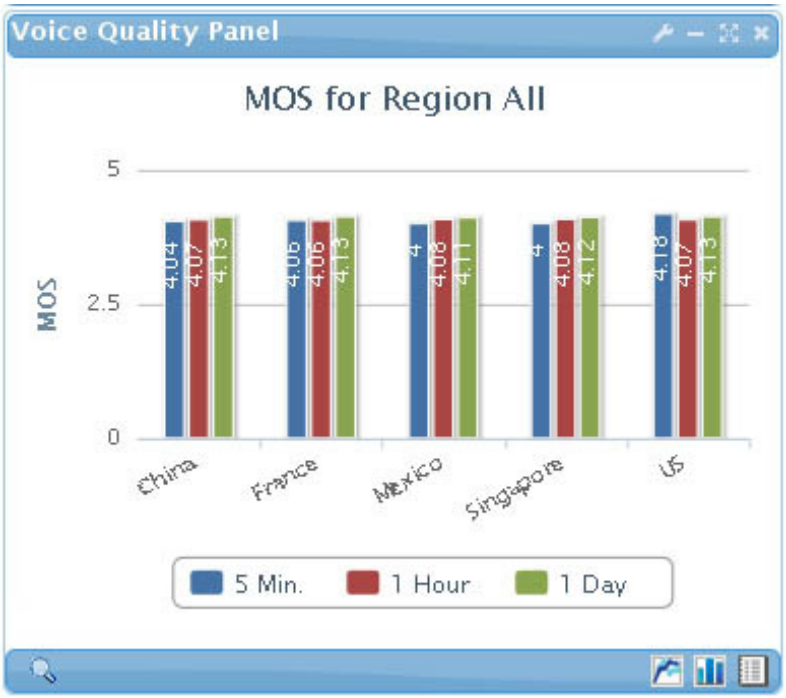


Figure 8.12. Voice Quality Panel – Bar Chart

Click on Bar to go to list of sub-region of selected region.

Click the Back button to go back to parent region.

Click the button to bring up voice quality analysis page of the selected region.

8.7.1 Voice Quality Lines

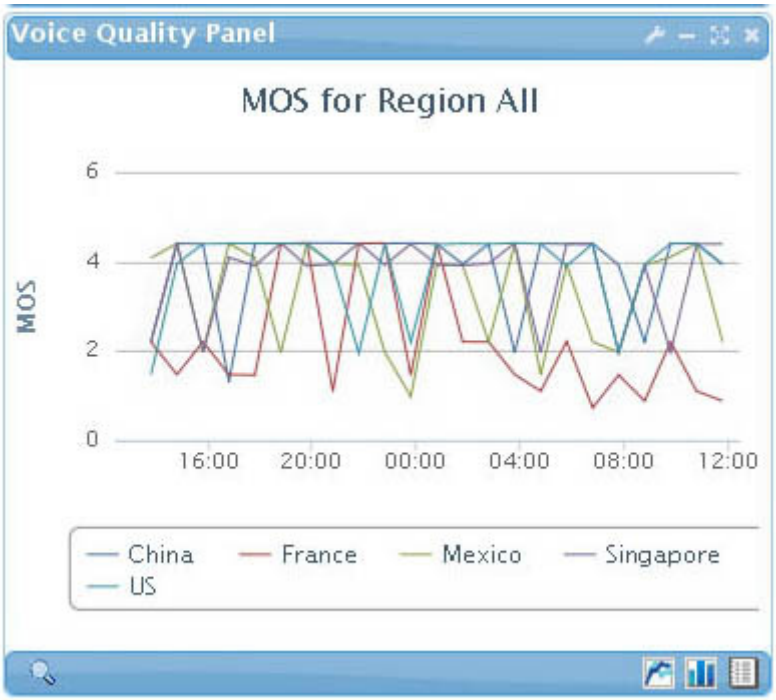


Figure 8.13. Voice Quality Panel – Line Chart

Click the button to change the panel to line chart. Voice Quality Lines Chart shows the Voice Quality value changes over the last 24 hours.

Click the button to go back to Bar Chart display.

8.7.2 Voice Quality Configuration

Click the configuration button to open the configuration panel:

Figure 8.14. Voice Quality Configuration Panel

Field	Description
Title	Panel Title
Select A Region	Set the Top view region
Watched VQ	Select one of the Voice Quality parameters for display
Refresh Rate	Panel refresh rate. Set this field to automatically refresh by assigned rate. Dashboard panel refresh rate is independent from other panels.

Click 

button to save and apply change.

Click 

button to cancel update and close configuration panel.

8.7.3 Network Map List

Click the button to open a list of device in selected region.

Click the button to go back to Bar Chart display.

Click the button change the panel to Line Chart display.

8.8 Call Alert

Call Alert Panel Shows how many calls are under the pre-defined quality thresholds in each region. Voice Quality threshold can be a combination of various range of values. Any call with VQ parameter within the defined range will be counted, within a defined period of time.

Click any bar to go to list of sub-region of selected region

Figure 8.15. Call Alert Panel

Click the Back button to go back to parent region.

8.8.1 Call Alert Configuration

Click the configuration button to open the configuration panel:

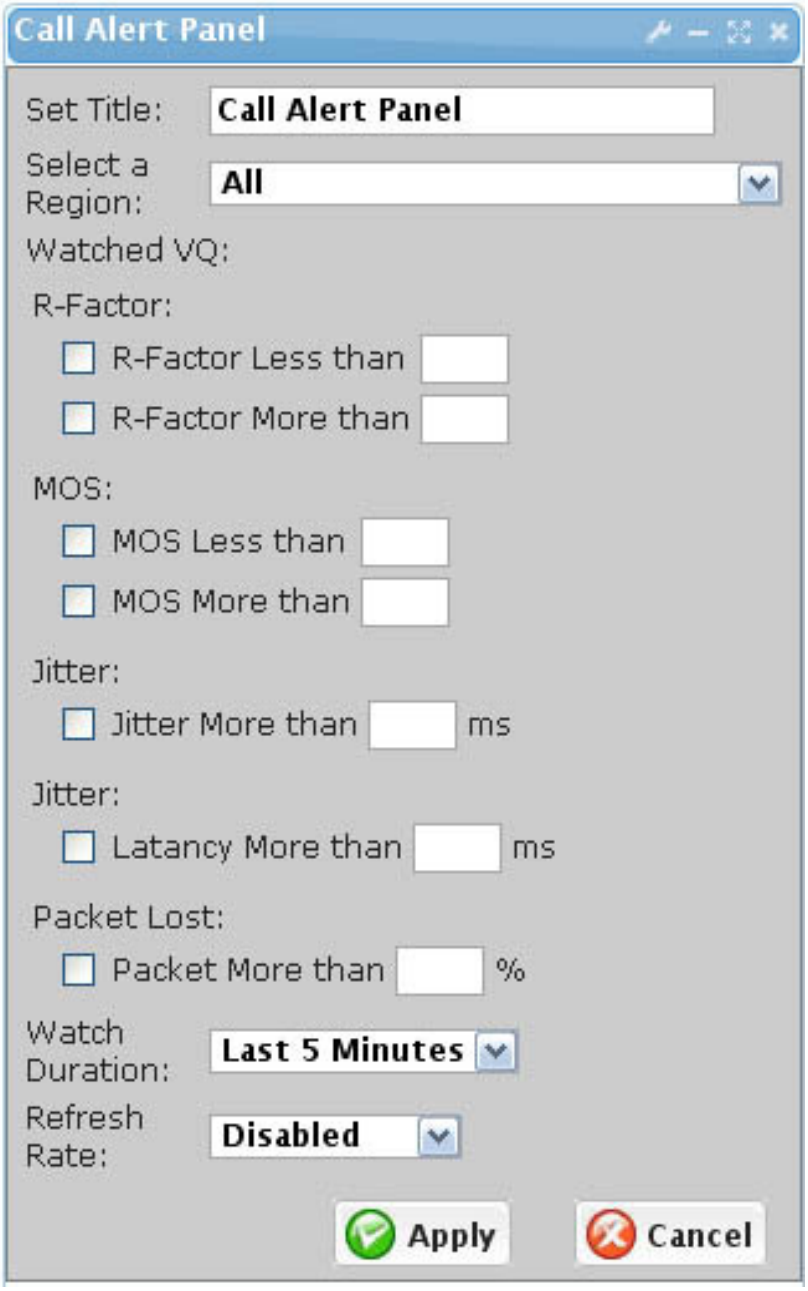


Figure 8.16. Call Alert Configuration Panel

Field	Description
Title	Panel Title
Select A	Set the Top view region

Region	
Watched VQ	Check the type of VQ to include the filter. Set the threshold value range for each selected VQ
Watch Duration	Collect call records starting the selected time duration to now.
Refresh Rate	Panel refresh rate. Set this field to automatically refresh by assigned rate. Dashboard panel refresh rate is independent from other panels.

Click 

button to save and apply change.

Click 

button to cancel update and close configuration panel.

8.8.2 Call Alert List

Click the button to open a list of CDR that matches the threshold in the selected region.

Click the button to go back to Bar Chart display.

8.9 Battery Status

Battery Status Panel Shows how many devices are running on AC/Battery modes which are present in the network. Battery Bar chart shows the number of devices by power source or battery status in each Region.

NOTE: This feature is not yet available in the EMS for the ESBC devices

Figure 8.17. Battery Panel

Click any bar to go to list of sub-region of selected region

Click the Back button to go back to parent region.

8.9.1 Battery Configuration

Click the configuration button to open the configuration panel:

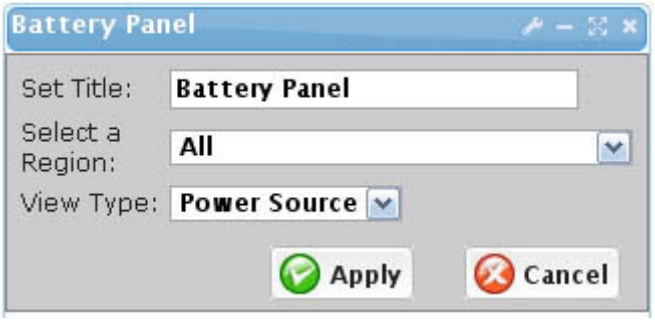


Figure 8.18. Battery Configuration Panel

Field	Description
Title	Panel Title
Select A Region	Set the Top view region
View Type	**Power Source**: Show number of devices powered by AC or Battery in each region. **Battery Bad**: Show number of device with bad or missing battery in each region. **Battery Low**: Show number of devices with low battery in each region.

Click 

button to save and apply change.

Click 

button to cancel update and close configuration panel.

8.9.2 Battery List

Click the button to open a list of device battery events.

Click the button to go back to Bar Chart display.

8.10 Talk Time

Talk Time Panel Shows total minutes of talk time by region or by device type.

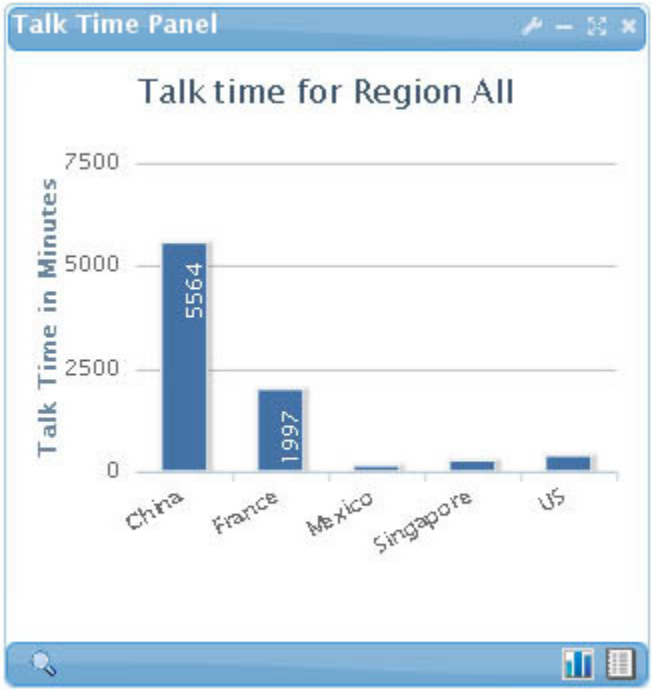


Figure 8.19. Talk Time Panel

Click any bar to go to list of sub-region of selected region.

Click the Back button to go back to parent region.

Click the button to bring up call statistic page of selected region or type.

8.10.1 **Talk Time Configuration**

Click the configuration button to open the configuration panel:

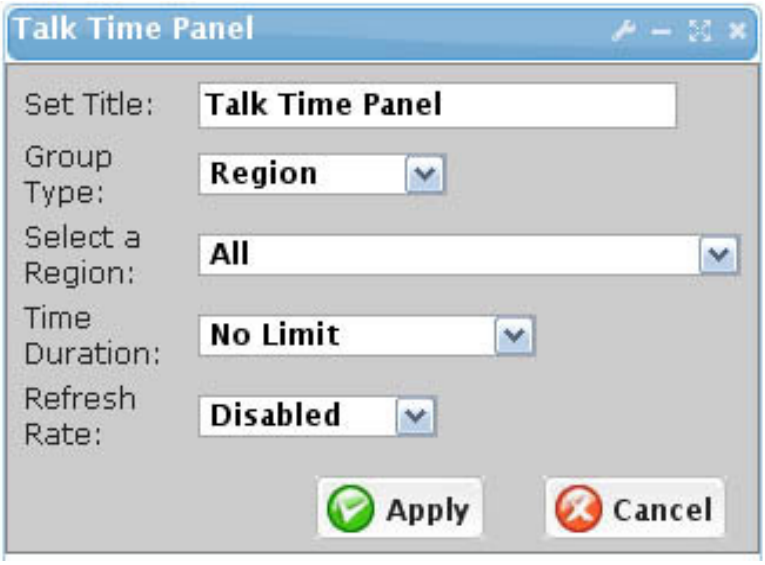


Figure 8.20. Talk Time Configuration Panel

Field	Description
Title	Panel Title
Group Type	**Region**: show total talk time for each region. **Device Type**: Show total talk time for each Device type.
Select A Region	Set the Top view region
Time duration	List the talk times starting for selected time duration to now.
Refresh Rate	Panel refresh rate. Set this field to automatically refresh by assigned rate. Dashboard panel refresh rate is independent from other panels.

Click 

button to save and apply change.

Click 

button to cancel update and close configuration panel.

8.10.2 **Talk Time List**

Click the button to open a list of devices in selected region or type with total talk minutes.

Click the button to go back to Bar Chart display.

9 EMS Auto-Provisioning System

The EMS **Auto-Provisioning System** automates the entire CPE provisioning process with the following attributes:

- Multiple protocol support
- Multiple configuration file formats
- Multiple encryption support
- Convenient Profile construction for configuration
- Hierarchical structures and multiple inheritances
- Device initiated and server initiated pre-scheduled provisioning
- Provisioning history records

9.1 Auto-Provisioning Protocol Support

The EMS auto-provisioning supports the following protocols: TFTP, HTTP, and HTTP with security. These are described below.

9.1.1 **TFTP Provisioning**

TFTP is a simple protocol with the following messages: Read Request (RRQ), Data (DATA), Acknowledge (ACK), and Error (ERROR). The TFTP provisioning allows downloading of configuration files as well as image files. The protocol exchange process between the CPE and the server is depicted in Figure 9-1.

Due to its simplicity, TFTP-based provisioning also has limited flexibility. Additionally, due to its lack of redirect capability, it has limited scalability.

The Configuration file can be encrypted using, for example, an encryption (e.g., RC4) with a shared secret key generation algorithm (e.g., hash function HMAC-MD5) using parameters unique to the device as input.

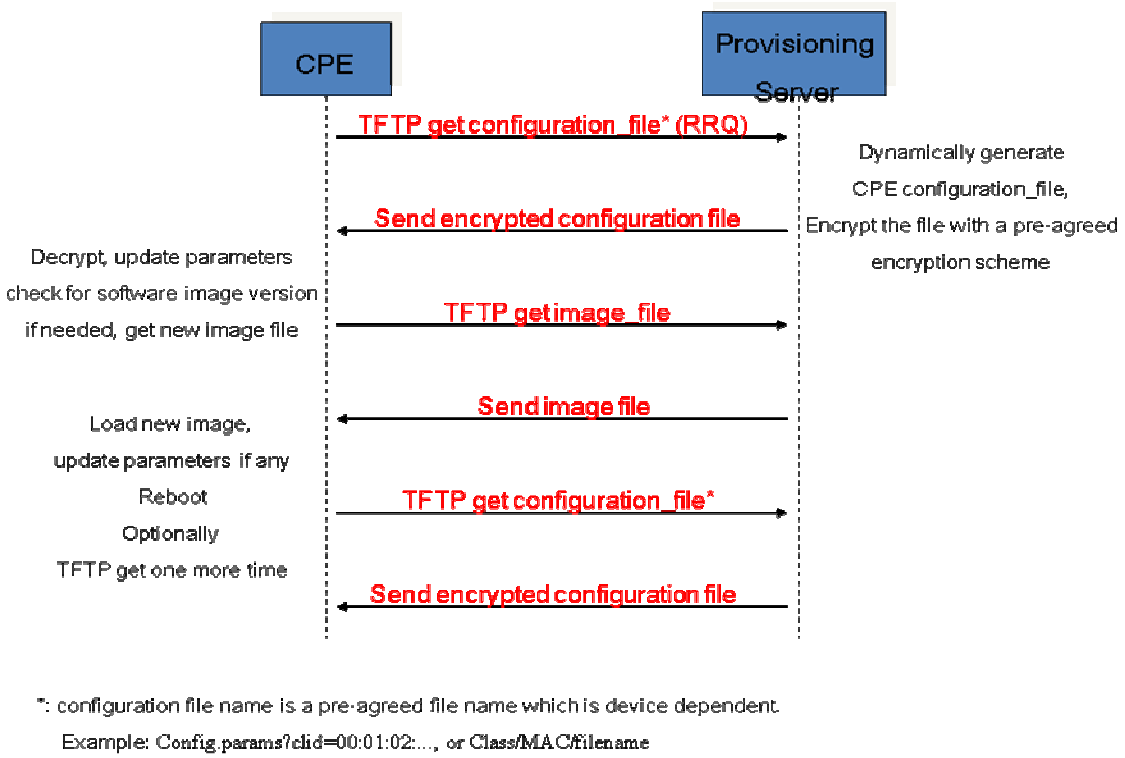


Figure 9-1. TFTP-based provisioning.

9.1.2 Provisioning with HTTP and HTTP with Security

HTTP is a widely used protocol and is flexible, scalable, and firewall friendly. A basic HTTP-based provisioning process is shown in Figure 9-2.

The HTTP provisioning can also be enhanced with authentication and encryption. This is shown in Figure 9-3 . The authentication process is as follows:

- A challenge string is sent by the server to the device when requested by the device for provisioning
- The device computes (MD5) digest using a shared secret algorithm
- The device requests for the configuration file again with the digest included in the request
- The server checks the digest for device authentication

The configuration file can also be encrypted with the following steps:

- The server generates a key based on a random “Nonce” and a secret algorithm, and encrypts the configuration file using, say, RC4.
- The “Nonce” is sent in the HTTP headers along with the encrypted configuration information

- The device generates the same key using the Nonce and the same shared secret algorithm, and decrypts the file

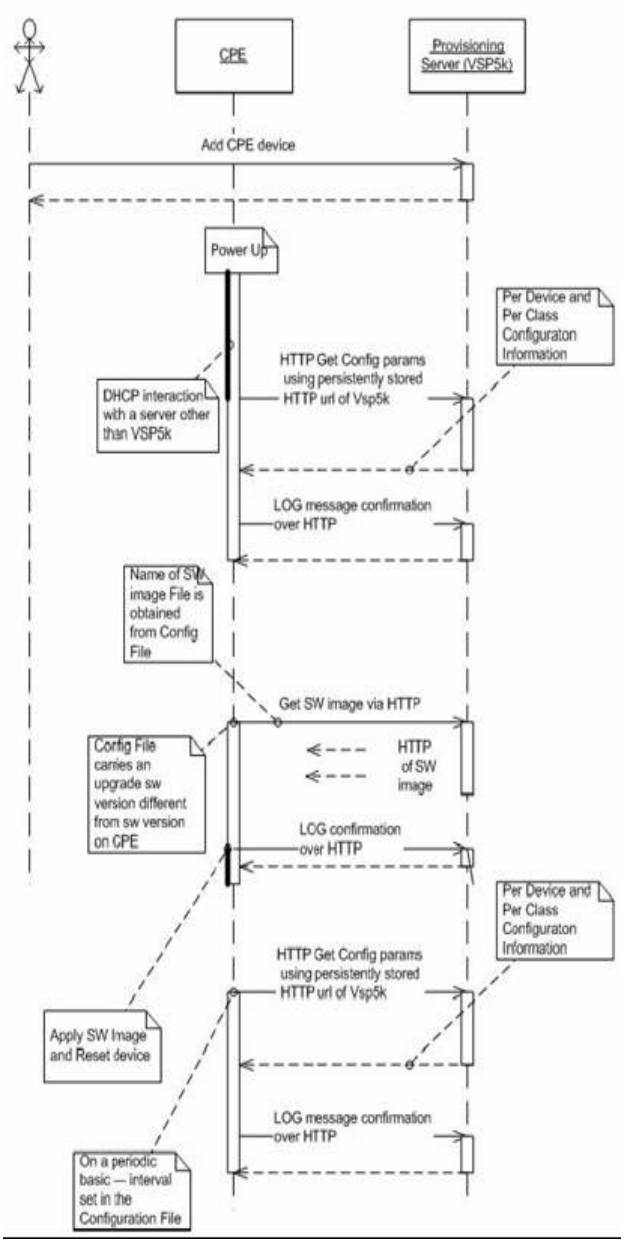


Figure 9-2. HTTP-based provisioning

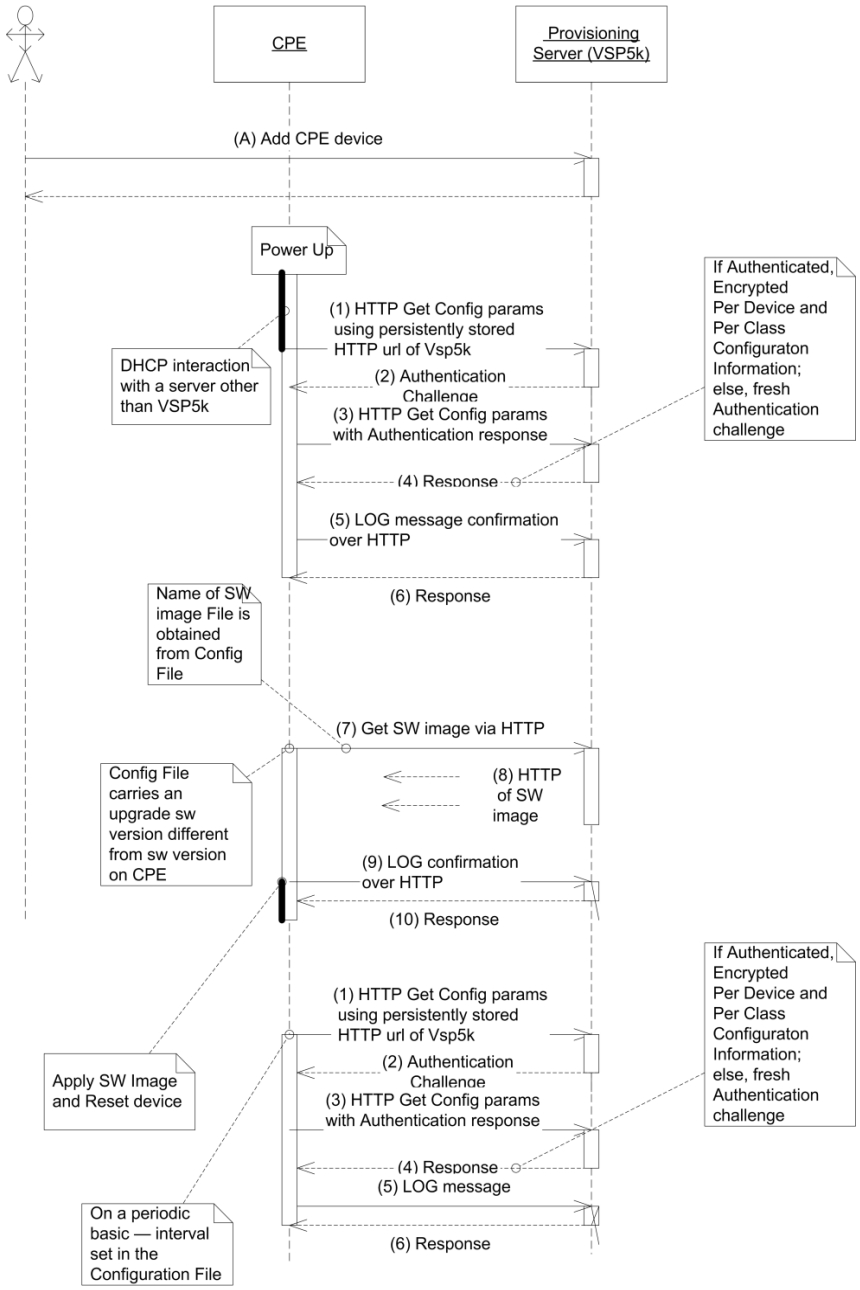


Figure 9-3. HTTP-based provisioning with authentication and encryption

9.2 Profile Configuration

Profile defines the common protocol related attribute when performing the provisioning. Profile defines the protocol, format and security method when sending provisioning data to device.

Profile Configuration screen has two sections:

1. Profile List

2. Profile Detail

The **Profile List** on the left panel shows available profiles previously defined; the **Profile Detail** on the right panel is used to configure different attribute for provisioning data.

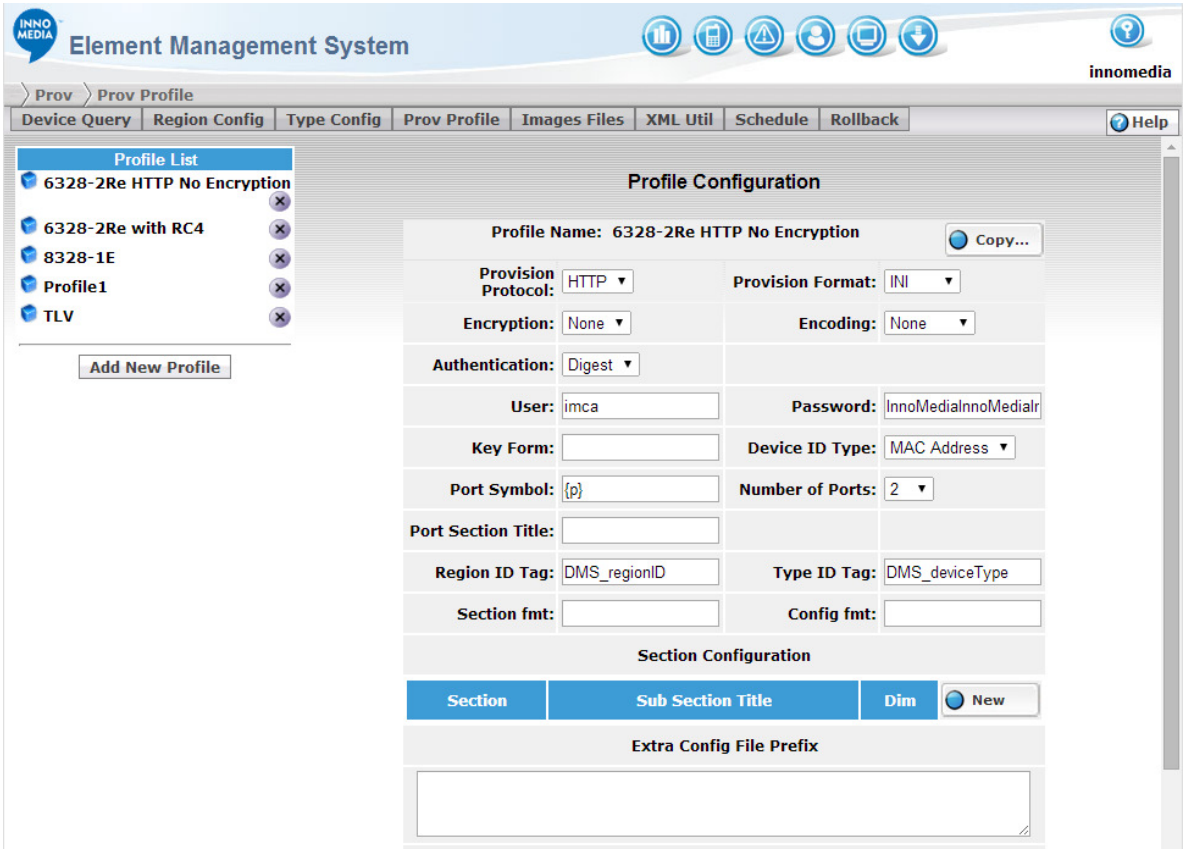


Figure 9-4. Profile Configuration Screen

9.2.1 Accessing Profile Configuration Screen

To access the Profile Configuration Screen, follow the steps:

1. Click Provisioning icon. 
2. Select the [Prov Profile] tab

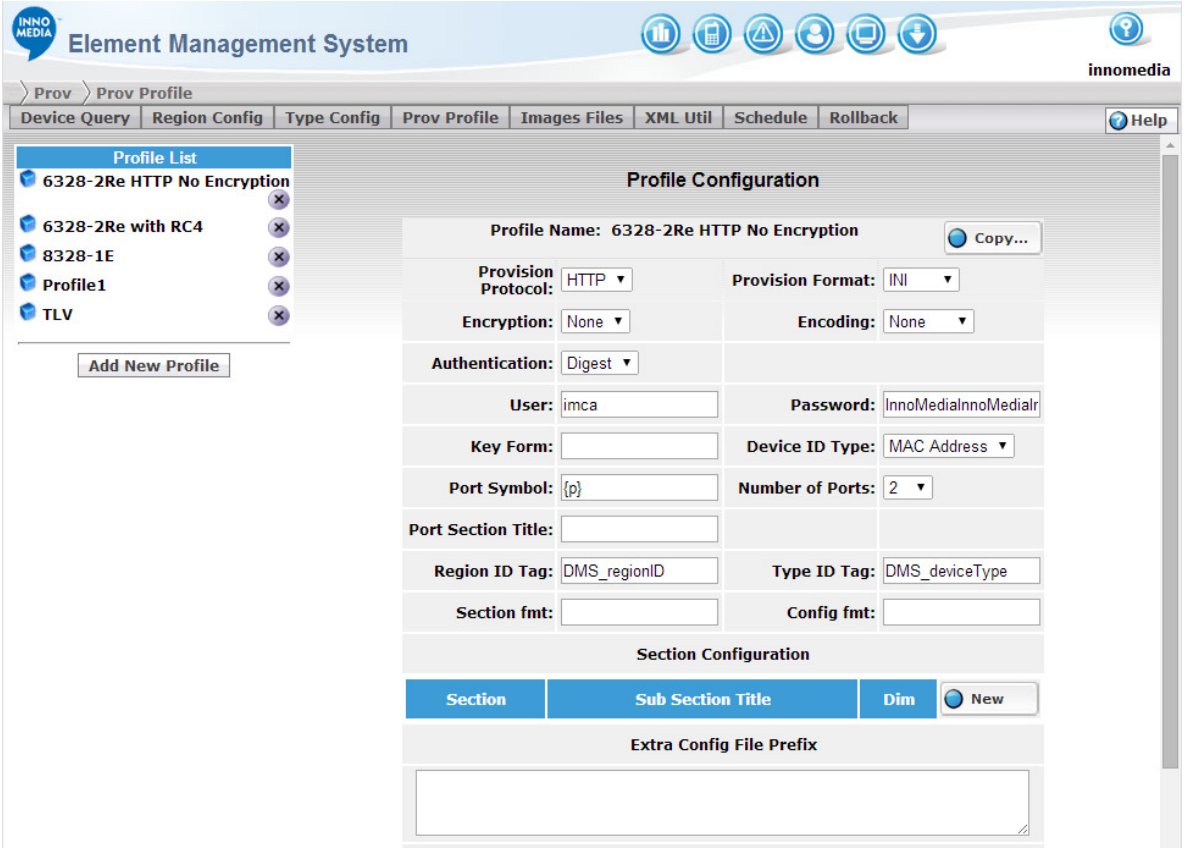


Figure 9.5. Accessing Profile Configuration Screen

9.2.2 Adding a Profile

To add a new Profile, follow the steps:

1. Click [Add New Profile] button on the bottom of left panel.
2. Input the fields on the right Profile Detail panel.
3. Click Save button to submit the change.

Field	Description
Provision Protocol	Select the protocol from the drop-down menu. EMS supports HTTP and TFTP provisioning.
Provision Format	Select the provisioning file format from the drop-down menu.
Encryption	Select the encryption algorithm from the drop-down menu.

Encoding	None or base64 encoded configuration file
Authentication	Select the authentication method from the drop-down menu.
User	User name for the HTTP authentication
Password	Encryption key. And authentication password. It must match with the Device provisioning password setting.
Key Form	Key Form is the formula about how EMS generates the hash key for encryption. Example of a Key: 1000,nonce,pass,pbkdf2 See page 137 for more information
Port Symbol	Enter the replaceable symbol for the port number. The port symbol will be used in tag of port related parameters. EMS will replace the symbol with port number (one base) to generate the real provisioning tags. If the port symbol is not defined, "_x" will be use as tag postfix where x is the port number. For example: the User ID parameter tags for a two-port device will look like this: Tag defined as "User_ID_{P}", and Symbol defined as "{P}", then the final tag will be User_ID_1 and User_ID_2. The number 1 and 2 is the port numbers.
Device ID Type	Select the Device ID type from the dropdown menu. Used by special key form
Number of Ports	Select the number of ports from the drop-down menu for this profile. Knowing the number of port, the device parameters page will automatically create exact same number of tags for port parameters.
Port Section Title	Add port section title in SCSV, SINI and USER format. Leave it empty to not generate the port section title
Region ID Tag	EMS will automatically append this tag with device region ID setting into configuration file
Type ID Tag	EMS will automatically append this tag with device Type ID setting into configuration file
Section fmt	Pattern of Section title when using **USER** format. Leave it empty if no need of section title
Config fmt	Pattern of configuration tag and data when using **USER** format

File Format

EMS Auto-Provisioning supports the following File formats. Furthermore, it allows segmented parameter configuration with different array dimensions including array for ports, array for accounts, and array for interfaces.

- **INI** - Tag equal Value format, value with double quote (tag="value")
- **XML** - XML format
- **INIv** - Tag equal Value format, value without double quote (tag=value)
- **CSV** - Column Separated Value (tag:value)
- **SCSV** - Segmented Column Separated Value (tag:value), segment name in square quote (<seg>)
- **SINI** - Segmented Tag equal Value format, segment name in square quote ([seg])
- **USER** - User defined pattern. Format is setting by **Section fmt** field and **Config fmt** field. **Section fmt** defines the format of section header. Macro **$seg** will be replaced by real section name. **Config fmt** defined each line of configuration data. **$tag** will be replaced by tag name, and **$val** will be replaced by value of this tag. **$tag** can have an optional length modifier to create fix length tag field. Use **$tag(length)** to set the tag size. If tag length shorter then the special length, space will be padding after the tag to fill up to the length.

Encryption Method

EMS supports the following Encryption:

NOTE: If AES or RC4 selected, you must enter password in the password field.

- **None** - Do not encrypt configuration file.
- **AES** - AES encrypted configuration file. (Currently not available on MTA 6328)
- **RC4** - RC4 encrypted configuration file.

Authentication Method

EMS supports the following Authentication methods:

- **None** - no authentication
- **Digest** - authenticated by comparing the user names with digest.
- **Basic** - authenticated by comparing the user names and password.

Key Format

The key form is a postfix calculation for the key string. The key is used for RC4 or AES encryption. Here is the list of operators:

```
#   -join    =>    # (s1,s2) -> "s1s2"
#   -colonjoin    => # (s1,s2) ->"s1:s2"
#   -md5    =>  # (s1) -> md5(s1)
#   -rmd160    =>    # (s1)  -> rmd160(s1)
#   -sha1    =>  # (s1)->  sha1(s1)
```

```
#   -binhex   =>  # (s1) -> binhex(s1)
#   -hmac_md5   =>  # (s1,s2) -> hmac_md5(s1,s2)
#   -pbkdf2   => # (s1,s2,s3) pbkdf2(s1,s2,s3)
#   -swap   =>  # (s1,s2) (s2,s1)
#   -drop   =>  # (...,s1) (...)
```

And available external variable names :
mac, //mac address
clid, //client id, also mac address
nonce
pass
variation

So the key form "1000,nonce,pass,pbdkdf2" is the result of
pdkdf2(1000,nonce,pass)

9.2.3 Section Configuration

Section Configuration is optional. It is required only you need defined multiple dimensional sections. Section defined in provision parameter (Type/Region/Device) can be multiple dimensions too. To specify the section dimension you need add an entry in profile section configuration.

Field	Description
Section	Name of Section that must match the name defined in parameter list.
Sub Section Title	Sub section title used to separate the common parameters and sub dimension parameters. Configuration file will generate the section title first, then the common parameters, then the sub section title, then the sub section parameters by dimension index. Leave the field empty to not generate sub section title. Sub section parameter must be defined in parameter attribute with scope value **Sub Section**.
Dim	Dimension of the section. By default section dimension is 1 and no entry is needed here.

Adding New Section Configuration

Click the New button 

to create a new section entry.

Deleting Section Configuration

Click the  button on right of section.

Editing Section Configuration

Put the new value in fields and click the Save button on bottom of Profile page.

Extra Config File Prefix

Any text specified here will be appended at the top of configuration file.

$tick is a special macro that tracks the latest time stamp of parameter being updated. It can be used as a version number for device. For example:

<<VOIP CONFIG FILE>>Version:2.$tick

And, in device configuration file it will look like:

<<VOIP CONFIG FILE>>Version:2.12782333

Extra Config File Postfix

Any text specified here will be appended at the end of configuration file.

9.2.4 Editing a Profile

To edit profile, follow these steps:

1. Click on the profile name you want to edit.
2. Update the fields on the right Profile Detail panel.
3. Click Save button to submit the change.

9.2.5 Deleting a Profile

To Delete a Profile, follow the steps:

1. Click on the Delete button on right of the profile name, a dialog box appears with the following message:

   Do you want to delete Profile?

2. Click OK to remove the profile from the list.

9.3 Region Configuration

Region Configuration Screen configures Region related parameters for device provisioning. Region Configuration screen has two sections:

- Region List
- Region Detail

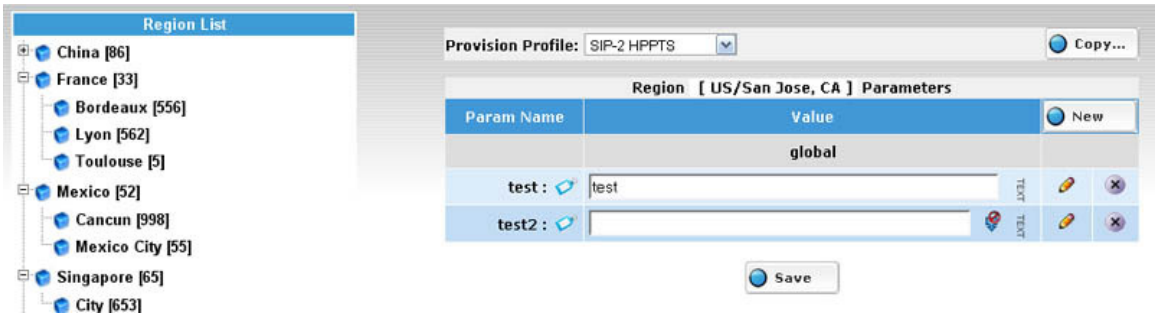


Figure 9-6. Region Configuration Screen

Region List lists available regions. Regions are defined in Region Table. You can't add or remove region from this screen. Please use Region Table to edit Region setting. Region may have sub-regions, using the expand (+)/collapse (−) button on left of region name to Expand/Close sub-regions.

Sub-Region parameters can inherit from the parent Region. All parameters and data defined in parent region will be automatically available in sub-region. Sub-Region can re-define the data by changing the value field, or re-define the parameter by adding a new parameter with the same section and tag name.

9.3.1 Accessing Region Configuration Screen

To access the Region Configuration Screen, following the steps:

1. Click Provisioning icon.
2. Select “Region Config” tab

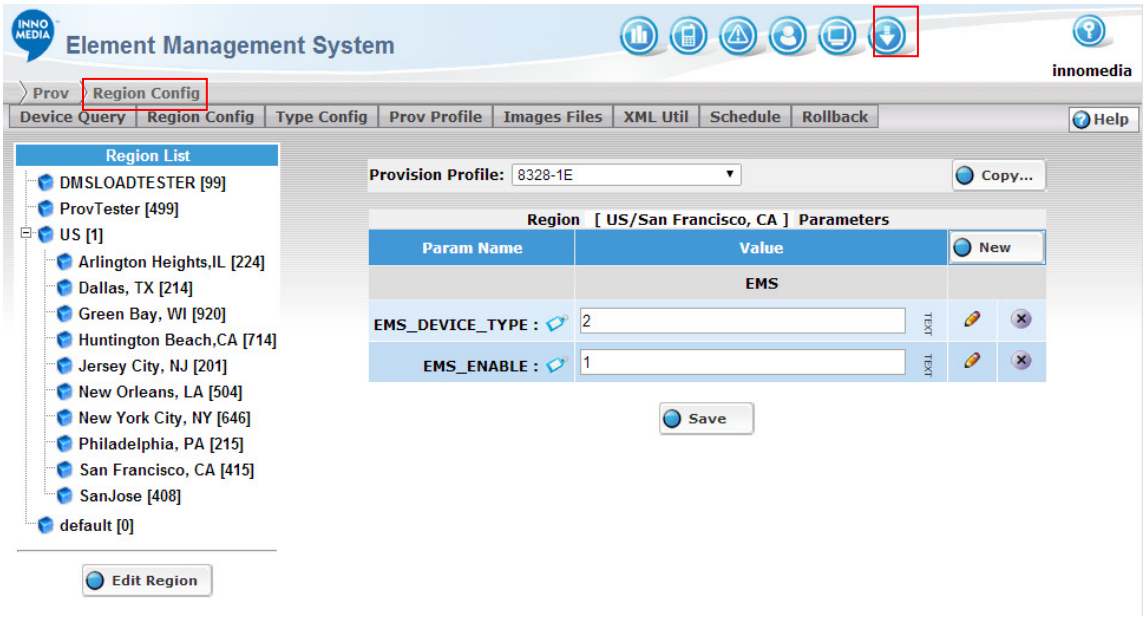


Figure 9-7. Accessing Region Configuration Screen

9.3.2 Editing Region Configuration

To Edit a Region Configuration, following the steps:

1. Click the region name on the left panel.
2. Edit the Region parameters on the right panel
3. Click Save button  to submit the change. Success or fail dialogs will pop-up.
4. Click OK or wait for few seconds will close the popup window.

9.3.3 Parameter Configuration Screen

Region, Type, and Device share the same style of Parameter configuration.

The Parameter Configuration Screen provides a GUI for administrator to manage device parameters at different levels. EMS parameter provides the flexibility to define individual types of parameters. Value input for parameter will be enforced by type validation. For example, no alphabetical characters are allowed to be typed in a number field.

9.3.3.1 Selecting a Profile

Each configuration can assign a profile. Region or Device inherits Profile from its parent class unless it has its own profile defined. Profile details are defined in Profile Configuration screen.

To select a Profile, Click the combo-box on top of configuration screen and it will save as soon as you select it.

9.3.3.2 Copy from other class

Parameter setting can be copied from another class of the same category. Region parameter only can be copied from another region parameter. Type parameter only can only be copied from another type parameter configuration and this is true for device.

To Copy parameter from other parameter configuration class, follow the steps

1. Click the Copy button on top right of the configuration screen. A Copy parameters dialog will pop up.
2. Select the source class you want to copy from.
3. Click Copy button on the dialog box to submit the request.

9.3.3.3 Parameter List

Parameter List shows all parameters defined in this class. Parameters in EMS can be categorized by a Section. A gray row in the list is a Section name. All parameters after the Section name belong to that section. In some configuration file format (SCVS and SINI), it will also generate the section name in the configuration data.

For Parameter rows:

1. **Param Name**: Name of parameter. This is a human friendly form of parameter name. Parameter name is used in EMS GUI only. Real configuration file will use tag name instead of parameter name.
2. **Value**: Value of parameter.
3. **Edit** : Click to edit Parameter attribute.
4. **Delete** : Click to delete this Parameter.

9.3.3.4 Inherited Parameters

Parameters may be inherited from its parent region or configured class. If a parameter is inherited, inherit indicator icon will replace the edit and delete buttons on the right of each parameter.

In replace of Edit ( ) icon:

- : This parameter is inherited from (parent) region.
- : This parameter is inherited from type.

In replace of Delete ( ) icon:

- : The parameter is inherited and the value of parameter is inherited from it original setting.

- : The parameter is inherited but the value of parameter is a local setting (an override). Click this icon will remove the local override and restore to inherited value.

9.3.3.5 Add New Parameter

To add a new parameter, follow the steps:

1. Click the New button on top-right of the parameter list. A parameters edit dialog will pop up.
2. Input parameter into each fields
3. Click Save button to save the change
4. A Success dialog will popup, click OK to close it or wait a few second it will close automatically.

9.3.3.6 Parameter Edit Dialog

Figure 9-8. Parameter Edit Dialog

Parameter Edit Dialog defines parameter attributes. Available parameter attributes include:

Attribute	Description
Section	Section of this parameter, you can choose from existing Section name or select --New Section Name--
New Segment Name	If you select --New Section Name-- then you have this input box to input the new section name.
Tag	The Tag name use for provision device. This tag will be use as a tag in tag-equal-value format.
Label	Label will displayed as Parameter Name in parameter list. Label is for reference use only.

Type	Type of value for this parameter. Please refer to Type and Option section for detail.
Option	Depends on value type, option provides extra configuration for possible value range. Please refer to Type and Option section for detail.
Disabled	Disable this parameter. Disabled parameter will not be provisioned. It can temporary remove the data from configuration file but does not delete data from database.
Scope	**inheritable**:common parameter applicable to whole device. **Port Only**:Port specific parameter, like account ID per port. **Sub Section**:Sub section parameter if section has multiple dimensions configured in Profile.
Read only	If checked operator cannot change the value in the parameter list (include all sub class that inherit it). The only way to change the value is edit the Value field in this dialog.
Value	Default/Initialize value for this parameter.

9.3.3.7 Type and Option

Available Types include:

Type	Description
text	The most common format of parameter value. No input limitation apply
number	Only 0-9 and period (.) allowed
checkbox	Boolean type value: checked=1, uncheck=0
option menu	A combo box provides a list of pre-defined value. Available value defined in Option field.
text area	A multiple line edit box for text value. No input limitation apply
radio box	A list of exclusive options. Available value defined in Option field. (Example of text LoopStart->0, GroundStart->1).
ip address	Only allow IP address format (255.255.255.255).
mac address	Only allow MAC Address format (XX:XX:XX:XX:XX:XX).
image file	This is a special type indicate the value comes from already uploaded image files. This type will display a combo box showing only the available image file in EMS system. When

	EMS creates the configuration file, EMS will attach full URL (depending on protocol) for device to download. For HTTP. EMS will generate http://host:port/image-file?hwid=mac; for TFTP EMS will use tftp://host:port/mac_xx_xx_xx_xx_xx_xx_image-file

9.3.3.8 Option Format

Option field is only used by **option menu** type and **radio box** type. Options are separated by common (,). e.g.

value1,value2,value3

Option also supports name→value format for more friendly prompt. e.g.

name1->value1,name2->value2,name3->value3

NOTE: The value field must use the value instead of name for correct initial value setting.

9.3.3.9 Sub Section

Each section can have its own subsections by number index. Sub section parameters need to use the **Sub Section** as parameter **scope**. Number of subsection index called **Dim**, which is defined in Profile. **Sub Section title** also defined in Profile.

9.3.3.10 Editing Parameter

To edit a parameter, follow the steps:

1. Click the Edit button on left of parameter. If the parameter is inherited, then you can not edit it in this screen.
2. Update the parameter attributes
3. Click the Save button to submit the update.
4. A successful dialog will popup. Click Ok to close it or wait for a few seconds and it will close automatically.

9.3.3.11 Editing Parameter Value

To Edit a parameter value simply put the new value into the value input box, Click the Save button at the bottom of list.

9.3.3.12 Restoring Parameter Value

If the parameter is an inherited, you can still have an override value set for this parameter. You can restore the parameter value to its original inherited value by clicking button to remove the override.

9.3.3.13 Deleting Parameter

To delete a parameter, follow the steps:

1. Click the Delete button on left of parameter. If the parameter is inherited, then you can not delete it in this screen.
2. A confirm box pop up with the message:

   Are you sure you want to delete this Param?

3. Click Ok to remove the parameter from the list.

NOTE: Delete parameter - all parameter values that were inherited from this parameter will be erased as well.

9.4 Type Configuration

Type Configuration Screen configures Device Type related parameters for device provisioning. Type Configuration screen has two sections:

- Type List
- Type Detail

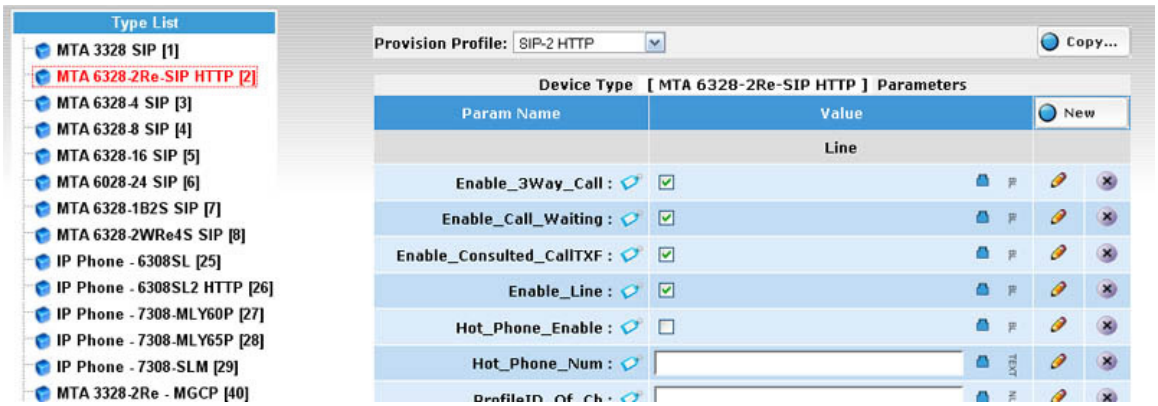
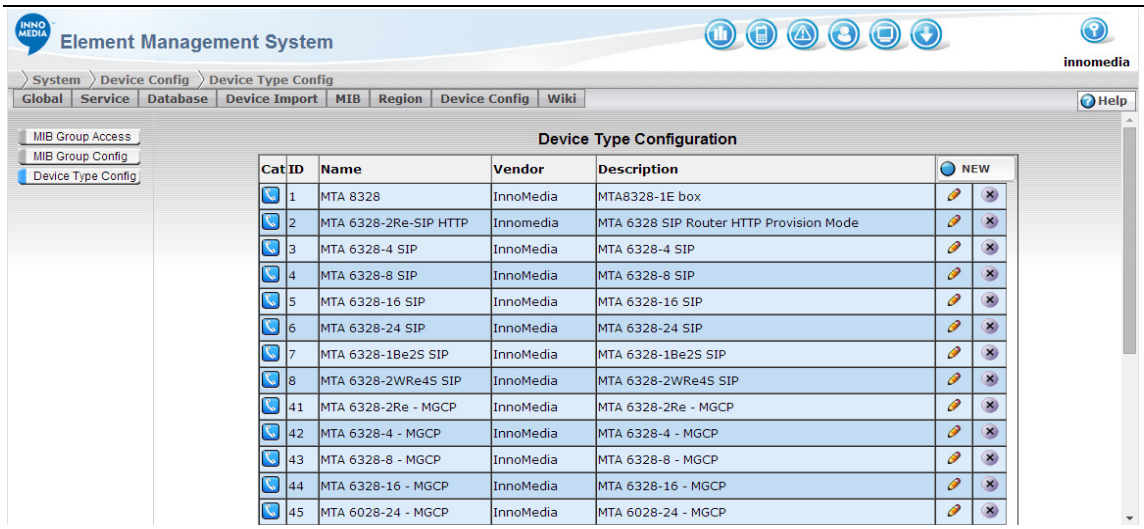


Figure 9-9. Type Configuration Screen

Type List lists available types. Types are defined in Device Type List. You can't add or remove Type from this screen. Please use Device Type List screen to edit Device Type setting.



Cat	ID	Name	Vendor	Description
	1	MTA 8328	InnoMedia	MTA8328-1E box
	2	MTA 6328-2Re-SIP HTTP	Innomedia	MTA 6328 SIP Router HTTP Provision Mode
	3	MTA 6328-4 SIP	InnoMedia	MTA 6328-4 SIP
	4	MTA 6328-8 SIP	InnoMedia	MTA 6328-8 SIP
	5	MTA 6328-16 SIP	InnoMedia	MTA 6328-16 SIP
	6	MTA 6328-24 SIP	InnoMedia	MTA 6328-24 SIP
	7	MTA 6328-1Be2S SIP	InnoMedia	MTA 6328-1Be2S SIP
	8	MTA 6328-2WRe4S SIP	InnoMedia	MTA 6328-2WRe4S SIP
	41	MTA 6328-2Re - MGCP	InnoMedia	MTA 6328-2Re - MGCP
	42	MTA 6328-4 - MGCP	InnoMedia	MTA 6328-4 - MGCP
	43	MTA 6328-8 - MGCP	InnoMedia	MTA 6328-8 - MGCP
	44	MTA 6328-16 - MGCP	InnoMedia	MTA 6328-16 - MGCP
	45	MTA 6028-24 - MGCP	InnoMedia	MTA 6028-24 - MGCP

NOTE: Only device type with the same view type will show on the type list

9.4.1 Accessing the Type Configuration Screen

To access the Type Configuration Screen, following the steps:

1. Click Provisioning icon  .
2. Select [Type Config] tab

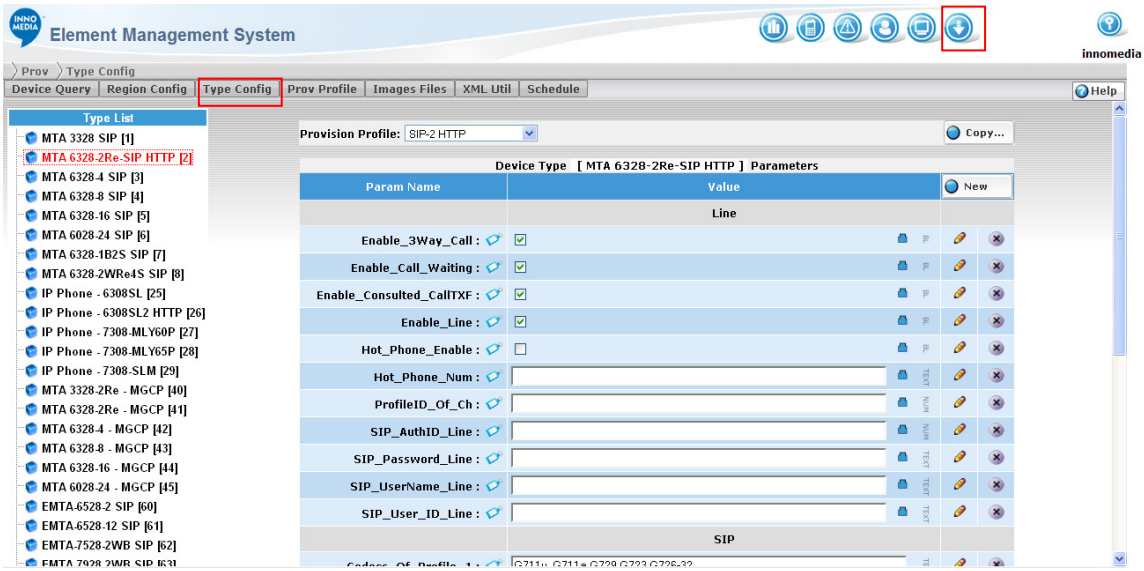


Figure 9-10. Accessing Type Configuration Screen

9.4.2 Editing Type Configuration

To edit a Type Configuration, following the steps:

1. Click the Type name on the left panel.
2. Edit the Type parameter on the right panel
3. Click Save button to submit the change. A success or fail dialog will pop-up.
4. Click Ok or wait for few seconds will close the popup window.

9.4.3 Editing Parameters

Region, Type and Device share the same style of Parameter configuration. Please reference to Parameter Configuration Screen on page 140 for more details.

9.5 Provisioning Device List

Device List Screen provides an interface to search and browse devices under EMS provisioning.

9.5.1 Accessing the Device List Screen

To access the Device List Screen, follow these steps:

1. Click Provisioning icon.
2. Select the [Device Query] tab

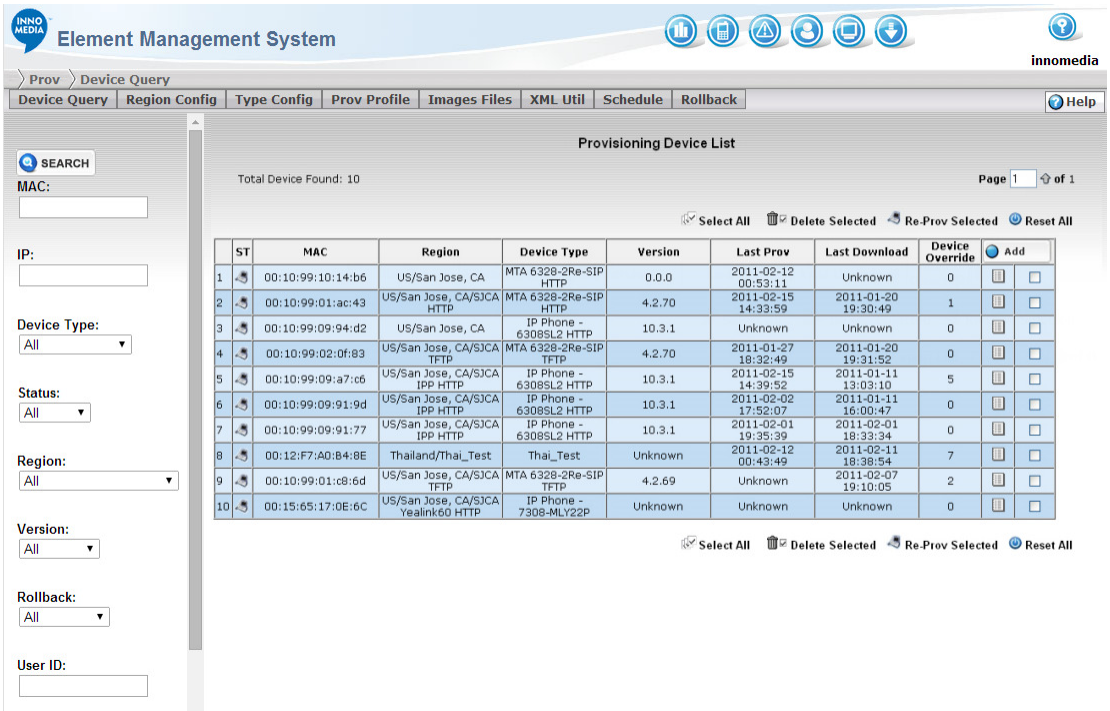


Figure 9-11. Device Query Screen

9.5.2 Query Device

The administrators can query devices by their MAC addresses, IP addresses, device types, device status, assigned regions, firmware versions and user IDs.

NOTE: System Administrators are only allowed to query devices in their own granted regions.

To query a device, follow these steps:

1. Enter your search criteria in the search fields in the left panel.
2. Click the Search button. Devices that matched the search criteria are displayed in the right panel.

Field	Description
MAC	The MAC address of the device. It is OK to enter only the first few digits of the MAC address. The system will match the entered digits in the field and list the searched result in the right panel.
IP	The IP address of the Device
Device Type	Type of the device. The available device type can be found in the drop-down box. The device types are defined on Device Type List screen (see Device Type List on page 63).

Status	The current status (i.e., all, off-line, or on-line) of the device.
Region	Device assigned region
Version	Device firmware version
Rollback	Search for Devices that have been Rolled back to a previous configuration
User ID	Device user ID (or phone number)
Record Per Page	The number of records you would like to see per page. The default setting is 100.

9.5.3 Device List

On the upper-left corner, you will find the total number of devices configured in EMS (that match the search filter). The number of records displayed on the screen will depend on what you have specified in the Records Per Page field. If the found records are more than the number you specified, you can either enter the page number in the field and click the Go To button, or just simply click the double arrow button for next or previous page.

The following table describes the fields on the Device List screen:

Field	Description
ST	Device current status. Green icon indicates Device is on line. Red icon indicates Device is off line. Gray icon indicates Device is lost (off line for more than 7 days or the max lost day define in global parameter page). Clicking the Status (ST) icon ( ) will popup a Device Configuration screen (see Device Configuration Screen on page 163).
MAC	The MAC address of the device.
Region	The device assigned region name.
Device Type	Type of the device.
Version	The current firmware version loaded to the device
Last Provisioning	The time stamp of when the device last performed provisioning.
Last Download	The time stamp of when the device last performed an image download.

Device Override	The number of device specific parameter value declared. Device has override value may imply that if you only changed the region or type parameter value, it may not show on the final configuration data due to the device override having the highest precedence.
Syslog ( )	Show the log message send from selected device. Click will pop up a Device Log Screen (see Device Logs on page 143).

There are several buttons on both top and bottom of the device list:

Button	Description
Select All	Check all check box in the device list
Delete Selected	Delete selected Devices
Re-Prov Selected	Send Re-Provision to selected Devices
Reset All	Send Reset to selected Devices

9.5.4 Device Configuration

Clicking the Status (ST) icon ( ) will popup a Device Configuration Screen. See Adding a Device Screen on page 142).

9.5.5 Adding Device

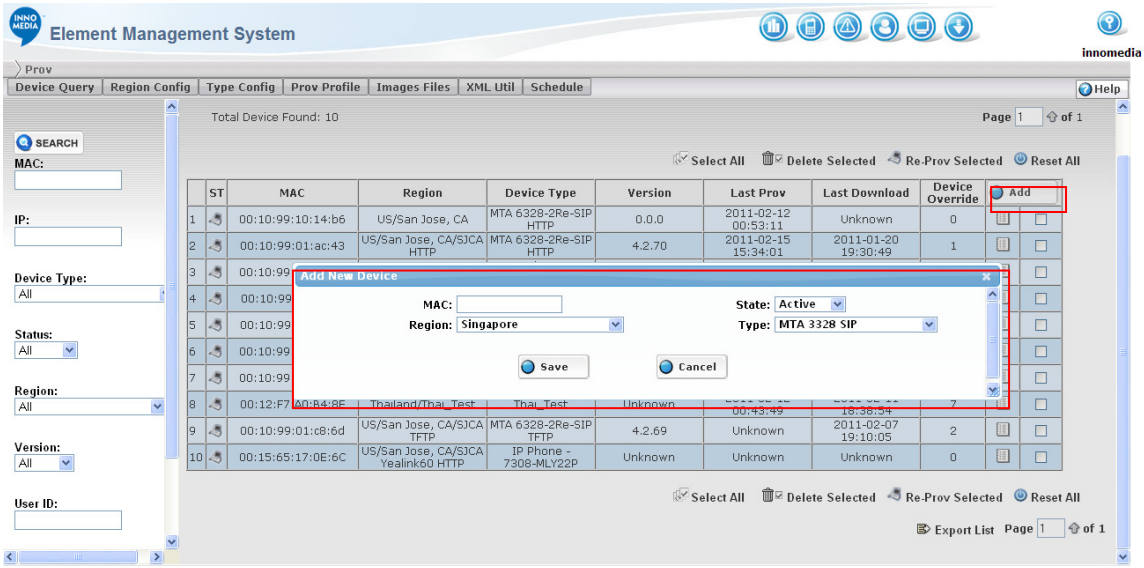


Figure 9-12. Adding a Device

1. Click the Add button on the top-right of device list will popup an “Add New Device” dialog box.
2. Fill in the fields.
3. Click Save button to submit the update.

Field	Description
MAC	MAC Address of new device.
State	The State value of either enable or disable EMS to provide provisioning to the device. **Active**: provisioning is enabled; **Inactive**: provisioning is disabled.
Region	Set the Region of the new device.
Type	Set the Type of the new device.

NOTE: Device also can be added from XML Utility Screen or EMS Device list Screen.

9.5.6 Deleting Device

To Delete a Device, follow the steps:

1. Click the check box on right of the device to be deleted.
2. Click the Delete Selected button to remove the device from list.

9.6 Device Logs

The Device Log screen allows the system administrator to view a device logs by the device-ID, date, and string. This section describes how to access Device Log screen and search the logs.

9.6.1 Accessing Device Logs

To access the Device Log screen, follow these steps:

1. Click Provisioning icon.
2. Select the Device Query.
3. Search for the device for device log.

4. Click the Syslog button to popup the Device Log Screen.

9.6.2 Device Log Screen

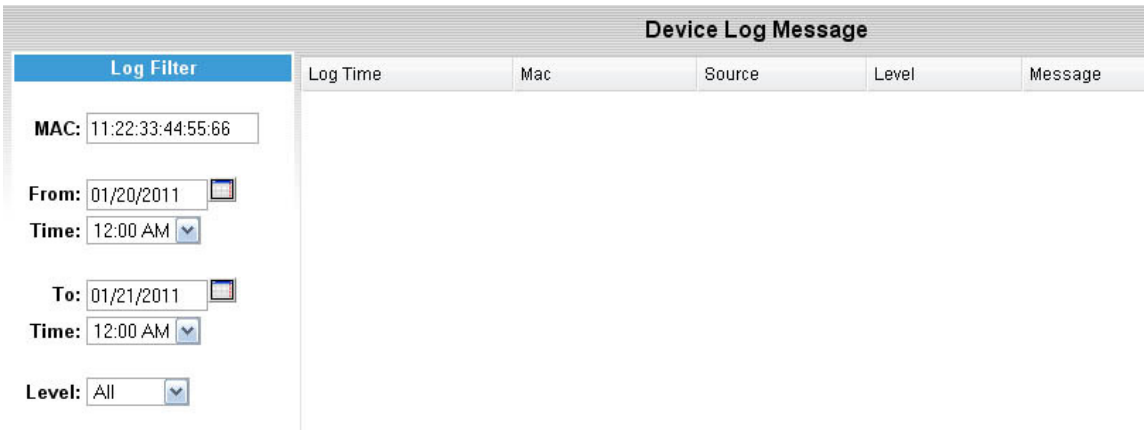


Figure 9-13. Device Log Screen

Search Panel

The left panel is a log filter. Input the search criteria and click Search button to search matched device log. The search field defined as follow:

Field	Description
MAC	The Mac Address of device. Leave empty for query all devices.
From Time	Enter the search starting date in the From field or select a date by clicking the Calendar( ).
To Time	Enter the search ending date in the To field or select a date by clicking the Calendar( ).
Level	Select the message severity level from the drop-down menu.

Message List

The right panel is a list of matched log list.

Field	Description
Log Time	Date Time when EMS received the message.

MAC	MAC Address of the device which sent the message.
Source	The IP Address of the device when it sent the message.
Level	Log message severity level.
Message	Content of the syslog message.

NOTE: EMS Syslog uses a circular buffer for expiring of old messages automatically. There is no need to clean up old log messages.

9.7 Device Configuration Screen

Device Configuration Screen provides an interface for configuring per-device provisioning parameters.

9.7.1 Access Device Configuration Screen

1. Click Provisioning icon.
2. Select [Device Query] tab.
3. Click status icon on the left of device.

9.7.2 Adding, Editing and Deleting Parameters

Region, Type and Device share the same style of Parameter Configuration Screen. Parameter Configuration Screen provides a GUI for administrator management device parameters in different level. Please refer to Parameter Configuration Screen on page 140.

In addition to common Parameter Configuration Screen, Device Configuration Screen supports more features:

9.7.3 Device Information

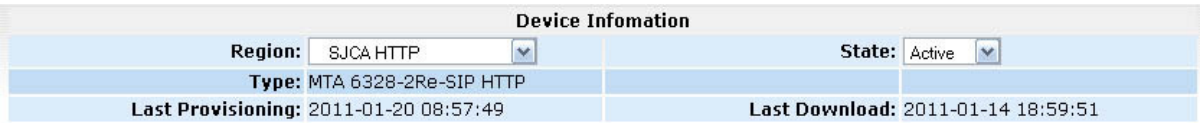


Figure 9-14. Device Information

Device Information Section provides the following fields:

Field	Description
Region	Which Region does this device belong to. Device region can be changed
State	The State value enable or disable EMS provide provisioning to the device. **Active**: provisioning is enabled; **Inactive**: provisioning is disabled.
Type	Pre-configured device type
Last Provisioning	The time stamp when the device last performed provisioning.
Last Download	The time stamp when the device last performed an image download.

9.7.4 Port Parameters Section

Figure 9.4. Port Parameters

Depending on the EMS Profile Port Number setting, Port Parameters Section creates same number of tabs as port number defined in selected profile. All ports share the same parameter setting; but each port will have it own parameter setting.

Click on port tag for configuring different port parameter values.

Port Tag Review

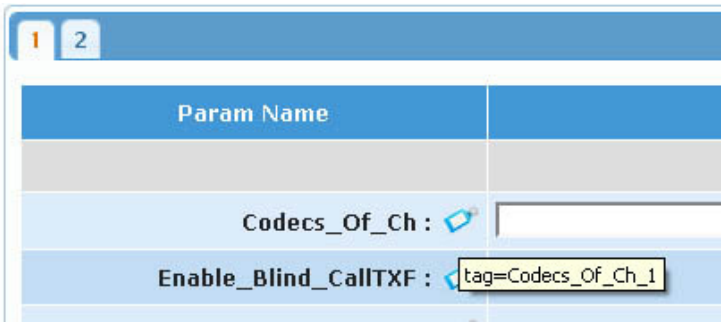


Figure 9-15. Port Tag Review

On right of each parameter name, move mouse over the tag icon ( ) will show the real tag used to generate configuration file. For port parameters, the tag will show the real tag after the port symbol substitution. Port Symbol is defined in Profile Screen.

9.7.5 Device Config File

You can download the device configuration file that is generated by EMS.

Click the Config button to view or download the configuration file to your local disk.

9.7.6 Device Provisioning History Chart

Figure 9-16. Device Provisioning History Chart

Clicking the History button on the top right of screen will open the Device Provisioning History Section. Device Provisioning History shows the historic time line of when the device did provision and image downloading.

Different tags mark the time on the time line for provisioning and downloading.

- Blue tag marks the time the device did successful provisioning,
- Green tag marks the time of device did successful image downloading.
- Red tag marks the time the device failed provisioning or image downloading.

Note: In the case of ESBC, currently only the success of image downloading is indicated.

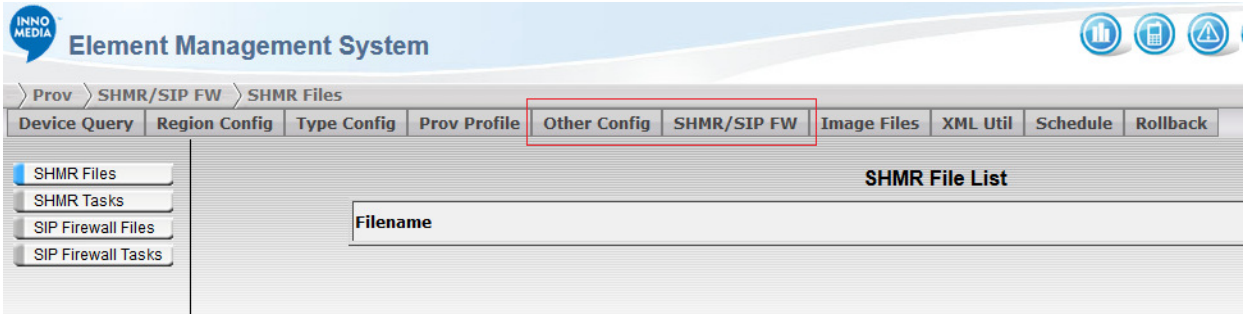
- Move the cursor on top of each tag to show the exact time of the provision or download happen.

- Time Range available on the lower right of Device Provisioning History Chart. Click the Time Range button allow quick zoom in and out of the time chart.
- Time Range also can use mouse to directly click and drag on the plot area to mark a selected range.
- Click “Reset View” button can zoom back to the time range set by the Time Range button.
- Click on the provision or download tag to pop up a Historical Parameter Screen. Historical Parameter Screen shows the parameter value snapshot at the time of device provisioning.

9.7.7 Historical Parameter Screen

Clicking the tag on Device Provisioning History Chart will bring up the Historical Parameter Screen. Historical Parameter Screen is a snapshot of provision parameter values used exactly at the time when the device provisioned. Historical Parameter Screen is similar to Device Configuration Screen but read only.

9.8 Other Config



This part is applicable to ESBC devices where you can import and select PBX Profiles, and build ACL scripts, which can be then be applied or used for specific ESBC devices

9.9 SHMR / SIP FW

This part is applicable to ESBC devices where you can import build SHMR scripts, and import or build SIP Firewall rules, which can be then be applied or used for specific ESBC devices

9.10 Image Upload

Image Upload Screen provides an interface for uploading an image file. Administrator needs upload image files before device can download it from EMS.

9.10.1 **Accessing Image Upload Screen**

To access Image Upload Screen, follow the steps:

1. Click the Provisioning icon.
2. Select the [Images Files] tab.

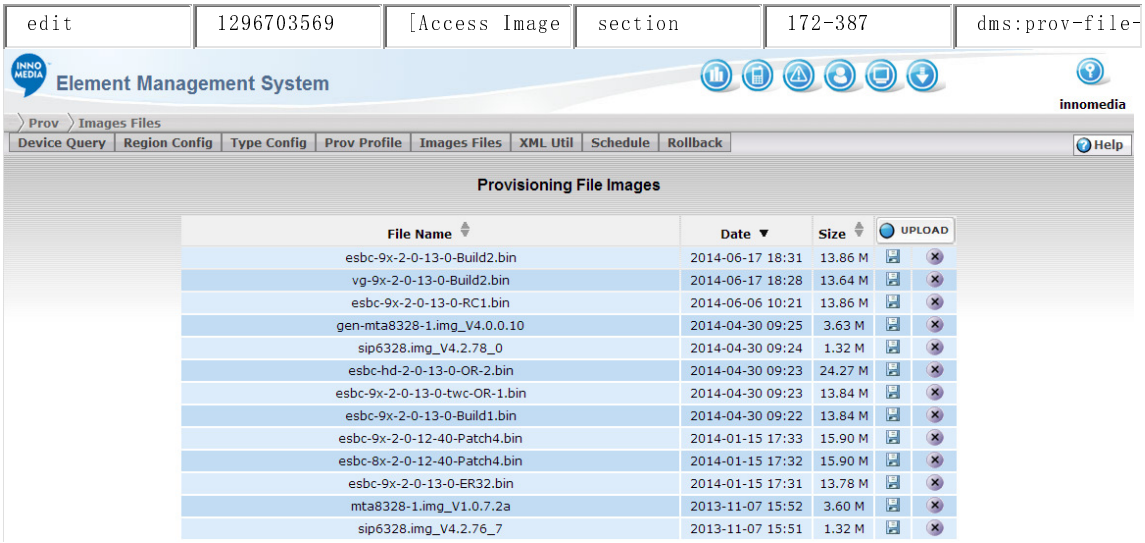


Figure 9-17. Provisioning File Upload Screen

9.10.2 **Image List**

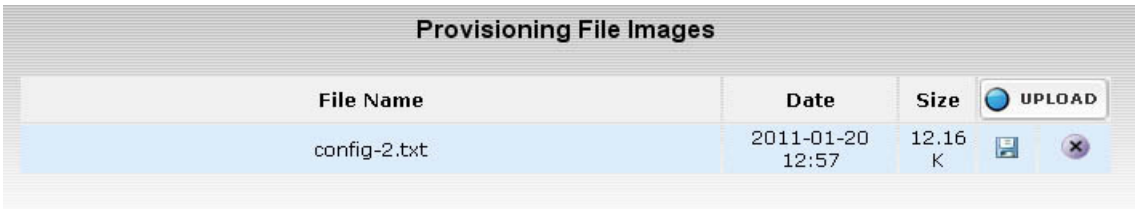


Figure 9-18. Provisioning File Image List

The Image List shows all image files already available in EMS.

Field	Description

File Name	Name of image file.
Date	File uploaded date.
Size	Size of image file.
Download ( )	Download the image file from EMS to local disk.
Delete ( )	Remove this image file from EMS list.

9.10.3 **Adding Image File**

To Add an Image File, follow the steps:

1. Click the Upload button on top-right of image list. A file select dialog box will pop up.
2. Pick the file from your local machine you want to upload and click "Open".
3. File will start upload with a progress bar until the upload complete.

NOTES:

All uploaded image files are stored in the path that defined in the Global Parameter page field "Prov Image Storage:". That directory must be accessible by the apache (HTTP) server.

File upload has file limitation. Large files will not be able to be uploaded by WEB GUI. The upload file size limitation is defined in /etc/php.ini. If a big file is required but not able upload from WEB GUI, you can directly copy the file into the image storage directory (defined in the Global Parameter page field "Prov Image Storage:").
For more details about Global Parameter Setting on page 29.

9.10.4 **Uploading Progress**

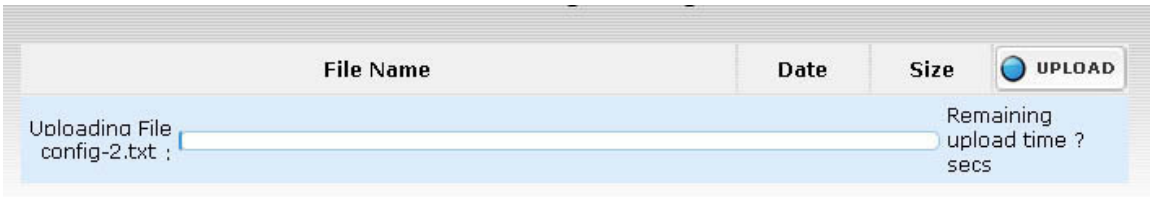


Figure 9-19. Provisioning File Image Uploading Progress

When uploading an image file, an upload progress bar will showing the current upload progress and estimated upload time.

9.10.5 **Deleting Image File**

To Delete an Image File, follow the steps:

1. Click the Delete button on right of image file name. A confirm dialog pop up with the message:

   Are you sure you want delete image file?

2. Click “Ok” to remove the image file from list.

9.10.6 **Downloading Image File**

To download an Image File, follow the steps:

1. Click the Save button ( ) on right of image file name. A Save dialog pop up.
2. Input the local file name and Click “Open” to save the image file to local machine.

9.11 XML Utility

The EMS XML Utility can be used to query the EMS device database and make changes to it. This section describes the XML Utility interaction with EMS provisioning system. XML file needs to follow the EMS XML syntax prov-config.dtd. EMS XML lines actually are executable commands. When importing an XML file, EMS executes the command within the XML file and reports the result of execution.

9.11.1 **Accessing the XML Utility**

To access the XML Utility, follow these steps:

1. Click the Provisioning icon.
2. Click the [XML Util] tab

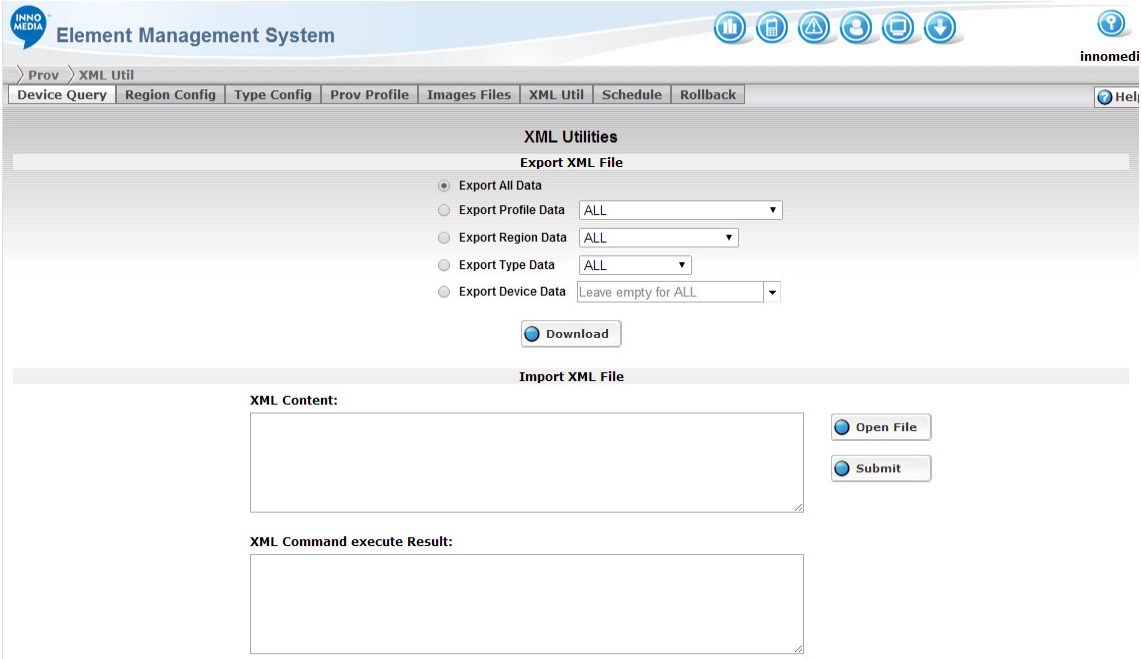


Figure 9-20. XML Utilities Screen

9.11.2 **Exporting XML File**

Administrator can export a whole or a partial EMS provision device database. The upper section of XML Utility is for XML export. To Export XML File, follow these steps:

NOTE: Device configuration does not include what it inherited from other class; therefore, only the override values or device's own parameters will be exported.

1. Pick one of the following categories:
   - Export All Data – Export all setting in database
   - Export Profile Data – Export all or selected profile configuration
   - Export Region Data – Export all or selected region configuration
   - Export Type Data – Export all or selected type configuration
   - Export Device Data – Export all or selected device configuration
2. Click the Download button and a File save dialog will pop up. Input a local file name and click "Open" to save it.

9.11.3 **Importing XML File**

Administrator can import previous exported file, or import an XML file created by a text editor or another system to EMS server.

NOTE: Import of XML file has size limit. The maximum upload file size is defined in /etc/php.ini

To import XML File, follow these steps:

1. Click [Open] button on right of XML content box. A file open dialog box pops up.
2. Enter the directory path of the file then click "Open" on the file open dialog box.
3. The content of file will upload to the **XML Content:** window.
4. Click Submit button to send the XML to server.
5. EMS will execute the XML and show the result in **XML Command Execute Result** window.

9.11.4 **Executing XML Commands**

Instead of uploading XML file, administrator can also type in the XML command in the **XML Content** window and then execute it.

To execute XML commands, follow these steps:

1. Enter the XML command in the **XML Content** window.
2. Click the Submit button to execute the commands.
3. Execute result will show in the **XML Command execute Result** window.

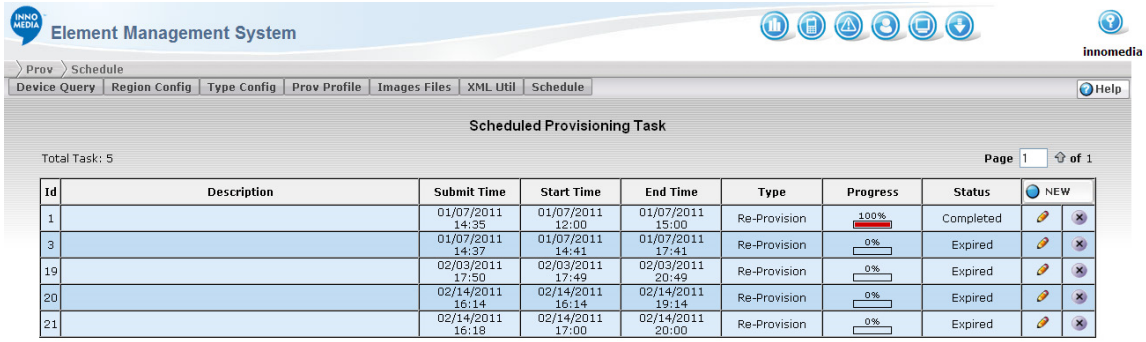
9.12 Task Scheduler

EMS can request device to reboot or re-provision. Reset or Re-prov all devices at once is not recommended since that will flood the EMS server. EMS provides a task scheduler interface that allows the administrator to scatter the requests within a predefined time period to reduce the burst of request from devices. EMS Task scheduler also provides a convenient interface to pick the target devices, check the task progress, and pause/resume/cancel the running task.

9.12.1 **Accessing Task Scheduler Screen**

To Access Task Scheduler Screen, follow these steps:

1. Click Provisioning icon. 
2. Select "Schedule" tab.



Id	Description	Submit Time	Start Time	End Time	Type	Progress	Status
1		01/07/2011 14:35	01/07/2011 12:00	01/07/2011 15:00	Re-Provision	100%	Completed
3		01/07/2011 14:37	01/07/2011 14:41	01/07/2011 17:41	Re-Provision	0%	Expired
19		02/03/2011 17:50	02/03/2011 17:49	02/03/2011 20:49	Re-Provision	0%	Expired
20		02/14/2011 16:14	02/14/2011 16:14	02/14/2011 19:14	Re-Provision	0%	Expired
21		02/14/2011 16:18	02/14/2011 17:00	02/14/2011 20:00	Re-Provision	0%	Expired

Figure 9-21. Scheduled Provisioning Task Screen

9.12.2 **Task List**

Id	Description	Submit Time	Start Time	End Time	Type	Progress	Status
1		01/07/2011 14:35	01/07/2011 12:00	01/07/2011 15:00	Re-Provision	100%	Completed
3		01/07/2011 14:37	01/07/2011 14:41	01/07/2011 17:41	Re-Provision	0%	Expired

Figure 9-22. Provisioning Task List

Task List shows all running tasks currently defined in EMS system. The field definition of Task list as follow:

Field	Description
ID	Task Id automatically generated by EMS system.
Description	A note about the task.
Submit Time	Time when the task was submitted to the scheduler.
Start Time	Time when the task will start execution.
End Time	Time estimate when the task will complete.

Type	This is a **Reset** or **Re-Prov** task
Progress	Task execution progress (in percentage). Progress only shows when task is during execution.
Status	**Unsubmit**: task not been submitted yet. **In progress**: task is executing now. **Complete**: task completed. **Expired**: task end time reached but has not been executed for all devices. **Canceled**: task been canceled.
New	Create New Task
Edit( )	Edit Task
Delete( )	Delete Task

9.12.3 **Creating New Task**

To create a new task, follow these steps:

1. Click the New button NEW on the top right of list.
2. A Task Detail screen will pop up.
3. Complete the form and click Submit button.

Please refer to Schedule Task Detail on page 164 for more details.

9.12.4 **Editing Task**

To edit a task, follow these steps:

1. Click the Edit button on the right of selected task.
2. A Task Detail screen will pop up.
3. Complete the update and click Submit button.

Please refer to Schedule Task Detail on page 164 for more details.

9.12.5 **Deleting Task**

To delete a task, follow these steps:

1. Click the Delete button of the selected task.
2. A confirm dialog with message:

Delete Task xx?

3. Click OK to remove the task from list.

9.12.6 **Schedule Task Detail**

Schedule Task Detail provides the interface for administrator to set the task type, schedule time, select the target device and submit/cancel/re-submit the task.

9.12.6.1 Accessing Schedule Task Detail Screen

To access Schedule Task Detail screen, follow these steps:

1. Click Provisioning icon.
2. Select "Schedule" tab
3. Click Edit on right of task or click the New button NEW.

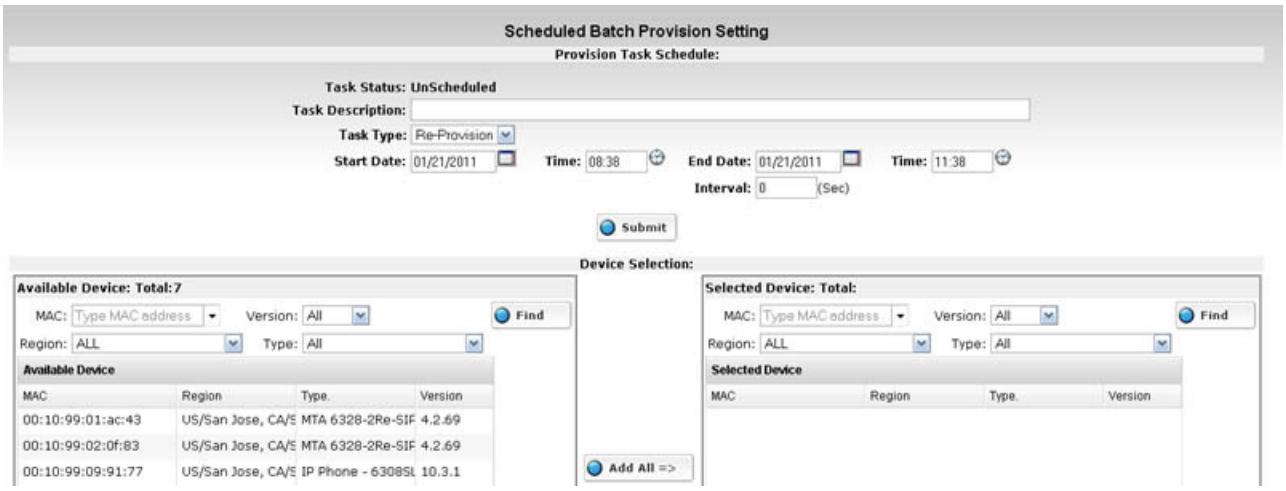


Figure 9-23. Schedule Task Detail Screen

The top section of Schedule Task Detail Screen is task information, schedule time and status:

Field	Description
Task Status	**Unscheduled**: task not been submit yet. **In progress**: task is executing now. **Complete**: task completed. **Expired**: task end time reached but has not been executed for all devices. **Canceled**: task been canceled.
Task	A note about the task.

Description	
Task Type	This is a **Reset** or **Re-Prov** task
Start Date Time	Time when the task will start execution.
End Date Time	Time estimate when the task will complete.
Interval	Estimated time interval between commands sent to devices.

9.12.6.2 Submitting a Task

To submit a new task, follow these steps:

1. Select the Task type, to reset the device or re-provision device.
2. Set the Start time and End time of the task.
3. Select Target Devices.
4. Click Submit button.

End Time and Interval will adjust automatically when you change the time range setting:

- If Start time Changes, End Time will be updated based on Interval and Number of selected devices.
- If End time changes, Interval will be updated based on End Time and Number of selected devices.
- If Number of device changes, End Time will be updated based on Interval and Number of selected devices.
- If Interval changes, End Time will be updated based on Interval and Number of selected devices.

9.12.6.3 Selecting Target Devices

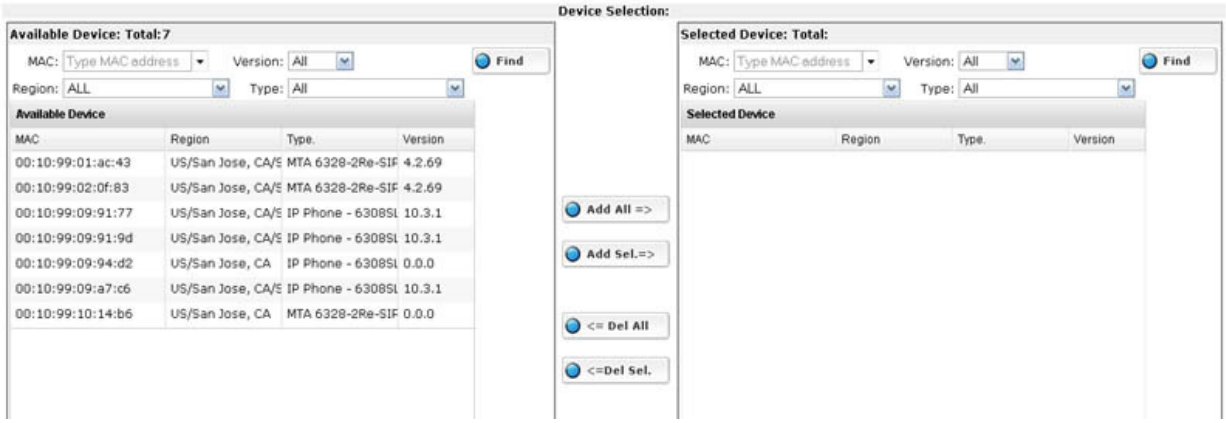


Figure 9-24. Selecting Target Devices

When creating a new task, or a task has not been submitted yet, Target selection interface will show on the lower section of Schedule Task Detail Screen.

The left panel of Target selection section is a list of all available devices defined in EMS system

The right panel of Target selection section is selected target devices to be submitted into task.

Both panels provide filter interface on top of each panel to help administrator locate the target devices.

Field	Description
MAC	Search device with this MAC Address
Version	Search devices with a specific version.
Region	Search devices in a specific Region.
Type	Search devices with a specific Type.
Find	Click the Find button to execute the filter.

To Add a device to the selected device panel, use the **Add All⇒** button or **Add Sel.⇒** button.

To remove device from the selected device panel, use the **⇐ Del All** button or **⇐ Del Sel.** button.

- **Add All⇒** button: Add All Available device to Selected Device panel.
- **Add Sel.⇒** button: Add selected device from available devices to selected device panel
- **⇐ Del All** button: Remove all devices from selected device panel.
- **⇐ Del Sel.** button: Remove selected devices from selected device panel

9.12.6.4 Deleting a Task

If a Task is in **Complete** or **Cancel** state, administrator can delete the task by click the Delete button.

9.12.6.5 Canceling a Task

If a Task is in **Progress** state, administrator can cancel the task by clicking the Cancel button. Canceled task still remains in EMS database but device command will not be executed.

9.12.6.6 Resuming a Task

If a Task in **Expired** or **Cancel** state, administrator can be resume the Task by clicking the Re-submit button. Administrator can reset the time range before re-submitting the Task and continue the unfinished devices within a new time range.

9.13 Rollback

EMS allows rollback for any changes made in Auto Provisioning Configuration.

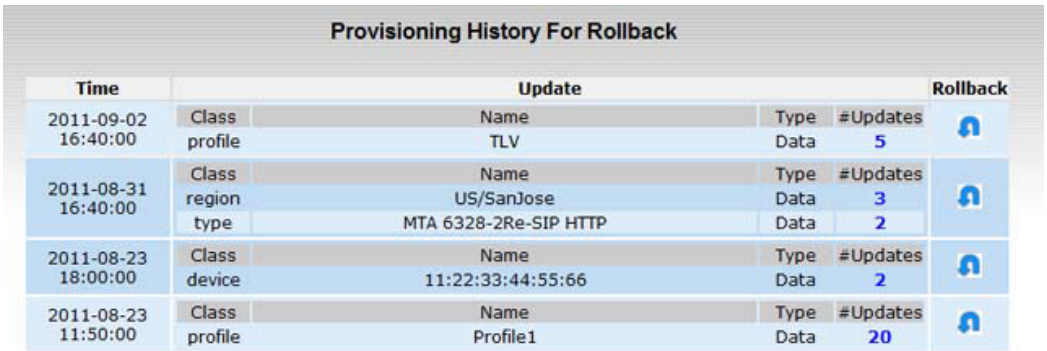
Rollback must done in a unit of a rollback group. Individual changes will be grouped into a 30 minutes time frame. That is, all and any changes made within the same 30 minutes time frame will be treated as a single group of changes. (e.g. Update time from 10:00 to 10:29 will be in 10:00 group; and update time within 10:30 to 10:59 will be in 10:30 group.) This ensures all related changes can be rollback at once.

9.13.1 **Accessing Rollback Screen**

Access Configuration Rollback Screen, follow these steps:

1. Click Provisioning icon. 
2. Select “Rollback” tab.

9.13.2 **Rollback Group List**



Provisioning History For Rollback

Time	Update				Rollback
2011-09-02 16:40:00	Class	Name	Type	#Updates	
	profile	TLV	Data	5	
2011-08-31 16:40:00	Class	Name	Type	#Updates	
	region	US/SanJose	Data	3	
	type	MTA 6328-2Re-SIP HTTP	Data	2	
2011-08-23 18:00:00	Class	Name	Type	#Updates	
	device	11:22:33:44:55:66	Data	2	
2011-08-23 11:50:00	Class	Name	Type	#Updates	
	profile	Profile1	Data	20	

The field definition of Task list as follow:

Field	Description

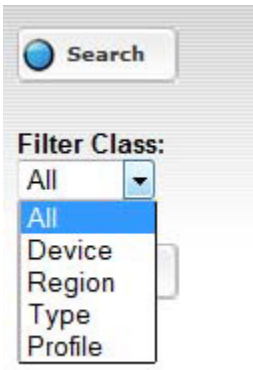
Time	Time frame of this rollback group
Update	Update shows the related parameter change in this group, which includes the updated class and name and the number of updates. [Class] column shows the class of updated data, [Name] column shows the name of updated class, [Type]column shows it is a parameter update or a data update, [#Updates] column shows the number of updated in this batch.
Rollback	Click to do rollback all change in this group. Once the rollback performed, the entry will be deleted automatically.

NOTE 1: Rollback from the top most entry is preferred. Rollback of a non-top entry may give unexpected result.

NOTE 2: Rollback action itself can NOT be undone.

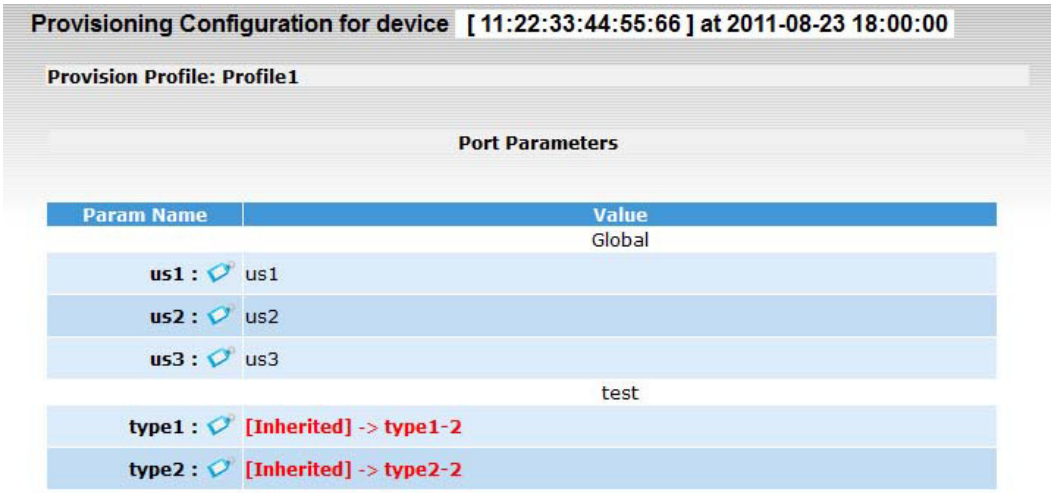
9.13.3 **Rollback Group Filter**

Rollback Group Filter can apply for a particular Type, Region or device. First select the filter class on the left panel, then select the type, region or device mac as a filter. Then click the [*Search] button to apply.



9.13.4 **Rollback History Page**

Click on the [#Update] column number show what value been updated. A historical configuration data window will popup with all parameters. Data whose value has been changed will be highlight in **RED**.



9.14 Rollback By Time

Rollback also can be done by giving a selected date-time, and rollback all updates from that target date to present by one click.

Rollback Time select can either using the date picker and time picker to input target date/time. Or simply click the time value in **Time** column above to set the target date-time.

After setting the target rollback date, click the rollback button to rollback all changes from target date to present.

10 SNMP Management of EMS System

InnoMedia EMS can also be managed by an external SNMP Manager where it can provide crucial information or send SNMP System Traps under certain conditions. For additional EMS system Traps and Alerts, see section 7.7.

10.1.1 **SNMP MIBs**

The Following SNMP MIBs will be required, and can be provided by InnoMedia upon request.

- HOST-RESOURCES-MIB
- UDC-SNMP-MIB
- COROSYNC-MIB

10.1.2 **SNMP Get or Walk**

1. Get EMS CPU usage information:
   % snmpwalk -v 2c -Lo -c m0n1t0r 192.168.15.21 **.1.3.6.1.2.1.25.3.3.1.2**
   HOST-RESOURCES-MIB::hrProcessorLoad.768 = INTEGER: 1
   HOST-RESOURCES-MIB::hrProcessorLoad.769 = INTEGER: 2
   HOST-RESOURCES-MIB::hrProcessorLoad.770 = INTEGER: 1
   HOST-RESOURCES-MIB::hrProcessorLoad.771 = INTEGER: 1

In this case, 192.168.15.21 is the EMS server which is being monitored. The above result shows that there are 4 processor cores in the system and lists the load of each core.

2. Get EMS memory usage information:
   % snmpwalk -v 2c -Lo -c m0n1t0r 192.168.15.21 **.1.3.6.1.4.1.2021.4.6**
   UCD-SNMP-MIB::memAvailReal.0 = INTEGER: 375444 kB

3. Get EMS disk available space and usage information:
   % snmpwalk -v 2c -Lo -c m0n1t0r 192.168.15.21 .1.3.6.1.4.1.2021.9.1.7
   UCD-SNMP-MIB::dskAvail.1 = INTEGER: 16042464
   % snmpwalk -v 2c -Lo -c m0n1t0r 192.168.15.21 **.1.3.6.1.4.1.2021.9.1.9**
   UCD-SNMP-MIB::dskPercent.1 = INTEGER: 18

4. Get EMS CPU load averages in the last 1, 5, and 15 minutes:
   % snmpwalk -v 2c -Lo -c m0n1t0r 192.168.15.21 **.1.3.6.1.4.1.2021.10.1.3**
   UCD-SNMP-MIB::laLoad.1 = STRING: 0.00
   UCD-SNMP-MIB::laLoad.2 = STRING: 0.03
   UCD-SNMP-MIB::laLoad.3 = STRING: 0.00

5. Get number of users logged in the EMS and number of processes loaded or running:
   % snmpwalk -v 2c -Lo -c m0n1t0r 192.168.15.21 **.1.3.6.1.2.1.25.1.5**
   HOST-RESOURCES-MIB::hrSystemNumUsers.0 = Gauge32: 1

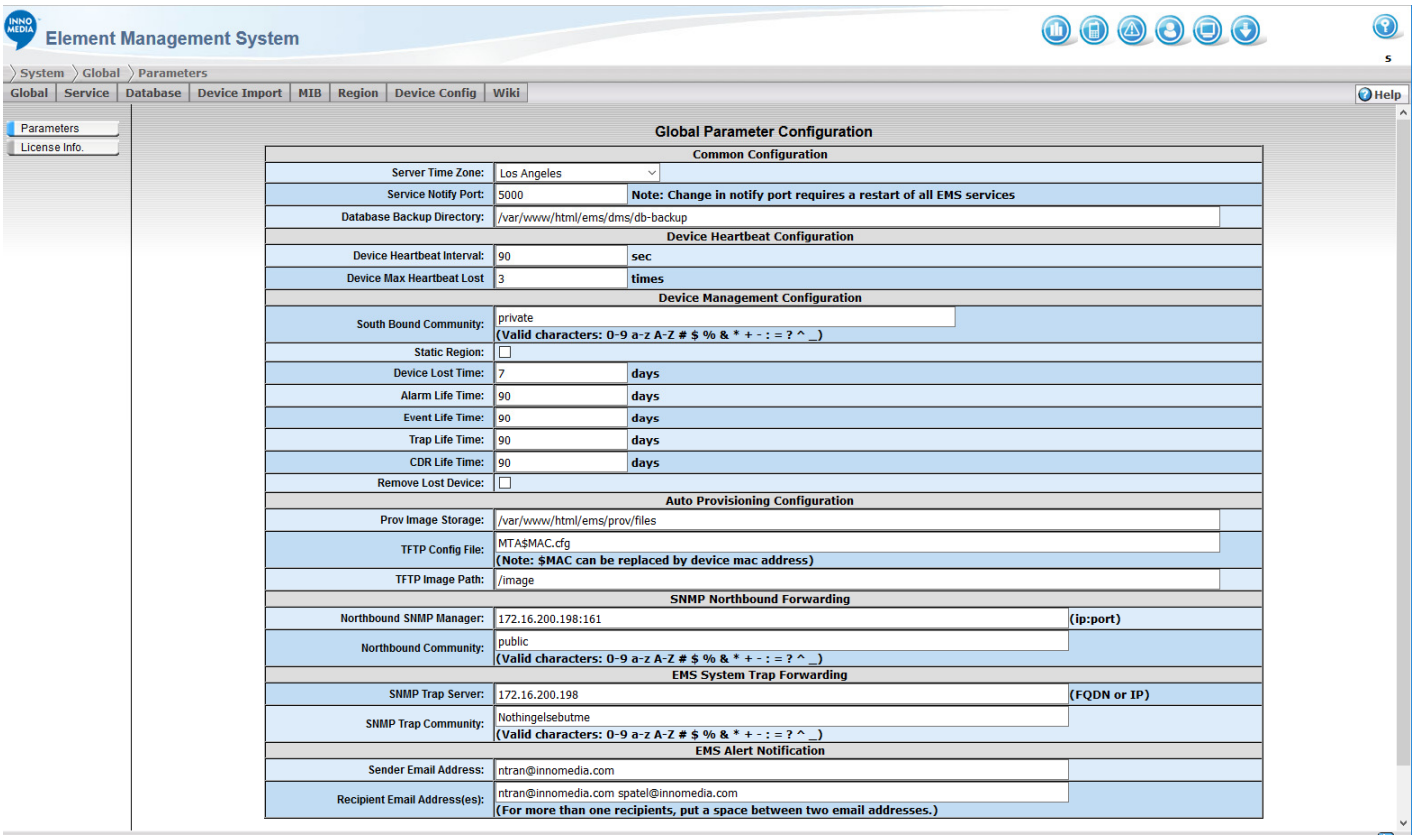
% snmpwalk -v 2c -Lo -c m0n1t0r 192.168.15.21 **.1.3.6.1.2.1.25.1.6**
HOST-RESOURCES-MIB::hrSystemProcesses.0 = Gauge32: 227

10.1.3 **SNMP Traps**

For a HA-based EMS system, it is critical to know when a particular node has gone down or switched. When that occurs, SNMP traps will be sent out to the SNMP Manager managing the InnoMedia EMS system.

Configure InnoMedia EMS to send EMS related Traps to an external SNMP Manager:

- Configure and save the appropriate "SNMP Trap Server" and "SNMP Trap Community "string in the "**EMS System Trap Forwarding**" portion



1. Node status is sent from the Master node when another node has joined or left the cluster.
   COROSYNC-MIB::corosyncNoticesNodeStatus
   corosyncObjectsNodeName : hostname of node
   corosyncObjectsNodeID : unique ID of node
   corosyncObjectsNodeAddress : address of node
   corosyncObjectsNodeStatus : "joined" or "left"

2. App status is sent from a node when it is started or stopped.

COROSYNC-MIB: corosyncNoticesAppStatus
objects:
corosyncObjectsNodeName : hostname of node
corosyncObjectsNodeID : ID of node
corosyncObjectsAppName : application name, e.g. “crmd:CMAN:xxx:xx”, “cib:CMAN:xx:xx”
corosyncObjectsAppStatus : “connected” or “disconnected”

Appendix A. Geographical Redundancy Design

The EMS's geographical redundancy uses the following design:

- **ACTIVE-ACTIVE APPROACH**

With an active-active design, the EMS servers at both sites are operational and provide services continuously and simultaneously. Devices (as in the case of the InnoMedia ESBC9xxx and ESBC10K) will first reach out to the primary server for services, and fall back to the redundant (secondary) server in case it cannot reach the primary site for any reason. In general, the design philosophy is that the primary site should deliver service as far as possible, unless it is not reachable or available. Therefore, while receiving services from the secondary server, the device will continue to ping the primary server (see description below), and will revert back to the primary server once the primary server has recovered from any outages.

- **Keep-Alive and Ping Messages**

There are two messaging mechanisms used in the communication between devices and EMS servers, namely Keep-alive and Ping messaging.

The keep-alive messaging employed by the EMS is a unidirectional approach, where devices will send the keep-alive messages to the primary server only without any acknowledgement from the server. The EMS servers utilize the information contained in the keep-alive messages to determine which server is communicating with the particular device, as well as to learn the status (e.g., online/offline) of the devices.

A Ping message is sent by the device in addition to the keep-alive messaging in order to discover the status of the servers. Devices will periodically send a Ping message to all configured EMS servers, and expect a reply or acknowledgement back from the respective EMS servers. If the device does not receive the required reply after 3 consecutive attempts, this particular EMS server will be considered offline. Devices will use this ping mechanism to maintain a list of active servers available to provide services based on the priority configured in the devices. The ping message does not affect the online status of the device in the EMS's database, and it is purely used by the devices to discover the status of the servers. Devices will then send a keep-alive message only to the highest priority server which is online. When the highest priority server becomes offline (based on responses to the ping messages), the device will register to the next server on the list by sending keep-alive messages to that server, but will continue to send ping messages to the highest priority server. The device will switch back to the highest priority server once it becomes available again.

- **EMS Server Database**

Geographical redundancy on the EMS server is achieved via MySQL replication. Two sets of EMS servers, one on each site, will synchronize their databases with each other using MySQL replication. Both EMS servers are active at the same time, implying that either server can modify and insert data into its own database at the same time, and then this updated information will be replicated to the other server. Both servers will also respond to ping messages sent from any legitimate devices.

Note: Each geographically redundant EMS server will generate binary log files to be used by the remote server to perform mysql replication. While a cron job will be running in the background to check for and remove the used/obsolete binary log files, in the case where connectivity between the two servers is lost for whatever reason (e.g., communication link failure, remote data center down, remote server down, etc.), the unused binary log files will be kept to allow the remote server to perform replication when the two servers re-establish communication. However, these unused/undeleted binary log files will gradually use up the allocated disk space in the appropriate partition. If the connectivity between the two servers recovers before the partition is full (or before the partition usage reaches a critical threshold) and the remote server is able to utilize those stored binary log files to complete the mysql replication, then the background cron job can delete the used binary log files and the system will resume synchronization and operate normally. On the other hand, if the connectivity is not restored or the replication cannot be completed before the disk space reaches a critical threshold (e.g., 90% partition full), a background

monitoring task will be triggered to remove unused binary log files. When this happens, the replication for the remote server may need to be conducted manually when the servers resume normal communication.

Consequently, it is recommended that a trap or an alarm be set upon the partition space usage reaching a certain threshold (e.g., 50%), so that an operator can check into the cause of the (abnormal) connectivity issue between the two geographically separated servers.

Appendix B. Protocol Acronyms and Terminologies

CMS Call Management Server: also called Call Agent in MGCP/SGCP terminology.

DHCP Dynamic Host Configuration Protocol: is an Internet protocol for automating the IP address configuration of computers that use TCP/IP.

DNS Domain Name System: is the software that lets you have name to number mappings on your computers.

DTD Document Type Definition: defines the legal building blocks of an XML document. It defines the document structure with a list of legal elements.

FQDN Fully Qualified Domain Name: is a hostname containing full, dotted qualification of its name up to the root of the Internet domain naming system tree.

HTTP Hypertext Transfer Protocol: is the set of rules for transferring files (text, graphic images, sound, video, and other multimedia files) on the World Wide Web. HTTP is an application protocol that runs on top of the TCP/IP suite of protocols (the foundation protocols for the Internet).

KDC Key Distribution Center: A Kerberos server and database program running on a network host.

MGCP Media Gateway Control Protocol: MGCP is a master/slave protocol whereby the gateways are under the direct control of the user agents.

PGP Pretty Good Privacy: is a powerful cryptographic product family that enables people to securely exchange messages, and to secure files, disk volumes and network connections with both privacy and strong authentication.

SNMP Simple Network Management Protocol: is the standard operations and maintenance protocol for the Internet.

SSH Secure Shell: is the standard for encrypted terminal connections and secure file transfers.

TFTP Trivial File Transfer Protocol: A simple file transfer protocol used for down-loading boot code to diskless workstations.

TGT Ticket Granting Ticket: is a credential that the key distribution center (KDC) issues to authenticated users. When users receive a TGT, they can authenticate to network services within the Kerberos realm represented by the KDC.

XML Extensible Markup Language: is the universal format for data on the Web. XML allows developers to easily describe and deliver rich, structured data from any application in a standard, consistent way.