MITEL PERFORMANCE ANALYTICS

RELEASE 2.1

SYSTEM GUIDE

NOTICE

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

Trademarks

Mitel Performance Analytics System Guide
Release 2.1 - January 5, 2017

INTRODUCTION

Mitel Performance Analytics is a fault and performance management system designed to provide users with fast actionable problem resolution so that optimal service quality levels are maintained for end customers.

Mitel Performance Analytics provides real-time alerts, detailed reporting and ubiquitous accessibility with secure remote access.

DOCUMENT PURPOSE AND INTENDED AUDIENCE

This document provides information required to administer and use a Mitel Performance Analytics (MPA) monitoring system.

This document is intended for Mitel Performance Analytics Software as a Service (SaaS) deployments. In these deployments, Mitel Performance Analytics is hosted in the cloud. For Mitel Performance Analytics on-premise deployments, where the software is hosted at the service provider or customer location, refer to the *Mitel Performance Analytics Installation and Maintenance Guide*.

This document describes all possible Mitel Performance Analytics features. Feature access depends on the Mitel offering you have purchased. Not all features may be available to all Mitel Performance Analytics users.

Note that screen captures in this document may not reflect the latest Mitel Performance Analytics User Interface updates.

For a summary of the features introduced by specific Mitel Performance Analytics releases, refer to the *Mitel Performance Analytics Release Notes*.

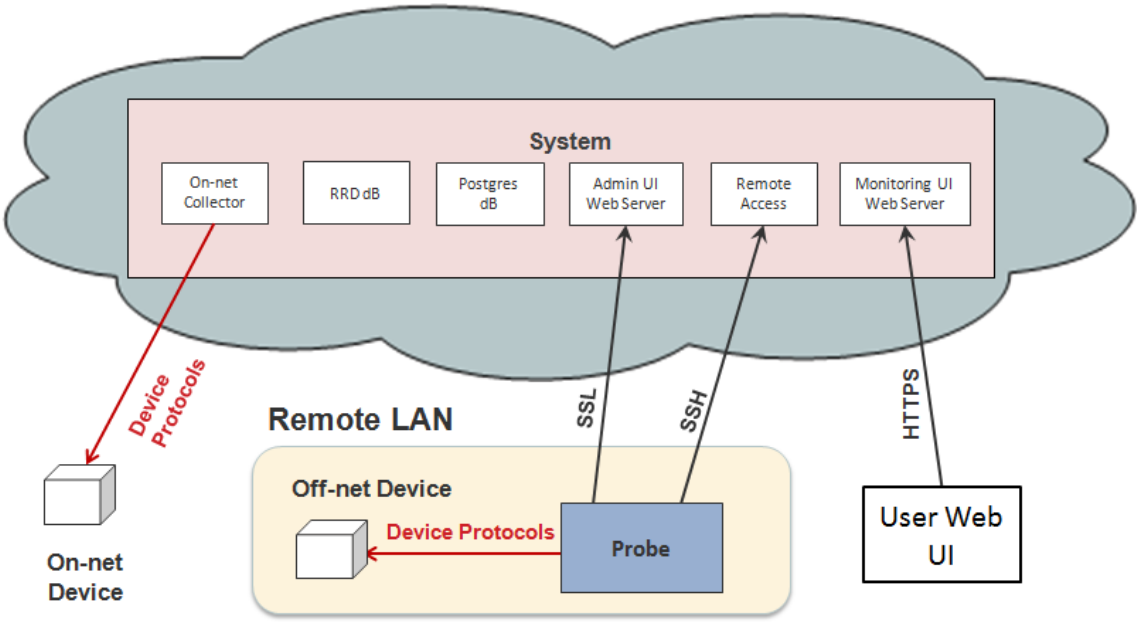
REVISION HISTORY

DOCUMENT DATE	DESCRIPTION
April 28, 2015	Updated to reflect MarWatch R5.0.
November 20, 2015	Updated to reflect MarWatch R5.1.
January 5, 2017	Updated to reflect Mitel Performance Analytics R2.1. Ongoing updates and improvements.

MITEL PERFORMANCE ANALYTICS OVERVIEW

MITEL PERFORMANCE ANALYTICS ARCHITECTURE

Mitel Performance Analytics consists of a number of web services running on either a cloud-hosted computing platform or on-premises computing platform. There are several components toMitel Performance Analytics. The remote 'Probe' installed in non-Internet accessible networks maintains databases of status and events, and provides a web portal with access security. Additionally, Mitel Performance Analytics has a Remote Access Service that provides a secure "cross-connect" for remote access to the customer network.



The various Mitel Performance Analytics components can run on a single or multiple servers, depending on capacity requirements.

PROBE

The **Probe** is a software application running on a server in the remote customer network. This software has several important functions. It initiates and maintains secure connections to Mitel Performance Analytics, collects performance data and alarms from devices in the customer networks, transfers performance data and alarm status to Mitel Performance Analytics, and enables secure remote access for the Mitel Performance Analytics user to the remote customer network. For a detailed description of the **Probe**, see "Probe Installation" on page 193.

MITEL PERFORMANCE ANALYTICS CAPABILITIES

Mitel Performance Analytics provides fault and performance management for multiple enterprise VoIP systems and associated network infrastructure, both LAN and WAN. Mitel Performance Analytics supports monitoring and remote access both for private networks, such as enterprise

LANs and MPLS VPNs, and for public network or Internet-reachable devices, such as access routers.

Mitel Performance Analytics provides:

- Cloud or on-premises packaging
- Provides real-time and historical fault and performance monitoring
- Provides an alarms analytics tool that customizes the alarm management environment according to the user's behavior and the behavior of others. Alarms that are deemed to be the most important to the user are shown first. Contains advanced tools for determining related alarms.
- Monthly or on-demand customer reporting
- Special focus on Mitel business communications equipment and VoIP Quality
- Supports a range of devices including network infrastructure
- IP SLA monitoring
- Flexible container architecture allowing users to configure data reporting to match their size and organization (for example, data reporting according to geographical locations, functional or organizational groupings, or customer groupings)
- Supports both Internet accessible and private network devices
- Simple deployment in remote customer networks with both software and hardware Probe available
- Integrated remote access to customer networks (with Probe)
- Supports multiple character sets allowing for internationalization
- Branded dashboard can be created for service providers, resellers and customers
- Resellers can choose any URL they own for their Mitel Performance Analytics login page

USER INTERFACE

Mitel Performance Analytics uses a standard Web browser for system access. Key user interface attributes are:

- Secure – HTTPS / SSL
- Login and logout with form-based authentication
- Standard Web browsers (Internet Explorer, Firefox, and Chrome)
- No special hardware or software needed to use Mitel Performance Analytics
- Dashboard views according to configured containers:
    - Entire Mitel Performance Analytics system (multiple regions and customers)
    - Geographical locations, functional or organizational groups, or customer groupings
    - Single customer
    - Single device
- Panel display paradigm – panels show current and historical performance data
- Data exploration capability – expand panels for more detailed views
- Geographic map with location status display
- Brandable – partner or customer logo

SUPPORTED BROWSERS

User access to Mitel Performance Analytics requires the use of a Web browser with JavaScript and Adobe Flash support enabled.

Mitel Performance Analytics is supported on:

- Firefox, Release 24.0 and later
- Chrome, Release 36.0 and later

Note: While Mitel Performance Analytics should work on any standards compliant browser, such as Internet Explorer, Safari and Opera, Mitel can only commit to resolving issues with specifically tested and supported browsers.

SUPPORTED DEVICES

Mitel Performance Analytics supports the following device types:

DEVICE	SUPPORTED VERSIONS
MiVoice MX-ONE	Release 6.0 SP2 or later
MX-ONE Application Server	
MiVoice Business, Mitel 3300, vMCD ICP systems	Release 5.0 or later
MiVoice Office 250 CP systems	Release 4.0 or later
MiCollab	Release 4.0 or later
Mitel Standard Linux (MSL)	Release 9.0 or later
MiVoice Border Gateway,	Release 7.1 or later
MiContact Center Business. all edtions	Release 6.0 and 7.0
MiVoice Call Recorder	
Red Box Call Recorder	
Innovation InnLine Voice Mail Server	
Standard Servers (Windows and Linux)	
VMWare ESXi Server	
Ethernet Switches (HP, Cisco, Dell, Avaya)	
Routers (Cisco and Adtran)	
PathSolutions Servers	

DEVICE	SUPPORTED VERSIONS
Uninterruptible Power Supplies (American Power Corporation),	Models with Ethernet network management interface
Avaya IP Office 500	v1 or v2
Avaya IP Office Server,	Release 7.0 or later
Basic IP Device	

FAULT AND PERFORMANCE MONITORING

Mitel Performance Analytics continuously monitors managed devices for key performance metrics and provides current and historical measurement of these metrics in various dashboards, to provide awareness of all device statuses.

The following table describes the devices and the performance and alarm monitoring supported by Mitel Performance Analytics.

DEVICE	SUPPORTED PERFORMANCE AND ALARM MONITORING
MiVoice MX-ONE	System alarms and SNMP events System reachability and availability Inventory (server hardware, software information, hardware ID) License inventory (System, Port, Key Attribute System, and Key Attribute Port) System performance metrics: memory, interface statistics Voice metrics: SIP set voice quality ratings by call (R factor) over multiple interfaces IPT user data Device and extension inventory Extension and terminal registration Route utilization Gateway utilization
MX-ONE Application Server	System information System reachability and availability Service activity monitoring for MiCollab Advanced Messaging, CMG, inAttend, and ACS Media Server applications Performance metrics: CPU, memory, file system and interface statistics

DEVICE	SUPPORTED PERFORMANCE AND ALARM MONITORING
MiVoice Business, Mitel 3300, vMCD ICP systems	System alarms System reachability and availability Inventory (system hardware, software information, hardware ID, app record) SMDR collection IP set inventory License inventory, node and cluster System performance metrics: memory, interface statistics Voice metrics: voice quality ratings by call (R factor) Digital trunk and SIP trunk utilization IPT user data
MiVoice Office 250 CP systems	System alarms Inventory (system hardware, software information, hardware ID, app record) SMDR collection System reachability and availability License inventory Performance metrics (CPU, memory)
MiCollab, Mitel Standard Linux (MSL)	System alarms System information and Mitel service ID System reachability and availability MiCollab application inventory IP set inventory Licensing inventory MiVoice Border Gateway/vMBG near end and far end call statistics and voice quality ratings by call (R factor) for SIP Teleworker sets, Minet and SIP Performance metrics: CPU, memory, file system and interface statistics

DEVICE	SUPPORTED PERFORMANCE AND ALARM MONITORING
MiVoice Border Gateway	System alarms System information and Mitel service ID System reachability and availability MiCollab application inventory IP set inventory Licensing inventory MiVoice Border Gateway/vMBG near end and far end call statistics and voice quality ratings by call (R factor) for: • SIP Teleworker sets, Minet and SIP • SIP trunks Performance metrics: CPU, memory, file system and interface statistics
MiContact Center Business, all editions	System alarms System information System reachability and availability Service availability monitoring for critical MiContact Center Business services Performance metrics: CPU, memory, file system and interface statistics
MiVoice Call Recorder	System information System reachability and availability Service availability monitoring for critical MiVoice services Performance metrics: CPU, memory, file system and interface statistics
Mitel Probe	System information Alarms for Probe connectivity IP SLA monitoring for up to four remote hosts
Red Box Call Recorder	System information System reachability and availability Service availability monitoring for critical Red Box services Performance metrics: CPU, memory, file system and interface statistics

DEVICE	SUPPORTED PERFORMANCE AND ALARM MONITORING
Innovation InnLine Voice Mail Server	System information System reachability and availability Service availability monitoring for critical InnLine services Performance metrics: CPU, memory, file system and interface statistics
Standard Servers (Windows and Linux)	System information System reachability and availability Service activity monitoring (Windows only) Performance metrics: CPU, memory, file system and interface statistics
VMWare ESXi Server	System information System reachability and availability Performance metrics: CPU, memory, and interface statistics
Ethernet Switches (HP, Cisco, Dell, Avaya)	System information System reachability and availability Performance metrics: CPU, memory, and interface statistics
Routers (Cisco and Adtran)	System information System reachability and availability Performance metrics: CPU, memory Statistics for one (Cisco and Adtran) or multiple interfaces (Cisco only) IP traffic reporting by Class of Service (Cisco and Adtran) and nested Class of Service (Cisco only)
PathSolutions Servers	System reachability and availability System alarms

DEVICE	SUPPORTED PERFORMANCE AND ALARM MONITORING
Uninterruptible Power Supplies (American Power Corporation)	System information System reachability and availability System alarms Performance metrics: • Battery run time remaining • Input and output line voltages • Input and output frequency • Load current • Output load
Avaya IP Office 500 Avaya IP Office Server	System information Reachability and availability Monitoring System alarms System Status Application (SSA) remote access SMDR collection Set inventory monitoring Interface performance monitoring Server performance monitoring (Server Edition)
Basic IP Device	System information Reachability and availability Monitoring

ALARMS AND ALERTS

If a monitored performance metric indicates a potential problem, Mitel Performance Analytics creates an alarm and displays it on the Mitel Performance Analytics web interface. The system can be configured to create an email, SMS message, Twitter Direct Message, SNMP trap, or desktop notification to notify support personnel that the alarm has been generated.

The following sections describe Mitel Performance Analytics alarm and alerting capabilities.

ALARMS

Mitel Performance Analytics provides the following alarms:

- System alarms (MiVoice MX-ONE, MiVoice Business, MiContact Center Business, MiVoice Office 250, MiCollab/MiVoice Border Gateway, Avaya IP Office, PathSolutions, UPS)
- Performance metric alarms (thresholding with both time and value hysteresis)
- Device ICMP Ping reachability
- Device SNMP reachability
- Device interface availability and utilization

- Device access credential problems
- Device registration delays
- Probe check-in
- MiVoice Business backup issues
- SMDR transfer issues
- Disconnected IP set (MiVoice Business and MiVoice Border Gateway)

MAP VIEW

Map view capabilities include:

- Shows customer locations with color coded location status
- Click on location to open container dashboard

ALARM MANAGEMENT INTERFACE

The alarm management interface provides the following capabilities:

- Show and sort alarms by severity, duration, customer and other criteria.
- Show current and historical alarms
- Historical view by table or timeline
- Basic alarm management (ticket number, assigned to, status)
- Hide and show alarms and My Alarms
- Flag alarms as 'My Favorites'

ALARM ANALYTICS

The Alarm Analytics tab provides the following capabilities:

- Learns from user's behavior and from the behavior of others to optimize how alarm information is presented. Displays alarms according to rating trends
- Create and follow alarm labels
- Filter and group alarm data
- Perform operations and editing on a group of alarms
- Save and share custom alarm data views
- Display time-related alarms
- Display the log of all operations that have occurred on an alarm of interest

ALERTING

The following alerting functionality is available:

- Selective alerting: Multiple alert profiles to enable alerting by customer or region, alarm severity, time of day, day of week
- Multiple alerting mechanisms supported – email, SMS, SNMP trap, Twitter direct message, or desktop notification
- Alarm digest and or single alarm alerting to minimize number of alerts
- Email alarms contain clickable link to device for quick response

REMOTE ACCESS

Mitel Performance Analytics provides integrated remote access to devices that are located behind a customer firewall or are not directly IP reachable. Each device dashboard has a “click-to-connect” link for rapid connection for maintenance or system administration. Additionally, the Mitel Performance Analytics Remote Access system allows connection to any other device on the customer network.

Key Mitel Performance Analytics Remote Access attributes are:

- Single-click access to monitored devices
- On-demand secure connection to a remote customer LAN
- No VPN required – supports multiple simultaneous access sessions to multiple customers from single user PC
- Customer manageable Remote Access Control settings
- Remote Access audit log
- Remote network tools (Ping, Traceroute, MTR, ifTop, SNMP browser)

REPORTING

Mitel Performance Analytics provides optional reporting on device performance by customer. Reports can be scheduled once per month, once per week, or can be created on-demand.

Key reporting capabilities are:

- Optional monthly reports by customer
- On-demand reports by customer to cover up to 90 days of history
- Reports in PDF format and emailed by Mitel Performance Analytics
- Reports provide:
  - Customer device inventory
  - Device availability summary
  - Device performance data, by device
- Reports can be branded with partner or customer logo

OPTIONAL FEATURES

Mitel Performance Analytics offers optional features intended to simplify the management and maintenance of monitored devices and networks.

REMOTE OFF-SITE BACKUP

Mitel Performance Analytics provides optional backup for MiVoice Business and MiVoice MX-ONE systems, with scheduled and on-demand backup options. The system can be configured to backup the device configuration and, optionally, call data and embedded voice mail configuration and data at regular intervals. Backups can optionally be stored on a server in the customer network. Supported protocols include FTP, SFTP, and FTPS (both implicit and explicit).

Scheduled Backups

Backups can be scheduled for a maintenance time window, 2 to 23 hours, on an hourly, daily, weekly or monthly basis. If the backup fails, Mitel Performance Analytics retries up to a configurable number of times during the backup window. The attempts are spread out in time to allow the issue that caused the failure to correct itself.

On-demand Backups

The system also provides on-demand backups.

Backup Retention

Specific backups can be designated for permanent retention. This capability is known as locking. Generally, Mitel Performance Analytics retains the 10 most recent backups. However, you can lock up to five backup files per device so they are retained indefinitely.

Backup Download

Backups are downloaded using the scheduler **Recent Results** or **Completed Files** queries. These queries show all backups that were made and indicate which backup files are downloadable. As with all tabular queries, results can be customized by filtering, grouping and other functions.

MIVOICE BUSINESS IP SET INVENTORY MONITORING

Mitel Performance Analytics supports an optional capability for MiVoice Business: IP set inventory monitoring. The system keeps a record of all IP sets known to the MiVoice Business, in various states.

The default view shows the number of IP sets connected to the MiVoice Business by state, where the possible states are:

- In Service: Set has set up a TCP/IP connection and has been programmed.
- Disconnected: Set has been programmed and then disconnected from the LAN.
- Never Connected: Set has been programmed but has not been connected to the LAN.
- Unprogrammed: Set is connected to the LAN but has not been programmed.

In the expanded view, the **MiVoice Business IP Set Inventory** panel displays the available information about all of the IP sets connected to the MiVoice Business on the LAN.

Disconnected Set Alarm

MiVoice Business IP Set inventory monitoring provides an optional alarm that is generated when a previously programmed, connected and registered IP set becomes disconnected from the MiVoice Business. The alarm is cleared when the set is reconnected or the MiVoice Business database is updated to reflect a change in set inventory.

AVAYA IP OFFICE SET INVENTORY MONITORING

Mitel Performance Analytics supports inventory monitoring for sets connected to an Avaya IP Office.

The default view shows the total number of IP Sets configured for the Avaya IP Office system by category, where the categories are:

- IP Sets: Avaya H.323/ SIP or third party H.323 / SIP sets

- Digital/Analog Sets: Avaya or third party digital or analog sets

In its expanded view, the **Set Inventory** panel displays all available information about the sets connected to the Avaya IP Office system.

SMDR COLLECTION

Mitel Performance Analytics provides collection and central storage for SMDR records from Mitel MiVoice Business call servers, MiVoice Office 250 systems, and Avaya IP Office systems.

For Mitel MiVoice Business call servers, you can select the collection method: FTP or socket:

- For the FTP method, Mitel Performance Analytics instructs the IPBX to send the SMDR file to Mitel Performance Analytics through FTP. The files are collected hourly, daily, weekly or monthly. The files can then be stored locally or you can have Mitel Performance Analytics send it to a remote file server using FTP, SFTP or FTPS (implicit or explicit). The remote file server can be either on the customer network or a distant network reachable over the Internet.
- For the socket method: Mitel Performance Analytics connects to the device using a local TCP socket and stores SMDR records as they are produced, as a file on the Probe. Every hour, the collected SMDR Record file is uploaded either to secure offsite storage (Amazon S3) or to a file server using FTP, SFTP or FTPS (implicit or explicit). This file server can be either on the customer network or a distant network reachable over the Internet.

For MiVoice Office 250 systems and Avaya IP Office systems, Mitel Performance Analytics connects to the device using the socket method.

As with the Mivoice Business, Mitel Performance Analytics stores SMDR records as they are produced, as a file on the Probe. Every hour, the collected SMDR Record file is uploaded to one of the following locations:

- For cloud-based installations, a secure offsite storage (Amazon S3)
- For on-premise installations, the Mitel Performance Analytics server's file system file store
- A file server using FTP, SFTP or FTPS (implicit or explicit). This file server can be either on the customer network or reachable over the Internet.

Mitel Performance Analytics retains an SMDR file for up to 31 days. SMDR files can be downloaded using the scheduler **Recent Results** query.

CAUTION: To retain SMDR files longer than 31 days, you must provide alternate storage and move the files there before they are erased by Mitel Performance Analytics.

MiVOICE BORDER GATEWAY IP SET INVENTORY MONITORING

Mitel Performance Analytics supports inventory monitoring for IP sets connected to MiVoice Border Gateway (Teleworker sets).

The default view provides a count of MiNet and SIP Sets connected to the MiVoice Border Gateway.

In the expanded view, the IP Set Inventory panel displays the available information about connected IP sets.

Disconnected Set Alarm

MiVoice Border Gateway IP set inventory monitoring provides an optional Disconnected Set alarm, which is generated when a previously connected and registered IP set is disconnected from the MiVoice Border Gateway.

The alarm is cleared when the set is reconnected, or the MiVoice Border Gateway database is updated to reflect a change in set inventory.

MITEL PERFORMANCE ANALYTICS SYSTEM DATA MODEL

Mitel Performance Analytics uses a hierarchical data model for status aggregation.

The following sections describe the various levels that can provide a status view.

SYSTEM

This level represents the entire Mitel Performance Analytics system and shows status and alarms for all containers and devices.

CONTAINERS

A container is a logical grouping of objects. Objects can include devices and other containers.

Containers can be used to represent:

- Geographical locations, such as Europe, North America, and Asia
- Functional or organizational groupings, such as Research and Development, Support, Finance, and Manufacturing
- Customer groupings, such as Large Customers, Small Customers, and Offshore Customers

Containers can be of type **None**, **Customer**, **Reseller**, or **Location**. Container types are used for data queries or reports.

There is no limit to the number of subcontainers or levels of subcontainers that can be created. Thus, users can create a hierarchical structure that best suits their business needs. For details, see "Planning Ahead" on page 31.

At this level, Mitel Performance Analytics shows aggregated status and alarms for this container and all the objects that it contains.

DEVICES

This is the lowest level element in the hierarchy. Mitel Performance Analytics supports a large variety of devices described in "Fault and Performance Monitoring" on page 18.

Devices are created within a container. Data reporting is done on a per container basis. So when a user accesses a dashboard page, it shows the data for the devices in that container and the devices in any subcontainer.

Probes

Mitel Performance Analytics requires a Probe to monitor devices. The Probe enables communication between Mitel Performance Analytics and the customer network. It also acts as a data collector between Mitel Performance Analytics and the monitored devices. The monitored devices send their data to the Probe which then relays it to Mitel Performance Analytics.

There are two kinds of Probes, single customer and multi-customer. A single customer Probe enables monitoring of multiple devices, all belonging to the same customer and on the same IP network.

The multi-customer Probe is intended for hosted vMCD and MiVoice Business deployments, where a single Private IP network supports multiple devices belonging to different customers. For example, a reseller with several customers, each subscribed to a separate MiVoice Business, can observe monitoring details for all MiVoice Business call servers, but the customers can see only their own MiVoice Business call servers.

Off-net Devices and On-net Devices

In a typical deployment, the Probe is installed behind the firewall guarding the customer network. In such deployments, the Probe is part of the customer private network and interacts with the customer devices. These are referred to as “Off-net” devices.

The Probe can also be co-located with the Mitel Performance Analytics server. In this case, Mitel Performance Analytics can directly monitor any device that is IP-reachable from the Internet. This could be an access router with a public IP address acting as a firewall guarding a customer network, an MPLS router in a customer LAN reachable with port forwarding from a public IP address, or a server with a public IP address. These are referred to as “On-net” devices. In such deployments, the Probe interacts only with the customer firewall and with other on-net devices. Such deployments can be used to identify Internet Service Provider (ISP) issues.

For users that have Mitel Performance Analytics installed on premise with their equipment, your installation already contains a Probe and you cannot install another.

For service providers that have Mitel Performance Analytics installed in their data center, your installation already contains a Probe. However, you can install more Probes. Typically, each additional Probe monitors a particular customer.

For cloud-based users, you must install a Probe as part of your configuration.

USERS

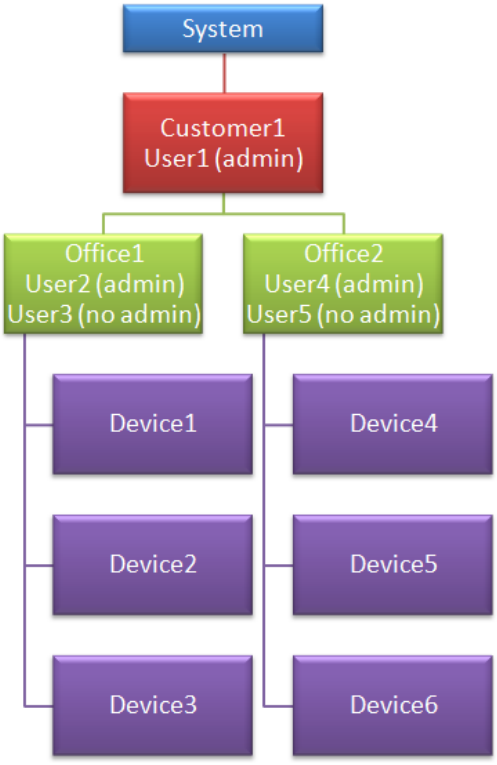
Mitel Performance Analytics users are created within a container. A user’s scope is strictly limited to that container and all objects that it contains, including subcontainers. A user’s dashboard shows aggregated status and alarms for all the devices in their container and its subcontainers.

Each user can also be granted permissions to perform tasks. So within a container, some users can do all administrative tasks, other users can only do some administrative tasks, while other users cannot do any administrative tasks.

When a user attempts an administrative task, they must supply their login credentials before they are granted access to the required Web pages.

DATA MODEL SMALL ORGANIZATION EXAMPLE

The following diagram shows a possible Mitel Performance Analytics configuration for a small organization.



In the previous diagram:

- **User1** is part of the container labeled **Customer1**. **User1** has full administrative privileges and can create subcontainers such as **Office1** and **Office2**, as well as other users such as **User2** and **User4**. **User1**'s dashboard shows alarm and status information for both offices and all devices.
- **User2** is part of the container labeled **Office1**. **User2** was created by **User1** and was granted administrative privileges for creating containers only. **User2** could use these privileges to create subcontainers in **Office1** representing floors and place new devices in those containers. **User2**'s dashboard shows alarm and status information for **Office1** and its devices only.
- **User3** is part of the container labeled **Office1**. **User3** was created by **User1** but was not granted any administrative privileges. **User3**'s dashboard shows alarm and status information for **Office1** and its devices only.
- **User4** is part of the container labeled **Office2**. Like **User2**, **User4** was created by **User1** and was granted administrative privileges for creating containers only. **User4**'s dashboard shows alarm and status information for **Office2** and its devices only.
- **User5** is part of the container labeled **Office2**. Like **User3**, **User5** was created by **User1** but was not granted any administrative privileges. **User5**'s dashboard shows alarm and status information for **Office2** and its devices only.

See "Planning Ahead" on page 31 for more examples of container hierarchies for different types of organizations.

PLANNING AHEAD

Before creating a container hierarchy, users should plan ahead the structure they need and want for effective data reporting.

Note: Once a user has been added to a container, it cannot be moved to another container.

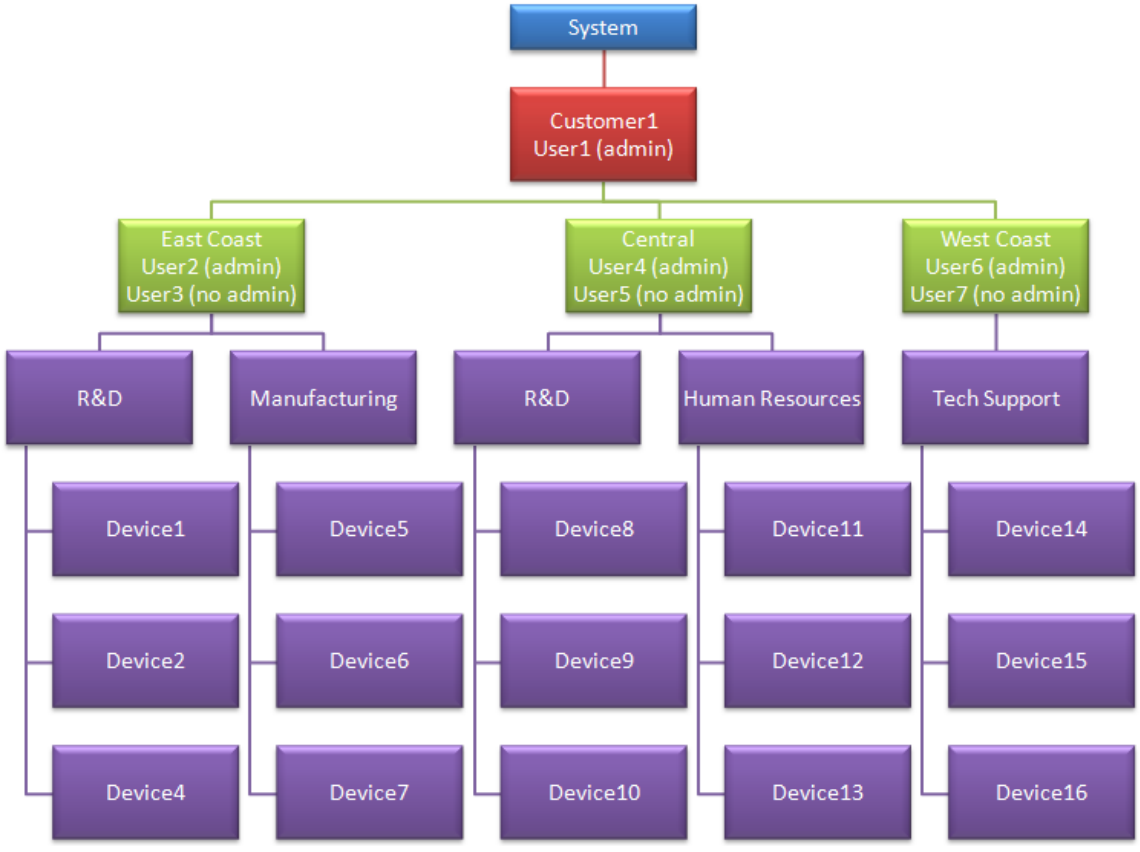
This section contains some examples of container hierarchies to help users implement effective data structures.

SMALL ORGANIZATIONS

See "Data Model Small Organization Example" on page 29.

LARGE ORGANIZATIONS

The following diagram shows a possible Mitel Performance Analytics configuration for a large organization.



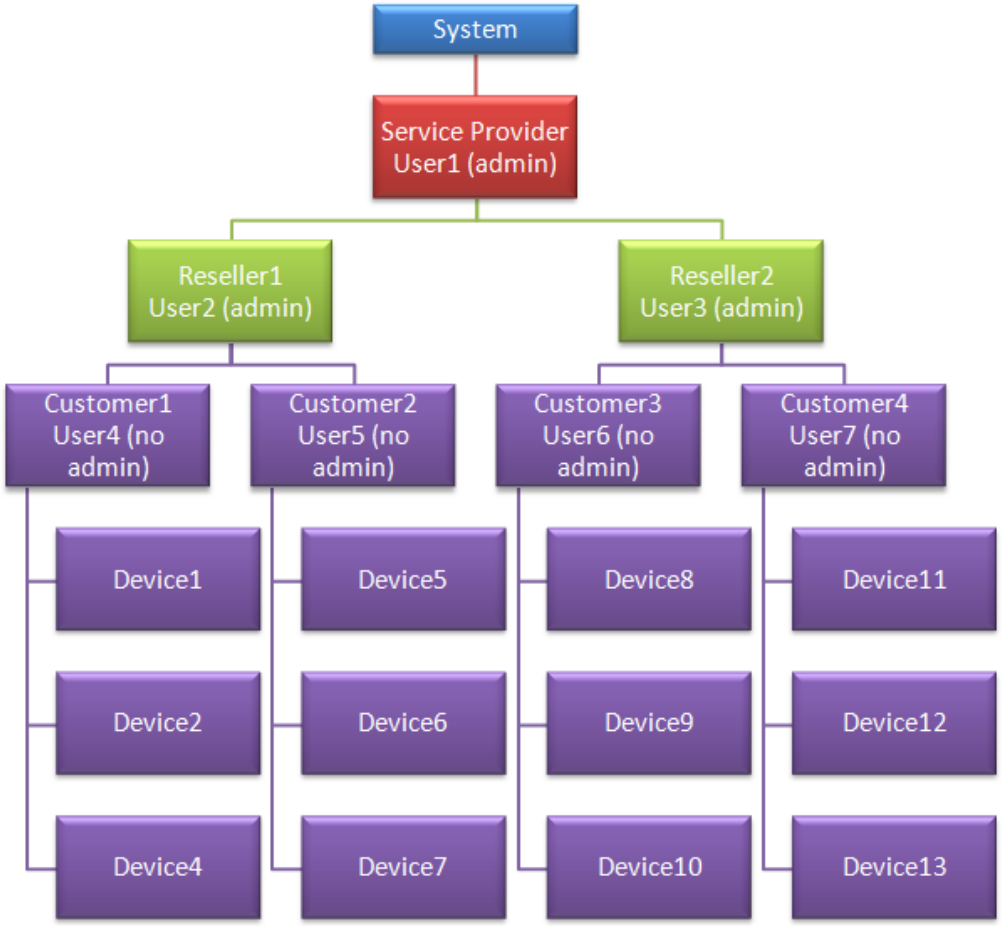
In the previous diagram:

- **User1** is part of the container labeled **Customer1**. **User1** has full administrative privileges and can create subcontainers such as **East Coast**, **Central**, and **West Coast**, as well as other users such as **User2** and **User4**. **User1**'s dashboard shows alarm and status information for all regions, organizations, and devices.

- **User2** is part of the container labeled **East Coast**. **User2** was created by **User1** and was granted administrative privileges for creating containers only. **User2** could use these privileges to create subcontainers in **East Coast** representing a new organization, such as Customer Service, new devices in those containers. **User2**'s dashboard shows alarm and status information for **East Coast** and all its devices only.
- **User3** is part of the container labeled **East Coast**. **User3** was created by **User1** but was not granted any administrative privileges. **User3**'s dashboard shows alarm and status information for **East Coast** and all its devices only. Similarly, if a user is created in the **Manufacturing** container, their dashboard would show only alarm and status information for **Manufacturing** devices.
- **User4** is part of the container labeled **Central**. Like **User2**, **User4** was created by **User1** and was granted administrative privileges for creating containers only. **User4**'s dashboard shows alarm and status information for **Central** and all its devices only.
- **User5** is part of the container labeled **Central**. Like **User3**, **User5** was created by **User1** but was not granted any administrative privileges. **User5**'s dashboard shows alarm and status information for **Central** and its devices only.

SERVICE PROVIDERS

The following diagram shows a possible Mitel Performance Analytics configuration for a service provider.



In the previous diagram:

- **User1** is part of the container labeled **Service Provider**. **User1** has full administrative privileges and can create subcontainers such as **Reseller1**, and **Reseller2**, as well as other users such as **User2** and **User3**. **User1**'s dashboard shows alarm and status information for all resellers, customers, and devices.
- **User2** is part of the container labeled **Reseller1**. **User2** was created by **User1** and was granted full administrative privileges. **User2** can create containers representing customers and users so customers can monitor their devices. **User2**'s dashboard shows alarm and status information for all **Reseller1** customers and all their devices.
- **User4** is part of the container labeled **Customer1**. **User4** was created by **User2** but does not have any administrative privileges. **User4**'s dashboard shows alarm and status information for all **Customer1** devices only.

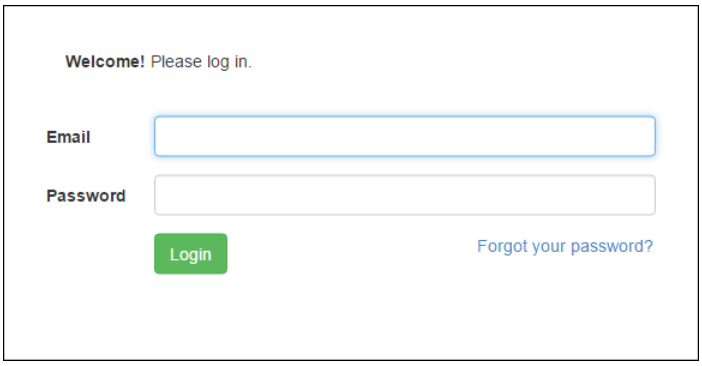
USER INTERFACE DESCRIPTION

The Mitel Performance Analytics user interface is web-based. Each user has access to a range of web pages that present status and performance information according to configured containers and subcontainers. Containers can represent any logical groupings, such as geographical locations, functional or organizational groupings, or customer groupings.

LOGIN PAGE

Mitel Performance Analytics uses SSL encryption to ensure that all communications between the browser and Mitel Performance Analytics are conducted over secure channels.

Enter the Mitel Performance Analytics URL (for example: `mpademo.mycompany.net`) in your browser to display a Login panel, such as the following:



Note: You must use a Fully Qualified Domain Name (FQDN) in the Mitel Performance Analytics URL; not an IP address.

To start a Mitel Performance Analytics session, enter your username and password and click the **Login** button.

DASHBOARDS

Mitel Performance Analytics has the following types of dashboards:

- **Device** dashboards display information about a particular device.
- **IPT User** dashboards display information about the users configured on the devices being monitored, such as MiVoice Business users or MiVoice MX-ONE users.
  Note: IPT User dashboards are currently limited to displaying only MiVoice Business users and MiVoice MX-ONE users. The MiVoice Business device must be configured to allow IP set inventories. The MiVoice MX-ONE device must be configured to allow extension and terminal registration.
- **Container** dashboards display information their content; that is, many devices and subcontainers.

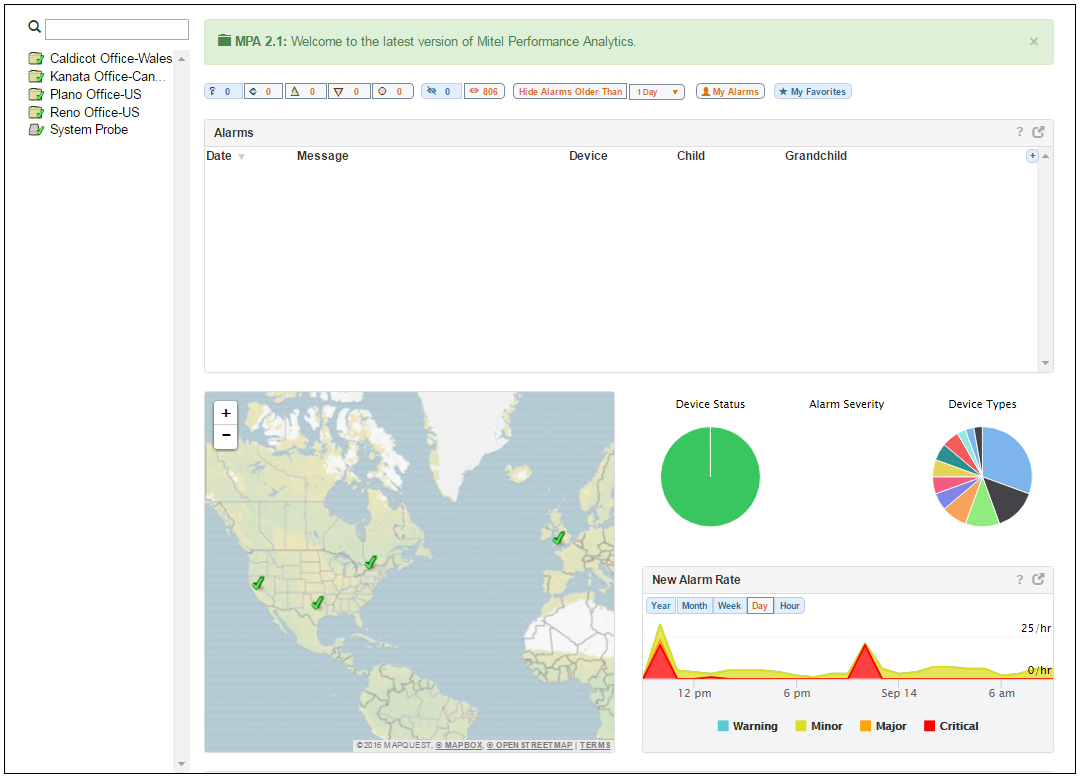
When you log in to Mitel Performance Analytics, you access a **Container** dashboard. Your login ID determines which dashboard, or system view, you are directed to.

The area to the left, below the search field, lists devices and subcontainers. Subcontainers are represented with folder icons. Click a device name to display its dashboard. Click a folder name to display that subcontainer's dashboard.

To display an **IPT User** dashboard, search for an IPT user name or extension number. Then click on the displayed IPT user name in the search results.

Tip: Use a query to get a list of IPT user names and extension numbers. You can also click on the IPT user extension to display the IPT User dashboard. See "Inventory Queries" on page 79.

Selecting a container that is high in the container hierarchy displays a dashboard with all the information of that container, including subcontainers. If containers represent regions, a system administrator sees an "All Regions" dashboard when they log in because that container includes all the subcontainers representing the regions. If users are created for subcontainers, then an administrator for certain regions sees a dashboard only for those regions because only that container is accessed when they log on. Finally, a customer sees all their devices on their dashboard because their user account was created for the container for their devices and no subcontainer. The following is typical "All Regions" dashboard.



Containers can represent items such as geographical locations, functional or organizational groupings, or customer groupings. In the previous graphic, Caldicot Office-Wales and Plano Office-US are containers representing regions.

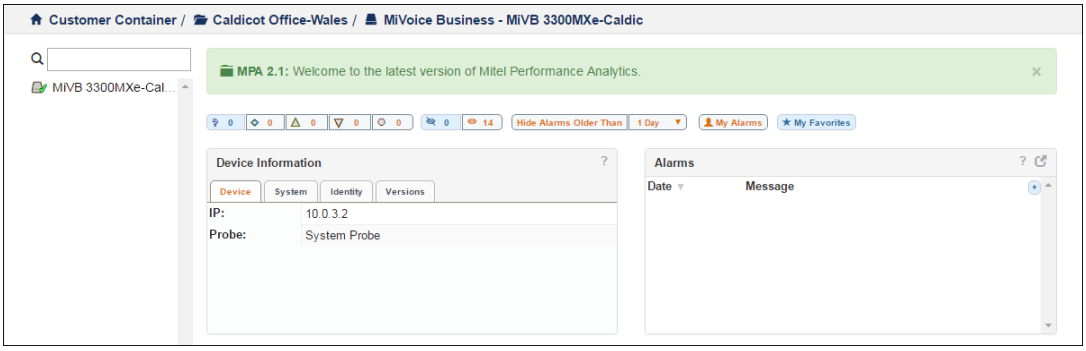
The Device dashboard also displays:

- A Message of the Day banner.
- A banner showing contact information for the container being displayed. In the previous graphic, it has a blue background.
- A series of display panels showing status and performance information for that device.

Both the Container and Device dashboards display an alarm summary and display filtering buttons. See "Alarm Summary and Filtering" on page 40 and "Mitel Performance Analytics Alarms and Alerts" on page 53.

BREADCRUMBS

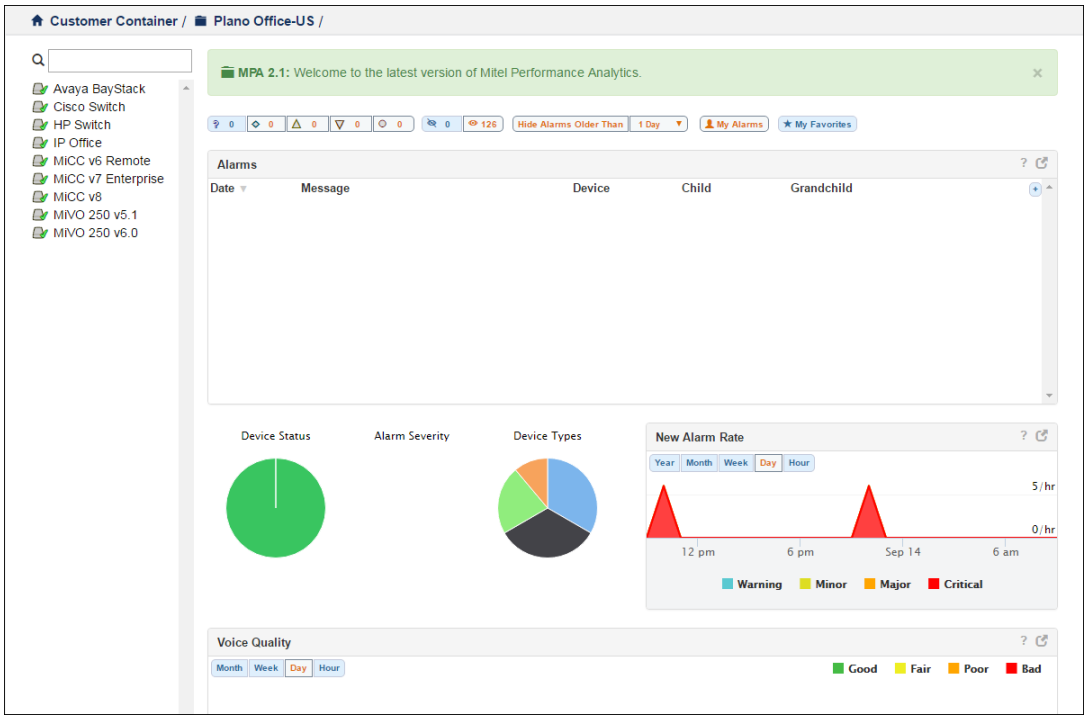
The top of the dashboard shows a series of “breadcrumbs” that provide links to navigate to previous screens. With the breadcrumb links, a user can easily return to a previous page after “drilling down” to specific information, such as a certain device from a customer. The following example shows the dashboard for a specific MiVoice Business device. Clicking any link to the left of **MiVoice Business – MiVB 3300MXe-Caldic** returns the user to a dashboard for that item.



DASHBOARD CONTEXT

If you click on a container, then the dashboard context switches to that container. The breadcrumb line at the top of the dashboard indicates coverage of the dashboard.

For example, in the following graphic containers represent regions. The **Customer Container** breadcrumb indicates the highest level that the user can access. It covers all containers (that is, regions) and customers. The **Plano Office-US** breadcrumb is the last in the chain and indicates that the dashboard covers the Plano Office-US container (that is, region) and its customers. All of the panels – Alarms, New Alarm Rate and Voice Quality – now display information only for the **Plano Office-US** container.

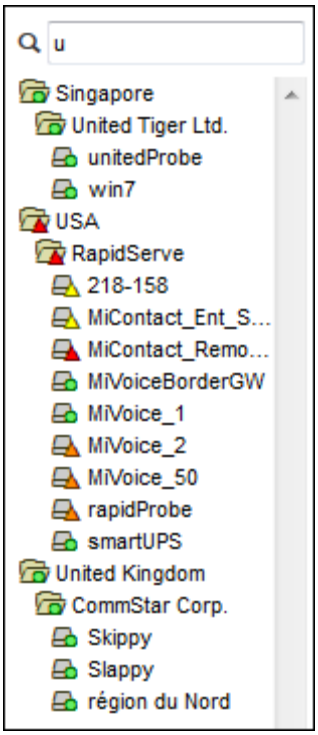


All display panels on the dashboard are updated to reflect the status in the current coverage.

SEARCH CAPABILITIES

Dashboards provide a search box to quickly locate any item managed by Mitel Performance Analytics. This includes containers, customers, devices, IPT users, device types, and Mitel Performance Analytics information fields such as names, IP addresses, notes and descriptions.

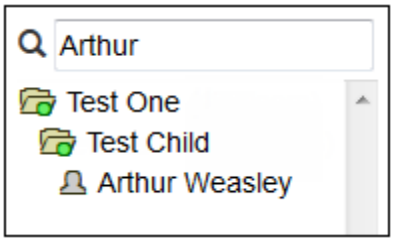
The search box is located at the top left of the dashboard. In the following graphic, a search for “u” in a Device dashboard yields a customer (United Tiger Ltd) and two regions (USA and United Kingdom).



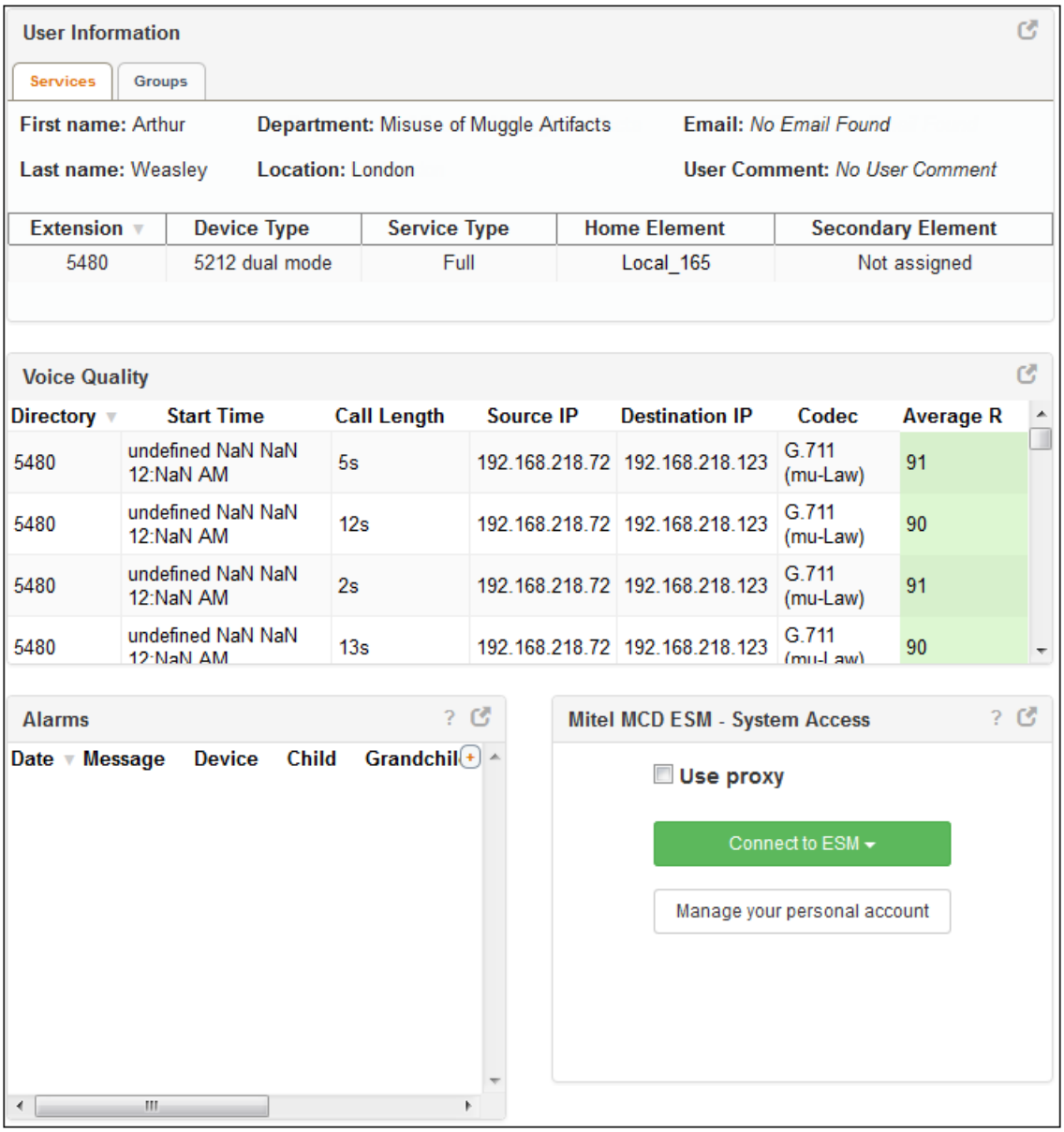
All search results are links. To change the dashboard context, click on the search result link.

DISPLAYING IPT USER DATA

To display IPT user data, search for either the user's name or extension number. In the following graphic, a search for "Arthur" yields the user **Arthur Weasley**.



Clicking the IPT user name, **Arthur Weasley**, displays information related to that IPT user. The following is an example.



You can also run an inventory query and click on the IPT user extension to display the IPT User dashboard.

The **User Information** panel displays a summary of the services and groups for that IPT user. For details, see "User Information Panel" on page 268.

The **Voice Quality** panel displays VQ information for each of the IPT user's extensions. For details, see "Voice Quality and SIP Voice Quality Panels" on page 269.

For details on the **Alarms** panel, see "Alarm Summary and Filtering" on page 40 and "Mitel Performance Analytics Alarms and Alerts" on page 53.

EXPANDED VIEWS AND CONTEXT SENSITIVE HELP

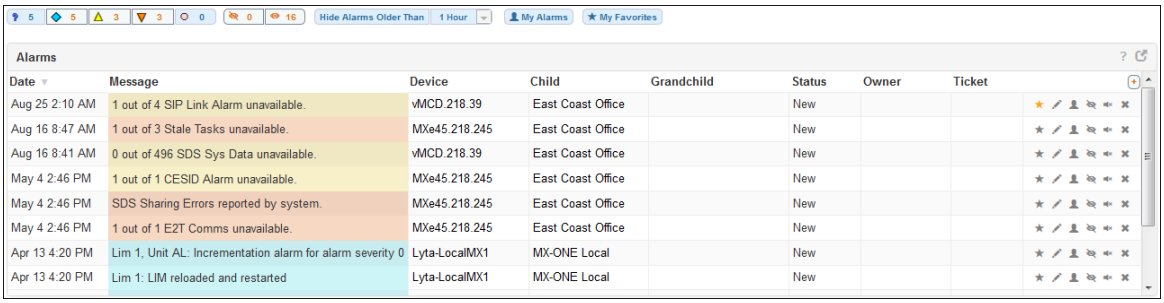
Many panels have the following icons to display additional information or context sensitive help.

ICON	FUNCTION
	Displays expanded view to show additional information
	Displays context sensitive help

When they apply, the icons are located in the top right of the panel.

ALARM SUMMARY AND FILTERING

Every device or container dashboard contains an alarm summary and alarm filtering buttons above the **Alarms** panel. The following is an example for a container dashboard.



The following icons are available for operations on alarms:

ICON	NAME	FUNCTION
	Favorite	Mark the alarm as a favorite.
	Edit	Edit related alarm information
	Assign	Assign alarm to me
	Hide	Hide the alarm
	Unhide	Unhide or show the alarm
	Silence	Silence the alarm
	Unsilence	Unsilence the alarm
	Acknowledge	Acknowledge or clear the alarm

Clicking the entries under **Device**, **Child** or **Grandchild** displays the dashboard for that container or device.

The five filter buttons above the **Alarms** panel and to the left summarize the number and type of alarms being reported by Mitel Performance Analytics. In the previous graphic, Mitel Performance Analytics is reporting: five indeterminate notifications, five warning alarms, three minor alarms, three major alarms, and no critical alarms.

Clicking the filter button controls whether those types of alarms are displayed. In the previous graphic, only warning, minor, and major alarms are displayed. Similarly, the **Alarms** panel can be filtered to hide alarms that are older than one hour, one day, or one week.

An alarm can also be hidden by clicking its icon. Hiding an alarm increments the **Hidden** filter button located above the **Alarms** panel. You can unhide an alarm by clicking on its icon.

Click the **Hidden** filter button to include or exclude hidden alarms from the **Alarms** panel. To quickly isolate hidden alarms, click the **Visible** filter button located beside the **Hidden** filter button. The **Visible** filter button displays the number of visible alarms.

Clicking the **My Alarms** filter button displays only the alarms where you are the owner.

Clicking the **My Favorites** button flags that alarm as begin of particular interest to you.

MENU ITEMS

The dashboard menu items are grouped under the following icons.

ICON	NAME	FUNCTION
	Tools	Accesses tools to help manage the object. For containers, this includes functions to manage: • Queries, see "Quick Queries" on page 78 and "Query Output Formats" on page 82. • Audit log, see "Audit Log" on page 89. • Reports, see "Generating Reports" on page 90. For devices, more and different tools may be displayed depending on the type of device.
	Add	Provides the ability to add containers and devices. Refer to "Step 2 - Add Containers" on page 44 and "Step 4 - Add Devices" on page 47.

ICON	NAME	FUNCTION
	Settings	Accesses functions to manage objects: • Current container or device settings. Refer to "Managing Containers" on page 94 or "Configuring Mitel Performance Analytics Devices" on page 111. • Alert profiles. Refer to "Alert Profiles" on page 67. • Users. Refer to "Step 3 - Add Users" on page 45. • Licenses. Refer to "Step 5 - Upload and Apply Licenses" on page 49.
	User	Provides the user with general information and the ability to control their session. Refer to "User Menu" on page 42.

The icons are located at the top right of the page. Different menu items are presented depending on the user's privilege level and the dashboard context.

USER MENU

The User menu provides the following functions.

MENU ITEM	FUNCTION
Help	Displays context-sensitive product documentation
About	Provides a summarized list of version details for Mitel Performance Analytics
Dashboard Settings	Displays the page for resetting the password and changing the time format. The time format can be either 12-hour with am/pm indication or 24-hour clock.
Logout	Closes all active web sessions and displays the login page

GETTING STARTED

After you access Mitel Performance Analytics for the first time, do the initial configuration steps described in the following sections.

STEP 1 - INITIAL LOG IN

Your system administrator supplies the Mitel Performance Analytics URL and your initial access credentials. The following is an example:

- URL: `example.mycompany.net`
- User: `j_smith@mycompany.com`
- Password: `change_me`

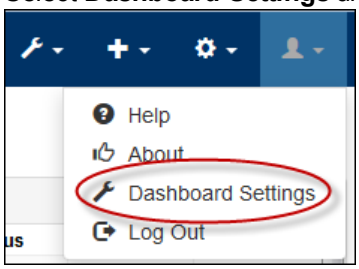
Note: You must use a Fully Qualified Domain Name (FQDN) in the Mitel Performance Analytics URL; not an IP address.

CHANGING YOUR PASSWORD

The initial user ID has full administrative privileges so they can add containers, users and devices.

Mitel **strongly recommends** that you change your username and password after your initial login. Do the following steps:

1. Go to the Mitel Performance Analytics URL and login using the provided initial access credentials.
2. Select **Dashboard Settings** under the **User** icon.

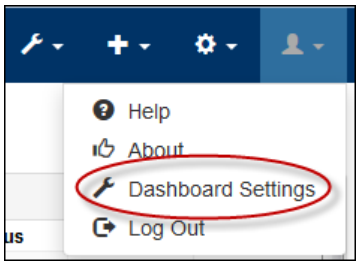


   The settings page for the user is displayed.
3. In the settings page, specify your current password, your new password, and your new password again to confirm it.
   To make it secure, ensure your new password contains at least eight characters and includes upper and lower case characters, symbols, and numbers.
4. Click the **Change Password** button.

CHOOSING THE TIME FORMAT

The default is to display a 12-hour clock with am/pm indication. But you can change it to display a 24-hour clock. Do the following steps:

1. Select **Dashboard Settings** under the **User** icon.



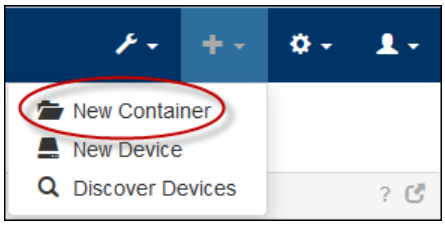
The settings page for the user is displayed.

2. In the **Dashboard Settings** area, choose the time format from the dropdown list.
   Your selection applies to all your sessions, regardless of which machine you log in from.

STEP 2 - ADD CONTAINERS

You can create a hierarchy of containers to meet your reporting and access needs. Refer to "Planning Ahead" on page 31. Do the following steps:

1. Select **New Container** under the **Add** icon.



The **New Container** window is displayed.

2. In the **New Container** window, specify the new properties. The properties cover the new container itself as well as the dashboard associated with the container.

CATEGORY OF PROPERTY	DESCRIPTION
General	Name associated with the new container.
Location	Information used by geographic map on dashboard.
Branding	Enables custom branding on the dashboard and in reports.
Contact Information	Information displayed in contact banner.
Container Message	Information displayed in the Message of the Day banner.
Container Type	One of **None**, **Customer**, **Reseller**, or **Location**.
Voice Quality	Display Voice Quality (VQ) information or not.

For details, see:

- "Configuring Containers" on page 94
- "Moving a Container Structure" on page 95
- "Broadcasting a Message of the Day" on page 97

- "Applying Branding" on page 98

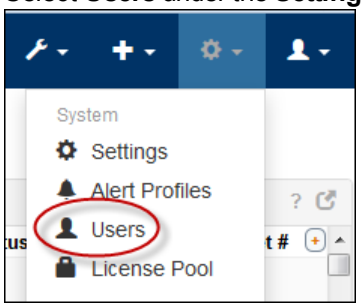
3. Click the **Create** button.

STEP 3 - ADD USERS

CAUTION: Once a user has been added to a container, the user cannot be moved to another container.

You can create additional users with varying privileges. Do the following steps:

1. Select **Users** under the **Settings** icon.



The Users window is displayed. It displays your initial user account.

2. Click the **Create New User** button.
The **New User** window is displayed.
3. In **New User** window, specify the new user's email address, first name, last name, and password.

Ensure you supply a valid email address.

Ensure the password contains at least eight characters and includes upper and lower case characters, symbols, and numbers.

4. Assign administrative and general permissions as required for the new user. Refer to "User Permissions" on page 46.
5. Click on the **Create** button.

USER PERMISSIONS

Mitel Performance Analytics users can be assigned various permissions to suite their administrative needs.

ADMINISTRATIVE PERMISSIONS	DESCRIPTION
Containers	Allows the account to add and remove containers, including changing their properties. If unchecked, that menu item is grayed out.
Branding	Allows the account to customize: • The logo used on the dashboard and reports. • The brand name that appears besides the logo at the top of the dashboard.
Users	Allows the account to add and remove Mitel Performance Analytics user accounts, including changing their properties. If unchecked, that menu item is grayed out.
Devices	Allows the account to add and remove devices, including changing their properties. If unchecked, that menu item is grayed out.
Probe Installer	Allows the account to install Probes. If unchecked, Mitel Performance Analytics does not supply the user with a configuration URL to complete the Probe installation process.
Alert Profiles	Allows the account to: • Add and remove alert profiles, including changing their properties. • Silence alarms If unchecked, that menu item is grayed out.
Licenses	Allows the account to add licenses to Mitel Performance Analytics, and to attach and detach from license targets.
License Policy	Allows the account to specify license policies. This capability is restricted to Mitel or on-premise deployments of Mitel Performance Analytics software.
Thresholds	Allows the account to modify default performance thresholds to generate alarms.
MIB Management	Allows users to upload MIBs to the MIB browser. See "Adding MIBs" on page 236.
System Admin	Allows users to perform tasks such as registering Mitel Performance Analytics, configuring an SMTP server, a Twitter account or a Twilio SMS account. This permission is configured when Mitel Performance Analytics is installed. See "System Administration Procedures" on page 174.

GENERAL PERMISSIONS	DESCRIPTION
Edit Tickets	Allows the account to edit trouble management information displayed in the Alarms panel. See "Editing Trouble Management Information" on page 64.
Remote Access	Allows the account to use Remote Access to access monitored devices. If unchecked, connection attempts automatically fail.
Share Views	Allows the account to share customized query views. See "Reusing Custom Views" on page 87.
Advanced User Operations	Allows the account to do advanced operations on monitored devices, such as moving a user from one device to another.
Shared SSO Credentials	Allows the account to use a shared account to log into a MiVoice Business ESM. For details, see "Configuring Mitel Performance Analytics for MiVoice Business" on page 123 and "Connecting to MiVoice Business ESM" on page 186. **Note**: Ensure you also grant **Remote Access** permission. Users require both **Remote Access** and **Shared SSO Credentials** permissions to use a shared account.

STEP 4 - ADD DEVICES

Devices may be added manually or through a discovery process. This section shows the manual process. For details on discovering devices, see "Discovering Mitel Performance Analytics Devices" on page 153.

The initial device to be added is generally a Probe device.

CAUTION: A Probe device must be configured for all devices to be monitored.

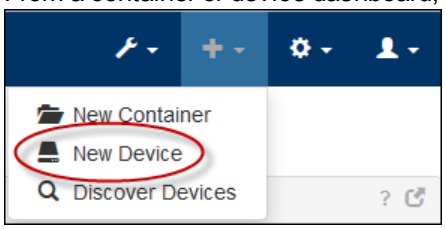
For users that have Mitel Performance Analytics installed on premise with their equipment, your installation already contains a Probe and you cannot install another.

For service providers that have Mitel Performance Analytics installed in their data center, your installation already contains a Probe. However, you can install more Probes. Typically, each additional Probe monitors a particular customer.

For cloud-based users, you must install a Probe as part of your configuration.

Do the following steps:

1. From a container or device dashboard, select **New Device** under the **Add** icon.



The New Device window is displayed.

2. In **New Device** window, select the device type from the dropdown list and click the **Next** button.
The following table describes the possible devices types:

MANUFACTURER	DEVICE TYPE	DESCRIPTION
Avaya	Avaya IP Office	Avaya IP Office 500, IP Office Server Edition
Innovation	Innline IP	Innovation Technologies InnLine Voice Mail
Mitel	MiVoice MX-ONE	MiVoice MX-ONE
	MX-ONE Application Server	MiVoice MX-ONE Application Server
	MiContact Center	MiContact Center Business, all editions
	MiVoice Office 250	MiVoice Office 250 PBX
	MiVoice Business	Mitel 3300 ICP, MiVoice Business, vMCD or MiVoice Business Instance IP PBX system
	MiCollab	MiCollab server
	MiVoice Border Gateway	MiVoice Border Gateway server, includes MiCollab
	MiVoice Call Recorder	MiVoice Call Recorder
	Probe	Software running on a server in an off-net network that enables Mitel Performance Analytics to monitor devices in a remote network.

MANUFACTURER	DEVICE TYPE	DESCRIPTION
Other	Basic IP Device	Any device supporting basic SNMP functionality
	Router	Cisco or Adtran router, used to provide IP network services
	Server	Generic Windows or Linux Server
	Switch	Managed Ethernet switch (HP, Dell, Cisco, Avaya (Nortel), and Extreme
	UPS	Uninterruptible Power Supply (APC Networked UPS)
Path Solutions	Path Solutions	PathSolutions VoIP Monitor
Red Box Recorders	RedBox CR	Red Box Call Recorder
VMWare	ESXi Server	VMWare ESXi server

The properties sheet for the new device is displayed. For device configuration property descriptions, see "Configuring Mitel Performance Analytics Devices" on page 111 and the *Mitel Performance Analytics System Guide*. For details on moving a device to another parent container, see "Moving a Device" on page 157.

3. Click the **Save** button.
   Mitel Performance Analytics verifies connectivity to the device with the configuration you entered.

STEP 5 - UPLOAD AND APPLY LICENSES

Mitel Performance Analytics includes a licensing framework to enable tracking of purchased and authorized system capabilities. The licensing framework covers devices, software features, capacity and services.

Mitel Performance Analytics has multiple trial license capabilities:

- An **All Features Licensed** trial is available that activates all features for all device types for a 30-day period. After the 30-day period, the system warns that licenses have expired and stops providing the licensed capability. The **All Features Licensed** trial can only be activated once per Mitel Performance Analytics system. After the trial period, all device type features are suspended.
- Per device type feature trials are available for a 30-day period. After the trial period, the system warns that licenses have expired and applies a 60-day grace period before the system stops providing the licensed capability. If a trial period for one device type feature expires, you can still activate a trial for another device type feature.

If you have not already done so, use the trial period and the grace period to complete your order for Mitel Performance Analytics with your supplier. If licensing has not been applied, Mitel Performance Analytics features are suspended after the grace period ends. Suspended features are indicated in a red banner on the dashboard and in the **Licensing** window of the root container.

Licensing, including trial licenses, begin to be enforced automatically shortly after initial installation. The period varies but is no longer than 24 hours. Mitel recommends that you use this initial startup period to set up Mitel Performance Analytics users, containers and devices. This step loads your Mitel Performance Analytics system with the device types needed for trial licenses. Additional devices can be added after licensing has been applied.

LICENSING FOR CLOUD-BASED USERS

Licensing for cloud-based users is automatic once their order is processed. You do not need to upload and apply licenses.

LICENSING FOR CUSTOMER PREMISE USERS OR SERVICE PROVIDERS

Customer premise users are users with Mitel Performance Analytics installed on-premise along with their own equipment.

Service providers are users who access Mitel Performance Analytics through Mitel's Premium Software Assurance and Support. Mitel Performance Analytics is installed on premise in a data center.

For both types of users, the licensing action depends on choices made during installation.

Online Licensing

If you chose online licensing, registered your system, and registered a valid license ID to a container, Mitel Performance Analytics downloads and applies licenses automatically. You do not need to upload and apply licenses.

See also "Registering a License ID to a Container" on page 175.

Offline Licensing

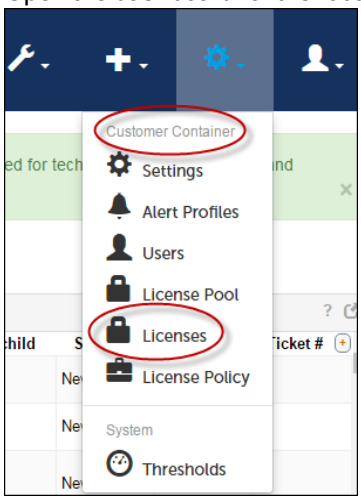
If you chose not to register your system or to use offline licensing, then you need to manually perform licensing tasks. Licensing tasks include providing a container GUID, uploading a license policy file, uploading license files, and applying licenses.

For additional details on licensing, see the"Mitel Performance Analytics Licensing" on page 100.

ACTIVATING THE ALL FEATURES LICENSED TRIAL

Do the following steps:

1. Open the dashboard for the root container and select **Licenses** under the **Settings** icon:



   The **Licensing** window for the root container is displayed. The **License Status** area shows your license tier and the number of licenses currently associated with your system.

2. To activate the All Features Licensed trial, click the indicated link beside your license tier.

   Adding devices after the start of the trial does not extend the trial period for that device type.

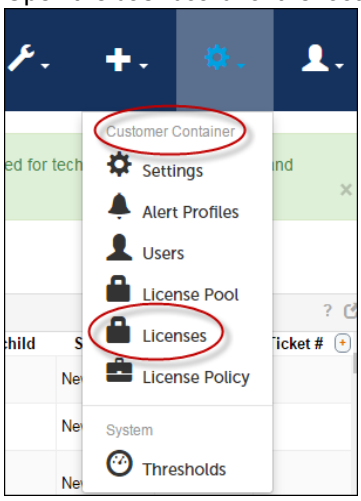
   Mitel Performance Analytics generates and applies the trial licenses. The trial licenses expiry date is displayed.

   Mitel Performance Analytics then starts collecting performance and fault management data from the device.

ACTIVATING PER DEVICE TYPE FEATURE TRIAL LICENSES

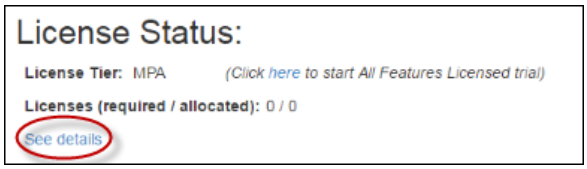
Do the following steps:

1. Open the dashboard for the root container and select **Licenses** under the **Settings** icon:



   The **Licensing** window for the root container is displayed.

2. Click **See details** under the License Status area.



   The license details shows devices types where trial licenses are available and the status of each of those licenses.

3. To obtain a per device type feature trial license, click the **Start Trial** button for any unlicensed Mitel Performance Analytics device type feature that you want to use. Typically, you want to start the trial license for your Probe and any other device types you have added to Mitel Performance Analytics.
   Adding devices after the start of the trial does not extend the trial period for that device type.

   Mitel Performance Analytics generates and applies the trial license. The trial license expiry date is displayed.

   Mitel Performance Analytics then starts collecting performance and fault management data from the device.

MITEL PERFORMANCE ANALYTICS ALARMS AND ALERTS

In addition to reporting alarms from monitored devices, Mitel Performance Analytics generates alarms for configured events or thresholds. Alarms are displayed on container or device dashboards on an **Alarms** panel with appropriate graphic attention indicators. The expanded **Alarms** panel offers tabs to present specialized information.

ALARM CATEGORIES

Mitel Performance Analytics reports the following categories of alarms:

- **Device Alarms**: Device alarms are alarms generated and reported by the devices and applications that Mitel Performance Analytics monitors. Mitel Performance Analytics receives the alarm information from the device or application and presents it on the **Alarms** panel. When viewed from a container dashboard, the panel shows the device, alarm severity, on time, and alarm details, as available.
- **Threshold Alarms**: Mitel Performance Analytics monitors certain performance parameters in monitored devices and applications and is configured to generate alarms when thresholds are exceeded.
- **System Alarms**: Mitel Performance Analytics generates alarms to indicate service problems. Some examples are “Incorrect Credentials to access a Device” and “Device SNMP or ICMP Unreachable”.

ALARM SEVERITY LEVELS

Mitel Performance Analytics supports the following alarm severity levels:

SEVERITY	ICON	MEANING
Critical		The system has detected a serious problem that severely impairs the service and immediate attention is required.
Major		A problem has been detected and is leading to the serious degradation of the service. Many users may be affected.
Minor		A minor problem has been discovered that may affect the service. This alarm is raised whenever the system is less than 100% operational.
Warning		A potential or impending service problem has been detected before any significant effects have been felt.

SEVERITY	ICON	MEANING
Indeterminate		The status of the device or service is indeterminate or unknown. This event can occur in a number of situations: This is a new device that has been configured in Mitel Performance Analytics but has not yet been connected to it, either directly or using a Probe. There is a network communications failure between the device and Mitel Performance Analytics. This may be due to an authentication error, a local network problem or an Internet connectivity issue. The Probe responsible for reporting the status of the device has failed to communicate with Mitel Performance Analytics. In this case, all of the devices being monitored by this Probe are placed into the indeterminate state.
Clear		The system is functioning properly.

ALARM STATUS

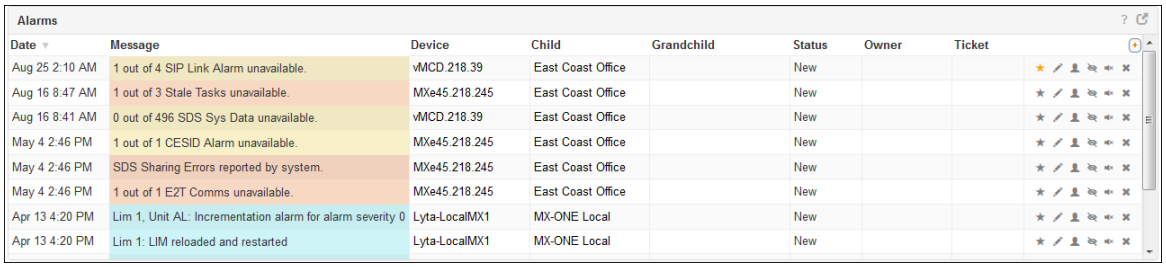
An alarm can have the following status:

- **New**: This is the initial status for all alarms.
- **Assigned**: Mitel Performance Analytics changes the status to **Assigned** when you enter trouble ticket information for the alarm.
- **Monitor**: Use this status for an alarm currently being monitored.
- **Resolved**: Use this status when the issue that caused the alarm has been resolved. Setting the alarm to **Resolved** also registers the ticket end time.
- **Dispatched**: Use this status when you need to dispatch resources to investigate or resolve the issue
- **8x5**: Use this status for an alarm that is processed only between the times of 8:00 am to 5:00 pm in the customer's local time zone.
- **Cleared**: This status indicates an alarm that has been cleared by the device that generated the alarm.
- **Forced Clear**: This status indicates an alarm that has been cleared by Mitel Performance Analytics instead of the device that generated the alarm.
- **Acknowledged**: Some alarms, such as those dealing with connectivity, persist on the Alarms panel even after they are cleared. You must acknowledge them before they are removed. See "Acknowledging Alarms" on page 66.
- **Hidden**: Use this status to hide an alarm from the dashboard alarm list. See "Hiding and Unhiding Alarms" on page 65.

Note: The status of an alarm can be set manually with the **Edit Alarm Information** panel or automatically by Mitel Performance Analytics.

ALARM PANEL AND TABS

Every device or container dashboard contains an **Alarms** panel. The following is an example of an **Alarms** panel for a container dashboard.



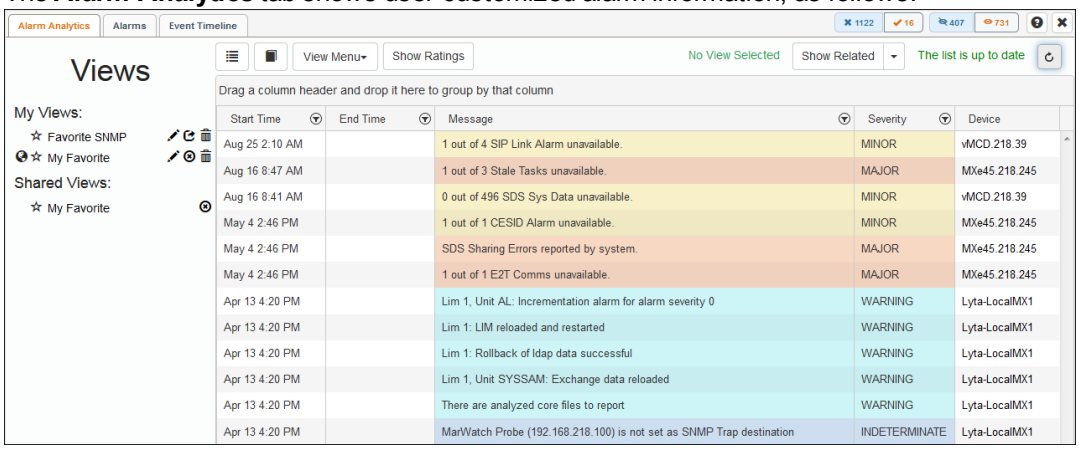
Note: The **Alarms** panel for a device dashboard presents only a subset of available functions.

The alarm list is updated every 5 minutes or when specific traps are received from certain devices; such as a MiVoice MX-ONE, a MiVoice Business, or a router. The device sends an Alarm Notification trap when an alarm condition is detected or cleared by the device. If a new alarm arrives, the alarm list automatically shows the most recent alarms. Bolded alarms are those generated for the current day.

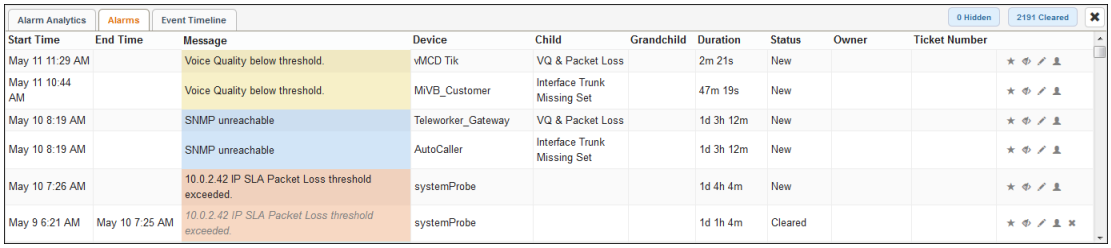
Click on the  icon in the top right corner of the Alarms panel to expand it and see its tabs.

Expanding the **Alarms** panel displays tabs with specialized information:

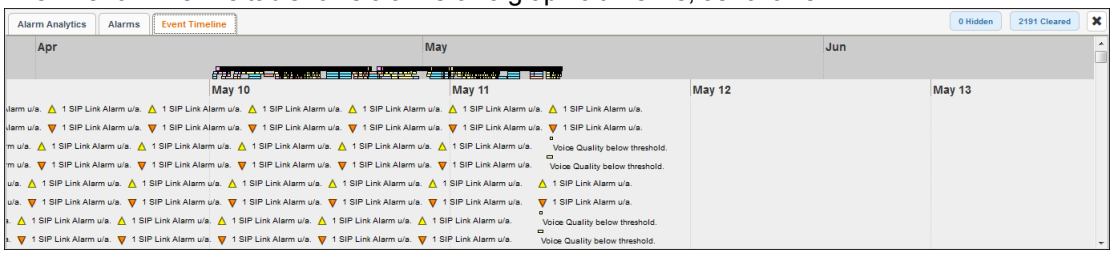
- The **Alarm Analytics** tab shows user-customized alarm information, as follows:



- The **Alarms** tab shows an expanded view of the alarm panel with further detail on current and historical alarms as follows:



- The **Event Timeline** tab shows alarms on a graphic timeline, as follows:



ALARM FILTERING

Device and container dashboards contain alarm filter buttons above the **Alarms** panel. The following is an example.

The filter buttons on the left display the number of Indeterminate, Warning, Minor, Major, Critical and Hidden alarms.

Clicking a filter button controls whether those types of alarms are displayed. In the previous graphic, only warning, minor, and major alarms are displayed. Similarly, the **Alarms** panel can be filtered to hide alarms that are older than one hour, one day, or one week.

Click the **Hidden** filter button to include or exclude hidden alarms from the **Alarms** panel. To quickly isolate hidden alarms, click the **Visible** filter button located beside the **Hidden** filter button. The **Visible** filter button displays the number of visible alarms.

Clicking the **My Alarms** filter button displays only the alarms where you are the owner.

Clicking the **My Favorites** filter button displays only the alarms that are of particular interest to you.

ALARM ANALYTICS

The **Alarm Analytics** tab allows you to customize your alarm management environment to help you see more easily the alarms that matter most to you. Alarms analytics allows Mitel Performance Analytics to learn from your behavior and from the behavior of other users to optimize how alarm information is presented. The alarms that are deemed to be the most important to you are shown first.

On the **Alarms Analytics** tab, alarms are presented according to their rating, which is a measure of the alarm's importance to you. An alarm's rating trends up when the following types of events occur:

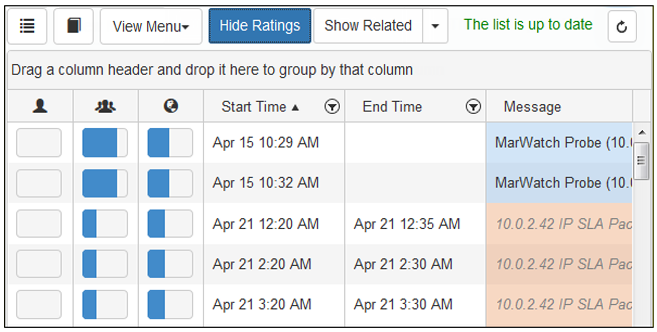
- The alarm is assigned to you or someone else.
- The alarm is assigned a trouble ticket number or a trouble ticket is updated.
- You flag the alarm as a favorite.
- You click through to a sub-container or device from the Alarms panel of a parent container dashboard.

An alarm's rating trends down when the following types of events occur:

- An alarm is hidden or cleared.
- You unflag the alarm as no longer a favorite.

These actions are monitored at three levels: your actions, all actions performed on alarms that share a label, and all actions performed by users globally, across the entire MPA system.

Click on the **Show Ratings** button to display the current alarm rating trend. In the following example, the top two alarms have a high rating due to a medium organization trend ( ) and a high label trend ( ), even though there is no personal trend ( ).



ALARM ANALYTICS OPERATIONS

Use the **Alarm Analytics** tab to customize your alarms work environment for maximum effectiveness.

Like the **Alarms** panel, clicking the entries under **Device**, **Child** or **Grandchild** displays the dashboard for that container or device.

MANAGING ALARM LABELS

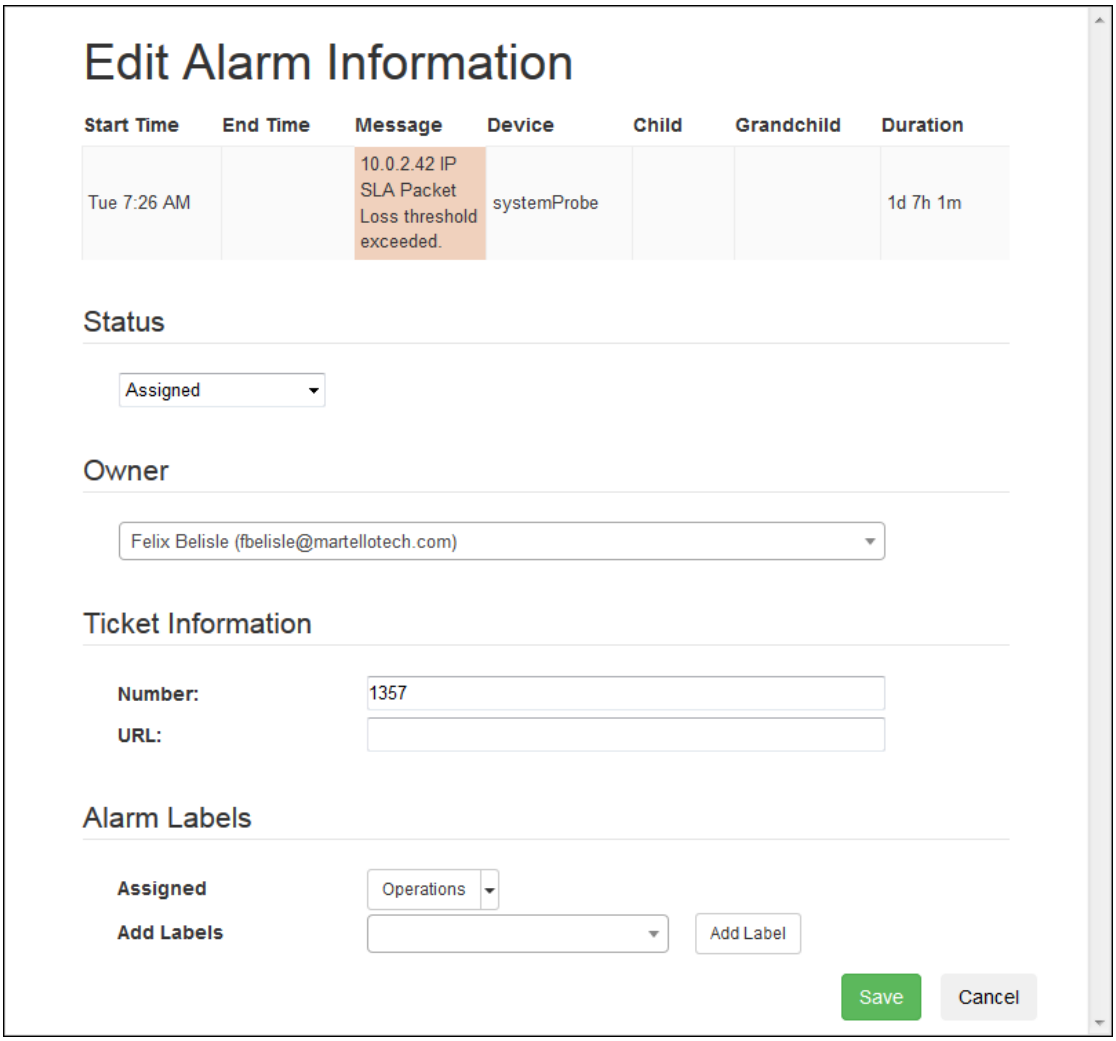
An alarm's rating is partially determined by actions performed on alarms that share a label. Labels are conceptually similar Twitter hashtags. Mitel Performance Analytics use labels to measure how an alarm's importance is trending.

You can assign a label to yourself to tell Mitel Performance Analytics you are particularly interested in that label, similar to following a Twitter hashtag.

Use the **Edit Alarm Information** panel to:

- See what labels are assigned to an alarm
- Add or remove a label from an alarm
- Assign a label to yourself
- Define new labels

To display the **Edit Alarm Information** panel, double-click the alarm on hte Alarm Summary or click its **Edit** icon. The following is an example.

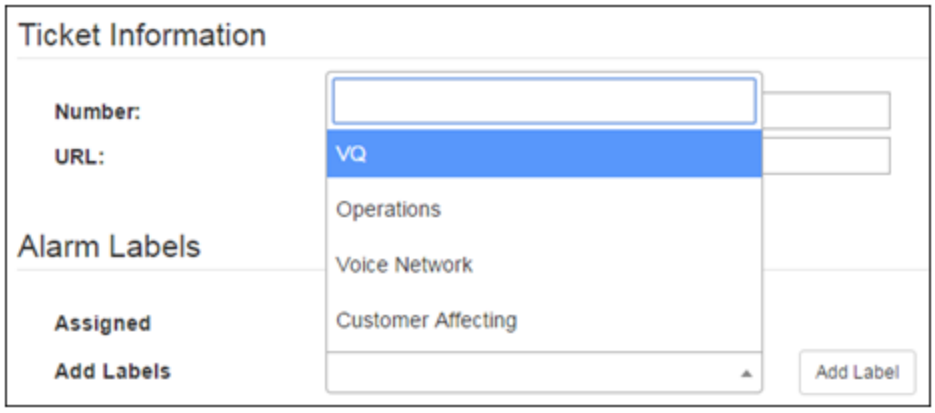


To assign a label to the alarm, select the label from the drop-down list and click **Add Label**.

Use the label name menu to remove the label from the alarm, or assign the label to yourself, as follows:

To define a new label, do the following steps:

1. Click on the label drop-down list.



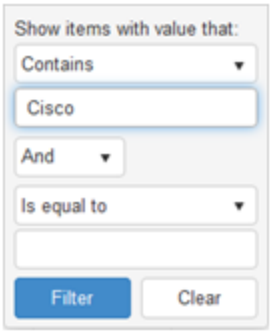
2. Enter the new label name in the blank field at the top.
3. Press **Enter**.

FILTERING THE ALARM ANALYTICS TAB

By default, the **Alarm Analytics** tab filters out hidden and cleared alarms. To display them, click on the **Hidden** or **Cleared** buttons in the top right corner.

The filtering icon in a column header indicates that the data can be filtered. Click on it to display the filtering menu. The filtering menu displays a variety of matching operations to restrict the display.

For example, an unfiltered **Alarms Analytics** tab can yield a table with many rows. To filter the display to show just alarms from Cisco devices, open the filter menu on the **Devices** column and use the following filter settings:



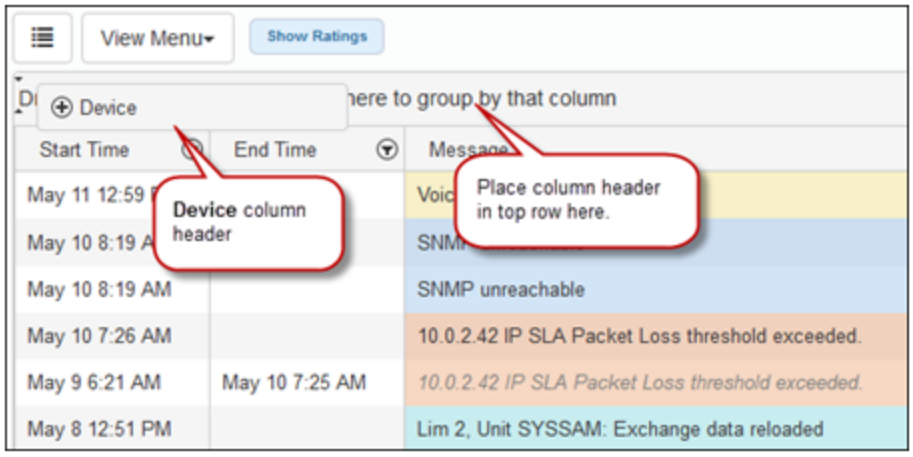
Use the **Clear** button to remove the filter and display the full set of query data. A filtering icon with a dark background indicates that a column has a filter.

GROUPING DATA ON THE ALARM ANALYTICS TAB

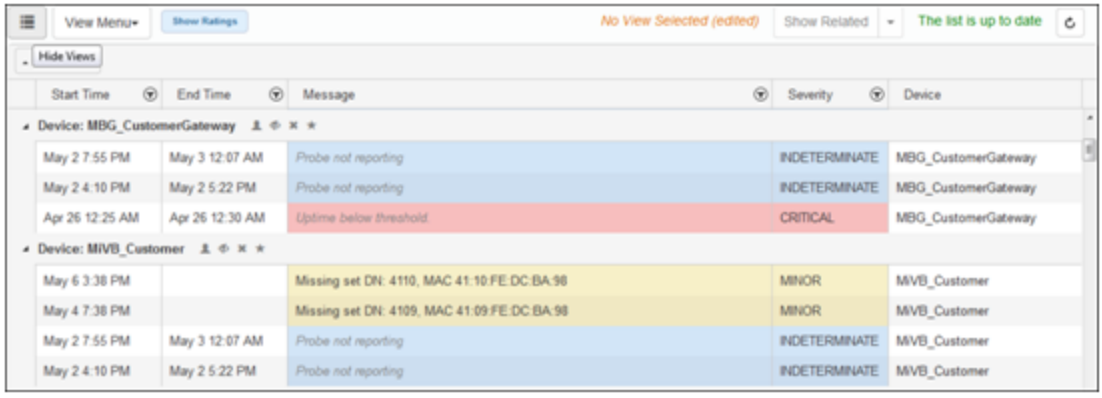
To group data, drag a column header to the row above the column headers.

For example to group the data by Device, do the following:

1. Drag the **Device** column header to the row above the column headers:

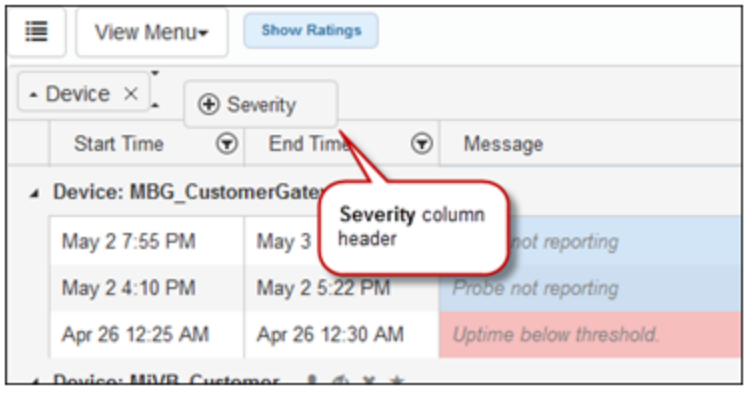


The data is rearranged as follows:

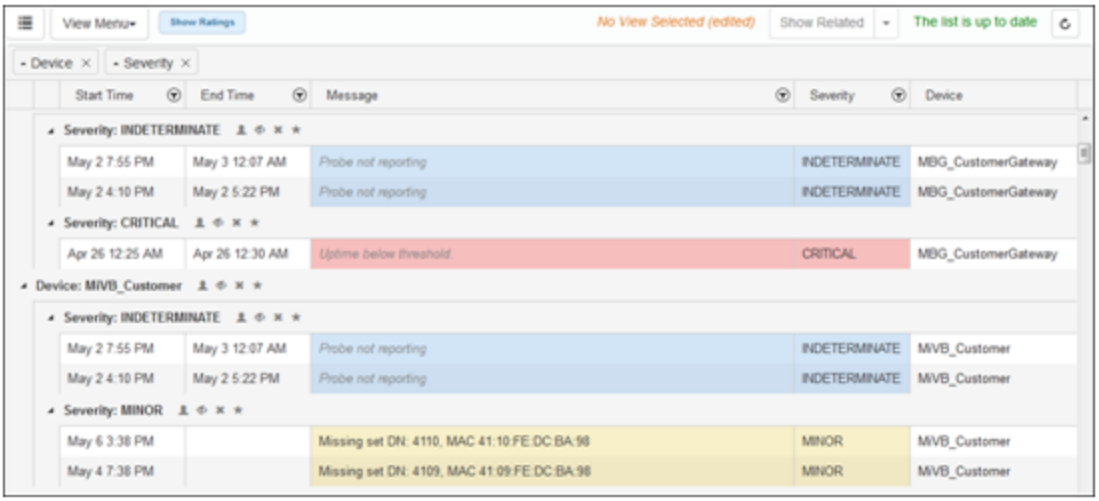


Groupings can be nested. For example, to further group by alarm severity, do the following:

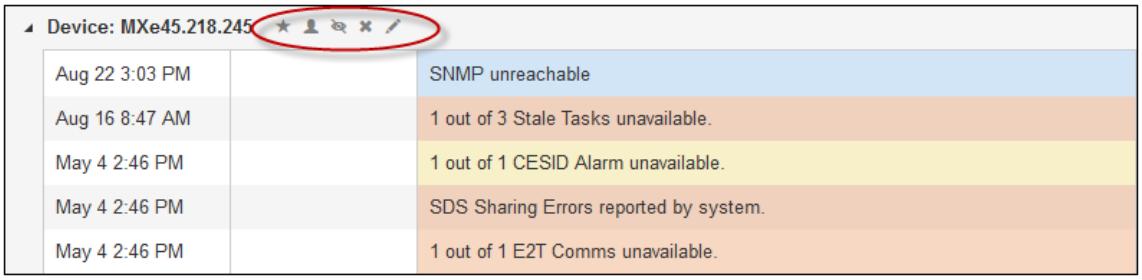
1. Drag the **Severity** column header to the row above the column headers where the **Device** column heading is:



The data is rearranged as follows:



Once alarms are grouped, you can perform operations that affect all the alarms that are in the group. Use the icons beside the group name. The following is an example:



When editing a group of alarms, any new information input with the **Edit Alarm Information** panel is applied to all alarms in the group. However, all other fields remain untouched. For example, if the Ticket Information number is set to 1350 and the URL field is left blank and untouched, only the number field is updated in all the alarms. If some of the alarms had information in their URL field, that URL information remains unchanged despite having left it blank in the **Edit Alarm Information** panel.

REARRANGING COLUMNS ON THE ALARM ANALYTICS TAB

Rearrange the column sequence by clicking the header of the column you want to move and dragging it to the new location.

ALARM VIEWS

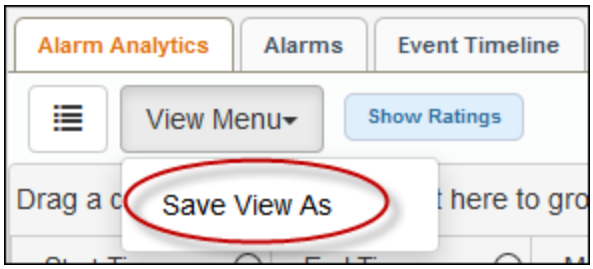
The **Alarm Analytics** tab allows you to save your customized views and share them.

By default the **Alarms Analytics** tab displays saved views. Click on the **Views** icon (≣) to hide or show saved views.

To apply a view, click on its name.

To save a view, do the following steps:

1. Click on the **View** menu and select **Save View As**:



2. In the resulting **Confirm Action** dialog, provide a name for your view and click **OK**.

A view is owned by the user who created it. Only that user can modify or delete it. Views are associated with the container where the owner logs in. Views are shared with anyone who can access that container or any subcontainer. You can always access your views regardless of the container you are working in.

The following icons are associated with saved views:

ICON	NAME	FUNCTION
	Globe	Indicates that a view is shared
	Favorite	Indicates the default view
	Rename	Rename the view
	Share	Share the view.
	Unshare	Stop sharing the view.
	Trash	Delete the view..

The **Share**, **Unshare**, and **Trash** icons have equivalent items under the **View** menu.

DISPLAYING TIME-RELATED ALARMS

Use the **Show Related** function to display alarms that occurred at a similar time to an alarm of interest. This capability can help display related data to help troubleshoot a potential issue.

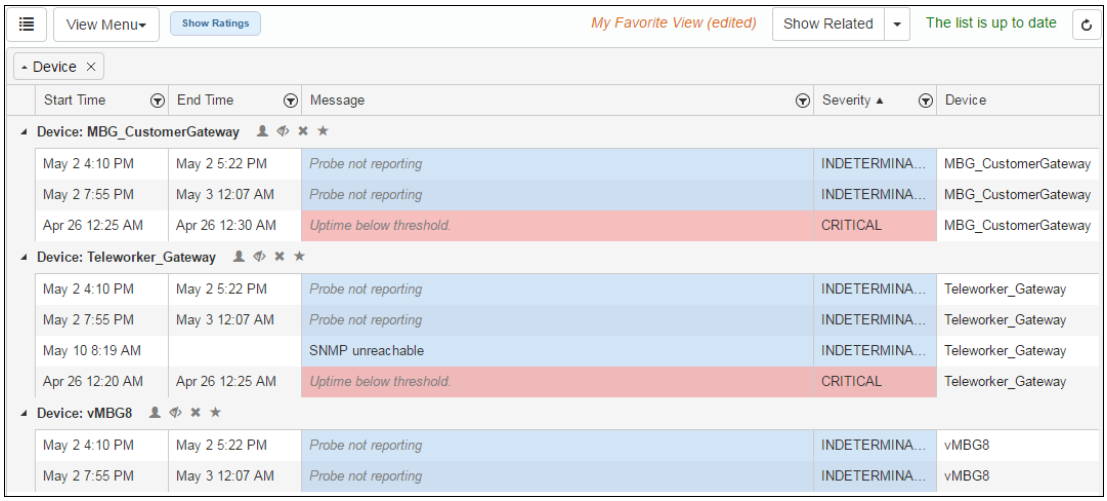
The **Alarm Analytics** tab offers varying time periods. The time period is centered on the occurrence of the alarm of interest. For example, if the alarm of interest occurred at 10:00, selecting a time of 2 minutes displays alarms that occurred from 9:59 to 10:01.

The **Show Related** function temporarily overrides any filtering currently in use. For example, if you use a custom view that uses a filter to show only MiVoice Border Gateway alarms, using the **Show Related** function displays alarms from all devices in your network. When you cancel the **Show Related** function, your view returns to displaying only MiVoice Border Gateway alarms.

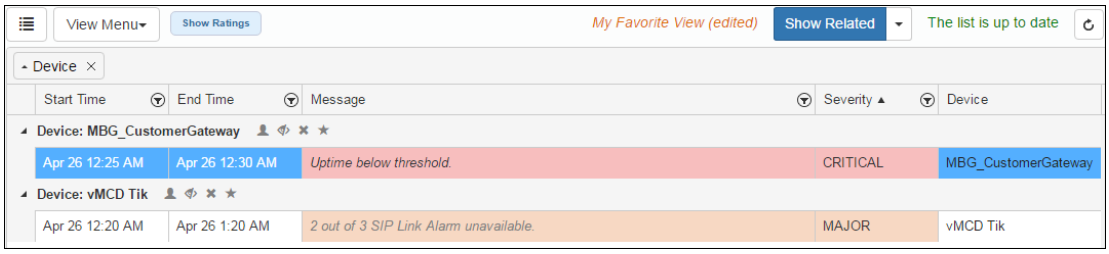
Use the dropdown list beside the **Show Related** button to select the time period of interest.

Click the **Show Related** button to invoke the function. Click it again to cancel the function.

For example, the following shows the **Alarms Analytics** tab displaying only MiVoice Border Gateway alarms.

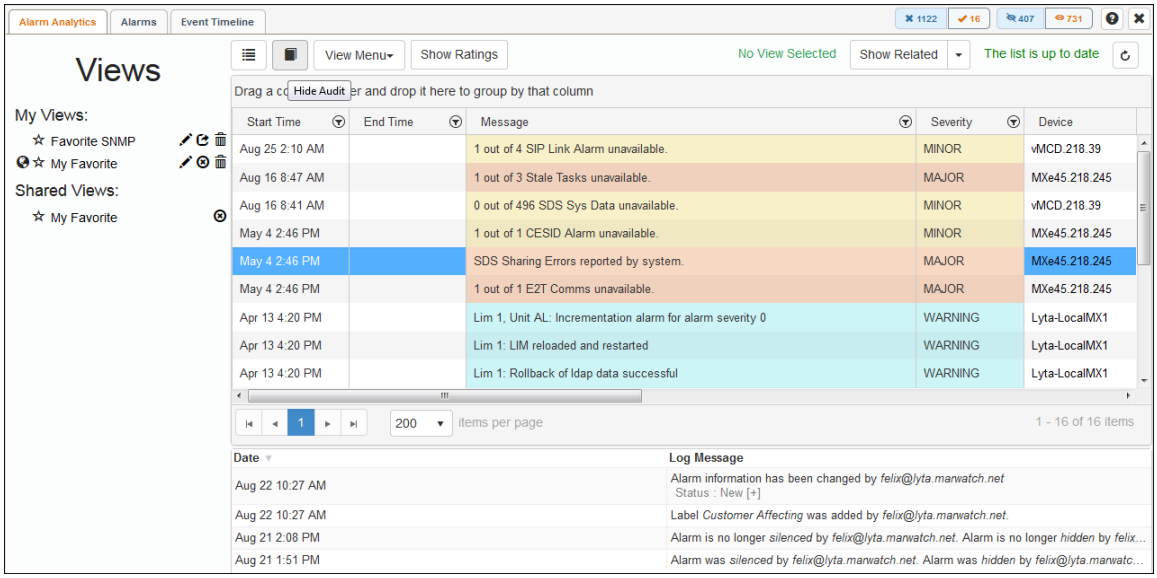


Invoking the **Show Related** function for a 10-minute period centered on one of the critical alarms results in the following display showing both MiVoice Business and MiVoice Border Gateway alarms.



DISPLAYING THE ALARM LOG

The alarm log shows all operations that have occurred on an alarm of interest. By studying the log, you can gain insights on why it ranks high or low on your filtered list of alarms. Click the **Log** icon () to show or hide it at the bottom of the **Alarm Analytics** tab. The following is an example.

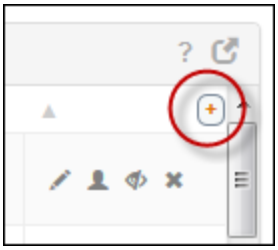


ALARM MANAGEMENT OPERATIONS

The following icons are available on the **Alarm Analytics** tab and the **Alarms** panel on a container dashboard. Use these icons to perform operations on individual alarms. To perform alarm operations from a device dashboard, access the **Alarm Analytics** tab.

ICON	NAME	FUNCTION
	Favorite	Mark the alarm as a favorite.
	Edit	Edit related alarm information
	Assign	Assign alarm to me
	Hide	Hide the alarm
	Unhide	Unhide or show the alarm
	Silence	Silence the alarm
	Unsilence	Unsilence the alarm
	Acknowledge	Acknowledge or clear the alarm

As well, the **Alarms** panel allows you to show or hide ticket information for a trouble management system. To do so, click the red **+** icon in the top right corner of the panel, as follows:



The setting to show or hide ticket information is stored as a browser cookie and is retained for future Mitel Performance Analytics sessions when you log in from the same computer and browser.

You can sort alarms by clicking the column title.

EDITING TROUBLE MANAGEMENT INFORMATION

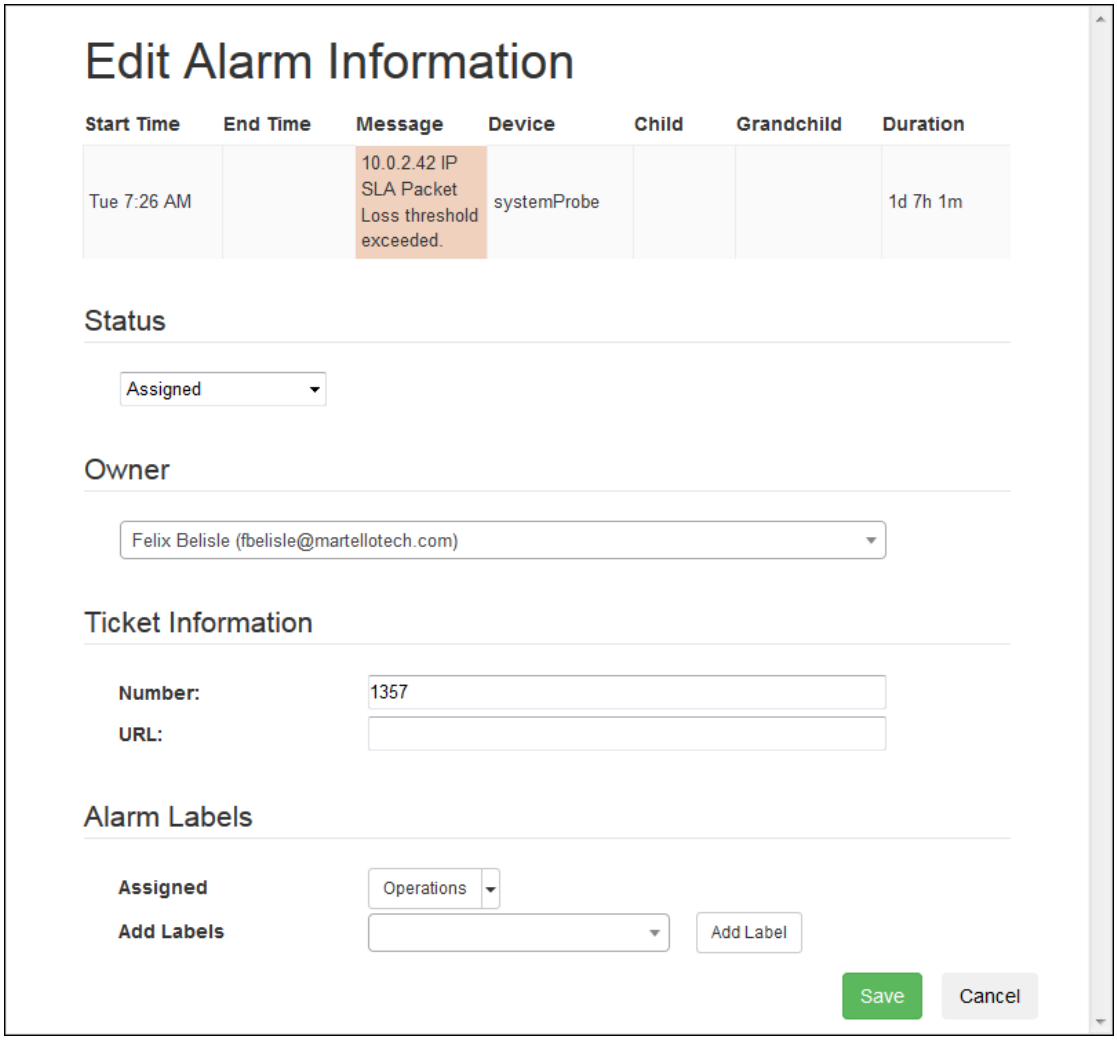
The **Alarms** panel and its tabs display **Status**, **Owner**, and **Ticket Number** information fields to assist in trouble management. Use the **Edit Alarm Information** panel to edit trouble management information.

There are multiple ways to display the **Edit Alarm Information** panel:

- From the Alarms panel of a container dashboard, double-click the alarm or click its **Edit** icon.
- From the **Alarms Analytics** tab, click its **Edit** icon.

- From the **Alarms** panel of a device dashboard, access the **Alarms Analytics** tab and click its **Edit** icon

The following is an example of the panel.



From the **Edit Alarm Information** panel, you can:

- Change the status of a ticket
  Note: Only some statuses are available through the **Edit Alarm Information** panel. The other alarm statuses are set automatically by Mitel Performance Analytics.
- Assign a ticket and select the assignee from a dropdown list.
- Enter a ticket number that matches the ticket number in your own ticket management system
- Enter a URL to the ticket in your own ticket management system

HIDING AND UNHIDING ALARMS

Hide an alarm by clicking its icon. Hiding an alarm increments the **Hidden** filter button located above the **Alarms** panel. You can unhide an alarm by clicking its icon.

The icons are available on the **Alarms** panel of a container dashboard and on the **Alarm Analytics** tab. From a device dashboard, access the **Alarm Analytics** tab to see the icons.

Click the **Hidden** filter button to include or exclude hidden alarms from the **Alarms** panel. To quickly isolate hidden alarms, click the **Visible** filter button located beside the **Hidden** filter button. The **Visible** filter button displays the number of visible alarms.

SILENCING RECURRENT ALARMS

Silencing an alarm means hiding all present and future instances of a particular type of alarm, regardless of the type of device that generated it. Typically, this is done to declutter your **Alarms** panel so you can focus on the alarms that you are interested in. For example, a person monitoring traffic routing may not be interested in Missing Set alarms. Silencing alarms also prevents alerts on those alarms from being sent.

Click the  icon to silence that alarm type. Alarms are silenced only for the person that invokes this function. Use the **Hidden** and **Visible** filter buttons to quickly isolate hidden alarms. Click on the  icon to unsilence an alarm type.

The icons are available on the **Alarms** panel of a container dashboard and on the **Alarm Analytics** tab. From a device dashboard, access the **Alarm Analytics** tab to see the icons.

Silenced alarms still appear in quick queries and reports.

ACKNOWLEDGING ALARMS

Some alarms, such as those dealing with connectivity, persist on the **Alarms** panel even after they are cleared. You must acknowledge them before they are removed.

Cleared alarms appear on the **Alarms** panel with a lighter font and the alarm message is italicized.

Alarms that require an acknowledgement have an  icon at the extreme right of the **Alarms** panel of a container dashboard and on the **Alarms Analytics** tab. From a device dashboard, access the **Alarm Analytics** tab to see the icon. Clicking the icon acknowledges the alarm and removes it from the **Alarms** panel.. However, the alarm is still visible in the **Alarms** tab view. See "Alarm Panel and Tabs" on page 55.

Alarms can only be acknowledged by users with permissions to edit trouble ticket information. The audit log records whenever an alarm is acknowledged.

TRAP DIRECTED POLLING

Arriving SNMP traps can be used to trigger immediate device polling. Alarms are then raised or cleared based on the poll results. This capability allows for closer and more responsive monitoring of critical devices.

This capability is currently restricted to SNMP **linkDown** and **linkUp** traps. To customize for other SNMP traps, contact Mitel support.

ALERT PROFILES

Alert profiles offer the ability to configure the system so it provides notification of an alarm when certain conditions are met. Notifications can be sent to an email address, to a desktop, by SMS, by Twitter Direct Message, or by a SNMP trap.

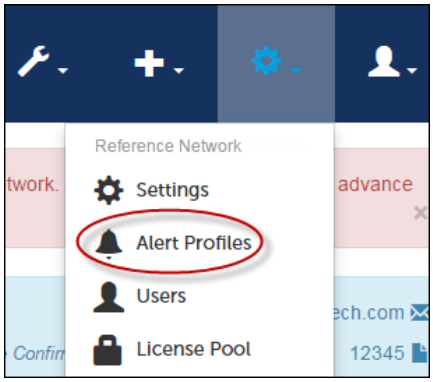
Multiple formats can be used for a single alarm. For instance you can set up an alert profile so you are notified by email for all major and critical alarms during working hours and by SMS for critical alarms only after working hours.

CAUTION: If Mitel Performance Analytics has not been configured with SMS and Twitter notification capabilities, then Alerts configured to be sent by SMS or Twitter fail with a logged error message. See "Configuring a Twitter Account" on page 179 and "Configuring a Twilio SMS Account" on page 180.

CONFIGURING ALERT PROFILES

Do the following steps:

1. From a container dashboard, select **Alert Profiles** under the **Settings** icon.



   The **Alert Profiles** window is displayed.
2. Click the **Create New Alert Profile** button.
   The **New Alert Profile** window is displayed.
3. In the **New Alert Profile** window, specify the properties for the new Alert profile.
   - **Profile name**: Descriptive name for the profile.
   - **Recipients**: Alerts can be sent to multiple recipients by email, desktop notification, SMS, Twitter or SNMP. Enter the recipient addresses in the **Recipients** list. For multiple recipients, separate addresses by commas or enter them on separate lines.

   Alert destination formats:

   - **Email**: Email is the default Alerting method. To send an email alert, use the address format: `emailaddress@fqdn`

     Example:
     Use email@alertreceiver.com to send email Alerts to email@alertreceiver.com if the Alert conditions are satisfied.

     Note: An SMTP server must be configured to use this functionality. See "Configuring the SMTP Server" on page 178.
   - **Desktop**: To send notifications to your desktop use the address format: `desktop:MPALoginEmailAddress@fqdn`

Example:
Use `desktop:fbelisle@mitel.com` to send desktop notifications to the user logged into Mitel Performance Analytics using the email address fbelisle@mitel.com.

The supplied email address must be the one used to log into Mitel Performance Analytics. To receive desktop notifications, you must be logged into Mitel Performance Analytics and you must have enabled notifications for the particular browser you are using. If you have multiple sessions to Mitel Performance Analytics with multiple browser types, Mitel recommends that you enable notifications for each type of browser.

If you have permissions to create and edit Mitel Performance Analytics users, then you can also specify their login email addresses as destinations. To see which user accounts you can control, select **Users** from the **Settings** menu. See "Step 3 - Add Users" on page 45

- **SMS**: To send an SMS or Text Message Alert use the address format: `sms:(country code) phone number`
  The country code is optional. If you do not supply it, the system assumes a default country code of 1 (North American Numbering Plan Area). Numbers may contain **+**, **(**, **)**, . and **-** characters.

  Examples:
  Use `sms:16135551212` to send SMS alerts to +1-613-555-1212 (Canada).
  Use `sms:+44(877)321-4321` to send SMS alerts to +44-877-321-4321 (UK).

  Note: A Twilio SMS account must be configured to use this functionality. See "Configuring a Twilio SMS Account" on page 180.
- **Twitter**: To send a Twitter Direct Message Alert use the address format: `twitter:@twitterusername`
  To receive a Twitter Direct Message, the destination Twitter account must be set up to follow the Mitel Performance Analytics Twitter account: http://twitter.com/MarWatch

  See http://support.twitter.com/groups/31-twitter-basics/topics/108-finding-following-people/articles/162981-how-to-follow-others for instructions on how to follow the Mitel Performance Analytics account.

  Examples:
  Use `twitter:@mitelreseller` to send Twitter Alerts to @mitelreseller.
  Use `twitter:@vartechsupport` to send Twitter Alerts to @vartechsupport.

  Note: A Twitter account must be configured to use this functionality. See "Configuring a Twitter Account" on page 179.
- **SNMPV1 or v2**:To configure SNMPv1 or v2 trap sending, enter a recipient in the format: `snmp:[//][community@]host[:port]`
  The default community string is `public`. The default port is `162`.

  Examples:
  Use `snmp://private@10.10.10.25:1062` to send SNMP traps to IP address `10.10.10.25`, port `1062` with `Community String = private`.
  Use `snmp:10.10.10.25` sends SNMP traps to IP address `10.10.10.25`, port `162` with `Community String = public`.
- **Notify on Clear**: When activated by clicking the selection box, this option sends an Alert notifying that an alarm has been cleared.

- **Digest**: This option is useful in reducing the number of Alerts for related alarm conditions on a device. If this option is selected, then when a matching alarm event occurs Mitel Performance Analytics waits 30 seconds before sending you an Alert email. The Alert email contains information on the triggering alarm event and other related alarm events that occurred during the 30-second wait period. Mitel Performance Analytics then waits for the configurable digest period before sending you subsequent Alert emails. Besides containing alarm information, the Alert emails summarize the overall status change for the device. The Digest option only applies to email notifications.
- **Severity**: Alarms are sent based on the severity chosen and any alarms with a higher severity. For instance, if you choose **Minor**, then the profile matches minor, major and critical alarms.
- **When**: Choose between **Week-Days**, **Weekends** and **Any Day** between particular hours. For example, one account administrator can create a profile that sends alerts only on week days, between 8:00 am and 5:00 pm.
- **Time zone**: Select the time zone for the profile.
- **Enabled**: Select the check-box to activate this profile. To disable, deselect the check-box.

4. Click on the **Save** button.
5. If applicable, configure any email spam blockers to allow Mitel Performance Analytics email notifications. See "Email configuration" on page 69.

EMAIL CONFIGURATION

Receiving notifications from Mitel Performance Analytics is an important part of being proactive in performance monitoring. Alarms and reports being blocked by spam filters or being redirected to a spam inbox can mean a late response to an important event.

To avoid such delays, all Mitel Performance Analytics email sources must be whitelisted by customers to prevent spam filters from acting on them.

Mitel Performance Analytics email sources include:

- reports@marwatch.net
- alarms@marwatch.net
- support@martellotech.com
- for Mitel Performance Analytics Plus on-premise users, any From and Reply-to email addresses configured during installation. See "Configuring the SMTP Server" on page 178.

For each of the previous email addresses:

1. Add them to your email contact lists.
2. When a corporate spam filter is in use, add them to the trusted whitelist.

THRESHOLD ALARM MANAGEMENT

Mitel Performance Analytics allows you to configure performance thresholds to generate alarms when the thresholds are crossed. The following alarm severities are related to performance thresholds:

- Warning – No immediate impact, but abnormal device behavior detected

- Minor – Non performance impairing
- Major – Performance impairing
- Critical – Device out of service

For each alarm severity level, the system applies value and time hysteresis to reduce the number of spurious alarms.

For example, the system can generate a minor alarm for IP SLA when packet loss is ≥ 2% for at least 10 minutes. The alarm is cleared when packet loss < 2% for at least 5 minutes.

Performance thresholds can be set for the following parameters:

- Probe check-in time
- IP SLA packet loss
- Ping (ICMP) round-trip time
- Ping (ICMP) packet loss
- CPU usage
- Memory usage
- Interface availability
- Bandwidth utilization
- Windows service inactivity
- Voice Quality R value

Windows service thresholds can be set per device by specifying the Windows Service(s) to be monitored.

Interface thresholds (for availability and bandwidth utilization) can be applied to the following interface types:

- ds1- 1.5 Mbps serial interface
- ds3 - 45 Mbps serial interface
- e1 - 2.0 Mbps serial interface
- ethernetCsmacd
- pppMultilinkBundle
- propPointToPointSerial
- hdlc
- sdlc

THRESHOLD CONFIGURATION

To set performance thresholds for a series of devices, you must first determine which Probe is monitoring those devices.

System performance thresholds are configurable from the container of the Probe that is monitoring the devices; or that container's parent containers up to the root of the container structure. A system administrator can set system wide-thresholds at the root container of a structure. The system thresholds apply to all Probes in the container structure; and therefore to all devices in the system. A local administrator, who has access to just a few containers with just one Probe for example, can set

thresholds for just the containers and the single Probe they can access. The local threshold settings apply to just the devices monitored by the local Probe.

Performance thresholds are applied hierarchically throughout a container structure. A threshold set in a lower container in the hierarchy overrides the same threshold set higher in the hierarchy. For example, a system administrator can set the following system thresholds for bandwidth utilization:

- Raise a minor alarm when utilization ≥ 75% for longer than 20 minutes; clear the minor alarm if it drops to < 70% for longer than 10 minutes
- Raise a major alarm when utilization ≥ 85% for longer than 20 minutes; clear the major alarm if it drops to < 80% for longer than 10 minutes

The previous thresholds apply to all Probes and monitored devices in the system.

A local administrator who can access a single Probe, called Probe A for example, can set the following thresholds from Probe A's container:

- Raise a minor alarm when utilization ≥ 65% for longer than 15 minutes; clear the minor alarm if it drops to < 60% for longer than 10 minutes
- Raise a critical alarm when utilization ≥ 95% for longer than 10 minutes; clear the critical alarm if it drops to < 90% for longer than 15 minutes

As a result of the previous settings, Mitel Performance Analytics generates the following alarms for the devices monitored by Probe A:

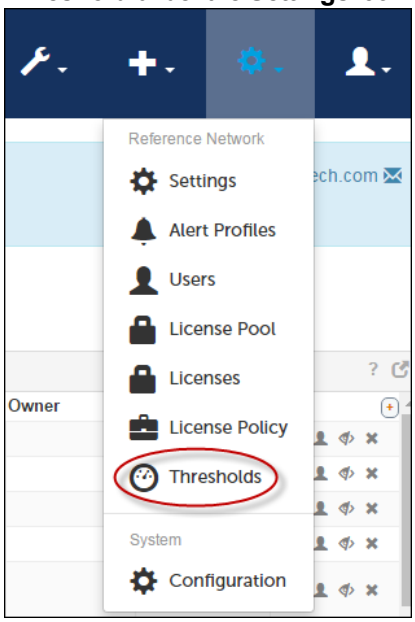
- Raise a minor alarm when utilization ≥ 65% for longer than 15 minutes; clear the minor alarm if it drops to < 60% for longer than 10 minutes (set locally)
- Raise a major alarm when utilization ≥ 85% for longer than 20 minutes; clear the major alarm if it drops to < 80% for longer than 10 minutes (inherited from the system thresholds)
- Raise a critical alarm when utilization ≥ 95% for longer than 10 minutes; clear the critical alarm if it drops to < 90% for longer than 15 minutes (set locally)

Only users with the appropriate privileges can set thresholds. See "User Permissions" on page 46.

To configure system thresholds, do the following steps:

1. Determine which Probe is monitoring the devices you want to set thresholds for.

2. Access the Probe's container dashboard or the dashboard of a parent container. Select **Threshold** under the **Settings** icon.



The **Global Thresholds** window is displayed, showing a table of all parameters with thresholds for all device types. The parameters are listed in the left. The device types make up the table columns. The following is an example.

	Avaya IP Office	Basic IP Device	ESXi Server	Inline IP	MX-ONE	Application Server	MiContactCenter	MiVoice Office 250	MiCollab	MiVoice Border Gateway	MiVoice Business	MiVoice MX-ONE	MiVoice Call Recording	Path Solutions	Probe	RedBox CR	Router	Server	Switch	UPS
CPU	-	-	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	-	-	⊙	⊙	⊙	⊙	-
Disk Usage	-	-	⊙	⊙	⊙	⊙	-	⊙	⊙	-	⊙	⊙	-	-	-	⊙	-	⊙	-	-
IP SLA Latency	-	-	-	-	-	-	-	-	-	-	-	-	-	-	⊙	-	-	-	-	-
IP SLA Packet Loss	-	-	-	-	-	-	-	-	-	-	-	-	-	-	⊙	-	-	-	-	-
Interface Availability	⊙	-	⊙	⊙	⊙	⊙	-	⊙	⊙	⊙	⊙	⊙	⊙	-	-	⊙	⊙	⊙	⊙	-
License Usage	-	-	-	-	-	-	⊙	-	⊙	⊙	-	-	-	-	-	-	-	-	-	-
Memory Usage	-	-	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	-	-	⊙	⊙	⊙	⊙	-
Missing IP Sets	-	-	-	-	-	-	-	-	⊙	⊙	-	-	-	-	-	-	-	-	-	-
Ping Latency	⊙	-	⊙	⊙	⊙	⊙	⊙	⊙	⊙	▼	⊙	⊙	⊙	-	⊙	⊙	⊙	⊙	⊙	⊙
Ping Packet Loss	⊙	-	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	-	⊙	⊙	⊙	⊙	⊙	⊙
Probe Check-in	-	-	-	-	-	-	-	-	-	-	-	-	-	-	⊙	-	-	-	-	-
Process Inactivity	-	-	-	⊙	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
RX Bandwidth Utilization	⊙	-	⊙	⊙	⊙	⊙	-	⊙	⊙	⊙	⊙	⊙	⊙	-	-	⊙	⊙	⊙	⊙	-
SDS Error Rate	-	-	-	-	-	-	-	-	-	⊙	-	-	-	-	-	-	-	-	-	-
Services Inactivity	-	-	⊙	⊙	⊙	⊙	-	-	-	-	-	⊙	-	-	-	⊙	-	⊙	-	-
TX Bandwidth Utilization	⊙	-	⊙	⊙	⊙	⊙	-	⊙	⊙	⊙	⊙	⊙	-	-	-	⊙	⊙	⊙	⊙	-
Time Sync	-	-	-	-	-	-	-	-	-	-	-	-	-	-	⊙	-	-	-	-	-
Uptime	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	-	-	-	⊙	⊙	⊙	⊙	⊙
Voice Quality	-	-	-	-	-	-	-	-	⊙	⊙	⊙	-	-	-	-	-	-	-	-	-

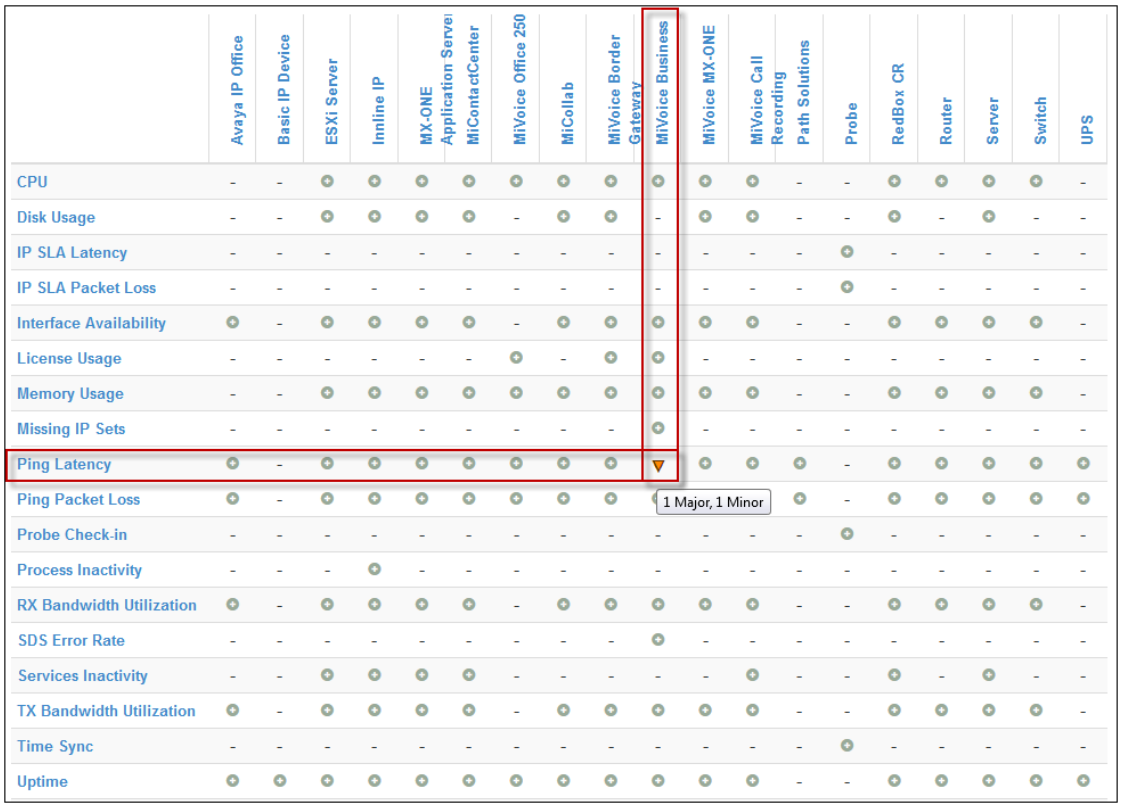
Note: The **Global Thresholds** window displays settings that apply to the current container and all its descendant containers only. It does not display settings inherited from parent or other ancestor containers.

Each element in the table indicates the most severe threshold that has been configured and enabled for that combination of parameter and device type. The following table describes the threshold icons that appear in the **Global Thresholds** window.

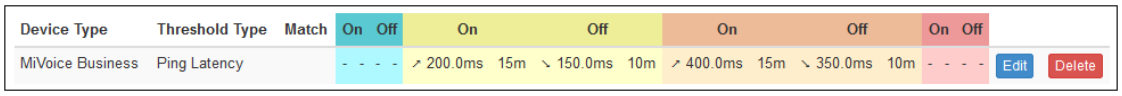
ICON	MEANING
–	Thresholding is not supported.
	Threshold is supported but not defined.
	Threshold is defined but not enabled.
	Most severe alarm defined for this threshold is Warning.
	Most severe alarm defined for this threshold is Minor.
	Most severe alarm defined for this threshold is Major.
	Most severe alarm defined for this threshold is Critical.

Hovering over a threshold icon provides more details on the thresholds defined for that particular parameter and device combination.

In the following example, there are two threshold alarms configured for MiVoice Business Ping Latency.



For further information on the threshold alarms, click on the icon at the intersection of the parameter and device type. The **Thresholds** page is displayed.

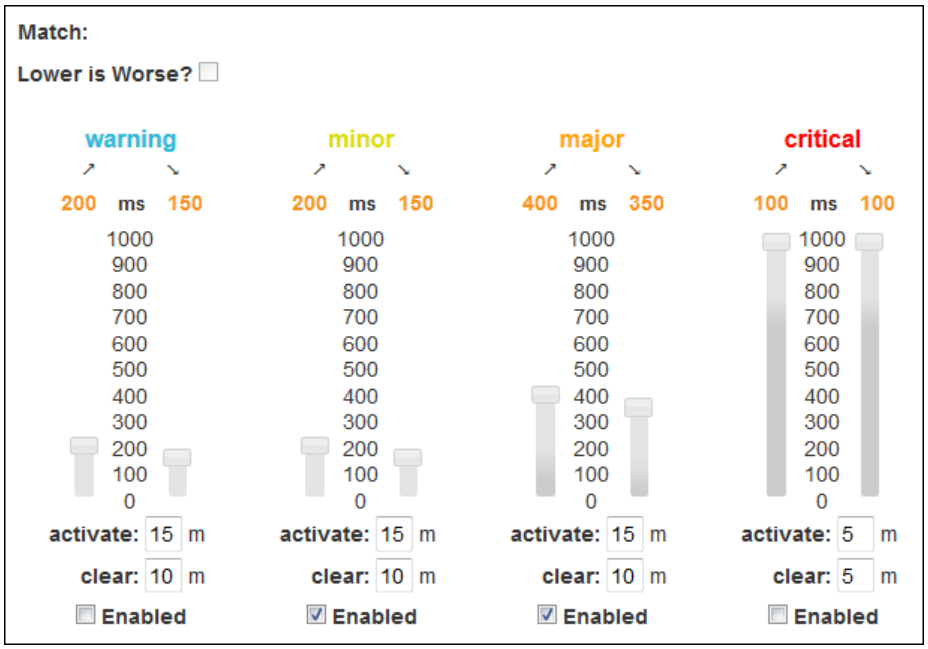


The **Thresholds** page shows the thresholds settings for that parameter and device pair. In this example, a minor alarm is generated when Ping Time > 200 ms for 15 minutes and cleared when Ping Time < 150 ms for 10 minutes. A major alarm is generated when Ping Time > 400 ms for 15 minutes and cleared when Ping Time < 350 ms for 10 minutes.

Threshold Editing

Click on the **Edit** button on the **Thresholds** page to open the **Edit** page.

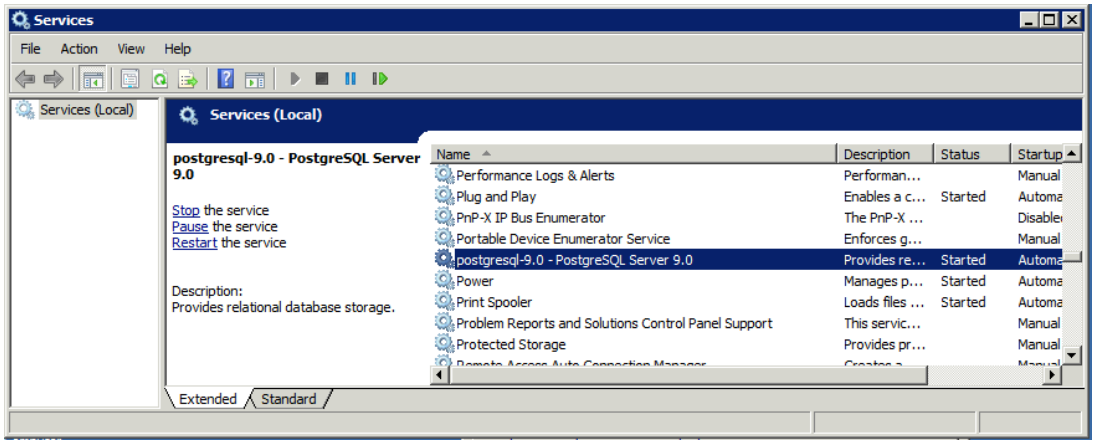
The threshold **Edit** page allows you to set warning, minor, major and critical alarm severity threshold values for a specific parameter and device pair.



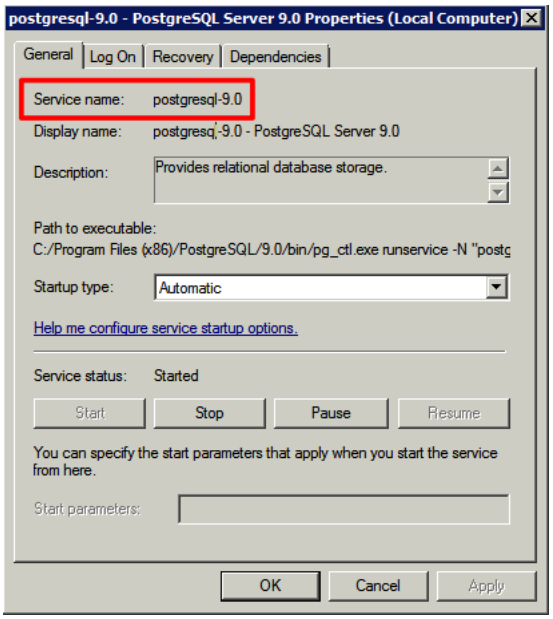
Match Options

Some parameters and thresholds pairs can have a **Match** value required for the threshold to be valid. The parameters with **Match** values are:

- **Interface Availability**, **RX Bandwidth Utilization** and **TX Bandwidth Utilization**: Matches are selected from: ppp, pppMultilinkBundle, propPointToPointSerial, hdlc, sdlc, e1, ds1, or ds3.
- **Disk Usage**: Matches are entered as text strings corresponding to an OS volume or mount point name. The following are examples:
  - For Windows: `C:\`, or `E:\data`
  - For Linux and Unix: `/`, `/root`, or `/data`
- **Services Inactivity:** Matches are entered as text strings to the **Windows Service** name field. The Windows Service name is available from the **Windows Service Management** console. The following is an example to monitor for the availability of PostgreSQL running on a Windows Server. In this example, you identify the Windows Service name using the **Services** Console.



Double-click on the Postgres service to find the **Service Name** (not the Display Name).



From the information on the previous dialog fox, you enter **postgresql-9.0** as the match parameter.

Lower is Worse?

Separate thresholds can be set for parameters which indicate worse conditions with higher values and for parameters which indicate better conditions with higher values. The default settings assume that a higher parameter value indicates a worse condition, except for the R value used in the **Voice Quality** thresholds.

For example, to generate an alarm if CPU usage is less than a certain value, ensure that the **Lower is Worse?** checkbox is selected.

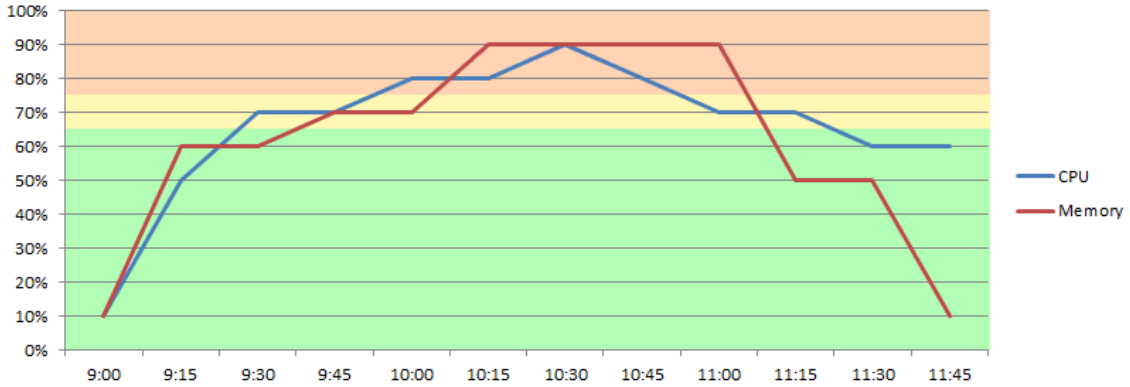
Threshold Values

You can set multiple alarm severity thresholds for each combination of parameter, device, match and lower is better.

Set threshold values by dragging the slider for the selected alarm severity or by entering the value below the slider. The slider moves to the nearest valid values for the threshold it is being set for. For instance, if the Ping Packet Loss is measured in 25% increments, the slider jumps to the nearest 25% increment.

Time and Value Hysteresis

Mitel Performance Analytics supports both time and value hysteresis for both raising alarms and clearing alarms. This feature reduces the number of nuisance alarms.



For example, in the previous graphic with standard settings for device CPU and memory utilization threshold alarms:

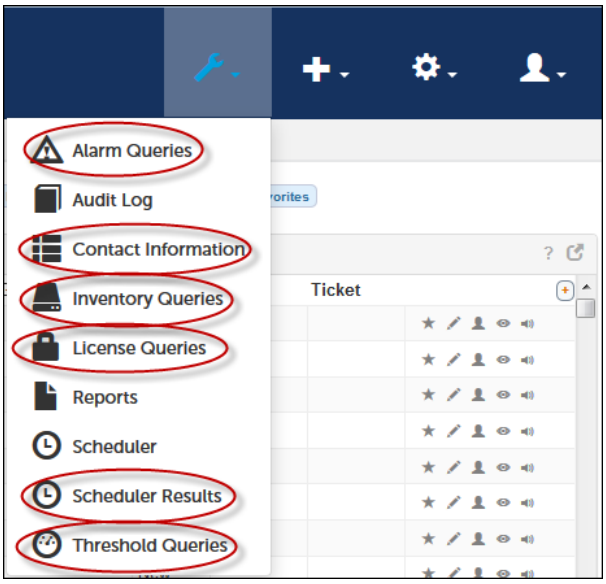
- CPU utilization:
  - A minor alarm is raised at 9:45 (utilization ≥ 75% at 9:30 + 15 minutes on time requirement).
  - A major alarm is raised at 10:15 (utilization ≥ 85% at 10:00 + 15 minutes on time requirement).
  - A major is downgraded to a minor alarm 10:55 (utilization < 80% at 10:45 + 10 minutes off time requirement).
  - A minor alarm is cleared at 11:25 (utilization < 70% at 11:15 + 10 minutes off time).
- Memory utilization
  - A minor alarm is raised at 10:30 (utilization ≥ 85% at 10:15 + 15 minutes on time requirement).
  - A minor alarm is cleared at 11:10 (utilization < 80% at 11:00 + 10 minutes off time).

The time and value hysteresis criteria are combined. In the previous example, if the memory utilization increases momentarily to 75% at 11:20, the alarm is not cleared until 11:30 (11:20 + 10 minutes off time requirement).

MITEL PERFORMANCE ANALYTICS REPORTING

Reporting is a standard option with any subscription to Mitel Performance Analytics. Mitel Performance Analytics provides two different types of reports. The first type consists of a series of on-demand quick queries of useful information. The second type is the ability to generate reports showing customer device status and performance for a period of time. Reports can be scheduled to run monthly, weekly, or immediately. As well, you can use the report scheduler to schedule any quick query to occur at a regular interval.

The queries and reporting functions are accessed under the **Tools** icon, as follows:



The container dashboard provides access to most queries. Some queries are available also from the dashboard of the device that the query applies to.

QUICK QUERIES

The following sections describe the available Mitel Performance Analytics on-demand quick queries.

ALARM QUERIES

Mitel Performance Analytics provides the following initial set of alarm queries. Use the time period selector to choose the timeframe for the report. Additional queries can be configured with the Reports menu item. Refer to "Generating Reports" on page 90.

QUERY NAME	DESCRIPTION
Alarm Export	All alarms inside this container or for this device for the selected time period.
All Device Availability	Availability and monitoring coverage of all devices with service impacting events.

QUERY NAME	DESCRIPTION
Child Device Availability	Availability and monitoring coverage of all devices with service impacting events.
Container Alert Profiles	All alert profiles for this container and its descendants.
Critical Alarms by Day	Details of critical alarm count by container for each day of the reporting period.
Critical Alarms by Device Type	Total count of new critical alarms by device type for the reporting period.
Top 10 Critical Customers	The 10 customers with the highest number of new critical alarms for the reporting period.
Top 10 Critical Devices	The 10 devices with the highest count of new critical alarms for the reporting period.

CONTACT INFORMATION

Mitel Performance Analytics provides the following initial set of contact information queries.

QUERY NAME	DESCRIPTION
All Contact Information	Contact information for the current container and all its subcontainers.
Customer Contact Information	Contact information for customer containers.

INVENTORY QUERIES

Mitel Performance Analytics provides the following initial set of inventory queries. Additional queries can be configured with the **Reports** menu item. Refer to "Generating Reports" on page 90.

QUERY NAME	DESCRIPTION
Device Count	Number of configured devices by type.
Device Inventory	Detailed inventory of network devices.
IPT Users Inventory	List of IPT users and the unique identifier of their host device. Use this query to determine the number of licenses you need. For details, see "Aggregate Licensing and IPT Users" on page 104.

QUERY NAME	DESCRIPTION
Inventory of Customer Devices	List of customer devices in the container.
MIVoice Business Licenses	Inventory of MiVoice Business licenses
MiVoice Business Users, Services & Sets	Detailed information for every user, service, or IP set hosted on a MiVoice Business system. See also "Reusing Custom Views" on page 87. **Note**: This query is available from the dashboard of a container that has MiVoice Business devices, and from the dashboard of a MiVoice Business device.
MiVoice Business Versions	Count of configured MiVoice Business call servers, by software version.
MiVoice MX-ONE Extensions	Lists MiVoice MX-ONE extension details such as container name, device name, IPT user names, extension numbers, and set types

LICENSE QUERIES

Mitel Performance Analytics provides the following initial set of license queries. Additional queries can be configured with the Reports menu item. Refer to "Generating Reports" on page 90.

QUERY NAME	DESCRIPTION
Device & Container License Expiry	List of devices and containers whose licenses have expired or will expire within 90 days.
Device & Container License Status	List of devices and containers in this container and its descendants with the status of their licenses.
Device & Container License Violations	List of devices and containers in this container and its descendants with license violations.

QUERY NAME	DESCRIPTION
Device & Container License Violations By Customer	List of devices and containers in this container and its descendants with license violations, sorted by the customer container in which they reside.
Installed Licenses	All of the licenses installed in this container. Installed licenses are licenses that have been uploaded and assigned to a device. Note that a device can have multiple licenses assigned to it. Licenses are uniquely identified by the GUID.
License Expiry	All licenses that either have expired in the previous 90 days or will expire in the next 90 days. Note that a device can have multiple licenses assigned to it. Licenses are uniquely identified by the GUID (Globally Unique Identifier).
Trial Licenses	All trial licenses. Trial licenses may be available for new devices and features, as defined by the Mitel Performance Analytics licensing policy. Note that a device can have multiple licenses assigned to it. Licenses are uniquely identified by the GUID.

SCHEDULER RESULTS

Mitel Performance Analytics provides the following queries for use with the Operations Scheduler and on-demand backups. See "Scheduling Device Operations" on page 159 and "On-Demand Backups" on page 168 for details.

QUERY NAME	DESCRIPTION
Completed Files	Results of completed on-demand backups, scheduled backups, and scheduled SMDR collection operations, including links to download backup file and SMDR collection file instances. Allows backup files to be locked for indefinite retention. See: • "Retrieving Scheduled SMDR or Backup Files" on page 166 • "Retrieving On-Demand Backup Files" on page 170
On-Demand State	State of all on-demand operations.
Recent Results	Results of scheduled backups and SMDR collection operations, including links to download backup file and SMDR collection file instances. See "Retrieving Scheduled SMDR or Backup Files" on page 166.

QUERY NAME	DESCRIPTION
Schedule State	Per device timestamp of last success, last failure, and next execution.
Success Rate	Per device and per schedule success rate.

For all **Scheduler Results** queries except **On-Demand State**, you can choose to display backup-only or SMDR-only results.

THRESHOLD QUERIES

Mitel Performance Analytics provides the following initial set of threshold queries. Additional queries can be configured with the Reports menu item. Refer to "Generating Reports" on page 90.

QUERY NAME	DESCRIPTION
Container or Device Thresholds	Thresholds that apply to this container or device.

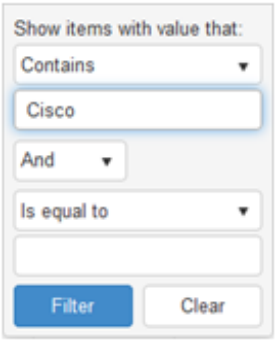
QUERY OUTPUT FORMATS

All query results are available in table format. When appropriate, query results can also be displayed in a pie chart or pivot table.

FILTERING TABULAR QUERY RESULTS

The filtering icon in a column header indicates that the data can be filtered. Click on it to display the filtering menu. The filtering menu displays a variety of matching operations to restrict the display.

For example, an unfiltered **Alarm Export** query can yield a table with many rows. To filter the display to show just alarms from Cisco devices, open the filter menu on the **Devices** column and use the following filter settings:



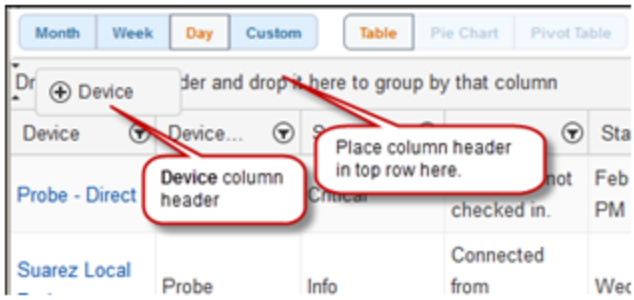
Use the **Clear** button to remove the filter and display the full set of query data. A filtering icon with a dark background indicates that a column has a filter.

GROUPING DATA IN TABULAR QUERY RESULTS

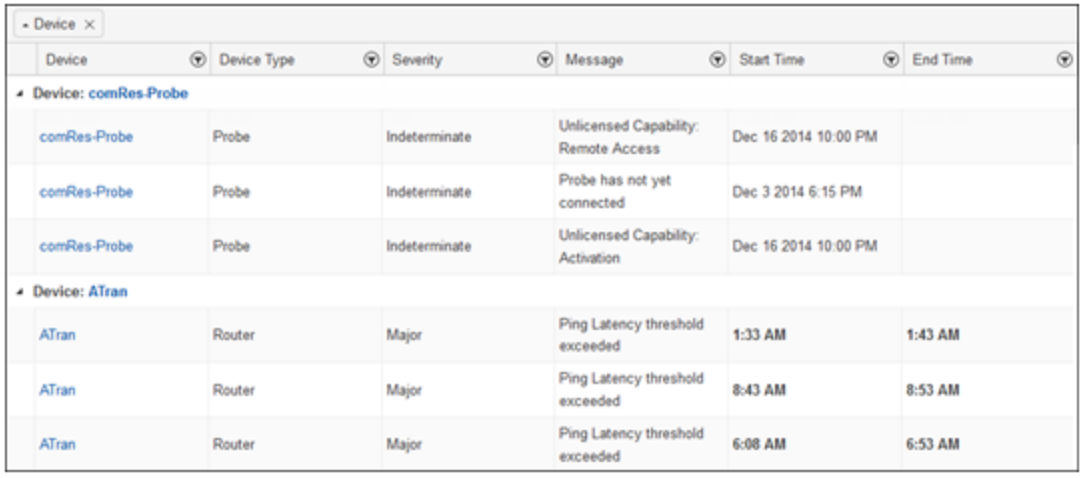
To group data, drag a column header to the row above the column headers.

For example to group the data by Device, do the following:

1. Drag the **Device** column header to the row above the column headers:

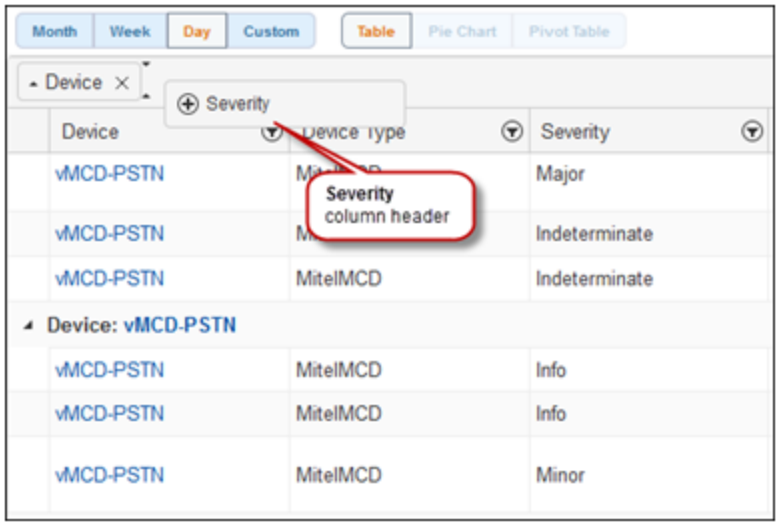


The data is rearranged as follows:

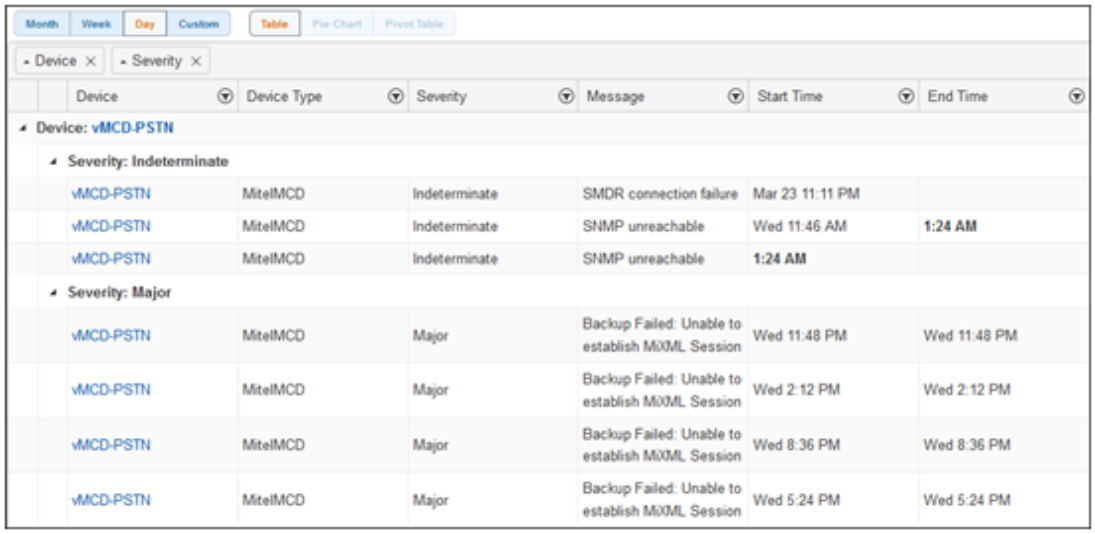


Groupings can be nested. For example, to further group by alarm severity, do the following:

1. Drag the **Severity** column header to the row above the column headers where the **Device** column heading is:

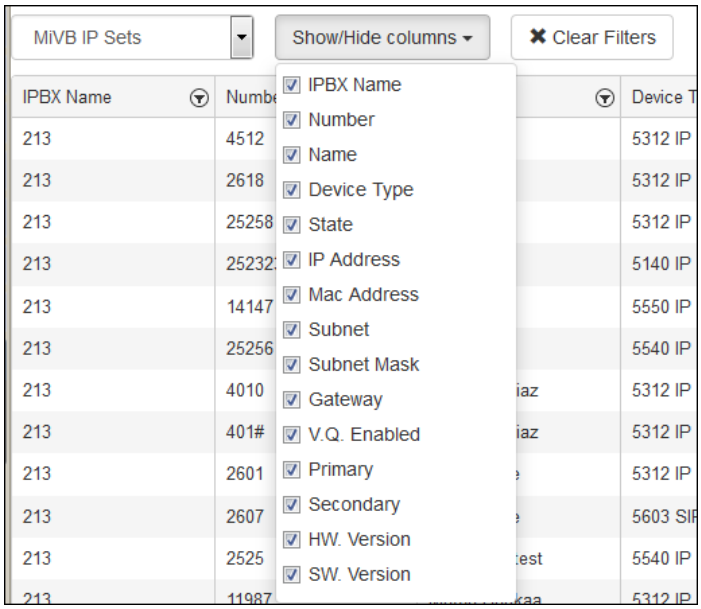


The data is rearranged as follows:



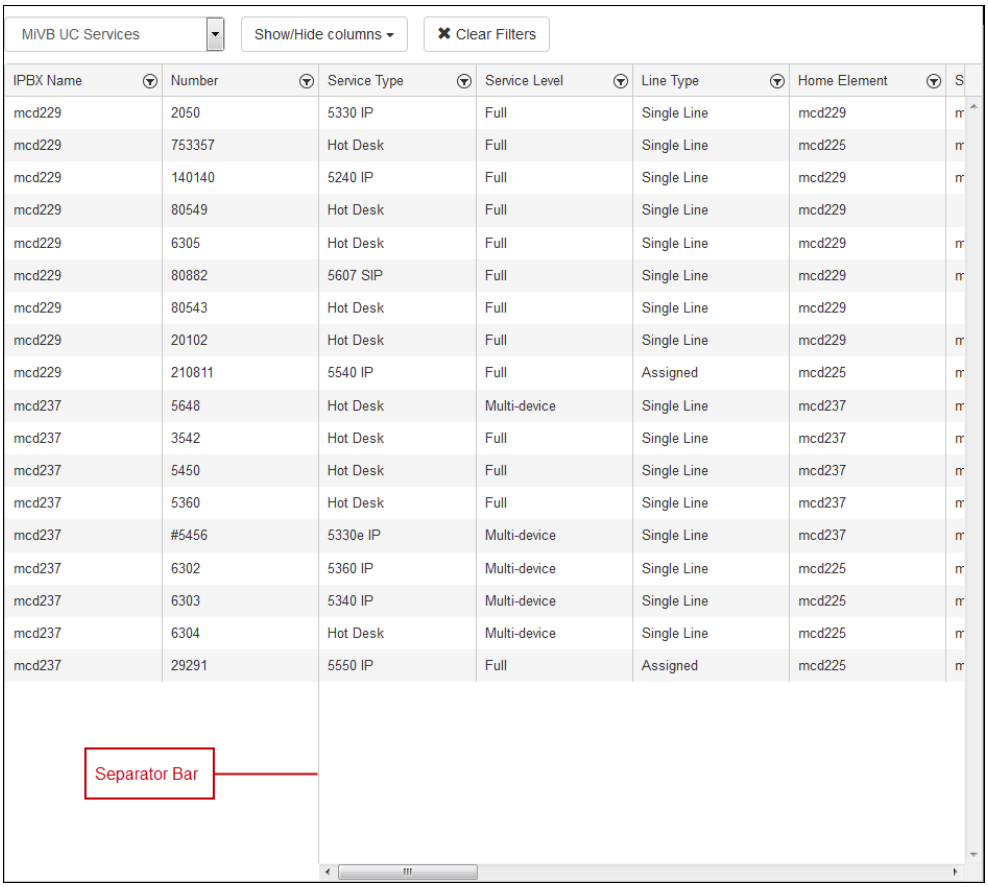
HIDING AND REARRANGING COLUMNS IN TABULAR QUERY RESULTS

Use the **Show/Hide Columns** button to remove unwanted columns.



Rearrange the column sequence by clicking the header of the column you want to move and dragging to the new location.

Some queries have a vertical bar that separates frozen columns from scrolling columns. Frozen columns are always displayed. Scrolling columns change as your use the scroll bar at the bottom. In the following example, the IPBX Name and the Number column are frozen while the other columns are scrolling columns.



To freeze a column, move it to the left of the vertical bar. To unfreeze it, move it to right of the vertical bar. When frozen columns apply, the query result must display at least one frozen column.

To reset the display, navigate away from the displayed query and perform a fresh query.

TABULAR RESULT NAVIGATION

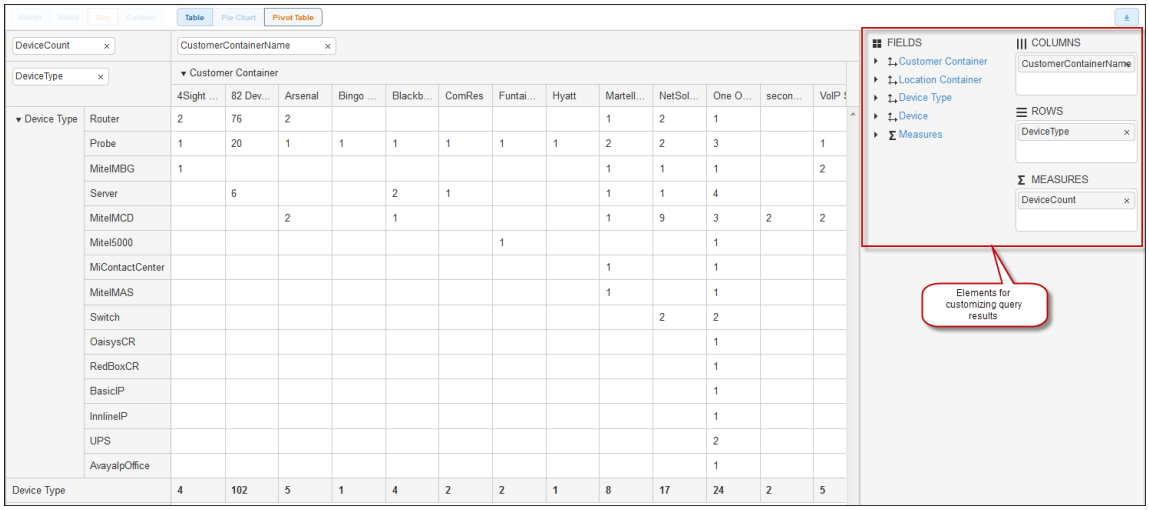
Where appropriate, query results contain pagination controls at the bottom of the screen.

The page navigation controls show you the current page being displayed and allows you to go to the first page, the previous page, the next page or the last page of the query.

The page size selector allows you to set how many items are displayed on each page.

PIVOT TABLE CUSTOMIZATION

The following is a typical **Inventory of Customer Devices** with results presented in a pivot table. Use the elements on the right of panel to customize the results.



REUSING CUSTOM VIEWS

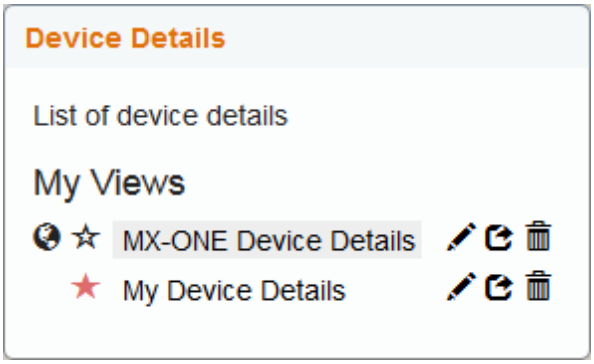
This functionality applies to the following queries only:

- Inventory queries:
  - Device Details
  - Inventory of Customer Devices
  - MiVoice MX-ONE Extensions
  - MiVoice Users, Services & Sets
- Alarm queries:
  - Container Alert Profiles
  - Critical Alarms by Device Type
  - Alarm Export

The following **View Management** buttons allow you to save any custom view you create with the functions described in "Query Output Formats" on page 82.

BUTTON	NAME	FUNCTION
	Save as	Displays the **Save View** dialog. Use this dialog to create a new view. Views are associated with the user who created them. You can always access your views regardless of the container you are working in.
	Save	Saves changes to the current view. Only the user who created it can modify a view.
	Delete	Deletes an existing view. Only the user who created it can delete a view

Views appear under the query they apply to. The following example shows two **Device Details** views. The **MX-ONE Device Details** view is shared, as indicated by the Globe ( ) icon. The **My Device Details** view is the default view for that type of query.



A view is owned by the user who created it. Only that user can modify or delete it. Views are associated with the container where the owner logs in. Views are shared with anyone who can access that container or any subcontainer. You can always access your views regardless of the container you are working in.

The following icons are associated with saved views:

ICON	NAME	FUNCTION
	Globe	Indicates that a view is shared
	Favorite	Indicates the default view
	Rename	Rename the view
	Share	Share the view.
	Unshare	Stop sharing the view.
	Trash	Delete the view..

CREATING A VIEW

Do the following steps:

1. Access a query and customize it as desired. See "Query Output Formats" on page 82.
2. Click on the **Save as** button. The **Save View** dialog is displayed.
3. Supply a new view name.
4. Click **OK**.

SAVING CHANGES TO AN EXISTING VIEW

Do the following steps:

1. Access the query you want to modify. Change it as desired. See "Query Output Formats" on page 82.
2. Click on the **Save** button. The **Confirm Action** dialog is displayed.

3. Click **Yes** to save the changes.

SHARING A VIEW

Do the following steps:

1. Access the query you want to share.
2. Click on the **Share** icon. The **Sharing Settings** dialog is displayed.
3. Select **Sharing Enabled**. The **Sharing Settings** dialog expands with a **Select Container** field.
4. Specify the container to associate to. The view will then be available to any user in the given container and its descendants.
5. Click **OK**.

EXPORTING CUSTOM VIEWS

All queries have the button described in the following table.

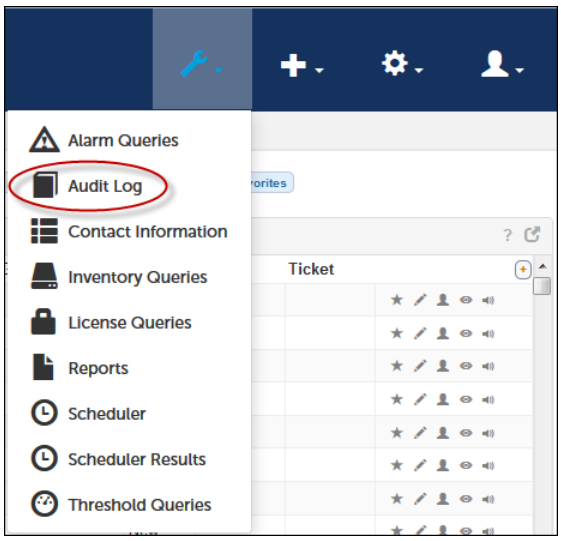
ICON	NAME	FUNCTION
	Export	Exports the view currently being displayed as a CSV file.

Do the following steps:

1. Access a query and customize it as desired. See "Query Output Formats" on page 82.
2. Click on the **Export** button. A CSV file containing the custom query data is downloaded to your machine.

AUDIT LOG

The audit log is accessed under the **Tools** icon, as follows:

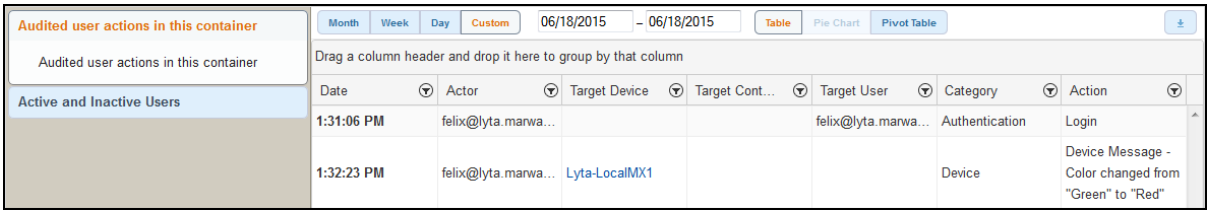


The audit log tracks the following activities:

- Login and other authentication
- Changes to any field of any container or device
- Remote access

As with other queries, Mitel Performance Analytics provides an initial set of audit log queries covering the past 24 hours, the past week, or the past month. You can also customize the duration of the audit log report.

The following is typical audit log for a particular day.



AUDIT LOG QUERIES

Mitel Performance Analytics provides the following initial set of audit log queries. Additional queries can be configured with the Reports menu item. Refer to "Generating Reports" on page 90.

QUERY NAME	DESCRIPTION
Active and Inactive Users	All of the users in this container and any subcontainers, and whether they are active or not. Active users have logged in within 30 days
Audited user actions in this container	All auditable user actions in this container and its content, including devices and subcontainers.

GENERATING REPORTS

You can choose to generate the following types of reports:

- Device reports
- Container reports
- Quick queries, including saved views

Device and container reports show performance, availability, and other data for devices over a period of time. The information is packaged into a PDF file and emailed to an individual.

Any quick query can be scheduled to occur at a regular interval. Query results are emailed to you as a CSV file. For the **MiVoice Business Users, Services & Sets** query an extra dropdown list allows you to specfity the report category: **Users**, **UC Services**, or **IP Sets**.

Reports and queries can be scheduled to run monthly, weekly or immediately.

Once you have specified the time span of the report, you can preview the report.

Generated reports are retained by Mitel Performance Analytics. You can download retained reports by clicking on the download icon ( ).

Mitel Performance Analytics requires Internet access for report generation. If this access is not possible, the reports are incomplete.

DEVICE REPORTS

Device reports include the following information about the device:

- Report date range
- Device information:
  - IP address
  - Check in time (if device is a Probe)
  - Associated Probe (if device is not a Probe)
- System information (if device is not a Probe):
  - Device name and description
  - Location
  - Contact
  - Uptime
- Version information
- Licensing information
- Alarms: List of major and critical alarms raised during the reporting period
- Availability:
  - Percentage of availability over the date range
  - Total Time: number of days the statistics compile
  - Availability as a percentage over 'Total Time'
  - Downtime: total system downtime over 'Total Time'
- Ping latency:
  - Latency displayed as milliseconds over a particular date range
  - Daily average in milliseconds
- Voice quality (if applicable for device):
  - Number of calls by voice quality (good, fair, poor, bad) over the reporting period
  - Call counts by voice quality over the reporting period
- Interface Availability (if applicable for device):
  - Availability per interface over the reporting period
  - Percentage availability per interface over the reporting period

CONTAINER REPORTS

Container reports summarize the following data about the container itself:

- Inventory: List of all devices in the container
- Device availability: List of devices that had service impacting events during the reporting period

- Alarms: List of all critical, major, minor and warning alarms during the reporting period
- Backup and Remote Access Summary: List of all devices in the container showing the number of backups, the number of locked backups, and the number remote access connection. If the container includes a Probe, it is listed with the other devices. Its number of remote access connections reflects connections to all the devices it manages, including those in other containers.

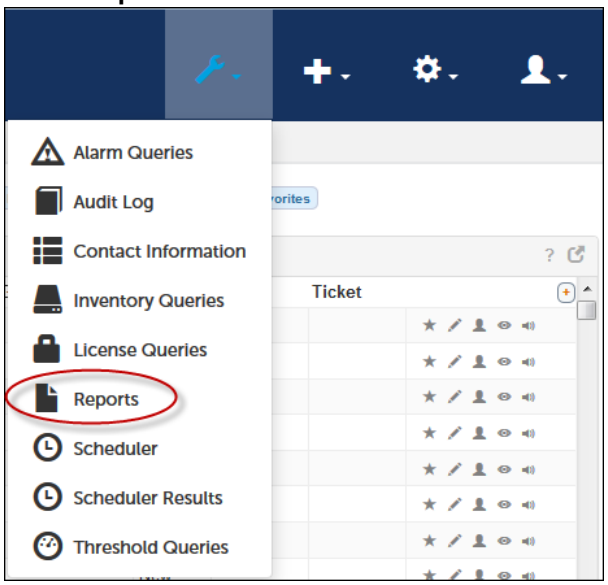
Container reports also collate the device reports for each device in the container.

Depending on what devices a customer has, specific report items may or may not be included.

REPORT GENERATION PROCEDURE

Do the following steps:

1. Select **Reports** under the **Tools** icon.



   The **Run & Schedule Reports** window is displayed.
2. In the **Run & Schedule Reports** window, specify the desired report properties.
   - **Report Type**: If the **Reports** menu item was selected from a container, this is **Container Report**. If it was selected from a device, this is **Device Report**.
   - **Recipient Email**: Specify the email address of the intended report recipient.
   - **Length of Report**: Specify the time span the report covers.
   - **Run**: Select **Now**, **Monthly**, or **Weekly**. For **Monthly**, specify the day of the month the report needs to be generated. For **Weekly**, specify the day of the week the report needs to be generated.
3. Click on the **Create Report** button.
4. If applicable, configure any email spam blockers to allow Mitel Performance Analytics email notifications. See "Email configuration" on page 69.

EXPORTING QUERIES AND REPORTS

Queries and reports can be downloaded as .csv files by clicking on the icon in top right corner of the panel.

MANAGING CONTAINERS

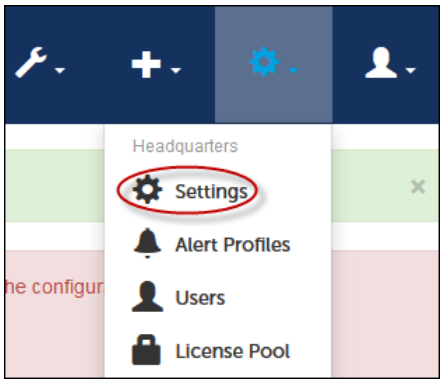
Containers are a key building block of how Mitel Performance Analytics monitors your network and generates reports. See "Mitel Performance Analytics System Data Model" on page 27 and "Planning Ahead" on page 31.

This chapter shows you how to manage and use your container structure in Mitel Performance Analytics.

CONFIGURING CONTAINERS

Do the following steps:

1. Access the container's dashboard and select **Settings** under the **Settings** icon.



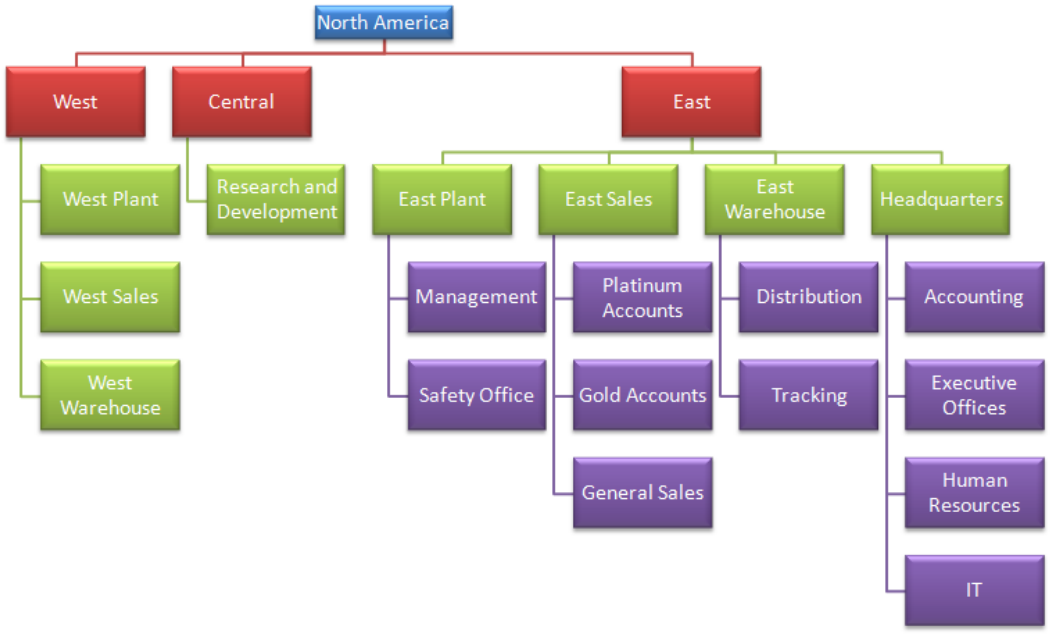
   The container's **Settings** page is displayed.
2. Supply a name for the container.
3. Under **Location**, optionally provide the GPS coordinates where the container is located. Alternatively, you can provide a street address and click on the **From Address** button. The GPS coordinates are determined based on the street address. The location data is used to populate the map in the top level container.
4. Under **Branding**, optionally customize the appearance of the dashboards and generated reports. See "Applying Branding" on page 98.
5. Under **Contact Information**, optionally supply information on who to contact for administrative support. The contact information appears as a banner on the container's dashboard.
6. Under **Container Type**, optionally specify the type of container. Containers can be of type **None**, **Customer**, **Reseller**, or **Location**. Container types are used for data queries or reports.
7. Under **Voice Quality**, optionally choose to have the container display Voice Quality (VQ) data.
8. Under **Container Message**, optionally specify a Message of the Day. The Message of the Day appears as a banner on the container's dashboard as well as the dashboards of all of its devices and subcontainers. See "Broadcasting a Message of the Day" on page 97.
9. Click on the **Save** button to implement the configuration.

MOVING A CONTAINER STRUCTURE

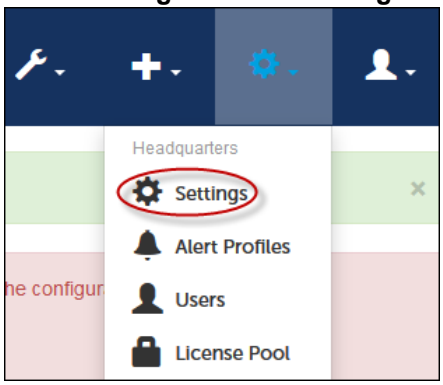
Moving a container applies to all objects that it contains, including users, devices, and subcontainers.

Do the following steps:

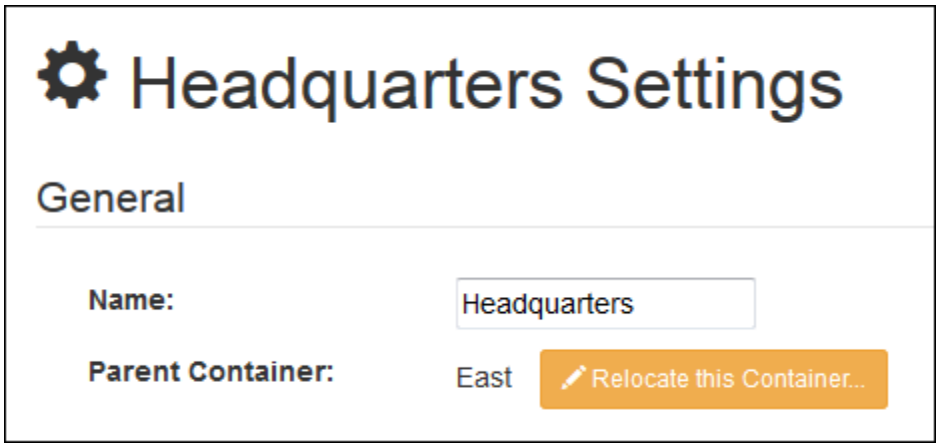
1. Access the dashboard of the container at the root of the structure you want to move. For example in the following structure, accessing the dashboard of the **Headquarters** container allows you to move the **Headquarters** container, its devices, its subcontainers, and all of their devices.



2. Select **Settings** under the **Settings** icon.

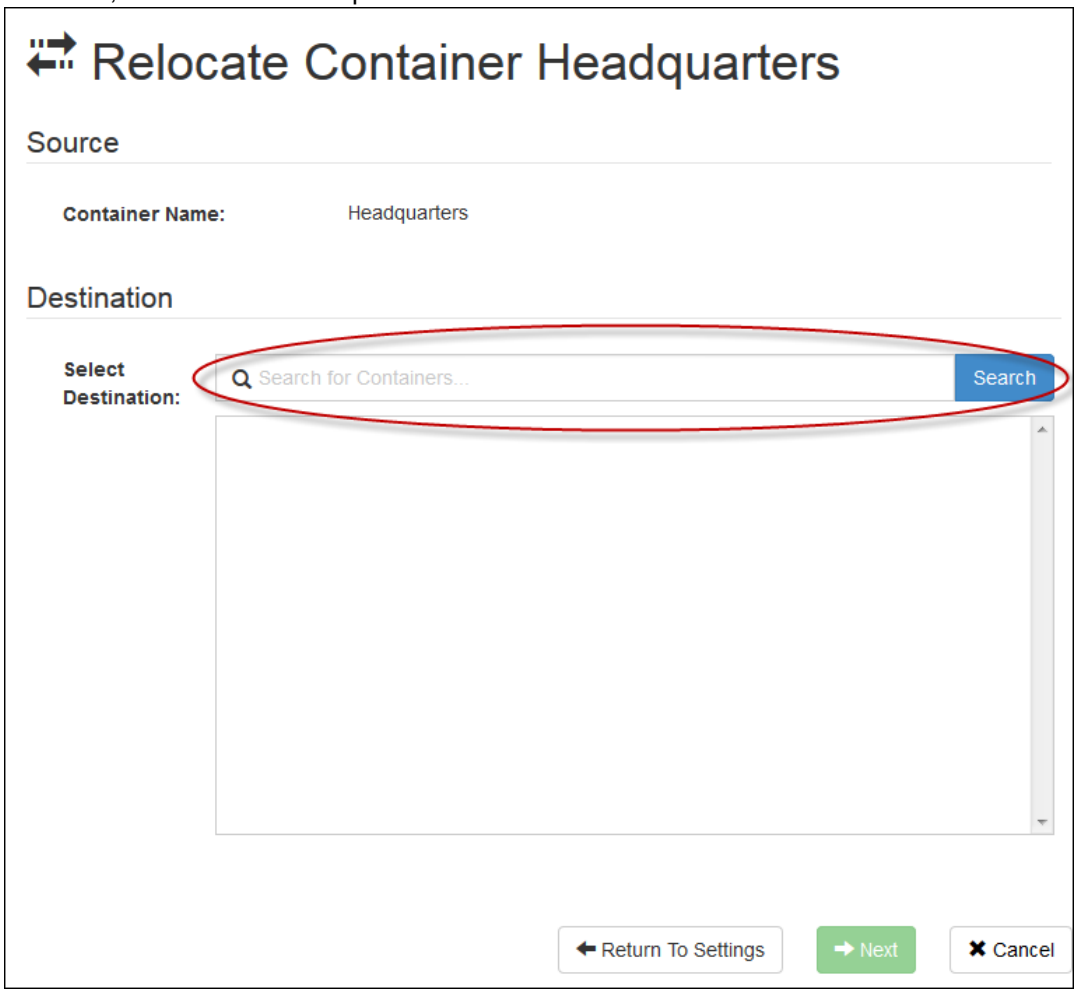


The container's **Settings** page is displayed.



Under **General**, the name of the container appears as well as its parent container. Click the **Relocate this Container…** button. The **Relocate Container** dialog appears.

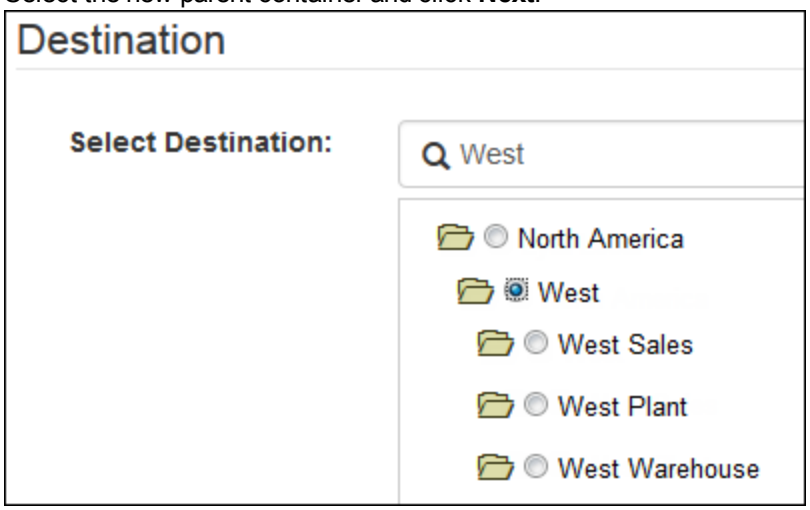
3. In the **Select Destination** field, enter either the full name or the partial name of the new parent container, and click **Search** or press **Enter**.



The **Relocate Container** dialog is populated with a destination container structure.

Note: The **Relocate Container** dialog does not display a destination container structure unless you click **Search** or press **Enter** after entering the full or partial name of the new parent container in the **Select Destination** field.

4. Select the new parent container and click **Next**.



The **Relocate Confirmation** dialog is displayed listing possible concerns associated with moving the container.

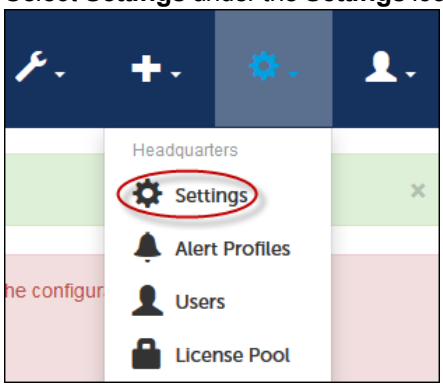
5. Select **Accept and continue** and click **Apply** to move the container. Licensing is automatically enforced on the moved container.

BROADCASTING A MESSAGE OF THE DAY

A container can be used to broadcast a Message of the Day. The Message of the Day appears as a banner on the container's dashboard as well as the dashboards of all of its devices and subcontainers.

Do the following steps:

1. Access the dashboard of the container at the root of the structure you want to broadcast the message to. For example in the previous figure, accessing the dashboard of the **Headquarters** container broadcasts the message to the **Headquarters** container, its devices, and all of its subcontainers and devices in the **Accounting**, **Executive Offices**, **Human Resources**, and **IT** subcontainers.
2. Select **Settings** under the **Settings** icon.



The container's **Settings** page is displayed.

3. Under **Container Message**, choose the background color for the banner.
4. Optionally specify a message title.
5. Provide the message to broadcast.
6. Click on the **Save** button to broadcast the message configuration.

APPLYING BRANDING

Containers can be used to customize the appearance of the dashboards and generated reports. Specifically, you can change:

- The logo that appears in the top left of dashboards and reports
- The name that appears besides the logo on dashboards and reports
- The color scheme of the dashboards

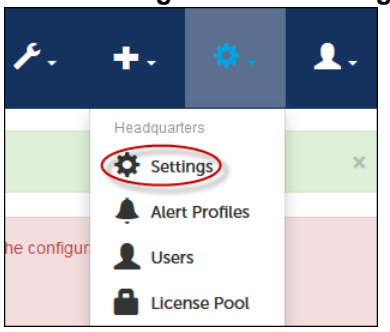
Branding changes apply to the dashboard of the container where they are implemented as well as to the dashboards of all of its devices and subcontainers.

The following restrictions apply to branding:

- Only cloud-based users can do branding changes.
- Only users defined for a container can change the branding settings for that container and its contents. See "Step 3 - Add Users" on page 45.
- Only users with the appropriate privileges can change the branding settings:
  - To change the logos and the brand name, users need **Branding** permissions. See "User Permissions" on page 46.
  - To change the color scheme of the dashboards, users need overall **System Admin** permissions.
- Logo files must be in PNG format.
- The low resolution image must be 180 x 50 pixels. The high resolution image must be 360 x 100 pixels. Mitel Performance Analytics selects which image to use depending on the display size.

Do the following steps:

1. Access the dashboard of the container at the root of the structure you want to apply the new branding. For example in the previous figure, accessing the dashboard of the **East** container and changing it branding affects the dashboards of the **East** container, its devices, its subcontainers, and all of their devices.
2. Select **Settings** under the **Settings** icon.



The container's **Settings** page is displayed.

3. Under **Branding**, select **Enable Custom Brand**.
4. Specify a brand name. The brand name is the name that appears besides the logo on dashboards and reports.
5. Use the **Browse** button to select a low resolution and a high resolution image.
6. Optionally supply the URL for a custom CSS. The CSS adds styles to the Mitel Performance Analytics CSS, allowing you to change branding colors used in the navigation bar, the sidebar and the page background.
7. Click on the **Save** button to implement the new branding.

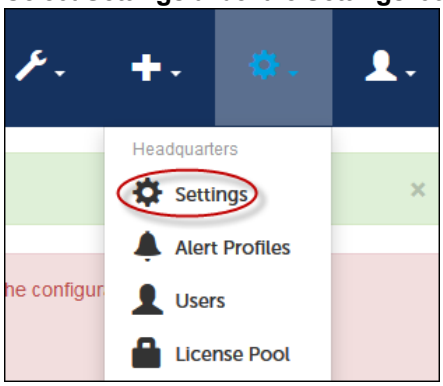
DELETING A CONTAINER

Deleting a container automatically deletes all of the devices that it contains.

You cannot delete a container if it has subcontainers. To delete a container structure, delete the individual containers starting from the bottommost container and continuing up the structure until you reach the root of the structure you want to remove.

Do the following steps:

1. Access the dashboard of the container you want to delete.
2. Select **Settings** under the **Settings** icon.



The container's **Settings** page is displayed.

3. Click on the **Delete** button at the bottom of the page. A confirmation dialog appears.
4. Click **OK** to delete the container and its devices. The display shifts to the dashboard of the parent container.

MITEL PERFORMANCE ANALYTICS LICENSING

LICENSING BASICS

Mitel Performance Analytics includes a licensing framework to enable tracking of purchased and authorized system capabilities. The licensing framework covers devices, software features, capacity and services.

License files are container specific and must be uploaded to the container that the license was generated for; typically the customer's root container.

LICENSE POLICY

Each Mitel Performance Analytics system can have a unique licensing policy. The licensing policy allows the system-licensing model to be customized by setting policies for:

- What requires licensing:
  - Devices
  - Features
  - User licenses or other countable items
- License duration – start and end dates
- Which licenses require or are fulfilled by other licenses
- Is a trial permitted for a specific feature
- What happens at license expiry or license violation

For details of the license policy that applies to a specific Mitel Performance Analytics system, contact your Mitel Performance Analytics support group.

LICENSABLE ITEMS

Depending on the Mitel Performance Analytics licensing policy, every device may require a license and may support additional optional licensable capabilities.

The following table summarizes the basic device licenses and additional items that can have licenses in Mitel Performance Analytics.

DEVICE	LICENSABLE ITEMS	LICENSE ENABLES
Probe	Activation	Configured device, use Probe for monitoring and remote access
	Basic IP SLA	Enable IP SLA on a Probe

DEVICE	LICENSABLE ITEMS	LICENSE ENABLES
Avaya IP Office	Monitoring / Users	Monitor device, license count ≥ number of users on IP Office System
	SMDR Collection	Enables SMDR collection for IP Office
	Set Inventory Monitoring	Enables set inventory monitoring for IP office
MiVoice Business	Monitoring / Users	Monitor device, license count ≥ number of IP users on MiVoice Business
		Enable standard VQ monitoring on MiVoice Business
		Enable SIP trunk and digital trunk utilization monitoring on MiVoice Business
	Backup	Device feature: Allows authorised administrators to add MiVoice Business to a backup schedule
	On-demand Backup	Container feature: If the container is licensed, users can run on-demand backups on each MiVoice Business
	IP Set Inventory Monitoring	Enable inventory monitoring for IP sets on MiVoice Business
	Advanced User Operations	Simplifies and reduces the time that it takes to complete the following MiVoice Business tasks: • Moving a user from one MiVoice Business to another one • Removing a User • Setting up and managing Busy Lamp Field (BLF) keys
	SMDR Collection	Enable SMDR collection from MiVoice Business
MiVoice Office 250	Monitoring / Users	Monitor device, license count ≥ number of users on MiVoice Office 250
	SMDR Collection	Enables SMDR collection from MiVoice Office 250
MiCollab	Monitoring	Monitor device

DEVICE	LICENSABLE ITEMS	LICENSE ENABLES
MiVoice MX-ONE	Monitoring	Monitor device
	Extension And Terminal Inventory	Device feature: Enables the collection of extensions, users and terminals inventory from MX-ONE
	Route And Gateway Utilization	Device feature: Enables collection of route utilization and gateway utilization
	Backup	Device feature: Allows authorised administrators to add MX-ONE to a backup schedule
	On-demand Backup	Container feature: If the container is licensed, users can run on-demand backups on each MX-ONE
MiVoice Border Gateway	Monitoring	Monitor device
	Count of Teleworker Standard VQ Sets	Monitor device, license count ≥ number of teleworker set licenses on MiVoice Border Gateway
Server	Monitoring	Monitor device
Router	Monitoring / Count of Number of Router Ports	Monitor device, license count ≥ number of ports on router
	IP COS	Enable IP COS monitoring on router
Switch	Monitoring / Count of Number of Switch Ports	License count ≥ number of ports on switch
Path Solutions	Monitoring	Monitor device
UPS	Monitoring	Monitor device
MiContact Center Business, all editions	Monitoring	Monitor device
MiVoice Call Recorder	Monitoring	Monitor device

DEVICE	LICENSABLE ITEMS	LICENSE ENABLES
Red Box Call Recorder	Monitoring	Monitor device
Innovation InnLine Voicemail	Monitoring	Monitor device

Some licensing entitlement is based on the total count of IPT users. See "Aggregate Licensing and IPT Users" on page 104 for details.

LICENSE FILES

Mitel provides license files to enable devices and capabilities. A license file contains one or more license records. A license record contains license elements.

License Record

A Mitel Performance Analytics license record contains a number of data elements that define how and when a license can be used by Mitel Performance Analytics. A license is assigned to a target, typically a container. Multiple licenses can be assigned to a single target.

License Elements

A Mitel Performance Analytics license record contains a number of data elements that define how and when a license can be used by Mitel Performance Analytics. The following table describes license elements.

ELEMENT NAME	DESCRIPTION
Globally Unique ID (GUID)	This is a unique identifier assigned by Mitel to each license record.
PO Number	This is an optional field that can be used to include PO information for a license record.
Scope	This element specifies the Mitel Performance Analytics system to which a license record can be assigned.
Category	This element is the broadest definition for a license. Categories include **Device**, **Capability** and **Capacity**.
Target	This element specifies what the license can be assigned to. Targets include the Mitel Performance Analytics device types.
Type	This element provides additional information on the license. Types include **Device**, **Digital Trunk**, **IP COS**, and others.

ELEMENT NAME	DESCRIPTION
Count	This element defines the number of individual countable items that a license includes. Only certain licenses include **Count**. These licenses are generally in the **Capacity** category. Typical license counts are **10**, **50**, and **100**.
Start Date	This element specifies the earliest date that a license is valid.
End Date	This element specifies latest date that a license is valid.
Transferable	This element specifies whether or not a license can be transferred between different devices or targets. If a license is transferable, it can be unassigned from its original target and reassigned. If a license is non-transferable, it can be assigned only once.
Signature	This element is a cryptographically secure hash generated by Mitel to verify that a license has not been altered or corrupted in transmission. The system does not accept licenses with a signature that is determined to be invalid.

AGGREGATE LICENSING AND IPT USERS

Mitel Performance Analytics devices automatically contact their parent containers to acquire licenses. If their parent container does not have a license for them, then they contact the next higher container in the hierarchy until the root container is reached.

Licensing for some device capabilities is based on the total count of IPT users. For example, if a container has a MiVoice Business call server configured for 1,000 IP users, a second MiVoice Business call server configured for 500 IP users, and a MiVoice Border Gateway configured for 100 IP users, then the container can be loaded with 1,600 licenses.

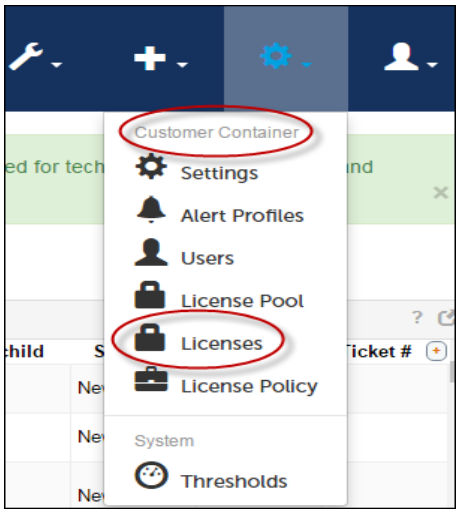
The container licenses are flexible. Licenses that are assigned to a container are available to any of the devices in the container. In the previous example, if the first MiVoice Business call server is reconfigured to have just 800 IP users, then 200 licenses are free to be applied against the second MiVoice Business call center or MiVoice Border Gateway.

Use the **IPT Users Inventory** query to determine the number of licenses you need. For details see "Inventory Queries" on page 79.

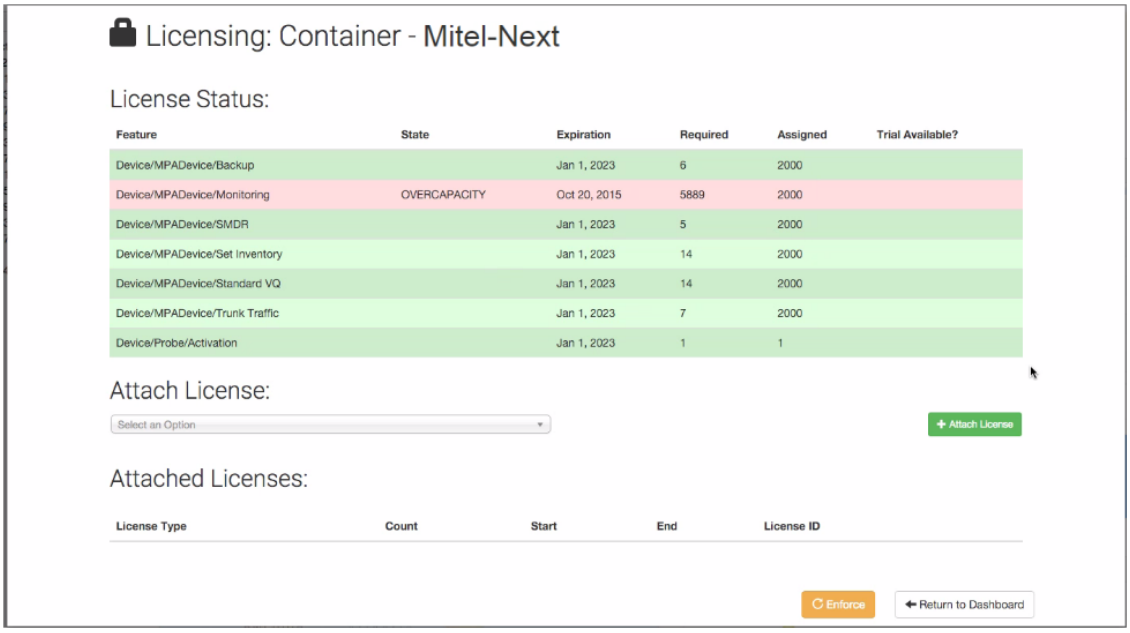
LICENSING STATUS AND OVERCAPACITY

Use the following procedure to verify licensing status and see if the total demand for licenses for IPT users exceeds the amount of licenses assigned to a container:

1. Access the dashboard of the container where the licenses have been assigned. Typically, this is the customer's root container.
2. From the dashboard, select **Licenses** under the **Settings** icon.



The **Licensing** window is displayed.



Line items in red indicate licensing issues that need to be resolved.

If the total demand for licenses for IPT users exceeds the amount of licenses assigned to a container, the line item state is **OVERCAPACITY**.

In the previous example:

- The IPT users require 5,889 licenses, but only 2,000 have been assigned to the container.
- The Expiration Date shows when the overcapacity event occurred.
- Services continue to be provided, but the 60-day grace period has begun.

To correct the overcapacity issue and ensure services continue, you must purchase additional licenses.

Once additional licenses have been purchased, uploaded to Mitel Performance Analytics, and assigned to the container, the license status returns to green and the expiration date returns to January 1, 2023.

CONTAINER GUID

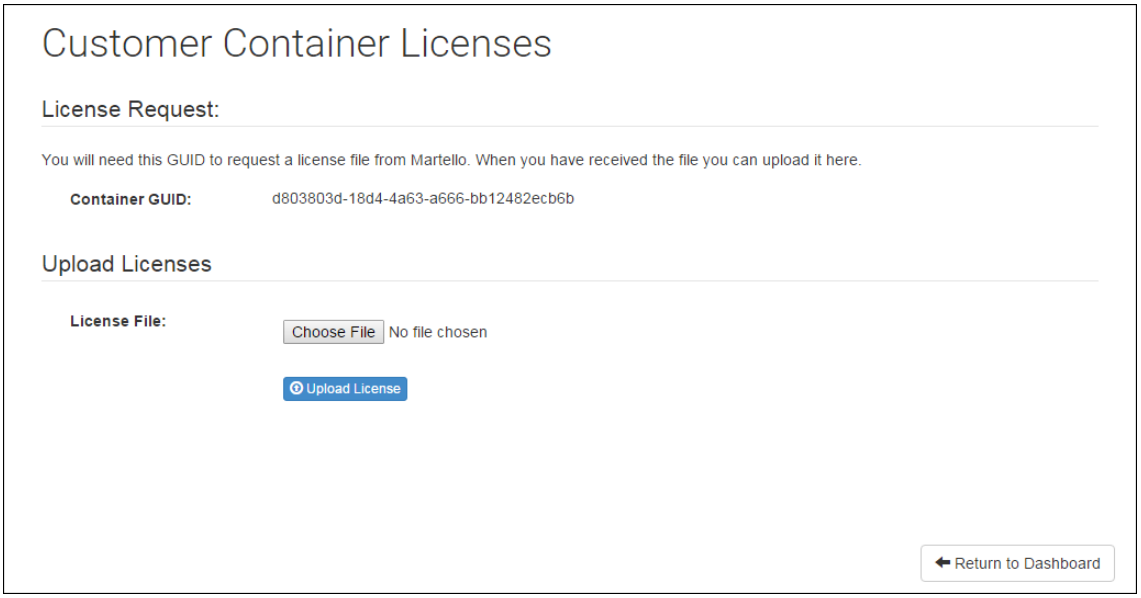
Mitel Performance Analytics licenses are tied to a globally unique identifier (GUID) for each Mitel Performance Analytics system container.

If you do not use online licensing, you need to provide this GUID as part of the license order process so that license can be created for your system.

To find your system GUID:

1. Log in as a user with System Administration privileges.
2. Navigate to the root Mitel Performance Analytics container.
3. Click on the **Settings** icon.
4. Select the **License Pool** menu item.

The resulting window displays the GUID for the container. The following is an example.



In this example, the container GUID is d803803d-18d4-4a63-a666-bb12482ecb6b.

UPLOADING A POLICY FILE

If you do not use online licensing, you need to manually install an updated license policy file.

Do the following steps:

1. Log in as a user with System Administration privileges.
2. Navigate to the root Mitel Performance Analytics container.
3. Click on the **Settings** icon.
4. Select the **License Policy** menu item.

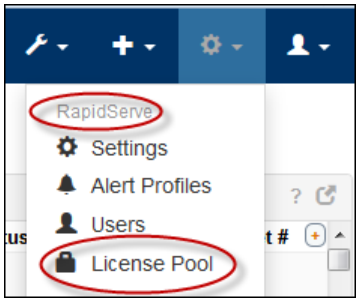
5. Click **Choose File** and navigate to the new policy file.
6. Click **Upload Policy File**.

UPLOADING A LICENSE FILE

If you do not use online licensing, you need to manually upload license files to Mitel Performance Analytics.

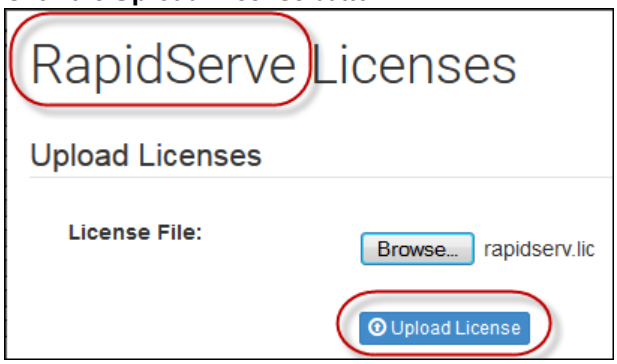
Do the following steps:

1. Access the dashboard for the container that the license was generated for. Typically this is the customer's root container.
2. From the container dashboard, select **License Pool** under the **Settings** icon.



The **Licenses** window for that container is displayed.

3. Click the **Browse** button. Navigate to the license file and select it.
4. Click the **Upload License** button.



If there is a problem, such as loading duplicate or invalid licenses, the **Licenses** window provides feedback to indicate the issue.

Once the licenses have been uploaded, the **Licenses** window provides information on the licenses that have been uploaded.

ASSIGNING A LICENSE

If you do not use online licensing, you need to manually assign license after the license file is uploaded to Mitel Performance Analytics. Licensing is applied differently depending on the type of device.

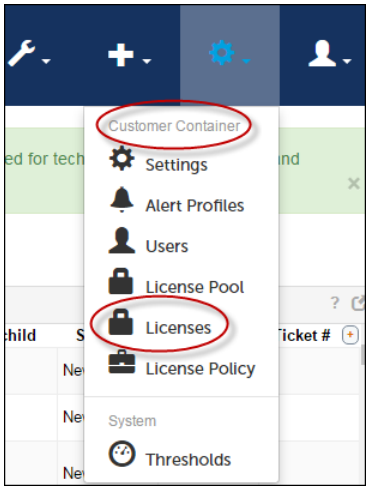
Some licensing is based on the total count of configured IPT users. Licensing for other devices is based on the total count of the device type.

You can assign a block of licenses to a container or a sub-container that has devices that need licensing. This is typically the customer's root container.

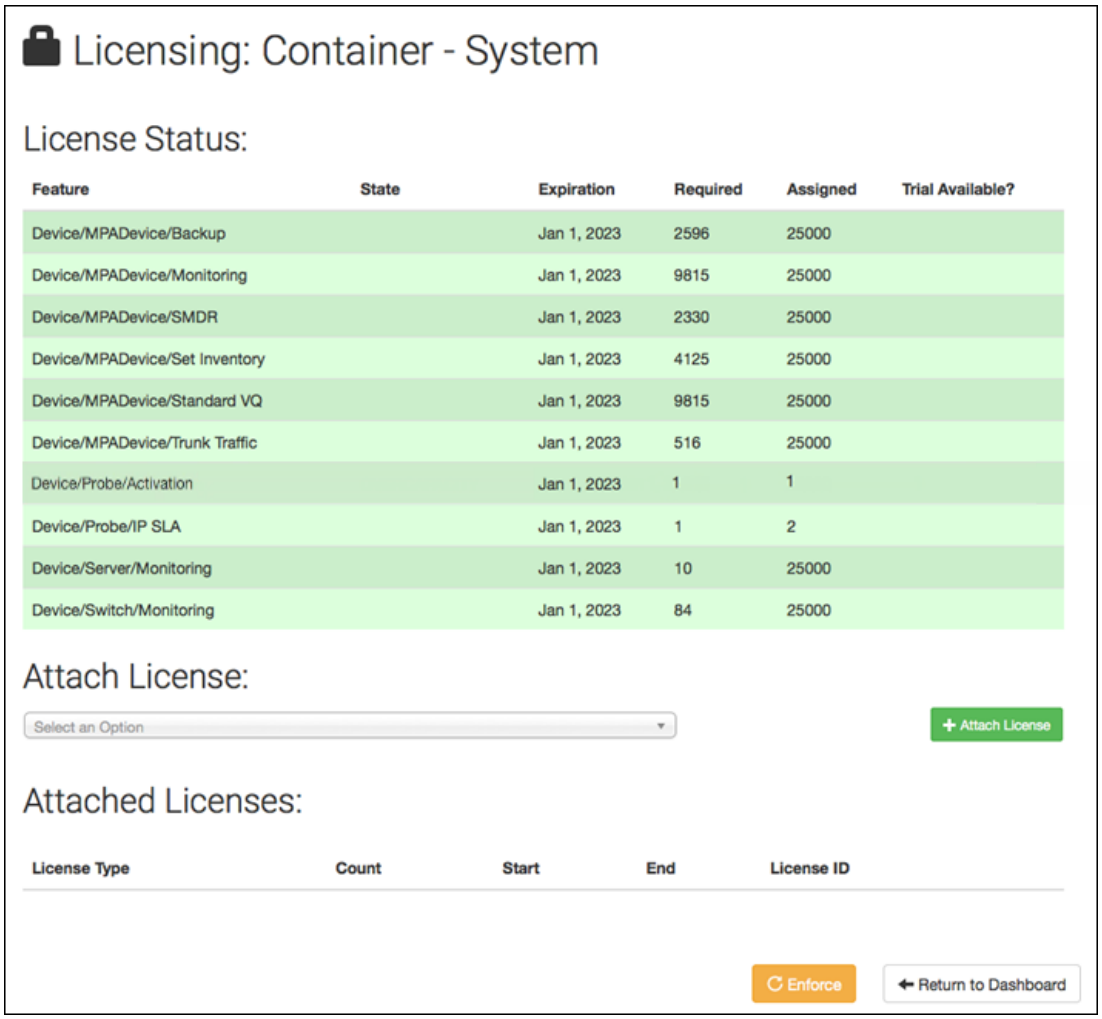
Devices automatically contact their parent containers to acquire licenses. If their parent container does not have a license for them, then they contact the next higher container in the hierarchy until the root container is reached.

Do the following steps:

1. Access the dashboard for a container requiring licensing.
2. From the dashboard, select **Licenses** under the **Settings** icon.



The **Licensing** window is displayed. The following is an example.



The top part indicates the status of the licenses for this container. The middle part allows you to attach more licenses. The bottom part lists the currently attached licenses.

3. From the dropdown list, select one of the available licenses.
4. Click the **Attach License** button.
5. If the license is non-transferable, a confirmation dialog box appears. Non-transferable licenses cannot be reassigned to other devices. Confirm your intent.
   If successful, the licensing window confirms that the license has been assigned by listing it in the bottom part of the window.

   The license is automatically enforced.

If multiple licenses are required then repeat the license assignment process as necessary.

EXPIRED LICENSES

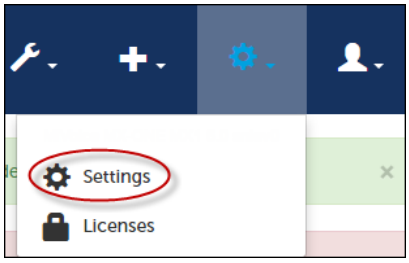
Expired licenses are normally hidden on the **Licensing** panel. If any licenses are hidden, you can click a button to display them under **Attached Licenses**.

LICENSE REPORTING

For information on license reporting, see "License Queries" on page 80 and "Generating Reports" on page 90.

CONFIGURING MITEL PERFORMANCE ANALYTICS DEVICES

Device configuration is managed by specifying settings on the device settings sheet. To display the device properties sheet, select **Settings** under the **Settings** icon of the dashboard for the particular device, as follows:



To add a device, see "Step 4 - Add Devices" on page 47.

COMMON OPTIONS

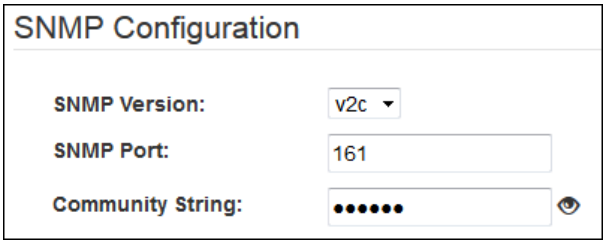
The following configuration options are common to most devices:

- **Device name**: Used for device identification on Mitel Performance Analytics dashboards.
- **Probe**: Probed used to monitor the device.
- **Description field**: Descriptive text that is displayed in the Device Information panel.
- **IP address**: Used to communicate with the device.
- **Fault and performance monitoring**: Enables monitoring by Mitel Performance Analytics.
- **Ping DSCP**: Sets Differentiated Services Code Point (DSCP) settings so that Ping packets more closely mimic real VoIP traffic. You can choose from **Best Effort (0)**, **High Priority (46)**, or a variety of Assured Forwarding (AF) or Class Selector (CS) settings.
- **SNMP configuration**: Used to gather event data from the device. See "SNMP Configuration" on page 111.
- **Interface filters**: Used to focus or clarify data about the device interfaces. See "Interface Filter Configuration" on page 113.
- **Maintenance mode**: While in maintenance mode, Mitel Performance Analytics provides only minimal monitoring of the device. This setting is useful to isolate a device with known issues so its alarms do not clutter the monitoring data of the rest of the network.
- **Device Message**: Settings for a message banner that appears on the device dashboard. Users can specify the banner color, message title, and message text.

SNMP CONFIGURATION

Mitel Performance Analytics supports SNMP v1, v2C, and v3 for retrieval of device information. The configuration options are different for SNMP v1 and v2C, and for SNMP v3.

The following is a typical settings sheet area for SNMP v1 or v2C configuration:



SNMP v1 and v2C use a community string to authenticate SNMP requests.

Mitel Performance Analytics allows configuration of the following:

- Community string (common default is “public”)
- SNMP port (standard port is 161)

SNMP v3 supports a user-based security model that enables:

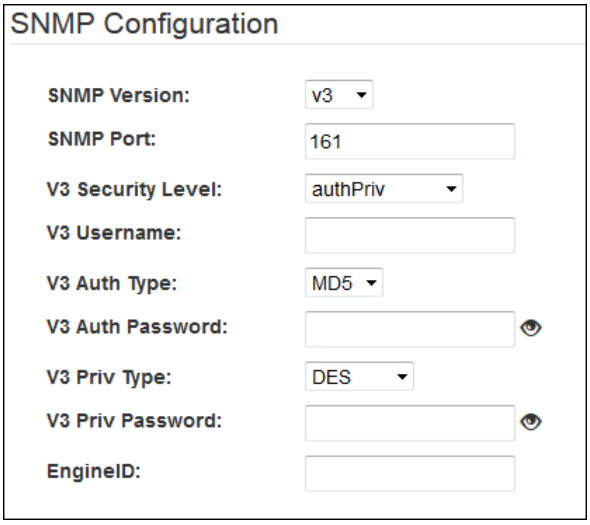
- No authentication or encryption
- Authentication only
- Authentication with encryption (also referred to as Privacy)

Authentication options are MD5 and SHA.

Encryption options are DES and AES128.

Certain SNMPv3 devices require that the SNMP agent requesting information use a specified engine ID.

The following is a typical settings sheet area for SNMP v3 configuration:



Mitel Performance Analytics SNMP v3 configuration options allow you to specify:

- **SNMP port** (standard port is 161)

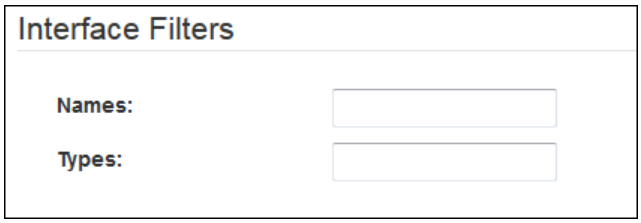
- **V3 security level**: One of the following:
  - NoAuthNoPriv — no security, not recommended
  - Auth — Authentication only
  - AuthPriv – Authentication and encryption (Privacy), recommended
- **V3 authentication type**: MD5 or SHA
- **V3 authentication password**: Required for authentication
- **V3 privacy type**: DES or AES128
- **V3 privacy password**: Required for privacy
- **EngineID**: Leave blank in most cases; certain SNMPv3 agents may require this to be specified

INTERFACE FILTER CONFIGURATION

Mitel Performance Analytics interface filtering allows you to select interfaces for monitoring. Some devices have multiple interfaces or ports, but only need monitoring for a small number of them (for example, WAN interfaces and MiVoice Business RTC ports).

On the device settings sheet, specify the interface name(s) and/or type(s) that you want to monitor. Note that this feature removes data collection and display from all interfaces except those specified.

The following is a typical settings sheet area for interface filtering configuration:

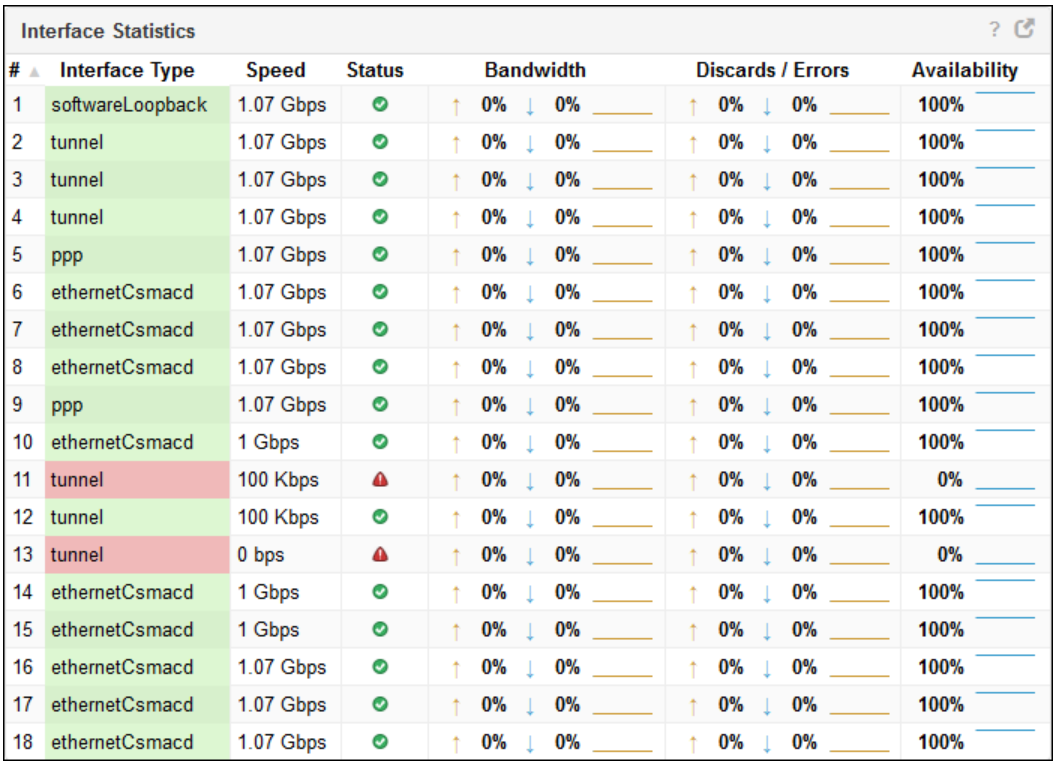


To filter by interface name, enter the Network Interface name(s) into the **Names** field. Multiple names can be entered by using commas to separate them. Sample names are **eth0** and **(Internal port) RTC's PowerPC to SW (1)**.

To filter by interface type, enter the Network Interface type(s) into the **Types** field. Multiple types can be entered using commas to separate them. Sample types are **ppp** and **ethernetCsmacd**.

Note: Changes in interface filtering may not be reflected immediately in dashboard views. Allow a few minutes for the dashboard to refresh with new data. Also, the web browser cache settings may delay the dashboard refresh. Clear the browser cache to ensure the dashboard displays the latest interface data.

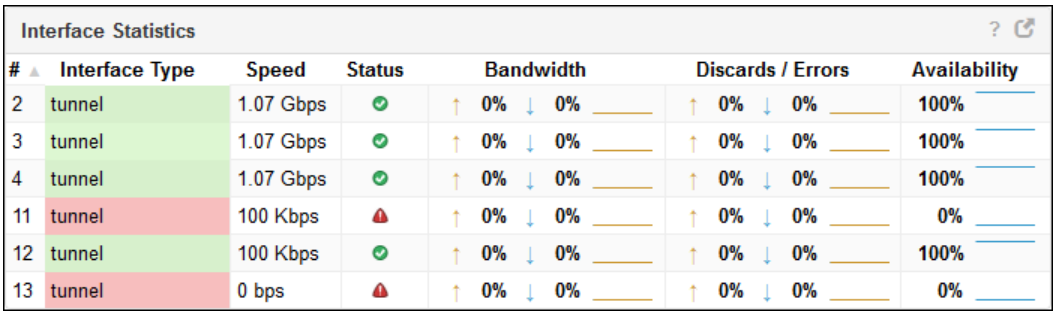
The following example shows the **Interface Statistics** panel for a server with multiple interfaces without interface filtering:



Interface Statistics

#	Interface Type	Speed	Status	Bandwidth	Discards / Errors	Availability
1	softwareLoopback	1.07 Gbps		↑ 0% ↓ 0%	↑ 0% ↓ 0%	100%
2	tunnel	1.07 Gbps		↑ 0% ↓ 0%	↑ 0% ↓ 0%	100%
3	tunnel	1.07 Gbps		↑ 0% ↓ 0%	↑ 0% ↓ 0%	100%
4	tunnel	1.07 Gbps		↑ 0% ↓ 0%	↑ 0% ↓ 0%	100%
5	ppp	1.07 Gbps		↑ 0% ↓ 0%	↑ 0% ↓ 0%	100%
6	ethernetCsmacd	1.07 Gbps		↑ 0% ↓ 0%	↑ 0% ↓ 0%	100%
7	ethernetCsmacd	1.07 Gbps		↑ 0% ↓ 0%	↑ 0% ↓ 0%	100%
8	ethernetCsmacd	1.07 Gbps		↑ 0% ↓ 0%	↑ 0% ↓ 0%	100%
9	ppp	1.07 Gbps		↑ 0% ↓ 0%	↑ 0% ↓ 0%	100%
10	ethernetCsmacd	1 Gbps		↑ 0% ↓ 0%	↑ 0% ↓ 0%	100%
11	tunnel	100 Kbps		↑ 0% ↓ 0%	↑ 0% ↓ 0%	0%
12	tunnel	100 Kbps		↑ 0% ↓ 0%	↑ 0% ↓ 0%	100%
13	tunnel	0 bps		↑ 0% ↓ 0%	↑ 0% ↓ 0%	0%
14	ethernetCsmacd	1 Gbps		↑ 0% ↓ 0%	↑ 0% ↓ 0%	100%
15	ethernetCsmacd	1 Gbps		↑ 0% ↓ 0%	↑ 0% ↓ 0%	100%
16	ethernetCsmacd	1.07 Gbps		↑ 0% ↓ 0%	↑ 0% ↓ 0%	100%
17	ethernetCsmacd	1.07 Gbps		↑ 0% ↓ 0%	↑ 0% ↓ 0%	100%
18	ethernetCsmacd	1.07 Gbps		↑ 0% ↓ 0%	↑ 0% ↓ 0%	100%

The following is the same panel with interface filtering enabled for **tunnel**.



Interface Statistics

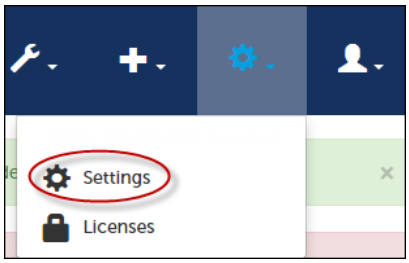
#	Interface Type	Speed	Status	Bandwidth	Discards / Errors	Availability
2	tunnel	1.07 Gbps		↑ 0% ↓ 0%	↑ 0% ↓ 0%	100%
3	tunnel	1.07 Gbps		↑ 0% ↓ 0%	↑ 0% ↓ 0%	100%
4	tunnel	1.07 Gbps		↑ 0% ↓ 0%	↑ 0% ↓ 0%	100%
11	tunnel	100 Kbps		↑ 0% ↓ 0%	↑ 0% ↓ 0%	0%
12	tunnel	100 Kbps		↑ 0% ↓ 0%	↑ 0% ↓ 0%	100%
13	tunnel	0 bps		↑ 0% ↓ 0%	↑ 0% ↓ 0%	0%

PROBE CONFIGURATION

A single Probe enables monitoring of multiple devices on the same IP network. If the container in which the Probe is added contains subcontainers, the Probe can monitor the devices in the subcontainers also.

Do the following steps:

1. Access the Probe's dashboard.
2. From the Probe's dashboard, select **Settings** under the **Settings** icon.

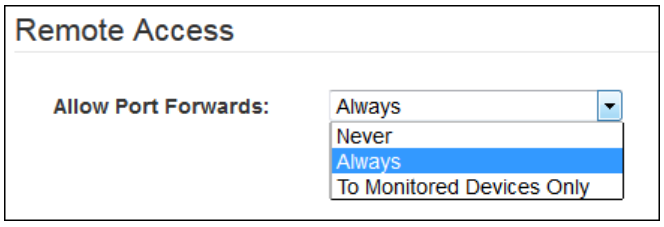


The Probe properties sheet is displayed.

3. Edit and change property settings as required. In addition to general settings available to all Mitel Performance Analytics device, Probe settings include:
   - **IP SLA Monitoring**: Enable the checkbox and enter up to four IP SLA targets, specifying either the target IP address or their FQDN. For each target, you can specify Differentiated Services Code Point (DSCP) settings. You can choose from **Best Effort (0)**, **High Priority (46)**, or a variety of Assured Forwarding (AF) or Class Selector (CS) settings.
   - **Probe Diagnostics**: Enabling these settings displays additional diagnostic tools. The tools should be used and interpreted with assistance from Mitel support.
   - **Probe Software Override JAR URL** field: This field is used for troubleshooting purposes. It allows for installation of special software. It is used only with assistance from Mitel support.
   - **Probe Password**: This setting appears only when you have the **Probe Installer** administrative permission. When a Probe is first added to Mitel Performance Analytics, Mitel Performance Analytics generates a random security password for Server to Probe communications. Afterwards, when the Probe is installed, it is automatically configured to use this password. At this stage, when first adding a Probe but before it is installed, users may choose to replace the random password with their own. The security password can contain only alphanumeric characters. Spaces or other special characters cannot be used. Changing the password after the Probe is installed and configured is not recommended because it disables Server to Probe communications.
   - **Remote Access Control**: See "Remote Access Control Configuration" on page 115.
4. Click the **Save** button when done.

REMOTE ACCESS CONTROL CONFIGURATION

Mitel Performance Analytics allows remote access controls on the Probe settings sheet. The following is a typical settings sheet area for interface filtering configuration:



Users can configure the Probe to:

- Never allow port forwarding, thereby blocking all remote access capabilities
- Allow port forwarding only to those devices monitored by the Probe
- Allow port forwarding for all devices on the subnet the Probe is connected to, thereby allow remote access to devices not monitored by the Probe

Permissive Port Forwarding

By default, users can remotely access a device only if they have Remote Access permission for both the device and the Probe monitoring it. The **Permissive Port Forwarding** option allows a user to remotely access a device if they have Remote Access permission for the device, but not for the Probe monitoring it.

Before enabling this option, consider carefully why you denied the user Remote Access for Probe. By enabling this option, the user can access the Probe's network environment and could harm it.

Disabling this option does not terminate existing Remote Access sessions. To terminate existing Remote Access sessions, use the Probe's **Port Forwards** panel.

MIVOICE MX-ONE DEVICE CONFIGURATION

To add a MiVoice MX-ONE device to Mitel Performance Analytics, you need the following information:

- IP address of the MiVoice MX-ONE device
- SSH username and password for the MiVoice MX-ONE server
- SNMP configuration information, including the SNMP community string used for SNMP Gets and Traps

MIVOICE MX-ONE SSH ACCESS CONFIGURATION

Mitel Performance Analytics uses the SSH CLI to retrieve information from the MiVoice MX-ONE. You should create a limited privileges account on the MiVoice MX-ONE for use by the Mitel Performance Analytics system. This account requires at least snlev0 privileges for normal operation. To enable scheduled and on-demand backups, this account must also be part of the **eri_sn_d** and **ldap** groups.

Ensure that the SSH login information configured on Mitel Performance Analytics matches the credentials required for the MiVoice MX-ONE SSH account.

MIVOICE MX-ONE SNMP CONFIGURATION

SNMP must be properly configured on the MiVoice MX-ONE server for correct operation with Mitel Performance Analytics.

To verify the SNMP configuration on the MiVoice MX-ONE:

1. Open the **snmpd.conf** file with the following command:
   `sudo vi /etc/snmp/snmpd.conf`

   The content of the file is displayed. The following is an example:

```
# Please see /usr/share/doc/packages/net-snmp/EXAMPLE.conf for a
# more complete example and snmpd.conf(5).
```

```
#
# Writing is disabled by default for security reasons.  If you'd like
# to enable it uncomment the rwcommunity line and change the community
# name to something nominally secure (keeping in mind that this is
# transmitted in clear text).

# don't use ' < > in strings for syslocation or syscontact
# Note that if you define the following here you won't be able to
change
 them with snmpset
syslocation Server Room
syscontact Sysadmin (root@localhost)

# These really aren't meant for production use.  They include all MIBS
# and can use considerable resources.  See snmpd.conf(5) for
information
# on setting up groups and limiting MIBS.
rocommunity public
# rwcommunity mysecret 127.0.0.1
# MX-ONE alarm traps uses agentx protocol
master agentx
AgentXSocket localhost:705
# MX-ONE alarm traps can trigger snmptrapd to sent mail and
textmessages
# trapcommunity: Default trap sink community to use
trapcommunity public
# trap2sink: A SNMPv2c trap receiver
trap2sink 172.16.1.222
```

2. Verify the **rocommunity** setting and the **trapcommunity** setting. In the previous example, they are highlighted in bold. Ensure both the rocommunity and trapcommunity values are the same and set to public. Ensure that Mitel Performance Analytics is configured with this value.
3. Ensure that at least one **trap2sink** destination value is set to the IP address of the Mitel Performance Analytics Probe that is used to monitor the MiVoice MX-ONE server. In the previous example, it is highlighted in bold.

CONFIGURING MX-ONE HANDSETS FOR SIP VOICE QUALITY MONITORING

Mitel Performance Analytics uses voice quality reports sent by Mitel SIP handsets. The SIP handsets must be configured to send the voice quality reports to the Mitel Performance Analytics Probe monitoring the MX-ONE as follows:

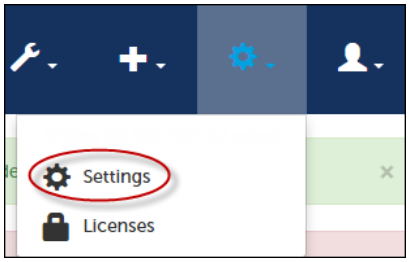
1. Ensure that the configuration file for the handset has the following lines:
   ```
   sip rtcp summary reports: 1
   sip rtcp summary report collector: collector@<Probe IP>
   sip rtcp summary report collector port: 5060
   ```
   Substitute <Probe IP> with the IP address for the Probe monitoring the MX-ONE. For on-premise systems, this is the IP address of the Mitel Performance Analytics server.

The general configuration file for Mitel SIP handsets is `aastra.cfg`. The SIP handset must reload its configuration file before it can start sending the required voice quality reports to Mitel Performance Analytics.

CONFIGURING MITEL PERFORMANCE ANALYTICS FOR MX-ONE

Do the following steps:

1. From the device dashboard, select Settings under the Settings icon.



2. Supply your email and password to enable administrative functions.
   The device properties sheet is displayed.
3. If necessary, change the name of the MiVoice MX-ONE device.
4. Verify that the suggested Probe is correct. Mitel Performance Analytics preselects a Probe with the fewest container levels between it and the device. If needed, select a different Probe from the drop-down list.
5. Enter a description for the MiVoice MX-ONE device.
6. Enter the IP address of the MiVoice MX-ONE device.
7. Enable fault and performance monitoring.
8. Choose the DSCP setting for Ping packets. You can choose from **Best Effort (0)**, **High Priority (46)**, or a variety of Assured Forwarding (AF) or Class Selector (CS) settings.
9. Select SNMP v1, v2c or v3. Mitel recommends SNMP v2c for MiVoice MX-ONE devices.
10. Enter the SNMP configuration information.
11. To enable the collection of Voice Quality statistics, select the **Collect Voice Quality** check box.
12. To enable Voice Quality threshold alarms, select the **Enable VQ Threshold** check box.
13. If the MiVoice MX-ONE has multiple interfaces and you want to receive SIP voice quality reports from the additional interfaces, enter a comma-separated list of IP addresses in the **Additional IP Registrars** field. You do not need to enter the IP address of the MiVoice MX-ONE device entered previously. Each IP address in this field supplements the IP address of the MX-ONE device.
14. To enable the collection of route and gateway utilization data, select **Traffic Monitoring**. Use the **Display IP Set Utilization** and **Display Legacy Set Utilization** checkboxes to select what data to display in the **Gateway Utilization** panel. To hide the entire **Gateway Utilization** panel, ensure that neither is selected.
    Note: Ensure that **Traffic Monitoring** is selected on only one MX-ONE Service Node in your telephone system.
15. To enable the collection of IPT user, extension, and terminal information select **Monitoring Enabled** under **Extension and Terminal Inventory**.

16. Enable **Interface Filtering** if required. See "Interface Filter Configuration" on page 113 for details.
17. Optionally enable maintenance mode for the device.
18. Optionally specify the device message.
19. Enter the user name and password for SSH access to the MiVoice MX-ONE device.
20. Click **Save** to save your changes.
    Clicking **Save** automatically runs a Probe connectivity check and verifies the new configuration.

MX-ONE APPLICATION SERVER DEVICE CONFIGURATION

To add a MX-ONE Application Server to Mitel Performance Analytics, you need the following information:

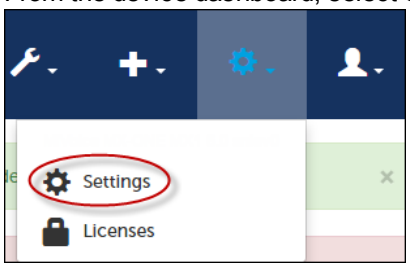
- IP address of the server
- SNMP configuration information
- Names of applications to be monitored

MX-ONE APPLICATION SERVER SNMP CONFIGURATION

SNMP support must be enabled for the monitored server with the same community string as that configured in Mitel Performance Analytics. You should also ensure that the server is configured to allow management traffic from the Probe for off-net monitoring or from the Internet for on-net monitoring.

CONFIGURING MITEL PERFORMANCE ANALYTICS FOR MX-ONE APPLICATION SERVER

Do the following steps:

1. From the device dashboard, select **Settings** under the **Settings** icon.
   

2. Supply your email and password to enable administrative functions.
   The device properties sheet is displayed.
3. If necessary, change the name of the MX-ONE Application Server.
4. Verify that the suggested Probe is correct. Mitel Performance Analytics preselects a Probe with the fewest container levels between it and the device. If needed, select a different Probe from the drop-down list.
5. Enter a description for the MX-ONE Application Server.

6. Enter the IP address of the MX-ONE Application Server. If no Probe is used, the IP address must be reachable from Mitel Performance Analytics. If a Probe is deployed, the IP address must be reachable from the Probe.
7. Enable fault and performance monitoring.
8. Choose the DSCP setting for Ping packets. You can choose from **Best Effort (0)**, **High Priority (46)**, or a variety of Assured Forwarding (AF) or Class Selector (CS) settings.
9. Select SNMP v1, v2C or v3. Mitel recommends SNMP v2C.
10. Enter the SNMP configuration information.
11. To display the **Service Sets** panel and monitor services, enable **Windows Service Monitoring**. See "Service Sets Panel" on page 262 for details on monitoring services. The **Applications to Monitor** settings are displayed.
12. Select the check box of the applications to monitor: **MiCollab Advanced Messaging**, **CMG**, **inAttend**, **ACS Media Server**.
13. Enable **Interface Filtering** if required. See "Interface Filter Configuration" on page 113 for details.
14. Optionally enable maintenance mode for the device.
15. Optionally specify the device message.
16. Click **Save** to save your changes.
    Clicking **Save** automatically runs a Probe connectivity check and verifies the new configuration.

MIVOICE BUSINESS DEVICE CONFIGURATION

The configuration procedures in this section apply to the following types of MiVoice Business devices:

- Mitel 300 ICP
- MiVoice Business
- MiVoice Business Server
- vMCD

To add a MiVoice Business system, you need the following information:

- MiXML username and password
- IP address of the 3300/MiVoice Business
- SNMP configuration information

The following optional features apply to the MiVoice Business:

- Voice Quality statistics collection
- Digital trunk statistics collection
- SIP trunk statistics collection
- Scheduled offsite backup
- Scheduled SMDR collection
- IP Set inventory collection
- ESM Single Sign-on shared account

MIVOICE BUSINESS USERNAME AND PASSWORD PRIVILEGES

For each MiVoice Business system being monitored, the MiVoice Business username and password supplied to Mitel Performance Analytics must have appropriate administration rights.

You can do this either by using the standard MiVoice Business administration username and password or by creating a new user for Mitel Performance Analytics, as follows:

1. Log into the MiVoice Business **System Administration Tool** as **super user** or **admin**.
2. Navigate to **System Properties** > **System Administration** and open the **User Authorization Profiles** form. Create a new User Profile Login ID.
3. Ensure that the username and password are the same as those entered when configuring the MiVoice Business Device in Mitel Performance Analytics.
4. Ensure that the user has the following permissions:
    - **Desktop**: Set to **False**
    - **Group Admin**: Set to **False**
    - **System Admin**: Set to **True**
    - **System Admin Policy Name**: Set to **root** or **system**
    - **Application**: Set to **True**

MIVOICE BUSINESS SNMP CONFIGURATION

SNMP access must be enabled for Mitel Performance Analytics to collect system alarms and memory utilization data.

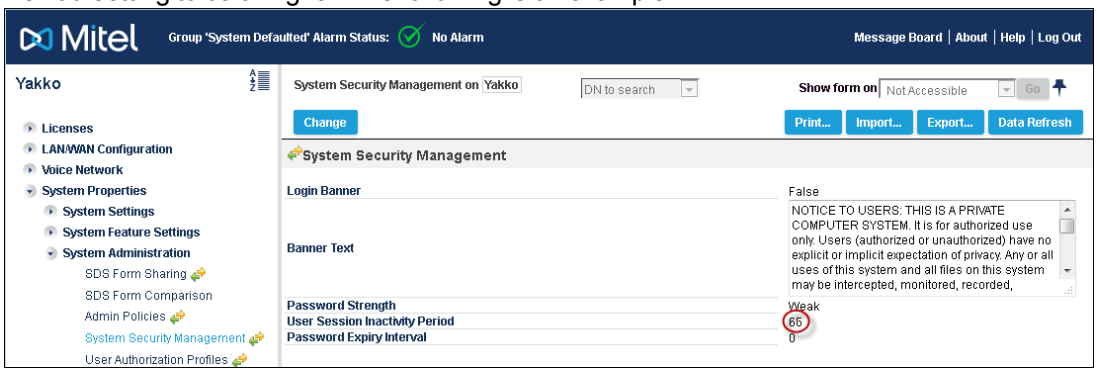
1. Log into the MiVoice Business System Administration Tool as super user or admin.
2. Navigate to **System Properties** > **System Administration** and open the **SNMP Configuration** form. Confirm the following:
    - Enable **SNMP Agent**: Set to **Yes**
    - **Read-Only Community** string: Same as that configured in Mitel Performance Analytics. The default is **public**.
    - **Accept Requests from All Managers**: Can be set to **Yes** or **No**. If set to **No**, ensure the **Accept Requests from the following Managers** panel contains the Probe IP address. For Mitel Performance Analytics on premise installation, the Probe IP address is the IP address of the Mitel Performance Analytics server.
3. Go to the **SNMP Trap Forwarding** form and add the Mitel Performance Analytics Probe IP address as a member in the **Trap Forwarding Attributes** table. Ensure that the SNMP trap community string is the same as the string used for SNMP reads.

MIVOICE BUSINESS USER SESSION INACTIVITY PERIOD CONFIGURATION

To prevent session timeouts between the Probe and the MiVoice Business, the **User Session Inactivity Period** on the **System Security Management** form must be set to 65 minutes or higher.

1. Log into the MiVoice Business **System Administration Tool** as **super user** or **admin**.
2. Navigate to **System Properties** > **System Administration** and open the **System Security Management** form.

3. Click on the **Change** button on the resulting form. Change the **User Session Inactivity Period** setting to **65** or higher. The following is an example:



4. Click **Save**.

MIVOICE BUSINESS VOICE QUALITY CONFIGURATION

For Mitel Performance Analytics to collect Voice Quality statistics, **Voice Quality Monitoring** must be enabled in the MiVoice Business management web interface as follows:

1. Log into the MiVoice Business **System Administration Tool** as **super user** or **admin**.
2. Navigate to **Maintenance and Diagnostics** > **Voice Quality** and open the **Voice Quality Configuration** form.
3. Set **Voice Quality Monitoring** to **True**. Use the default **Voice Quality SNMP Trap Latency Threshold** value.

MIVOICE BUSINESS DIGITAL TRUNK AND SIP TRUNK UTILIZATION MONITORING CONFIGURATION

To enable digital and SIP trunk utilization monitoring, MiVoice Business Traffic Data Collection must be enabled using the **Traffic Report Options** form:

1. Log into the MiVoice Business System Administration Tool as super user or admin.
2. Navigate to System Properties > System Feature Settings and open the Traffic Report Options form
3. Click the **Change** button.
4. Scroll to the bottom of the dialog box and change the default settings to the following:
    - **Time Slot 6**
        - **Active: Yes**
        - **Start Time (HH:MM): 00:00**
        - **Stop Time (HH:MM): 00:00**
    - **Period Length: 15**
    - **Usage Units: CCS**
    - **Maximum Number of Traffic Files: 10**
    - **Trunk Groups: Yes**
    - **Trunks: Yes**
5. Click **Save**.

6. Ensure that CCS Trace is not running on the MiVoice Business.

The previous procedure shows recommended settings to enable digital and SIP trunk utilization monitoring. At a minimum, the following settings must be configured:

- **Stop Time (HH:MM): 00:00** or **23:59** (to ensure time slot lasts 24 hours)
- **Period Length: 15**
- **Maximum Number of Traffic Files: 10**
- **Trunk Groups: Yes**
- **Trunks: Yes**

The **Traffic Report Options** form can contain additional settings.

MIVOICE BUSINESS SMDR COLLECTION

You must configure the MiVoice Business to enable SMDR collection. The type of configuration depends on the selected SMDR collection method: FTP or socket. See "SMDR Collection" on page 26 for details.

If you select the FTP method, make sure that the following options are enabled on the MiVoice Business:

- SMDR is on for external calls and that the trunk routes have SMDR enabled in their Class of Service options.
- "SMDR file transfer support" is enabled under "SMDR options".

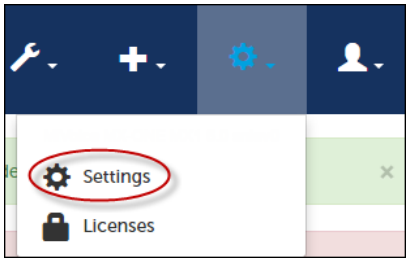
To receive the SMDR file, Mitel Performance Analytics temporarily changes the “External FTP configuration” on the MiVoice Business call server. The configuration is reset immediately after the file is sent by the MiVoice Business call server.

If you select the socket method, make sure that SMDR is on for external calls and that the trunk routes have SMDR enabled in their Class of Service options. The MiVoice Business streams SMDR records from the system IP address on port 1752.

CONFIGURING MITEL PERFORMANCE ANALYTICS FOR MIVOICE BUSINESS

Do the following steps:

1. From the device dashboard, select **Settings** under the **Settings** icon.



2. Supply your email and password to enable administrative functions.
   The device properties sheet is displayed.
3. If necessary, change the name of the MiVoice Business.

4. Verify that the suggested Probe is correct. Mitel Performance Analytics preselects a Probe with the fewest container levels between it and the device. If needed, select a different Probe from the drop-down list.
5. Enter a description for the MiVoice Business.
6. Enter the IP address of the MiVoice Business. If no Probe is used, the IP address must be reachable from Mitel Performance Analytics. If a Probe is deployed, the IP address must be reachable from the Probe.
7. Enable fault and performance monitoring.
8. Choose the DSCP setting for Ping packets. You can choose from **Best Effort (0)**, **High Priority (46)**, or a variety of Assured Forwarding (AF) or Class Selector (CS) settings.
9. Select SNMP v1, v2C or v3. Mitel recommends SNMP v1 for MiVoice Business call servers.
10. Enter the SNMP configuration information.
11. Enter the MiXML username and password.
12. To enable a shared account for ESM logon, select the **Enable SSO shared account** checkbox. Supply the credentials in the new fields. All users with **Remote Access** and **Shared SSO Credentials** permissions can use the shared account to log into the EMS.
13. To enable the collection of Voice Quality statistics, select the **Collect Voice Quality** check box.
14. To enable Voice Quality threshold alarms, select the **Enable VQ Threshold** check box.
15. To enable SDS error rate monitoring, select the **Enabled** check box.
16. To enable collection of digital trunk statistics, select the **Traffic Monitoring** check box.
17. Select the severity level for the resiliency failover alarm. Your choices are **Major** or **Minor**.
18. To enable collection of SIP trunk statistics, select the **SIP Traffic Monitoring** check box.
19. To enable MiVoice Business IP set inventory, select the **Inventory Monitoring** check box. You must enable this setting before you can enable Disconnected Set alarms.
20. To enable the **Disconnected Set Alarm**, select the check box.
21. Enable **Interface Filtering** if required. See "Interface Filter Configuration" on page 113 for details.
22. Optionally enable maintenance mode for the device.
23. Optionally specify the device message.
24. If necessary change the SMDR collection method for the MiVoice Business: **FTP** or **Socket**. See "SMDR Collection" on page 26 for details. Ensure SMDR collection has been scheduled. See "Scheduling Device Operations" on page 159.
25. Click **Save** to save your changes.
    Clicking **Save** automatically runs a Probe connectivity check and verifies the new configuration.

MIVOICE BORDER GATEWAY DEVICE CONFIGURATION

To add a MiVoicel Border Gateway device to Mitel Performance Analytics, you need the following information:

- IP address of the MiVoice Border Gateway
- SNMP configuration information

- Administrator account password

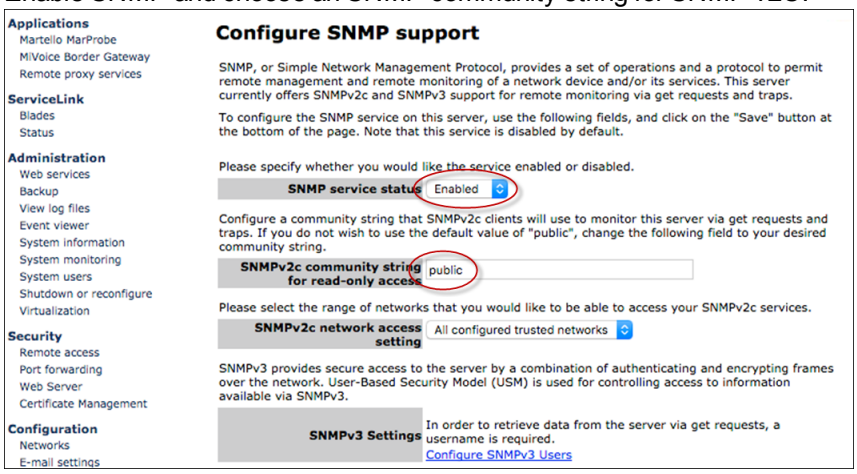
MIVOICE BORDER GATEWAY SNMP CONFIGURATION

Use the MBG Server Manager web interface to enable SNMP for Mitel Performance Analytics.

Mitel recommends that you configure SNMP v2C. You can optionally create an SNMP v3 user with user name, password, authentication type and privacy options as required. The following procedure covers SNMP v2C configuration.

Do the following steps:

1. In the **Mitel Standard Linux Management** panel, select **SNMP** in the **Configuration** menu.
2. Enable SNMP and choose an SNMP community string for SNMP v2C.



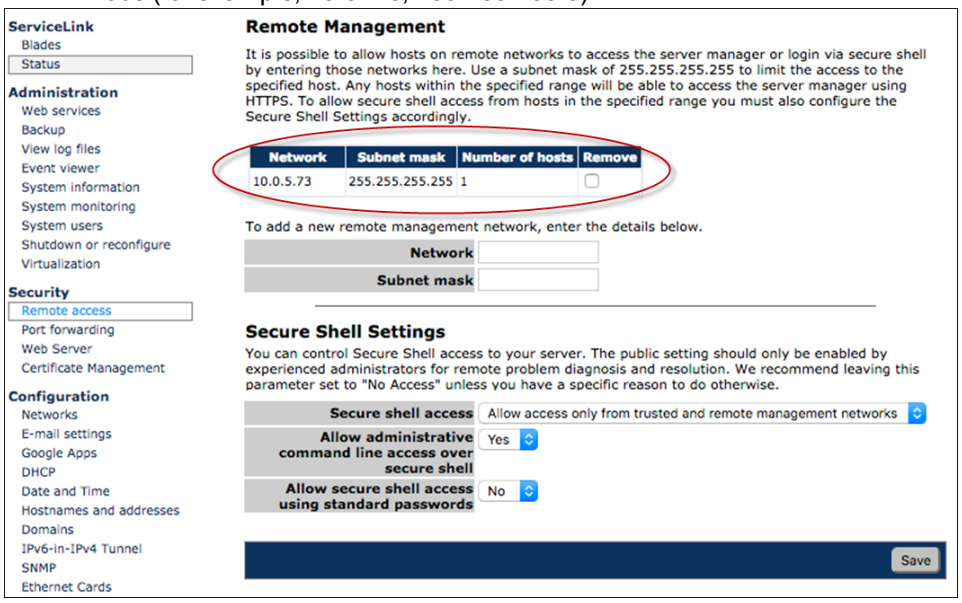
MIVOICE BORDER GATEWAY REMOTE MANAGEMENT CONFIGURATION

Use the MBG Server Manager web interface to enable Remote Management from Mitel Performance Analytics.

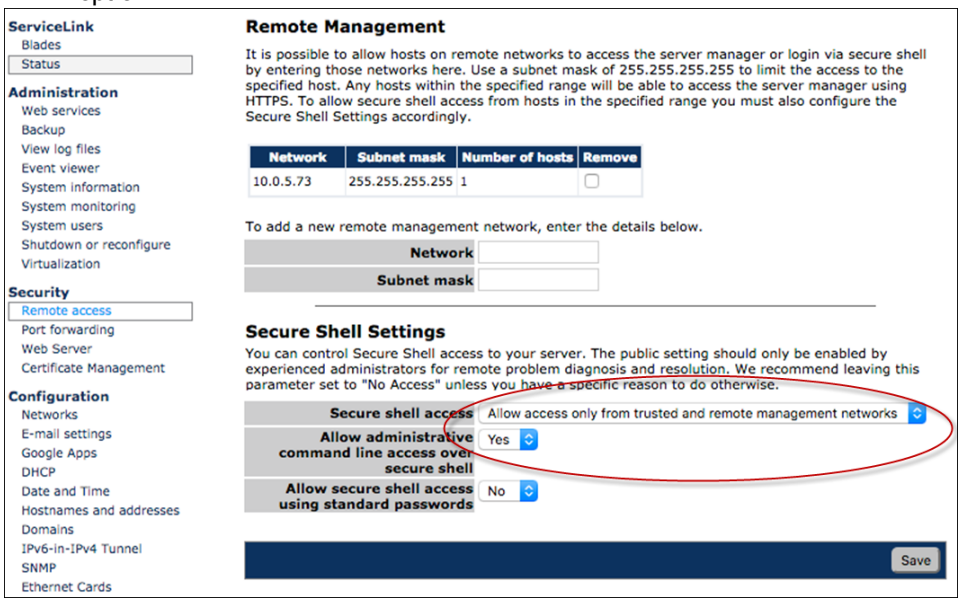
Do the following steps:

1. In the **Mitel Standard Linux Management** panel, select **Remote Access** in the **Security** menu.

2. In the **Remote Management** area, ensure that the Mitel Performance Analytics Probe is allowed to access the device by doing either of the following actions:
   - Add the IP address of the Mitel Performance Analytics Probe with a subnet mask of 255.255.255.255 (recommended).
   - Add the network and subnet mask information for the Mitel Performance Analytics Probe (for example, 10.0.7.0, 255.255.255.0).



3. In the **Secure Shell Setting** area, ensure that SSH access is enabled by doing all of the following actions:
   - Choose **Allow access only from trusted and remote management networks**.
   - Enable the **Allow administrative command line access over secure shell** option.
   - If the system administration password has not been set to a strong value, reset it to a strong value, or enable the **Allow secure shell access using standard passwords** option.



MIVOICE BORDER GATEWAY VOICE QUALITY CONFIGURATION FOR MBG BEFORE 9.0

Previous to release 9.0, MiVoice Border Gateway and Mitel Performance Analytics provides Voice Quality monitoring for Teleworker sets only. The MiVoice Border Gateway must be configured so that:

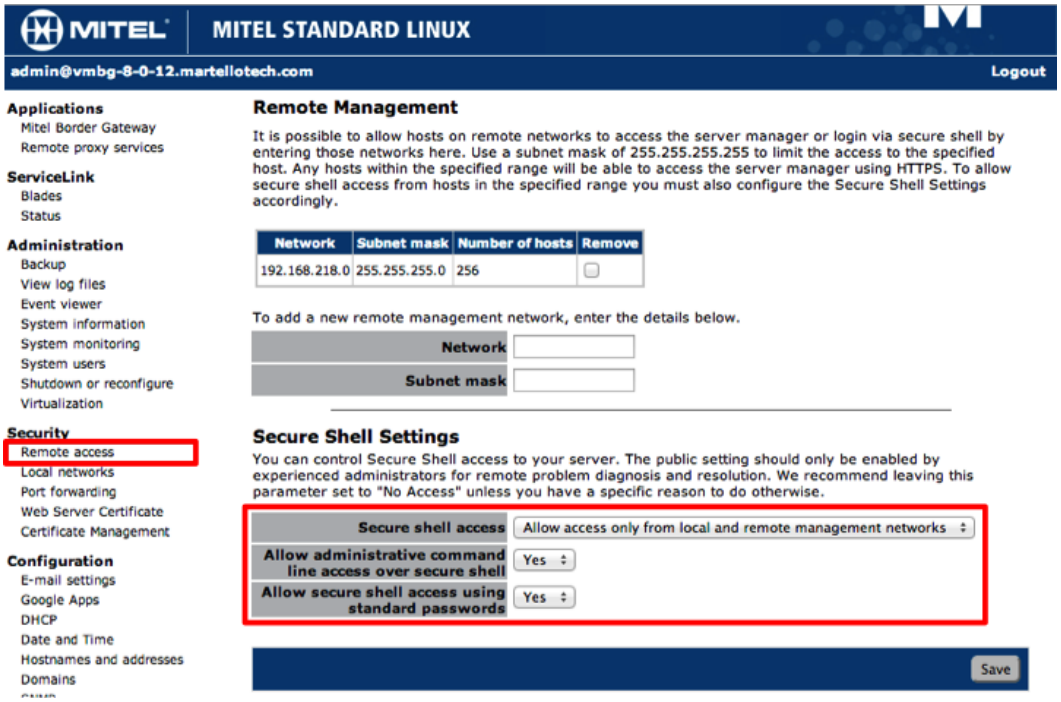
- Remote Access through Secure Shell (SSH) is enabled
- MiVoice Border Gateway Call Recording option is activated
- Secure Call Connecter is approved to receive a connection from the Probe

After Mitel Performance Analytics has been configured, it attempts to communicate with the MiVoice Border Gateway. The MiVoice Border Gateway requires that you manually accept a Mitel Performance Analytics Certificate request.

MiVoice Border Gateway Access using SSH

To enable SSH access, go to the MiVoice Border Gateway **Server Management** web page, select the **Security/Remote Access** tab on the left hand menu, and set the following options:

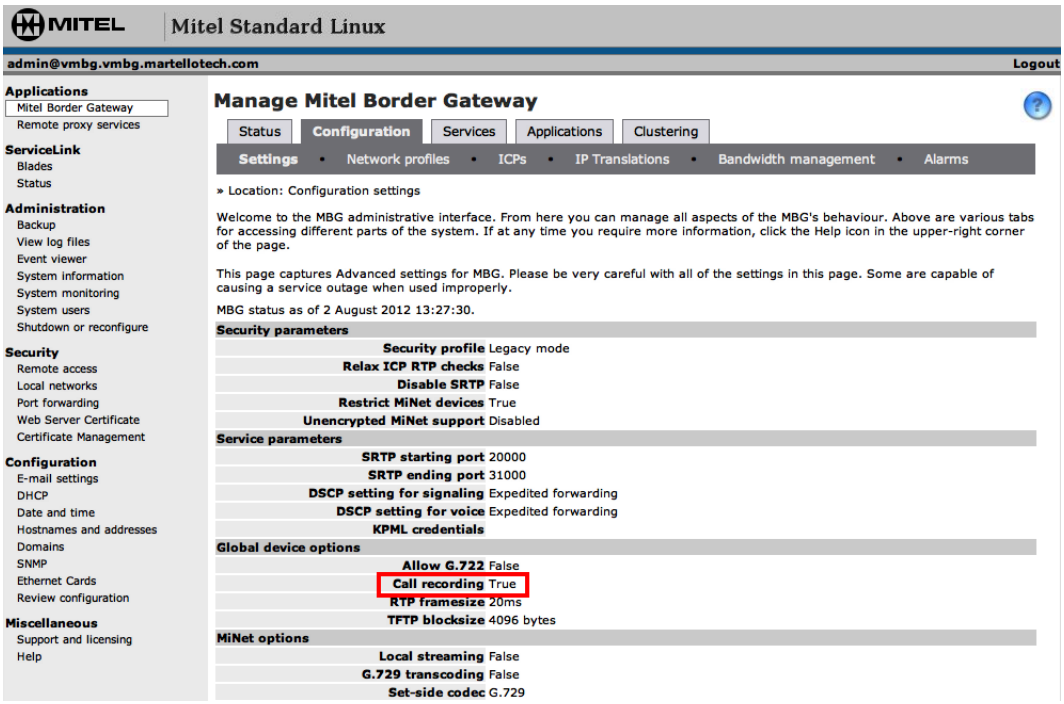
- **Secure shell access**: Set to **Allow access only from local and remote management networks**
- **Allow administrative command line access over secure shell**: Set to **Yes**
- **Allow secure shell access using standard passwords**: Set to **Yes**



MiVoice Border Gateway Call Recording Configuration

To enable Call Recording on the MiVoice Border Gateway, go to the MiVoice Border Gateway **Server Management** web page panel. Select the **Configuration** tab with the Settings subtab opened. Ensure that the **Call recording** option is set to **True**.

Mitel Performance Analytics does not access any call content. Mitel Performance Analytics uses the Secure Call Recording Connector to receive only Voice Quality performance information from the MiVoice Border Gateway.

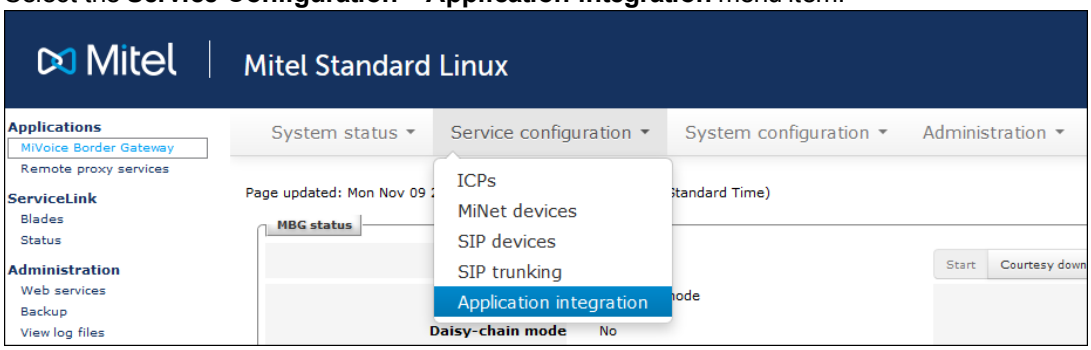


MIVOICE BORDER GATEWAY VOICE QUALITY CONFIGURATION FOR MBG 9.0 AND LATER

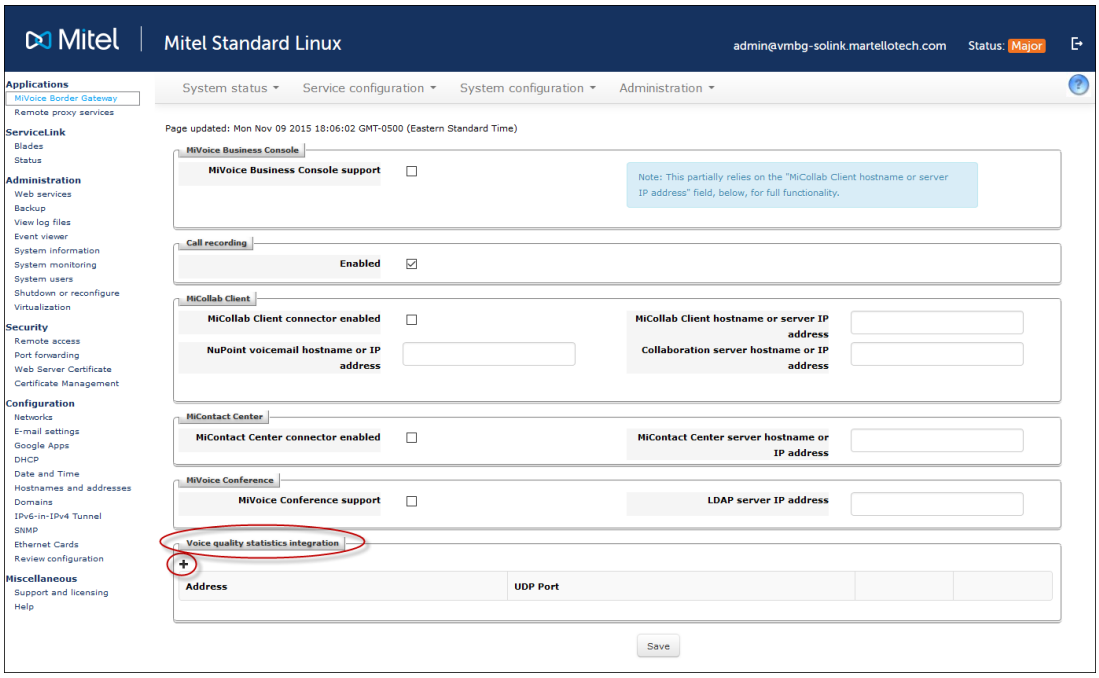
For MBG 9.0 and later, Mitel Performance Analytics provides Voice Quality monitoring for Teleworker sets, SIP Teleworker sets, and SIP trunks. The MiVoice Border Gateway must be configured so that VQ statistics are sent to the Mitel Performance Analytics Probe IP address and port 26262.

To configure the MiVoice Border Gateway:

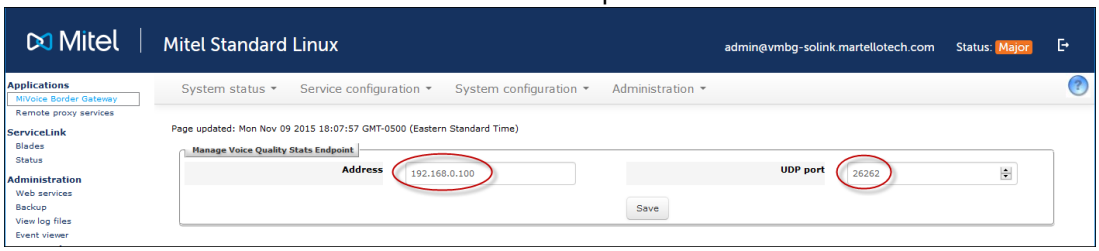
1. Go to the MiVoice Border Gateway **Server Management** web page.
2. Select the **Service Configuration** > **Application integration** menu item.



3. In the **Voice quality statistics integration** panel at the bottom of the page, click on the plus (+) icon.



4. Enter the Probe's IP address and **26262** as the UPD port.

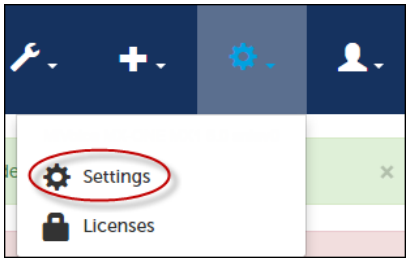


5. Click **Save**.

CONFIGURING MITEL PERFORMANCE ANALYTICS FOR MIVOICE BORDER GATEWAY

Do the following steps:

1. From the device dashboard, select **Settings** under the **Settings** icon.



2. Supply your email and password to enable administrative functions.
   The device properties sheet is displayed.
3. If necessary, change the name of the MiVoice Border Gateway.

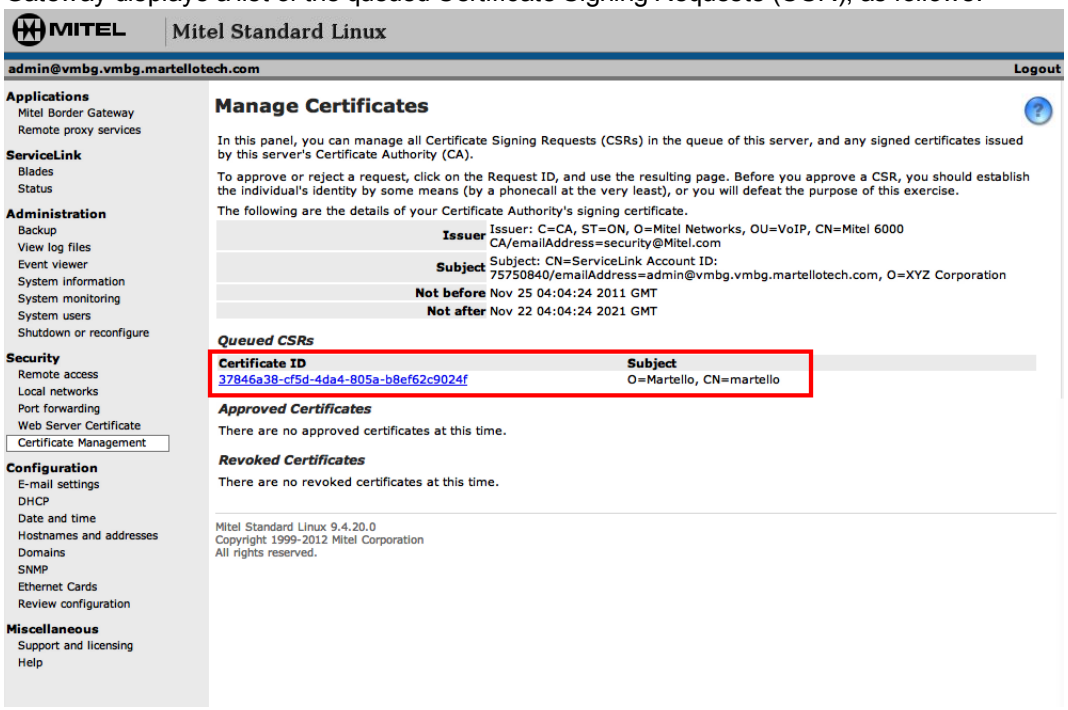
4. Verify that the suggested Probe is correct. Mitel Performance Analytics preselects a Probe with the fewest container levels between it and the device. If needed, select a different Probe from the drop-down list.
5. Enter a description for the MiVoice Border Gateway.
6. Enter the IP address of the MiVoice Border Gateway. If no Probe is used, the IP address must be reachable from Mitel Performance Analytics. If a Probe is deployed, the IP address must be reachable from the Probe.
7. Enable fault and performance monitoring.
8. Choose the DSCP setting for Ping packets. You can choose from **Best Effort (0)**, **High Priority (46)**, or a variety of Assured Forwarding (AF) or Class Selector (CS) settings.
9. Select SNMP v1, v2C or v3. Mitel recommends SNMP v2C.
10. Enter the SNMP configuration information.
11. Enter the MSL Administration password for the MiVoice Border Gateway.
12. Enable or disable MSL Alarm Status monitoring.
13. To enable collection of Voice Quality statistics, select the **Collect Voice Quality** check box. This selection controls Voice Quality data collection for SIP Teleworker sets and for SIP trunks.
14. To enable Voice Quality threshold alarms, select the **Enable VQ Threshold** check box.
15. If you want to monitor trunk utilization, select the **Trunk Utilization** check box.
16. To enable **IP Set Inventory**, select the check box. You must enable this setting before you can enable Disconnected Set alarms.
17. To enable the **Disconnected Set Alarm**, select the check box.
18. Enable **Interface Filtering** if required. See "Interface Filter Configuration" on page 113 for details.
19. Optionally enable maintenance mode for the device.
20. Optionally specify the device message.
21. Click **Save** to save your changes.
    Clicking **Save** automatically runs a Probe connectivity check and verifies the new configuration.

ACCEPTING THE MITEL PERFORMANCE ANALYTICS CERTIFICATE REQUEST AT THE MIVOICE BORDER GATEWAY

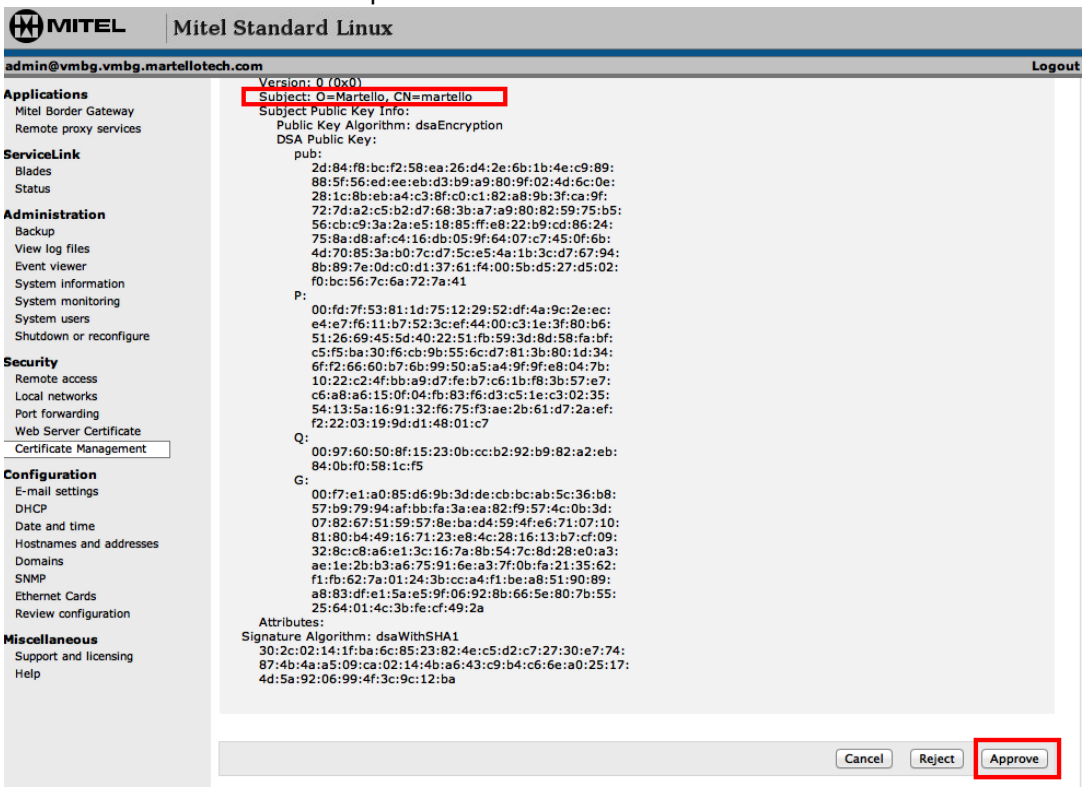
Once Mitel Performance Analytics has been configured with the MiVoice Border Gateway details, it attempts to establish a Secure Call Recording Connector connection to the MiVoice Border Gateway. To maintain the security of this connection, the MiVoice Border Gateway requires you to manually accept the Mitel Performance Analytics Certificate Request.

To approve the request, do the following steps:

1. Access to the MiVoice Border Gateway **Server Management** web page. The MiVoice Border Gateway displays a list of the queued Certificate Signing Requests (CSR), as follows:



2. Click on the Certificate ID. This provides further information on the CSR as follows:



3. Verify that the CSR is from Mitel Performance Analytics by confirming that **Subject: CN=martello, O=Martello** is in the CSR details.
4. If you are satisfied that this is the Mitel Performance Analytics CSR, click on **Approve**. Mitel Performance Analytics can then connect to the MiVoice Border Gateway to retrieve Voice Quality information.

MIVOICE OFFICE 250 DEVICE CONFIGURATION

To add a MiVoice Office 250 device to Mitel Performance Analytics, you need the following information:

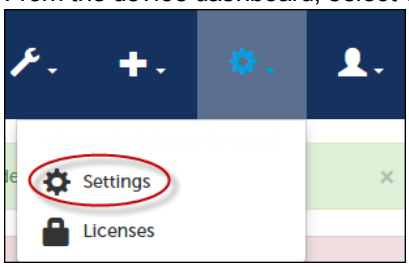
- MiVoice Office 250 admin username and password
- IP address of the MiVoice Office 250 device
- Message print password

If SMDR records are being collected, then you also need the SMDR password.

CONFIGURING MITEL PERFORMANCE ANALYTICS FOR MIVOICE OFFICE 250

Do the following steps:

1. From the device dashboard, select **Settings** under the **Settings** icon.



2. Supply your email and password to enable administrative functions.
   The device properties sheet is displayed.
3. If necessary, change the name of the MiVoice Office 250 device.
4. Verify that the suggested Probe is correct. Mitel Performance Analytics preselects a Probe with the fewest container levels between it and the device. If needed, select a different Probe from the drop-down list.
5. Enter a description for the MiVoice Office 250 device.
6. Enter the IP address of the MiVoice Office 250 device. If no Probe is used, the IP address must be reachable from Mitel Performance Analytics. If a Probe is deployed, the IP address must be reachable from the Probe.
7. Enable fault and performance monitoring.
8. Choose the DSCP setting for Ping packets. You can choose from **Best Effort (0)**, **High Priority (46)**, or a variety of Assured Forwarding (AF) or Class Selector (CS) settings.
9. Select the software version for the MiVoice Office 250 device.
10. Enter the MiVoice Office 250 admin username and password.
11. Enter the MiVoice Office 250 message print password to enable collection of system maintenance messages.

12. To enable SMDR collection from the MiVoice Office 250 device, enter the SMDR password. See "SMDR Collection" on page 26 for details. Ensure SMDR collection has been scheduled. See "Retrieving Scheduled SMDR or Backup Files" on page 166.
13. Optionally enable maintenance mode for the device.
14. Optionally specify the device message.
15. Click **Save** to save your changes.
    Clicking **Save** automatically runs a Probe connectivity check and verifies the new configuration.

MIVOICE CALL RECORDER DEVICE CONFIGURATION

To add a MiVoice Call Recorder device to Mitel Performance Analytics, you need the following information:

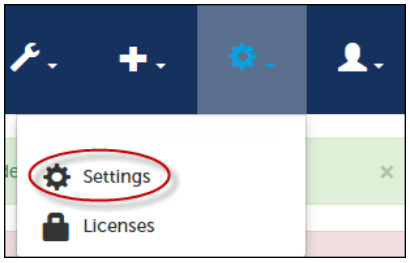
- IP address of the MiVoice Call Recorder device
- SNMP configuration information

MIVOICE CALL RECORDER SNMP CONFIGURATION

SNMP support must be enabled for the monitored MiVoice Call Recorder device with the same community string as that configured in Mitel Performance Analytics. You should also ensure that the MiVoice Call Recorder device is configured to allow management traffic from the Probe for off-net monitoring or from the Internet for on-net monitoring.

CONFIGURING MITEL PERFORMANCE ANALYTICS FOR MIVOICE CALL RECORDER

Do the following steps:

1. From the device dashboard, select **Settings** under the **Settings** icon.
   

2. Supply your email and password to enable administrative functions.
   The device properties sheet is displayed.
3. If necessary, change the name of the MiVoice Call Recorder device.
4. Verify that the suggested Probe is correct. Mitel Performance Analytics preselects the Probe with the fewest container levels between it and the device. If needed, select a different Probe from the drop-down list.
5. Enter a description for the MiVoice Call Recorder device.
6. Enter the IP address of the MiVoice Call Recorder device. If no Probe is used, the IP address must be reachable from Mitel Performance Analytics. If a Probe is deployed, the IP address must be reachable from the Probe.
7. Enable fault and performance monitoring.

8. Choose the DSCP setting for Ping packets. You can choose from **Best Effort (0)**, **High Priority (46)**, or a variety of Assured Forwarding (AF) or Class Selector (CS) settings.
9. Select SNMP v1, v2C or v3. Mitel recommends SNMP v2C.
10. Enter the SNMP configuration information.
11. To display the **Service Sets** panel and monitor services, enable **Windows Service Monitoring**. See "Service Sets Panel" on page 262 for details on monitoring services.
12. Enable Interface Filtering if required. See "Interface Filter Configuration" on page 113 for details.
13. Optionally enable maintenance mode for the device.
14. Optionally specify the device message.
15. Click **Save** to save your changes.
    Clicking **Save** automatically runs a Probe connectivity check and verifies the new configuration.

MITEL MSL/MICOLLAB DEVICE CONFIGURATION

To add a Mitel Standard Linux (MSL) or MiCollab server to Mitel Performance Analytics, you need the following information:

- IP address of the server
- SNMP configuration information
- Administrator account password

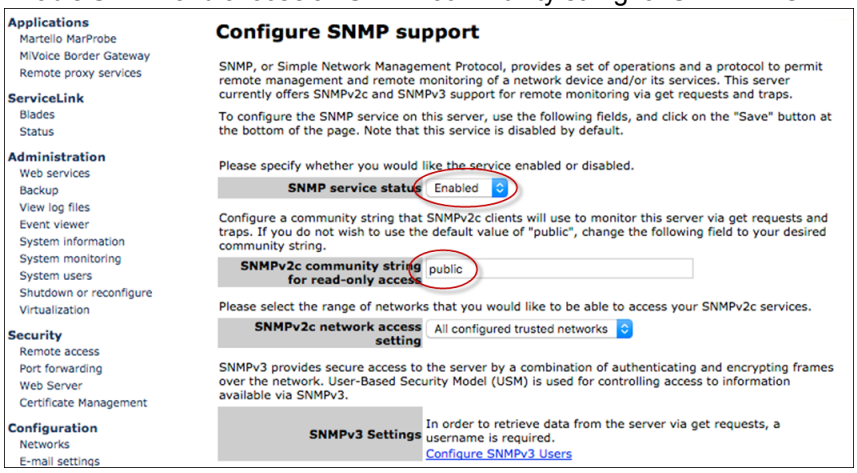
MSL/MICOLLAB SNMP CONFIGURATION

Use the MSL/MiCollab Server Manager web interface to enable SNMP for Mitel Performance Analytics.

Mitel recommends that you configure SNMP v2C. You can optionally create an SNMP v3 user with user name, password, authentication type and privacy options as required. The following procedure covers SNMP v2C configuration.

Do the following steps:

1. In the **Mitel Standard Linux Management** panel, select **SNMP** in the **Configuration** menu.
2. Enable SNMP and choose an SNMP community string for SNMP v2C.

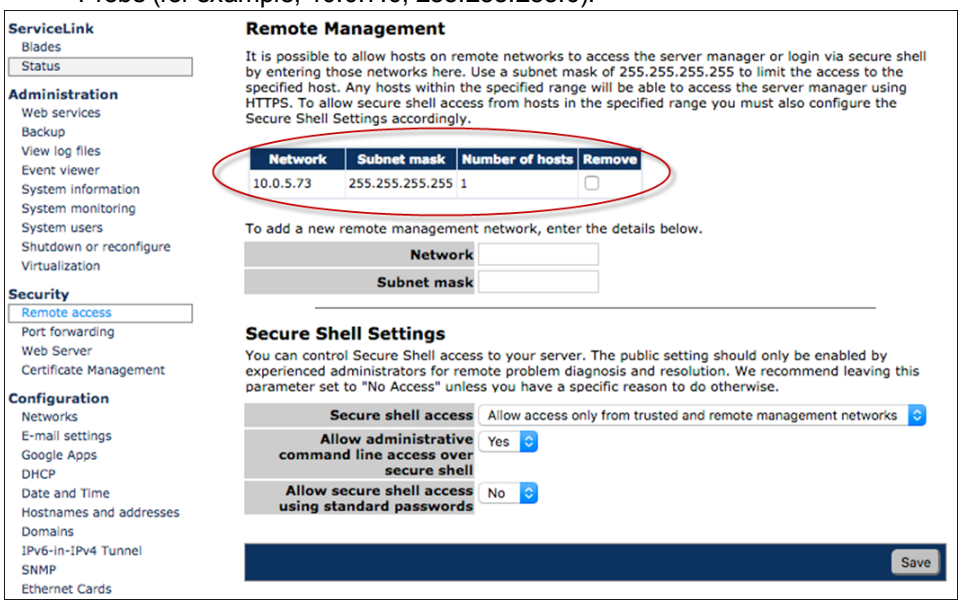


MSL/MICOLLAB REMOTE MANAGEMENT CONFIGURATION

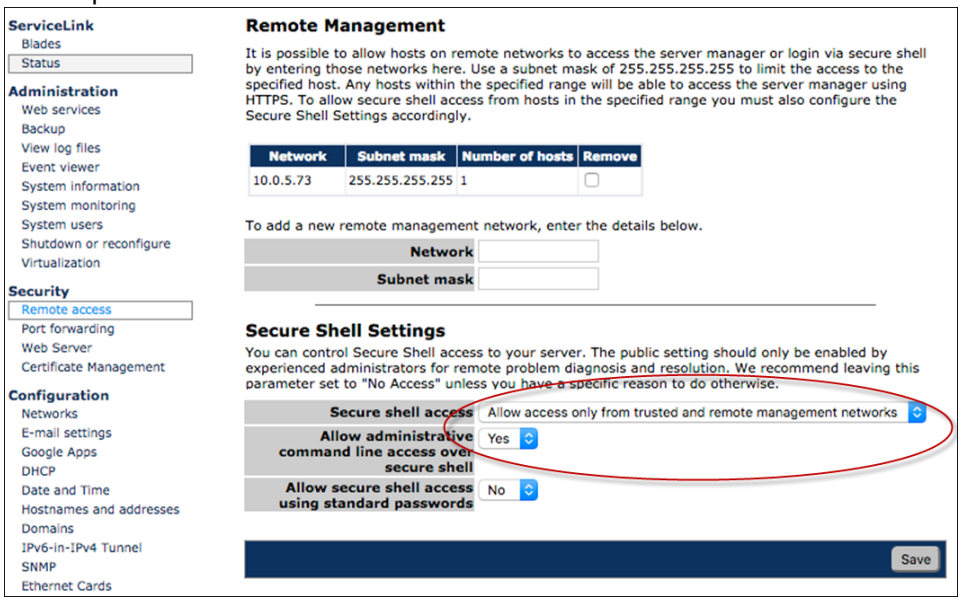
Use the MSL/MiCollab Server Manager web interface to enable Remote Management from Mitel Performance Analytics.

Do the following steps:

1. In the **Mitel Standard Linux Management** panel, select **Remote Access** in the **Security** menu.
2. In the **Remote Management** area, ensure that the Mitel Performance Analytics Probe is allowed to access the device by doing either of the following actions:
   - Add the IP address of the Mitel Performance Analytics Probe with a subnet mask of 255.255.255.255 (recommended).
   - Add the network and subnet mask information for the Mitel Performance Analytics Probe (for example, 10.0.7.0, 255.255.255.0).



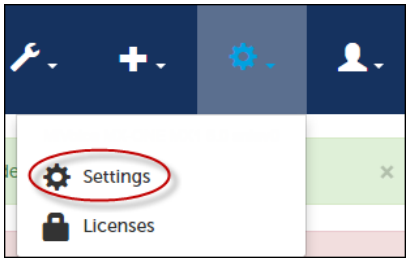
3. In the **Secure Shell Setting** area, ensure that SSH access is enabled by doing all of the following actions:
   - Choose **Allow access only from trusted and remote management networks**.
   - Enable the **Allow administrative command line access over secure shell** option.
   - If the system administration password has not been set to a strong value, reset it to a strong value, or enable the **Allow secure shell access using standard passwords** option.



CONFIGURING MITEL PERFORMANCE ANALYTICS FOR MITEL MSL/MICOLLAB

Do the following steps:

1. From the device dashboard, select **Settings** under the **Settings** icon.



2. Supply your email and password to enable administrative functions.
   The device properties sheet is displayed.
3. If necessary, change the name of the MSL/MiCollab server.
4. Verify that the suggested Probe is correct. Mitel Performance Analytics preselects a Probe with the fewest container levels between it and the device. If needed, select a different Probe from the drop-down list.
5. Enter a description for the MSL/MiCollab server.

6. Enter the IP address of the server. If no Probe is used, the IP address must be reachable from Mitel Performance Analytics. If a Probe is deployed, the IP address must be reachable from the Probe.
7. Enable fault and performance monitoring.
8. Choose the DSCP setting for Ping packets. You can choose from **Best Effort (0)**, **High Priority (46)**, or a variety of Assured Forwarding (AF) or Class Selector (CS) settings.
9. Select SNMP v1, v2C or v3. Mitel recommends SNMP v2C.
10. Enter the SNMP configuration information.
11. Enter the Administration password for the MiCollab.
12. Enable or disable MiCollab Alarm Status monitoring.
13. Enable **Interface Filtering** if required. See "Interface Filter Configuration" on page 113 for details.
14. Optionally enable maintenance mode for the device.
15. Optionally specify the device message.
16. Click **Save** to save your changes.
    Clicking **Save** automatically runs a Probe connectivity check and verifies the new configuration.

MITEL CONTACT CENTER BUSINESS DEVICE CONFIGURATION

To add a Mitel Contact Center Business device to Mitel Performance Analytics, you need the following information:

- IP address of the Mitel Contact Center Business device
- SNMP configuration information
- Mitel Contact Center Business version number
- Mitel Contact Center Business options installed

To allow communication between Mitel Performance Analytics and the Mitel Contact Center Business , ensure that **Anonymous Authentication** is enabled and that no other authentication method is active for the Internet Information Services (IIS) Manager **Help** application.

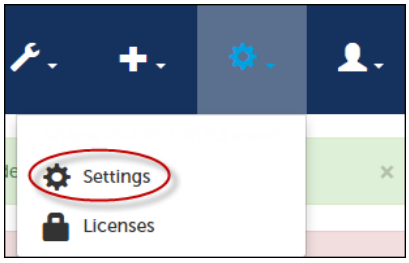
MITEL CONTACT CENTER SNMP CONFIGURATION

SNMP support must be enabled for the monitored MiContact Center Business with the same community string as that configured in Mitel Performance Analytics. Also ensure that the Mitel Contact Center Business is configured to allow management traffic from the Probe for off-net monitoring or from the Internet for on-net monitoring.

CONFIGURING MITEL PERFORMANCE ANALYTICS FOR MITEL CONTACT CENTER BUSINESS

Do the following steps:

1. From the device dashboard, select **Settings** under the **Settings** icon.



2. Supply your email and password to enable administrative functions.
   The device properties sheet is displayed.
3. If necessary, change the name of the Mitel Contact Center device.
4. Verify that the suggested Probe is correct. Mitel Performance Analytics preselects a Probe with the fewest container levels between it and the device. If needed, select a different Probe from the drop-down list.
5. Enter a description for the Mitel Contact Center device.
6. Enter the IP address of the Contact Center device. If no Probe is used, the IP address must be reachable from Mitel Performance Analytics. If a Probe is deployed, the IP address must be reachable from the Probe.
7. Enable fault and performance monitoring.
8. Choose the DSCP setting for Ping packets. You can choose from **Best Effort (0)**, **High Priority (46)**, or a variety of Assured Forwarding (AF) or Class Selector (CS) settings.
9. Select SNMP v1, v2C or v3. Mitel recommends SNMP v2C.
10. Enter the SNMP configuration information.
11. To display the **Service Sets** panel and monitor services, enable **Windows Service Monitoring**. See "Service Sets Panel" on page 262 for details on monitoring services.
    The **MiContact Center Service Monitoring** settings are displayed.
12. Specify which services to monitor. Start by choosing the Mitel Contact Center version. Options are: **Version 6**, **Version 7**, and **Version 8**.
13. Choose the Mitel Contact Center server type. Options are:
    For **Version 6**:
    - **Contact Center Manager**: This is the central server hosting the MiContact Center Business manager.
    - **Remote Server**: This is a remote server used to offload the central MiContact Center Business manager.
    - **Webchat Server**: This is a server that provides Webchat services.

    For **Version 7**:
    - **Contact Center Manager**: This is the central server hosting the MiContact Center Business manager.
    - **Remote Server**: This is a remote server used to offload the central MiContact Center Business manager.

    For **Version 8**: **Enterprise** or **Standalone**

The type of server you choose depends on how the Mitel Contact Center has been deployed. For additional details, refer to your Mitel Contact Center user documentation.

14. Choose the Mitel Contact Center device options:
    For **Version 6** or **Version 7**:
    - If Multimedia Contact Center is enabled, select the check box for monitoring.
    - If **IVR** is enabled, select the check box for monitoring.
    - If there is a SQL server database in the Mitel Contact Center server, select the type. Options are: **none**, **SQL Server**, and **SQL Express**.

    For **Version 8**:
    - **Server Location**: **Local** or **Remote**.
    - If **IVR** is enabled, select the check box for monitoring.
    - If **Message and Routing** is enabled, select the check box for monitoring.
    - If **Multimedia** is enabled, select the check box for monitoring.
    - If **Workforce Management** is enabled, select the check box for monitoring.
    - If there is a SQL server database in the Mitel Contact Center server, select the type. Options are: **none**, **SQL Server**, and **SQL Express**.
15. Enable **Interface Filtering** if required. See "Interface Filter Configuration" on page 113 for details.
16. Optionally enable maintenance mode for the device.
17. Optionally specify the device message.
18. Click **Save** to save your changes.
    Clicking **Save** automatically runs a Probe connectivity check and verifies the new configuration.

GENERIC SERVER DEVICE CONFIGURATION

To add a generic server to Mitel Performance Analytics, you need the following information:

- IP address of the server
- SNMP configuration information
- Server OS type: Windows or Linux
- Names of Windows services to be monitored

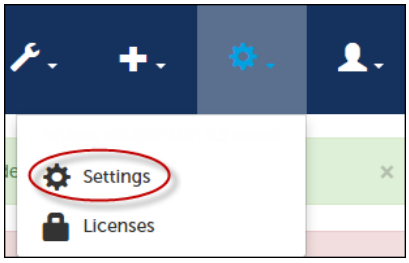
GENERIC SERVER SNMP CONFIGURATION

SNMP support must be enabled for the monitored server with the same community string as that configured in Mitel Performance Analytics. You should also ensure that the server is configured to allow management traffic from the Probe for off-net monitoring or from the Internet for on-net monitoring.

CONFIGURING MITEL PERFORMANCE ANALYTICS FOR A GENERIC SERVER

Do the following steps:

1. From the device dashboard, select **Settings** under the **Settings** icon.



2. Supply your email and password to enable administrative functions.
   The device properties sheet is displayed.
3. If necessary, change the name of the server.
4. Verify that the suggested Probe is correct. Mitel Performance Analytics preselects a Probe with the fewest container levels between it and the device. If needed, select a different Probe from the drop-down list.
5. Enter a description for the server.
6. Enter the IP address of the server. If no Probe is used, the IP address must be reachable from Mitel Performance Analytics. If a Probe is deployed, the IP address must be reachable from the Probe.
7. Enable fault and performance monitoring.
8. Choose the DSCP setting for Ping packets. You can choose from **Best Effort (0)**, **High Priority (46)**, or a variety of Assured Forwarding (AF) or Class Selector (CS) settings.
9. Select SNMP v1, v2C or v3. Mitel recommends SNMP v2C.
10. Enter the SNMP configuration information.
11. To display the **Service Sets** panel and monitor services, enable **Windows Service Monitoring**. See "Service Sets Panel" on page 262 for details on monitoring services.
12. Enable **Interface Filtering** if required. See "Interface Filter Configuration" on page 113 for details.
13. Optionally enable maintenance mode for the device.
14. Optionally specify the device message.
15. Click **Save** to save your changes.
    Clicking **Save** automatically runs a Probe connectivity check and verifies the new configuration.

VMWARE ESXI SERVER DEVICE CONFIGURATION

To add a VMWare ESXi server to Mitel Performance Analytics, you need the following information:

- IP address of the server
- SNMP configuration information

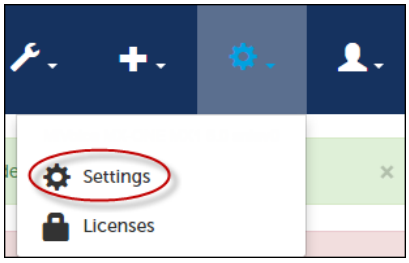
EXSI SERVER SNMP CONFIGURATION

SNMP support must be enabled for the monitored server with the same community string as that configured in Mitel Performance Analytics. You should also ensure that the server is configured to allow management traffic from the Probe for off-net monitoring or from the Internet for on-net monitoring.

CONFIGURING MITEL PERFORMANCE ANALYTICS FOR A VMWARE ESXI SERVER

Do the following steps:

1. From the device dashboard, select **Settings** under the **Settings** icon.



2. Supply your email and password to enable administrative functions.
   The device properties sheet is displayed.
3. If necessary, change the name of the server.
4. Verify that the suggested Probe is correct.Mitel Performance Analytics preselects a Probe with the fewest container levels between it and the device. If needed, select a different Probe from the drop-down list.
5. Enter a description for the server.
6. Enter the IP address of the server. If no Probe is used, the IP address must be reachable from Mitel Performance Analytics. If a Probe is deployed, the IP address must be reachable from the Probe.
7. Enable fault and performance monitoring.
8. Choose the DSCP setting for Ping packets. You can choose from **Best Effort (0)**, **High Priority (46)**, or a variety of Assured Forwarding (AF) or Class Selector (CS) settings.
9. Select SNMP v1, v2C or v3. Mitel recommends SNMP v2C.
10. Enter the SNMP configuration information.
11. Enable **Interface Filtering** if required. See "Interface Filter Configuration" on page 113 for details.
12. Optionally enable maintenance mode for the device.
13. Optionally specify the device message.
14. Click **Save** to save your changes.
    Clicking **Save** automatically runs a Probe connectivity check and verifies the new configuration.

ROUTER DEVICE CONFIGURATION

To add a router to Mitel Performance Analytics, you need the following information:

- IP address of the router
- SNMP configuration information
- Router type: **Cisco** or **Adtran**

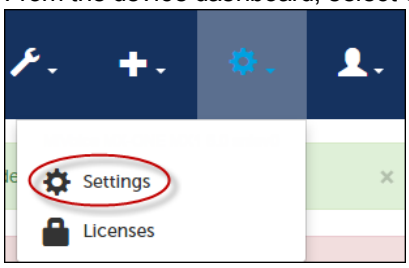
ROUTER SNMP CONFIGURATION

SNMP support must be enabled for the monitored router with the same community string as that configured in Mitel Performance Analytics. You should also ensure that the router is configured to allow management traffic from the Probe for off-net monitoring or from the Internet for on-net monitoring.

CONFIGURING MITEL PERFORMANCE ANALYTICS FOR A ROUTER

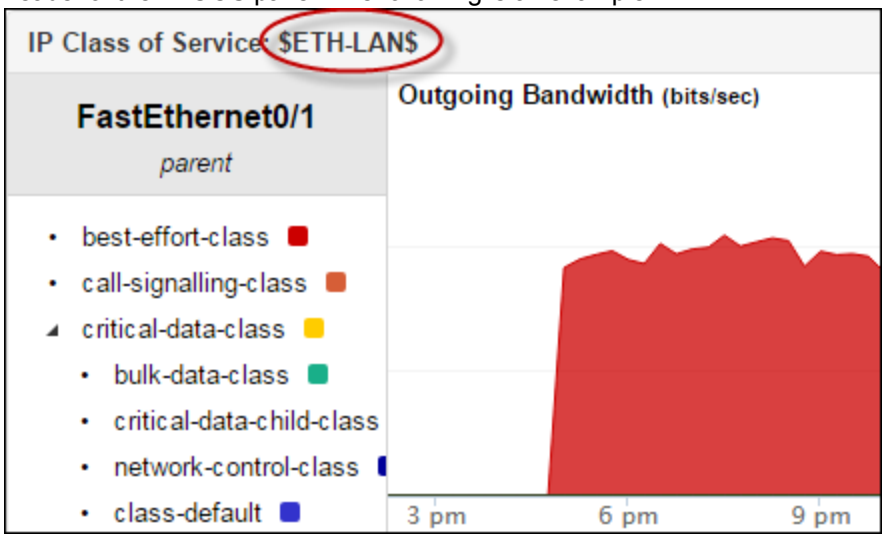
Do the following steps:

1. From the device dashboard, select **Settings** under the **Settings** icon.



2. Supply your email and password to enable administrative functions.
   The device properties sheet is displayed.
3. If necessary, change the name of the router.
4. Verify that the suggested Probe is correct. Mitel Performance Analytics preselects a Probe with the fewest container levels between it and the device. If needed, select a different Probe from the drop-down list.
5. Enter a description for the router.
6. Enter the IP address of the router. If no Probe is used, the IP address must be reachable from Mitel Performance Analytics. If a Probe is deployed, the IP address must be reachable from the Probe.
7. Enable fault and performance monitoring.
8. Choose the DSCP setting for Ping packets. You can choose from **Best Effort (0)**, **High Priority (46)**, or a variety of Assured Forwarding (AF) or Class Selector (CS) settings.
9. Select SNMP v1, v2C or v3. Mitel recommends SNMP v2C.
10. Enter the SNMP configuration information.
11. Select the router type (**Adtran** or **Cisco**) from the drop-down list.
12. To display the IP route table on the device dashboard, select the checkbox.
13. To enable IP Class of Service monitoring, select the checkbox.

14. For Cisco routers, Mitel Performance Analytics provides IP COS panels for each router interface. By default, IP COS panels are displayed for all interfaces. To restrict the number of panels, enter the names of the interfaces to be displayed in the **List of Visible Interfaces** field. Use a comma to separate multiple interface names. Interface names are displayed in the header of the IP COS panel. The following is an example.



15. Enable **Interface Filtering** if required. See "Interface Filter Configuration" on page 113 for details.
16. Optionally enable maintenance mode for the device.
17. Optionally specify the device message.
18. Click **Save** to save your changes.
    Clicking **Save** automatically runs a Probe connectivity check and verifies the new configuration.

ETHERNET SWITCH DEVICE CONFIGURATION

To add an Ethernet switch to Mitel Performance Analytics, you need the following information:

- IP address of the Ethernet switch
- SNMP configuration information
- Switch type: **HP**, **Dell**, **Cisco**, **Avaya** (Nortel), or **Extreme**

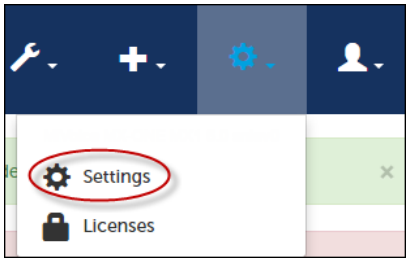
ETHERNET SWITCH SNMP CONFIGURATION

SNMP support must be enabled for the monitored switch with the same community string as that configured in Mitel Performance Analytics. You should also ensure that the switch is configured to allow management traffic from the Probe for off-net monitoring or from the Internet for on-net monitoring.

CONFIGURING MITEL PERFORMANCE ANALYTICS FOR AN ETHERNET SWITCH

Do the following steps:

1. From the device dashboard, select **Settings** under the **Settings** icon.



2. Supply your email and password to enable administrative functions.
   The device properties sheet is displayed.
3. If necessary, change the name of the switch.
4. Verify that the suggested Probe is correct. Mitel Performance Analytics preselects a Probe with the fewest container levels between it and the device. If needed, select a different Probe from the drop-down list.
5. Enter a description for the switch.
6. Enter the IP address of the switch. If no Probe is used, the IP address must be reachable from Mitel Performance Analytics. If a Probe is deployed, the IP address must be reachable from the Probe.
7. Enable fault and performance monitoring.
8. Choose the DSCP setting for Ping packets. You can choose from **Best Effort (0)**, **High Priority (46)**, or a variety of Assured Forwarding (AF) or Class Selector (CS) settings.
9. Select SNMP v1, v2C or v3. Mitel recommends SNMP v2C.
10. Enter the SNMP configuration information.
11. Choose the switch type from the drop-down list. Options are: **HP**, **Dell**, **Avaya** or **Extreme**.
12. Enable **Interface Filtering** if required. See "Interface Filter Configuration" on page 113 for details.
13. Optionally enable maintenance mode for the device.
14. Optionally specify the device message.
15. Click **Save** to save your changes.
    Clicking **Save** automatically runs a Probe connectivity check and verifies the new configuration.

PATHSOLUTIONS DEVICE CONFIGURATION

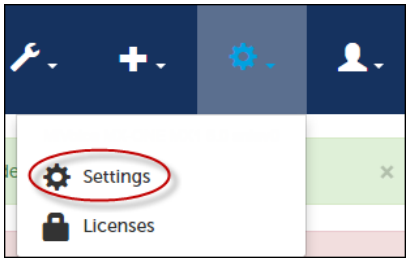
To add a PathSolutions VoIP monitor to Mitel Performance Analytics, you need the following information:

- IP address of the server running the PathSolutions software
- Port number used for PathSolutions web interface; normally **8084**

CONFIGURING MITEL PERFORMANCE ANALYTICS FOR A PATHSOLUTIONS DEVICE

Do the following steps:

1. From the device dashboard, select **Settings** under the **Settings** icon.



2. Supply your email and password to enable administrative functions.
   The device properties sheet is displayed.
3. If necessary, change the name of the PathSolutions VoIP monitor.
4. Verify that the suggested Probe is correct. Mitel Performance Analytics preselects a Probe with the fewest container levels between it and the device. If needed, select a different Probe from the drop-down list.
5. Enter a description for the PathSolutions VoIP monitor.
6. Enter the IP address of the PathSolutions VoIP monitor. If no Probe is used, the IP address must be reachable from Mitel Performance Analytics. If a Probe is deployed, the IP address must be reachable from the Probe.
7. Enable fault and performance monitoring.
8. Choose the DSCP setting for Ping packets. You can choose from **Best Effort (0)**, **High Priority (46)**, or a variety of Assured Forwarding (AF) or Class Selector (CS) settings.
9. Enter the port number for the PathSolutions web interface.
10. Optionally enable maintenance mode for the device.
11. Optionally specify the device message.
12. Click **Save** to save your changes.
    Clicking **Save** automatically runs a Probe connectivity check and verifies the new configuration.

UNINTERRUPTIBLE POWER SUPPLY DEVICE CONFIGURATION

To add an Uninterruptible Power Supply (UPS) to Mitel Performance Analytics, you need the following information:

- IP address of the UPS
- SNMP configuration information
- UPS manufacturer: only APC models with Network Management modules are supported

UPS SNMP CONFIGURATION

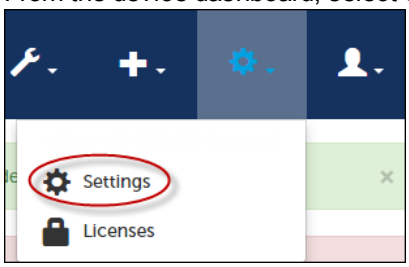
SNMP support must be enabled for the Network Management module on the monitored UPS with the same community string as that configured in Mitel Performance Analytics.

To send alarms to Mitel Performance Analytics using SNMP traps, determine the LAN address of the Probe monitoring the UPS and configure this IP address as a trap receiver in the UPS Network Management module. (Use the **Notification** > **SNMP Traps** > **Trap Receivers** pages.)

CONFIGURING MITEL PERFORMANCE ANALYTICS FOR A UPS

Do the following steps:

1. From the device dashboard, select **Settings** under the **Settings** icon.



2. Supply your email and password to enable administrative functions.
   The device properties sheet is displayed.
3. If necessary, change the name of the device.
4. Verify that the suggested Probe is correct. Mitel Performance Analytics preselects a Probe with the fewest container levels between it and the device. If needed, select a different Probe from the drop-down list.
5. Enter a description for the UPS.
6. Enter the IP address of the UPS. If no Probe is used, the IP address must be reachable from Mitel Performance Analytics. If a Probe is deployed, the IP address must be reachable from the Probe.
7. Enable fault and performance monitoring.
8. Choose the DSCP setting for Ping packets. You can choose from **Best Effort (0)**, **High Priority (46)**, or a variety of Assured Forwarding (AF) or Class Selector (CS) settings.
9. Select SNMP v1, v2C or v3. Mitel recommends SNMP v2C.
10. Enter the SNMP configuration information.
11. Choose the UPS manufacturer from the drop-down list. Currently, only APC models with Network Management modules are supported.
12. Optionally enable maintenance mode for the device.
13. Optionally specify the device message.
14. Click **Save** to save your changes.
    Clicking **Save** automatically runs a Probe connectivity check and verifies the new configuration.

AVAYA IP OFFICE DEVICE CONFIGURATION

To add an Avaya IP Office device to Mitel Performance Analytics, you need the following information:

- IP Office system type — IP Office 500 / 500v2 or IP Office Server Edition
- IP address for the system
- System User Name and Password
- SNMP configuration information
- SMDR port number for the system (if collecting SMDR records)

AVAYA IP OFFICE SNMP CONFIGURATION

To enable or verify SNMP settings on the Avaya IP Office device:

1. Access the IP Office System Manager.
2. Load the configuration for the system to be monitored.
3. Go to the System / Events / Configuration tab.
4. Ensure that SNMP is enabled. Set the SNMP community string (the default is **public**) and the SNMP port to **161** (the default).
5. Save the new configuration.

Enabling or changing SNMP requires a system merge on the Avaya IP Office device and may require a system reboot.

AVAYA IP OFFICE SMDR CONFIGURATION

To enable SMDR for the Avaya IP Office device:

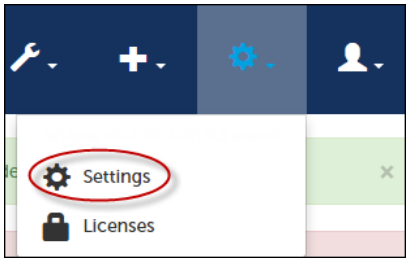
1. Access the IP Office System Manager.
2. Load the configuration for the system to be monitored.
3. Go to the System / SMDR tab.
4. Enable SMDR using the dropdown menu **SMDR only**.
5. Set the **Station Message Detail Recorder Communications** IP address to **0.0.0.0** and the TCP port to be the same port as configured on Mitel Performance Analytics for SMDR collection. Mitel recommends you use **4400** as the TCP port number. Leave other settings at their default values.
6. Save the new configuration.

Enabling SMDR for the Avaya IP Office device does not require a system reboot.

CONFIGURING MITEL PERFORMANCE ANALYTICS FOR AN AVAYA IP OFFICE DEVICE

Do the following steps:

1. From the device dashboard, select **Settings** under the **Settings** icon.



2. Supply your email and password to enable administrative functions.
   The device properties sheet is displayed.
3. If necessary, change the name of the device.
4. Verify that the suggested Probe is correct. Mitel Performance Analytics preselects a Probe with the fewest container levels between it and the device. If needed, select a different Probe from the drop-down list.
5. Enter a description for the Avaya IP Office device.
6. Enter the IP address of the Avaya IP Office device. If no Probe is used, the IP address must be reachable from Mitel Performance Analytics. If a Probe is deployed, the IP address must be reachable from the Probe.
7. Enable fault and performance monitoring.
8. Choose the DSCP setting for Ping packets. You can choose from **Best Effort (0)**, **High Priority (46)**, or a variety of Assured Forwarding (AF) or Class Selector (CS) settings.
9. Select **SNMP v1** because SNMP v2C or v3 are not supported in some IP Office releases.
10. Enter the SNMP configuration information.
11. Enter the Avaya IP Office system username and password.
12. Select the IP Office Type from the dropdown list. Options are:
    - **IP Office**: Select this option for an IP Office 500 or 500 v2 System.
    - **IP Office Server**: Select this option for an IP Office Server Edition System.
13. Optionally enable the Avaya System Monitor. Supply the password as needed.
14. Optionally enable IP Set Inventory Monitoring.
15. Enable **Interface Filtering** if required. See "Interface Filter Configuration" on page 113 for details.
16. To enable SMDR collection, supply the TCP port number that Mitel Performance Analytics must use to connect to the IP Office to retrieve the SMDR records. This must be the same as the TCP port number configured previously in the IP Office System. See "SMDR Collection" on page 26 for details. Ensure SMDR collection has been scheduled. See "Retrieving Scheduled SMDR or Backup Files" on page 166.
17. Optionally enable maintenance mode for the device.
18. Optionally specify the device message.
19. Click **Save** to save your changes.

Clicking **Save** automatically runs a Probe connectivity check and verifies the new configuration.

BASIC IP DEVICE CONFIGURATION

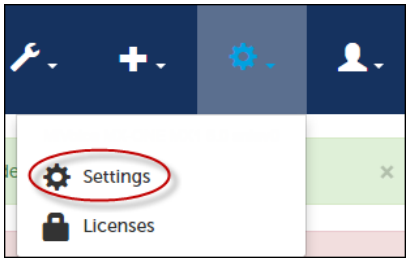
To add a basic IP device to Mitel Performance Analytics you need the following information:

- IP address for the system
- SNMP configuration information

CONFIGURING MITEL PERFORMANCE ANALYTICS FOR A BASIC IP DEVICE

Do the following steps:

1. From the device dashboard, select **Settings** under the **Settings** icon.



2. Supply your email and password to enable administrative functions.
   The device properties sheet is displayed.
3. If necessary, change the name of the basic IP device.
4. Verify that the suggested Probe is correct. Mitel Performance Analytics preselects the Probe with the fewest container levels between it and the device. If needed, select a different Probe from the drop-down list.
5. Enter a description for the basic IP device.
6. Enter the IP address of the basic IP device. If no Probe is used, the Enter the IP address of the basic IP device. If no Probe is used, the IP address must be reachable from Mitel Performance Analytics. If a Probe is deployed, the IP address must be reachable from the Probe.
7. Enable fault and performance monitoring.
8. Choose the DSCP setting for Ping packets. You can choose from **Best Effort (0)**, **High Priority (46)**, or a variety of Assured Forwarding (AF) or Class Selector (CS) settings.
9. Enter the SNMP configuration information.
10. Optionally enable maintenance mode for the device.
11. Optionally specify the device message.
12. Click **Save** to save your changes.
    Clicking **Save** automatically runs a Probe connectivity check and verifies the new configuration.

RED BOX CALL RECORDER DEVICE CONFIGURATION

To add a Red Box Call Recorder device to Mitel Performance Analytics, you need the following information:

- IP address of the Red Box Call Recorder device
- SNMP configuration information

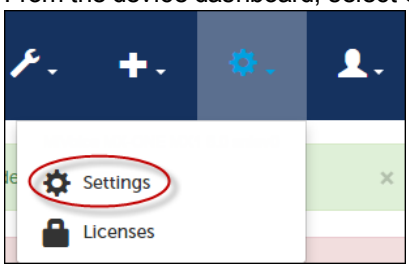
RED BOX CALL RECORDER SNMP CONFIGURATION

SNMP support must be enabled for the monitored Red Box Call Recorder device with the same community string as that configured in Mitel Performance Analytics. You should also ensure that the Red Box Call Recorder device is configured to allow management traffic from the Probe for off-net monitoring or from the Internet for on-net monitoring.

CONFIGURING MITEL PERFORMANCE ANALYTICS FOR A RED BOX CALL RECORDER

Do the following steps:

1. From the device dashboard, select Settings under the Settings icon.



2. Supply your email and password to enable administrative functions.
The device properties sheet is displayed.
3. If necessary, change the name of the Red Box Call Recorder device.
4. Verify that the suggested Probe is correct. Mitel Performance Analytics preselects the Probe with the fewest container levels between it and the device. If needed, select a different Probe from the drop-down list.
5. Enter a description for the Red Box Call Recorder device.
6. Enter the IP address of the Red Box Call Recorder device. If no Probe is used, the IP address must be reachable from Mitel Performance Analytics. If a Probe is deployed, the IP address must be reachable from the Probe.
7. Enable fault and performance monitoring.
8. Choose the DSCP setting for Ping packets. You can choose from **Best Effort (0)**, **High Priority (46)**, or a variety of Assured Forwarding (AF) or Class Selector (CS) settings.
9. Select SNMP v1, v2C or v3. Mitel recommends SNMP v2C.
10. Enter the SNMP configuration information.
11. To display the **Service Sets** panel and monitor services, enable **Windows Service Monitoring**. See "Service Sets Panel" on page 262 for details on monitoring services.
12. Enable **Interface Filtering** if required. See "Interface Filter Configuration" on page 113 for details.

13. Optionally enable maintenance mode for the device.
14. Optionally specify the device message.
15. Click **Save** to save your changes.
    Clicking **Save** automatically runs a Probe connectivity check and verifies the new configuration.

INNOVATION INNLINE VOICE MAIL DEVICE CONFIGURATION

To add an InnLine Voice Mail device to Mitel Performance Analytics you need the following information:

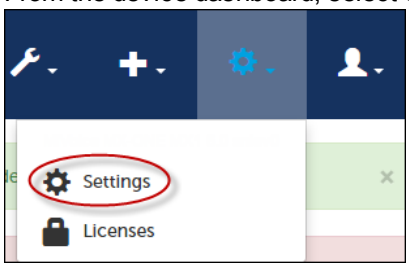
- IP address of the InnLine Voice Mail device
- SNMP configuration information

INNOVATION INNLINE VOICE MAIL SNMP CONFIGURATION

SNMP support must be enabled for the monitored InnLine Voice Mail device with the same community string as that configured in Mitel Performance Analytics. You should also ensure that the InnLine Voice Mail device is configured to allow management traffic from the Probe for off-net monitoring or from the Internet for on-net monitoring.

CONFIGURING MITEL PERFORMANCE ANALYTICS FOR AN INNOVATION INNLINE VOICE MAIL DEVICE

Do the following steps:

1. From the device dashboard, select **Settings** under the **Settings** icon.
   

2. Supply your email and password to enable administrative functions.
   The device properties sheet is displayed.
3. If necessary, change the name of the InnLine Voice Mail device.
4. Verify that the suggested Probe is correct. Mitel Performance Analytics preselects the Probe with the fewest container levels between it and the device. If needed, select a different Probe from the drop-down list.
5. Enter a description for the InnLine Voice Mail device.
6. Enter the IP address of the InnLine Voice Mail device. If no Probe is used, the IP address must be reachable from Mitel Performance Analytics. If a Probe is deployed, the IP address must be reachable from the Probe.
7. Enable fault and performance monitoring.
8. Choose the DSCP setting for Ping packets. You can choose from **Best Effort (0)**, **High Priority (46)**, or a variety of Assured Forwarding (AF) or Class Selector (CS) settings.

9. Select SNMP v1, v2C or v3. Mitel recommends SNMP v2C.
10. Enter the SNMP configuration information.
11. To display the **Service Sets** panel and monitor services, enable **Windows Service Monitoring**. See "Service Sets Panel" on page 262 for details on monitoring services.
12. Enable **Interface Filtering** if required. See "Interface Filter Configuration" on page 113 for details.
13. Optionally enable maintenance mode for the device.
14. Optionally specify the device message.
15. Click **Save** to save your changes.
    Clicking **Save** automatically runs a Probe connectivity check and verifies the new configuration.

MANAGING DEVICES

This chapter shows you how to do various operations on Mitel Performance Analytics devices such as discovering them, moving them from one container to another, and performing backups.

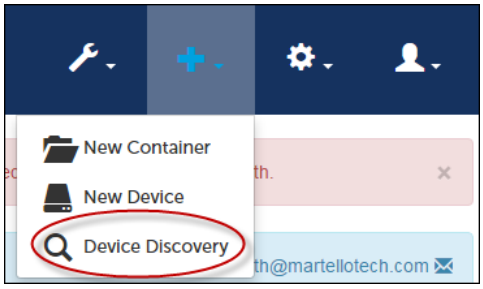
DISCOVERING MITEL PERFORMANCE ANALYTICS DEVICES

The **Device Discovery** panel automates the task of adding devices to Mitel Performance Analytics. The **Device Discovery** panel uses SNMP to determine devices that can be monitored by Mitel Performance Analytics.

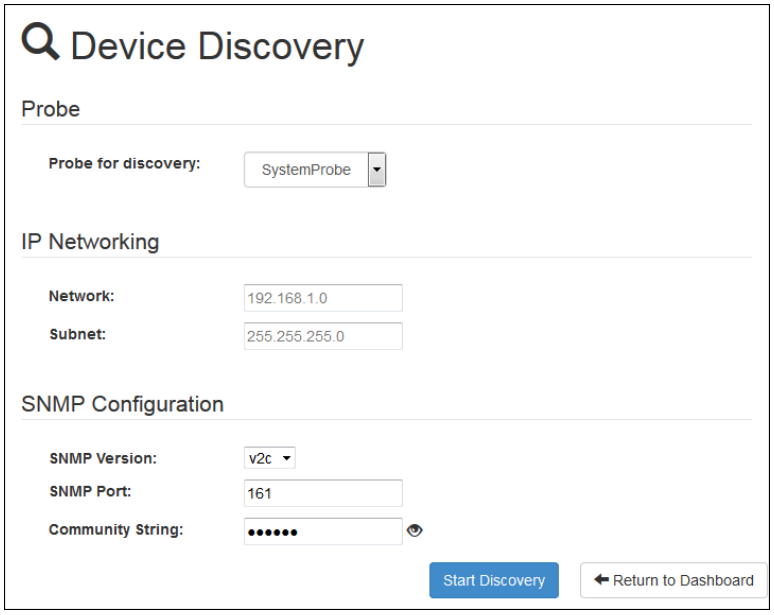
STARTING DEVICE DISCOVERY

To configure a new set of discovery criteria and start the discovery process, do the following steps:

1. From a container dashboard, select **Device Discovery** under the **Add** icon:

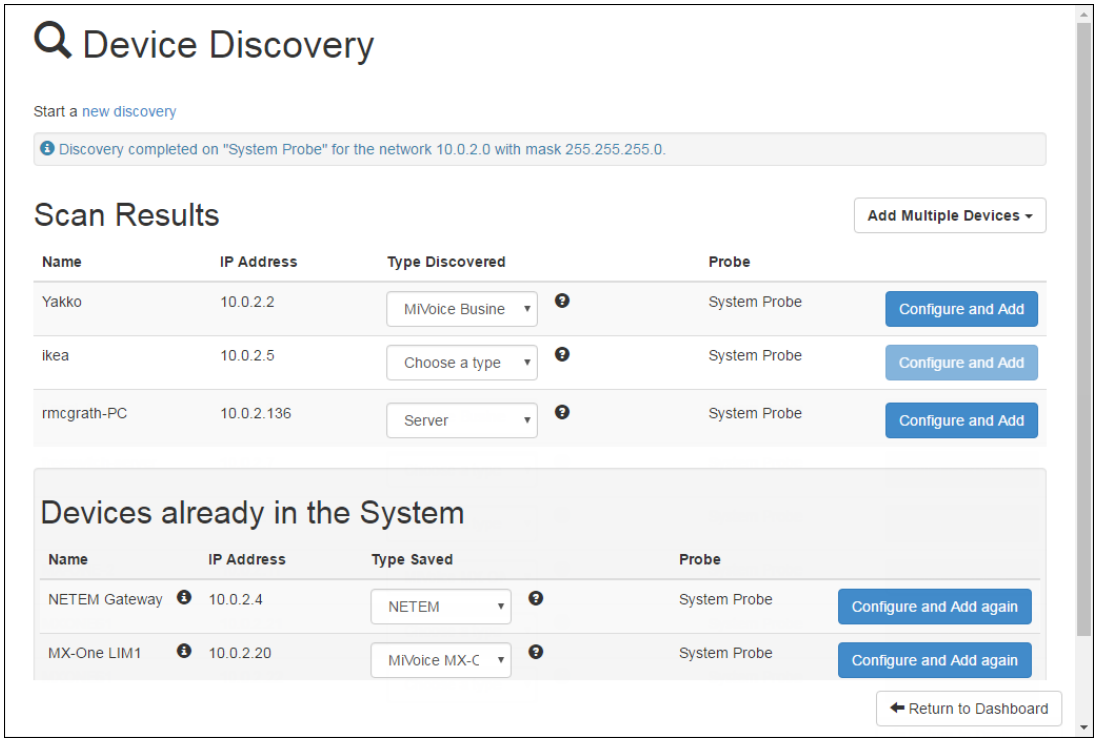


The **Device Discovery** panel is displayed.



2. Choose the Probe that you want to use to monitor the devices once they are discovered.
3. Specify the base IP address of the network to be scanned and a netmask (for example, 255.255.255.0). The base IP address and the netmask specify the range IP addresses to scan for devices.

4. Specify the SNMP configuration information for the devices. See "SNMP Configuration" on page 111 for details. Note that the Device Discovery panel does not support SNMPv3.
5. Click the **Start discovery** button. The **Device Discovery** panel lists devices in the network that it has discovered.



Devices that are not monitored by Mitel Performance Analytics are listed under **Scan Results**. You can add them to Mitel Performance Analytics by clicking on the **Configure and Add** button for each device. See "Adding Discovered Devices" on page 154. You can also add multiple devices to Mitel Performance Analytics by using the **Add Multiple Devices** dropdown list. See "Bulk Adding Devices" on page 155.

Devices that are already monitored by Mitel Performance Analytics are listed under **Devices already in the System**. You can change their configuration by clicking on the **Configure and Add again** button. See "Reconfiguring Existing Devices" on page 155.

The discovery process respects user access rules. The **Device Discovery** panel only lists devices that a user has access to.

ADDING DISCOVERED DEVICES

Do the following steps:

1. From the **Scan Results** list in the **Device Discovery** panel, verify the device type.
   The initial device type is determined by the SNMP data returned by the device. If the discovery process cannot determine a device type, it displays **Choose a Type**. Determine additional device details by hovering over the icon.

   Change the device type if necessary. For example, the discovery may suggest a device type of Server, when in fact the device would be better suited to be a MiCollab. The **Configure and Add** button is activated only when a device type is selected.

2. Click the **Configure and Add** button beside the device to be added to Mitel Performance Analytics.
   The device's **Settings** sheet is displayed. The fields and settings are pre-populated with the SNMP data supplied by the device.
3. Configure the device by changing the **Settings** page as required. See "Configuring Mitel Performance Analytics Devices" on page 111 for details.
4. Click on the Save button. The **Device Discovery** panel is displayed so you can add another device to Mitel Performance Analytics.

RECONFIGURING EXISTING DEVICES

Do the following steps:

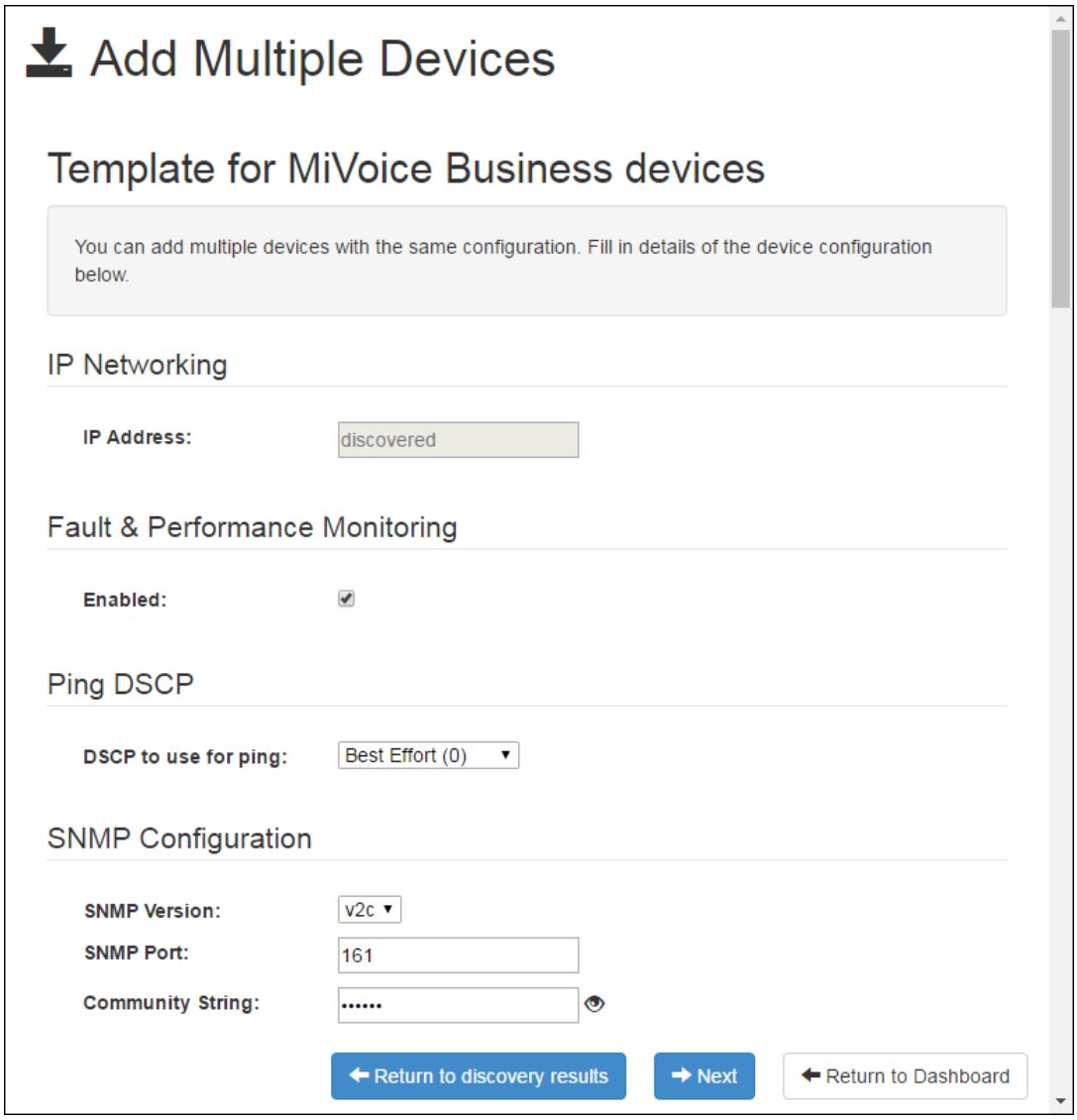
1. From the **Devices already in the System** list in the **Device Discovery** panel, click on the **Configure and Add again** button.
   The device's **Settings** sheet is displayed. The fields and settings are pre-populated with the SNMP data supplied by the device.
2. Reconfigure the device by changing the **Settings** page as required. See "Configuring Mitel Performance Analytics Devices" on page 111 for details.
3. Click on the **Save** button. The **Device Discovery** panel is displayed so you can modify the configuration of another device.

BULK ADDING DEVICES

Do the following steps:

1. From the **Scan Results** list in the **Device Discovery** panel, verify the device type.
   The initial device type is determined by the SNMP data returned by the device. The suggested device type may need to be changed. For example, the discovery may suggest a device type of Server, when in fact the device would be better suited to be a MiCollab. If the discovery process cannot determine a device type, it displays **Choose a Type**. Determine additional device details by hovering over the icon.

From the **Add Multiple Devices** dropdown list, select the first device type to be applied to multiple discovered devices. The **Add Multiple Devices - Template** panel is displayed.



The **Add Multiple Devices - Template** panel displays a configuration template based on the Settings page for the type of device selected from the **Add Multiple Devices** dropdown list.

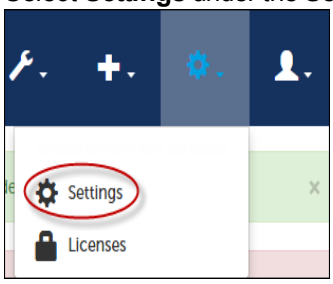
2. Fill out the configuration template as required. See "Configuring Mitel Performance Analytics Devices" on page 111 for details. When done, click on the **Next** button.
   The **Add Multiple Devices – Validate and save** panel is displayed.
3. On the **Add Multiple Devices – Validate and save** panel, select which discovered devices you want to apply the configuration template to. You can also change the device name and the container where to add the device.
4. Click on the **Add devices** button. The **Add multiple devices** panel confirms the selected devices were added to Mitel Performance Analytics.

MOVING A DEVICE

Moving a device means changing its parent container. Moving a device applies to all objects associated with it, incuding alarms, events and licensing.

Do the following steps:

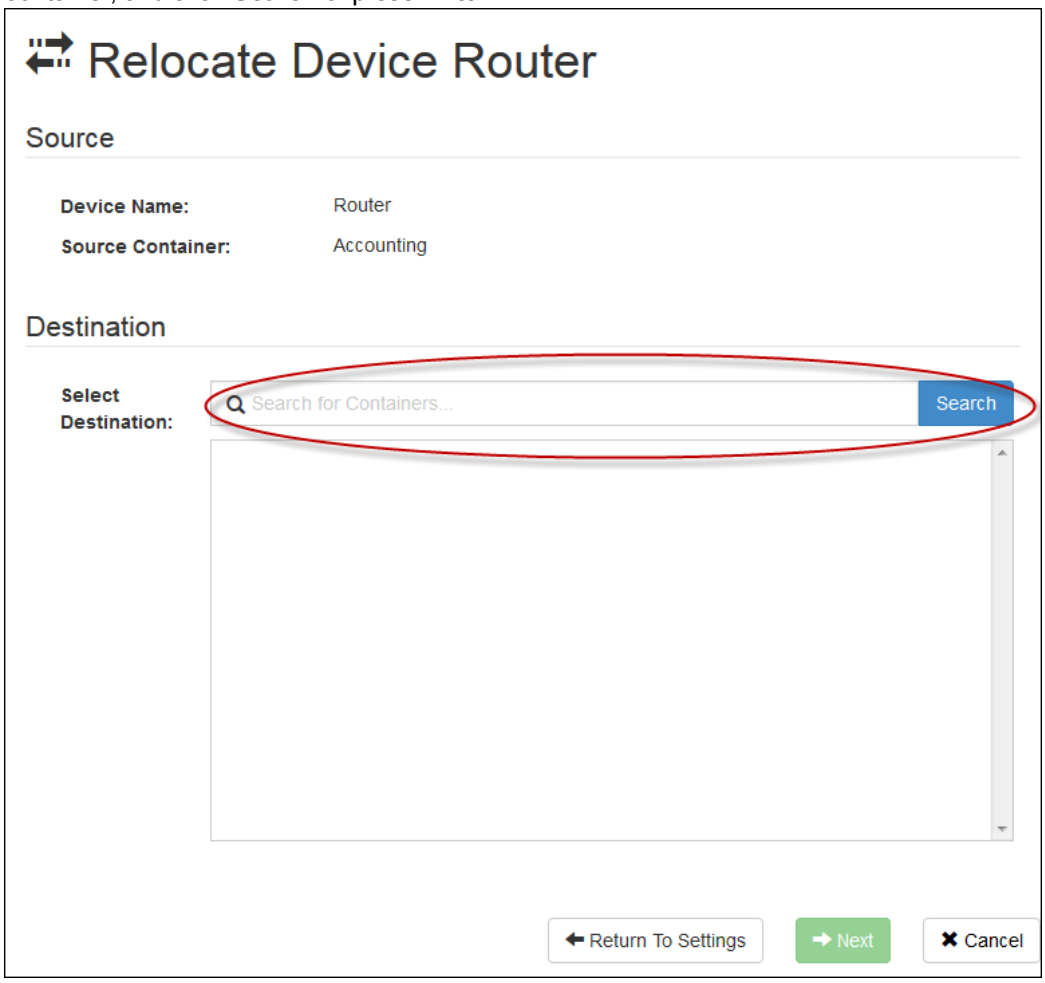
1. Access the dashboard of the device you want to move.
2. Select **Settings** under the **Settings** icon.



The device's **Settings** page is displayed.

Under **General**, the name of the device appears, its Probe, and its parent container. Click the **Relocate this Device...** button. The **Relocate Device** dialog appears.

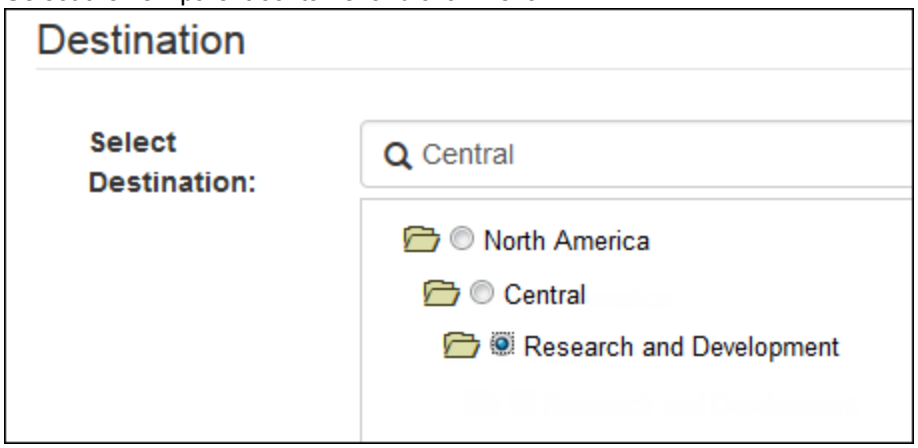
3. In the **Select Destination** field, enter either the full name or the partial name of the new parent container, and click **Search** or press **Enter**.



The **Relocate Device** dialog is populated with a destination container structure.

Note: The **Relocate Device** dialog does not display a destination container structure unless you click **Search** or press **Enter** after entering the full or partial name of the new parent container in the **Select Destination** field.

4. Select the new parent container and click **Next**.



The **Relocate Confirmation** dialog is displayed listing possible concerns associated with moving the device.

5. Select **Accept and continue** and click **Apply** to move the device.
   Licensing is automatically enforced on the moved device.

SCHEDULING DEVICE OPERATIONS

Use the **Operations Scheduler** to schedule operations on multiple devices at once . Supported operations include:

- Backup:
  - MiVoice Business
  - MiVoice MX-ONE
- SMDR collection
  - MiVoice Business
  - MiVoice Office 250
  - Avaya IP Office
- MiVoice Business activities:
  - HotDesk Logout
  - Go to Day Service
  - Go to Night Service
  - Incremental IDS Sync
  - Full IDS Sync

Note: Mitel recommends that you avoid using the FreeFTPd server due to known issues and limitations with that product.

Mitel Performance Analytics retains:

- The 10 most recent backups
- An SMDR file for up to 31 days

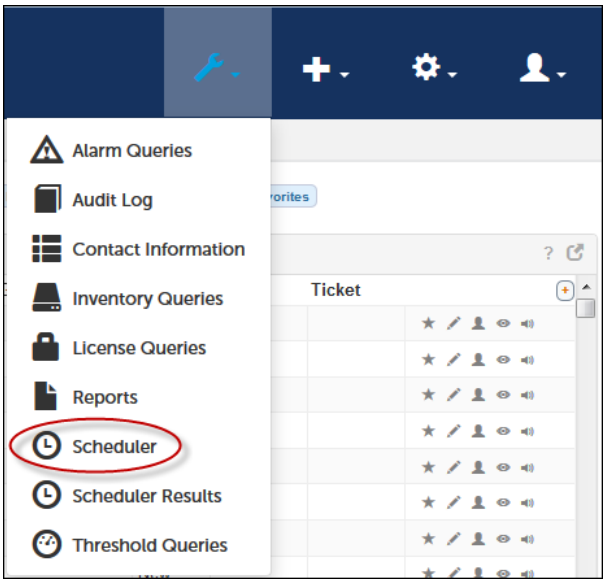
CAUTION: To retain SMDR files longer than 31 days, you must provide alternate storage and move the files there before they are erased byMitel Performance Analytics.

Scheduled operations are performed by the Probe; not the Mitel Performance Analytics server. The Probe is aware of scheduled operation requirements for the next 24-48 hours. This mechanism allows scheduled operations to occur even if the Probe loses communications with the Mitel Performance Analytics server.

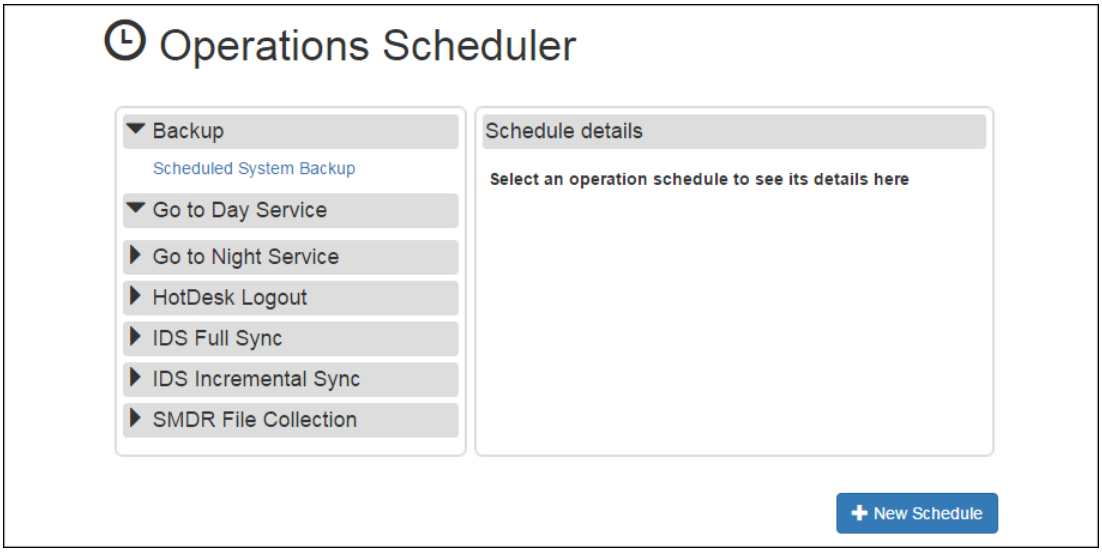
Schedules apply only to the devices in a container and its subcontainers. A device can only be a member of a single SMDR collection schedule. However, a device can be a member of multiple backup schedules. For example, a MiVoice Business or MiVoice MX-ONE can be a member of a daily backup schedule and a monthly backup schedule.

For SMDR collection, the devices (MiVoice Business, MiVoice Office 250, or Avaya IP Office) must be correctly configured. For details, see "MiVoice Business SMDR Collection" on page 123, "MiVoice Office 250 Device Configuration" on page 132 or "Avaya IP Office Device Configuration" on page 147.

When applicable, the **Operations Scheduler** panel is available by clicking **Scheduler** under the **Tools** icon of a container dashboard, as follows:



The **Operations Scheduler** panel displays a list of configured operation schedules. The following is an example:

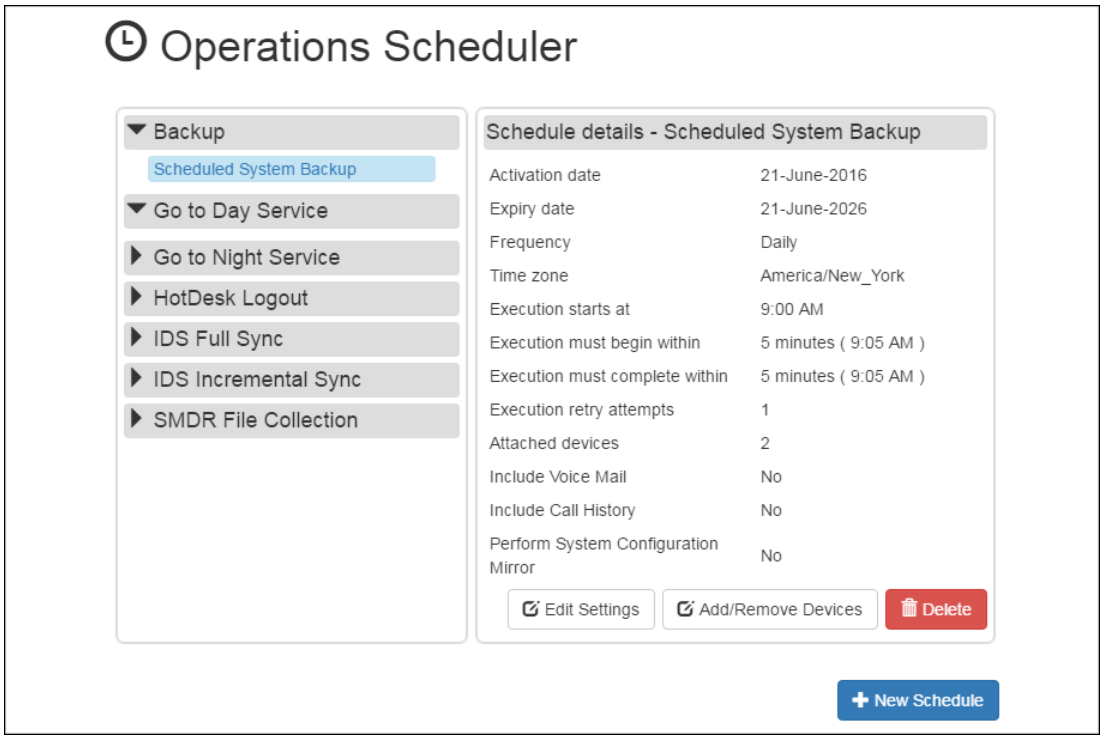


DISPLAYING SCHEDULE DETAILS

Do the following steps:

1. Access the **Operations Scheduler**.

2. Click on the schedule name on the left of the panel; for example **Scheduled System Backup**. The schedule details are displayed on the right of the panel under **Schedule details**.



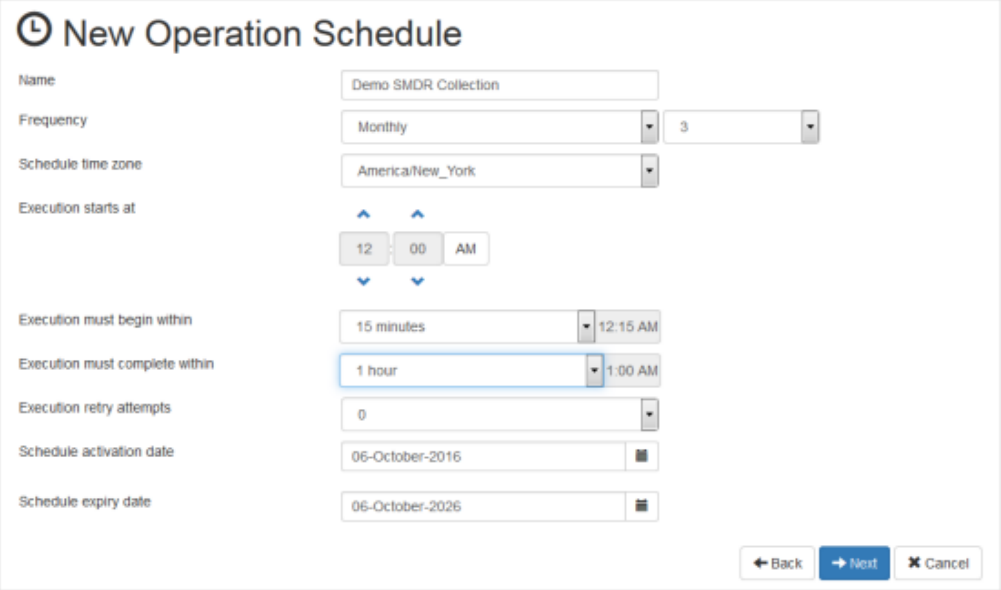
SCHEDULING AN OPERATION

Do the following steps:

1. Access the **Operations Scheduler**.
2. Click on the **New Schedule** button.
3. Select the type of operation from the dropdown list and click on the **Next** button. The **Operations Scheduler** displays new schedule parameters.
4. Specify the schedule parameters:
   - **Name**: The name of the operation to be created
   - **Frequency**: The frequency at which the operation is to be executed. Other fields on the panel might change depending on the selected frequency.
   - **Schedule time zone**: The time zone that is used to execute the scheduled operation
   - **Execution starts at**: This field appears if **Frequency** is set to**Hourly**, **Daily**, **Weekly**, or **Monthly**. The time that the scheduled operation is to begin. The operation begins at this time for all devices associated with the schedule operation, regardless of the local time of the devices.
   - **Execution must begin within**: The time period within which the operation must begin. When taken with the **Schedule start time**, this setting determines the latest time that the operation can begin.
   - **Execution must complete within**: The maximum time period that the operation can run for. When taken with the **Schedule start time**, this setting determines the latest time that the operation can finish.

- **Execution retry attempts**: The operation attempts at least once in the scheduled time period. However in case of failture, Mitel Performance Analytics attempts the operation this number of additional times.
- **Schedule activation date**: The date that the scheduled operation begins.
- **Schedule expiry date**: The last date that the scheduled operation can occur.

The following is an example.



In the previous example, SMDR collection is schedule to occur on the third of each month, starting between 12:00 midnight and 12:15 am and lasting no later than 1:00 am. If SMDR collection fails, no retries are attempted. The SMDR collection starts June 8th, 2016 and runs until June 8th, 2026.

5. Specify the operation-specific parameters as required.
   For MiVoice Business backup, the parameters are:
   - **Include Call History**: Optionally include Call History in the backup.
   - **Include Voice Mail**: Optionally include Voice Mail in the backup.

   For MiVoice MX-ONE backup, the parameters are:
   - **Perform System Configuration Mirror**Optionally backup all nodes of the telephony system. A regular MX-ONE backup stores telephone user data only. A mirror backup also stores the configuration data of all the nodes.

   Note: A mirror backup can consume significant MX-ONE resources. Perform a mirror backup only during off peak hours.

   The default file storage location varies depending on the type of installation:
   - For cloud-based installations, Mitel Performance Analytics stores the files to secure offsite storage (Amazon S3).
   - For on-premise installations, Mitel Performance Analytics stores the files on its file system file store.

   To use an external server, select **Use external FTP server**:
   - Select the protocol from the dropdown list. You can use the following protocols: SFTP (SSH File Transfer Protocol), FTP (File Transfer Protocol), or FTPS (Secure File Transfer Protocol). Both implicit and explicit FTPS are supported.

- Supply the URL to the server.
- Supply the credentials to access the server.
- Supply the port to use.

For MiVoice Business internal scheduler activities, refer to for related details. The related parameters are:

- **Go to Night Service**:
  - **Service Option**: Night 1 or Night 2
- **HotDesk Logout**:
  - **User Option**: All, Internal, or External
- **IDS Full Synch**:
  - **Use Global Catalog**
  - **Domain Set**: List of domains to scan when not using the global catalog
  - **Synchronization Type**: Apply, Detain, or Compare
  - **Allow Delete Operation**
- **IDS Incremental Synch**:
  - **Use Global Catalog**
  - **Domain Set**: List of domains to scan when not using the global catalog
  - **Synchronization Type**: Apply, Detain, or Compare
  - **Use Default Query String**
  - **Query String**: Query string to use when not using the default string

Click **Save** when all the parameters have been specified.

6. Select the devices that the operation applies to:
   - Use click, shift-click, and ctrl-click to select the devices from the left list.
   - Click the **Add** button to move the devices to the right list. Or double-click on the selected devices.

   Use the search fields at the top of the device lists to locate devices to move.

   Click the **Done** button at the bottom of the panel when you are done selecting the devices that the operation applies to.
7. Click the **Done** button.

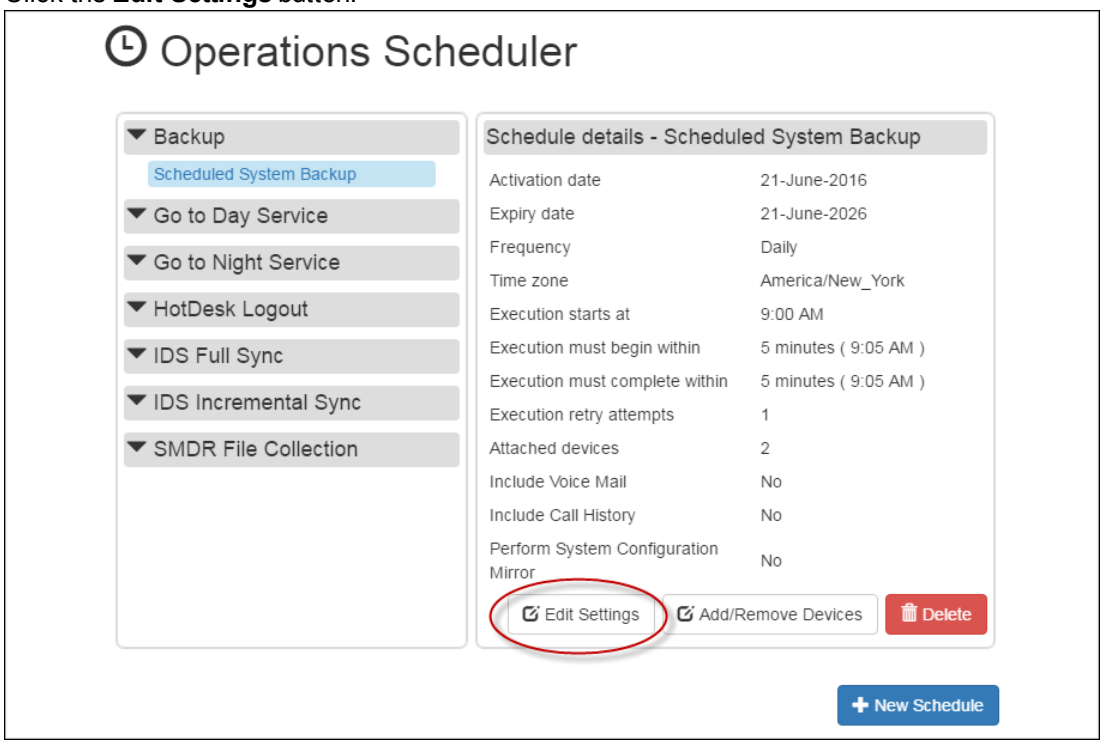
ABOUT MIVOICE BUSINESS ACTIVITIES

You can use Mitel Performance Analytics to centrally configure the details of these activities and schedule them on multiple MiVoice Business call servers. Once configured, Mitel Performance Analytics performs these activities. However it is still possible to use the individual MiVoice Business internal schedulers to schedule activities that might conflict with the Mitel Performance Analytics scheduled activities. For this reason, Mitel recommends that you use either method to schedule MiVoice Business activities but not both.

CHANGING THE SETTINGS OF A SCHEDULE

Do the following steps:

1. Access the **Operations Scheduler**.
2. Click on an existing schedule to display its details.
3. Click the **Edit Settings** button.



The **Edit Operation Schedule** panel displays schedule parameters. Change the parameters as needed. For details on each parameter, see "Scheduling an Operation" on page 161.

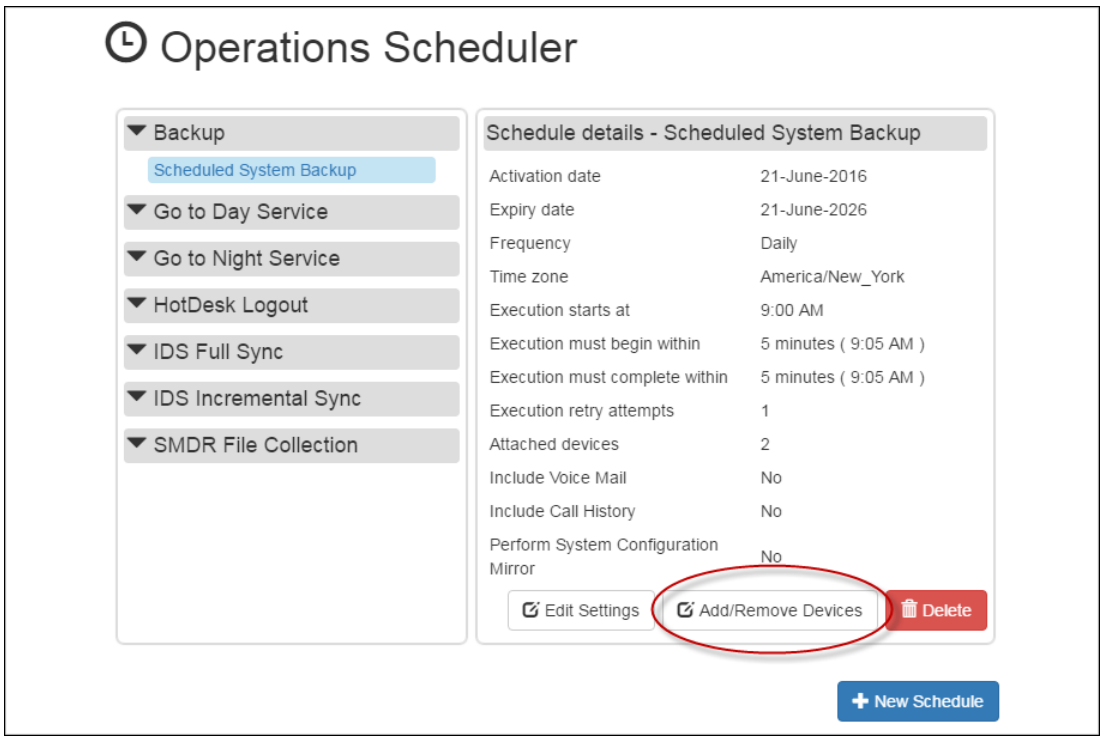
4. Click the **Save** button when done.

ADDING OR REMOVING DEVICES FROM A SCHEDULE

Do the following steps:

1. Access the **Operations Scheduler**.
2. Click on an existing schedule to display its details.

3. Click the **Add/Remove Devices** button.



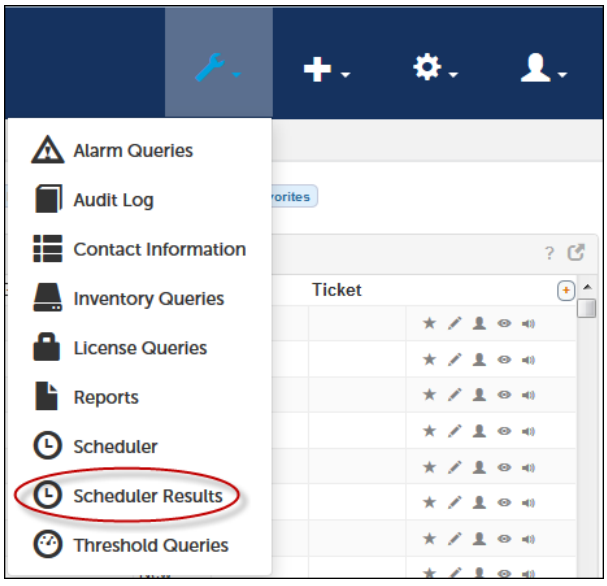
The **Add/Remove Devices** panel displays the devices that are currently associated with the schedule. Add or remove devices as needed.

4. Click the **Save** button when done.

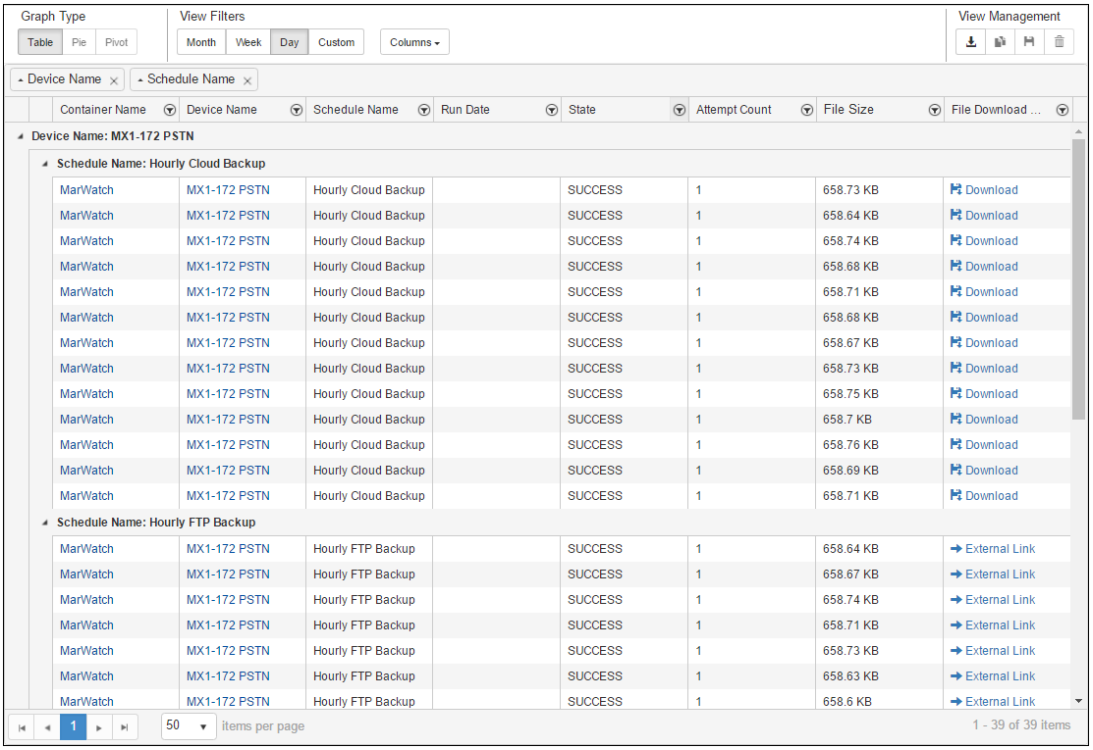
DISPLAYING OPERATION RESULTS

Do the following steps:

1. Select **Scheduler Results** under the **Tools** icon.



2. Choose the **Recent Results** query. The following is an example.

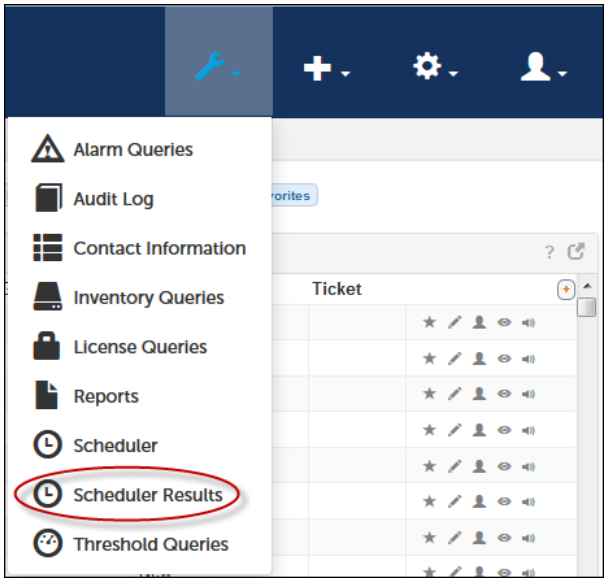


RETRIEVING SCHEDULED SMDR OR BACKUP FILES

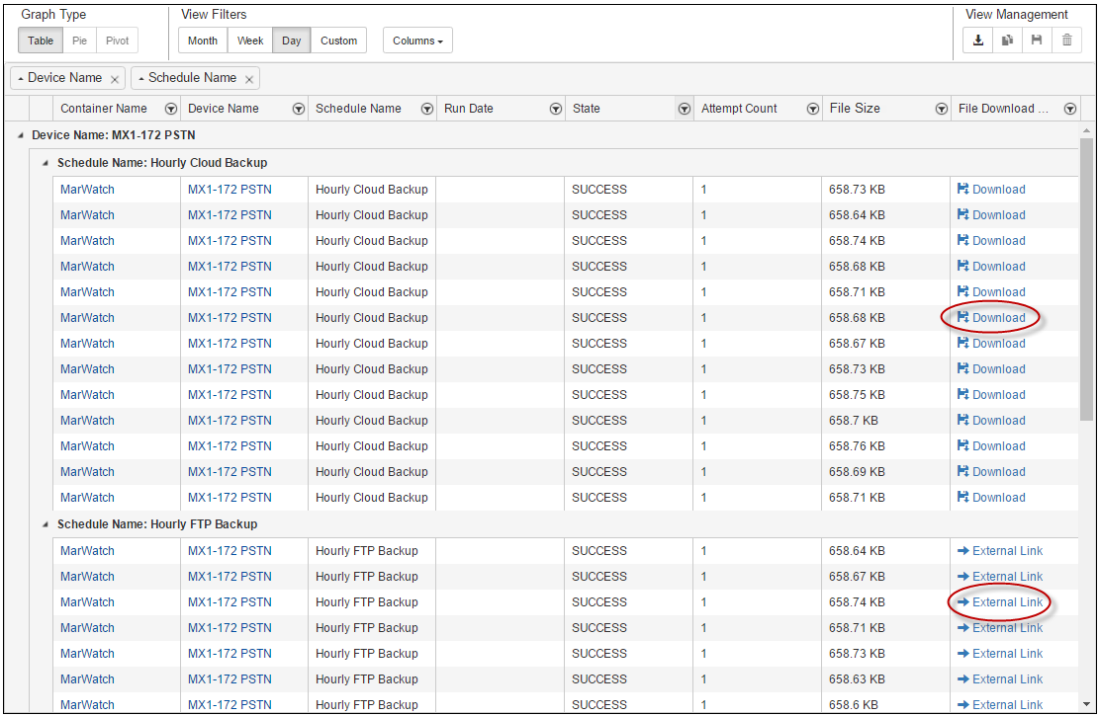
Use the **Recent Results** query or the **Completed Files** query to retrieve scheduled SMDR or backup files.

Do the following steps:

1. Select **Scheduler Results** under the **Tools** icon.



2. Choose the **Recent Results** query or the **Completed Files** query. The following is an example of the **Recent Results** query.



3. Locate the scheduled SMDR or backup file of interest. Click the **Download** link or **External Link** button to download the file to your local computer.

Backup File Name Convention

Mitel Performance Analytics names the backup files using the following convention:

backup_<DeviceType>_<DeviceGUID>_<TimeStampCreated>.tar

where:

- <DeviceType> is the Mitel Performance Analytics device type; currently `MCD` or `MX-ONE`.
- <DeviceGUID> is the GUID of the device.
- The timestamp is the UTC time with the format: yyyy-MM-ddTHH-mm-ssZ.
  The timestamp is the time at the beginning of backup preparation.
- The file extension is `.tar`.

The following is an example:

```
backup_MCD_939de843-3e77-4b06-bd92-ed772cc7a618_2016-06-14T08-00-00Z.tar
```

In the previous example the file is a backup file for a MiVoice Business call server with 939de843-3e77-4b06-bd92-ed772cc7a618 as a GUID; starting 2016, June 14th, 08:00:00 UTC.

SMDR File Name Convention

Mitel Performance Analytics names the SMDR files using the following convention:

<DeviceType>_<DeviceGUID>_<TimeStampCreated>.smdr

where:

- <DeviceType> is the Mitel Performance Analytics device type, one of `MCD`, `Mitel5000` or `AvayaIpOffice`.
- <DeviceGUID> is the GUID of the device.
- The timestamp is the UTC time with the format: yyyy-MM-ddTHH-mm-ssZ.
  The timestamp is the time at the beginning of record collection for a particular SMDR file.
- The file extension is `.smdr`.

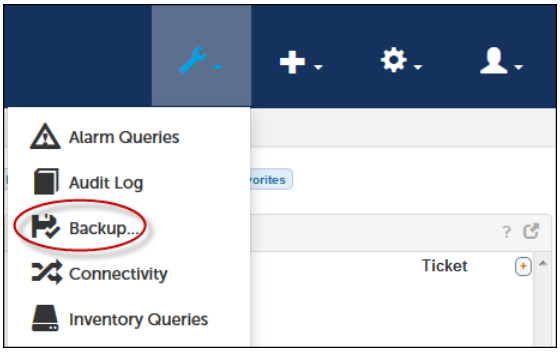
The following is an example:

```
MCD_939de843-3e77-4b06-bd92-ed772cc7a618_2016-09-07T23-00-00Z.smdr
```

In the previous example the file is an SMDR file for a MiVoice Business call server with 939de843-3e77-4b06-bd92-ed772cc7a618 as a GUID; starting 2016, Sep 7th, 00:00:00 UTC.

ON-DEMAND BACKUPS

When applicable, the **On Demand Backup** panel is available by clicking **Backup** under the **Tools** icon of a device dashboard, as follows:



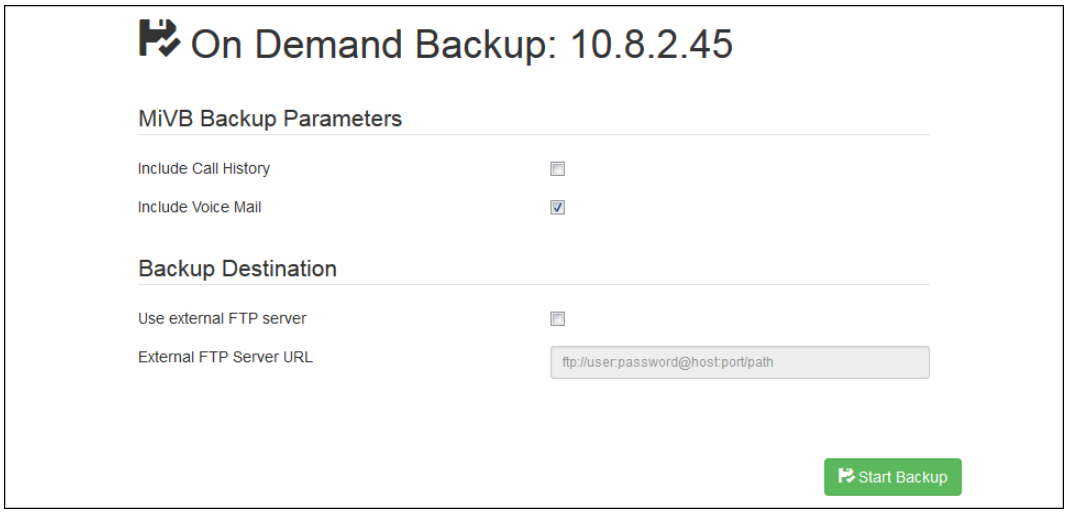
On-demand backups are available for MiVoice Business and MiVoice MX-ONE devices.

Note: Mitel recommends that you avoid using the FreeFTPd server due to known issues and limitations with that product.

PERFORMING AN ON-DEMAND BACKUP

Do the following steps:

1. Access the dashboard for the device you want to backup.
2. Select **Backup** under the **Tools** icon.
   The **On Demand Backup** panel is displayed.



3. If applicable, specify the operation-specific parameters.
   For MiVoice Business backup, the parameters are:
   - **Include Call History**: Optionally include Call History in the backup.
   - **Include Voice Mail**: Optionally include Voice Mail in the backup.

   For MiVoice MX-ONE backup, the parameters are:
   - • **Perform System Configuration Mirror**: Optionally backup all nodes of the telephony system. A regular MX-ONE backup stores telephone user data only. A mirror backup also stores the configuration data of all the nodes.

   Note: A mirror backup can consume significant MX-ONE resources. Perform a mirror backup only during off peak hours.

   The default storage location varies depending on the type of installation:
   - For cloud-based installations, Mitel Performance Analytics stores the backup files to secure offsite storage (Amazon S3).
   - For on-premise installations, Mitel Performance Analytics stores the backup files on its file system file store.

   To use an external server, select **Use external FTP server**:
   - Select the protocol from the dropdown list. You can use the following protocols: SFTP (SSH File Transfer Protocol), FTP (File Transfer Protocol), or FTPS (Secure File Transfer Protocol). Both implicit and explicit FTPS are supported.
   - Supply the URL to the server.
   - Supply the credentials to access the server.
   - Supply the port to use.
4. Click **Start Backup**.
   The **On Demand Backup** panel displays the operation progress.

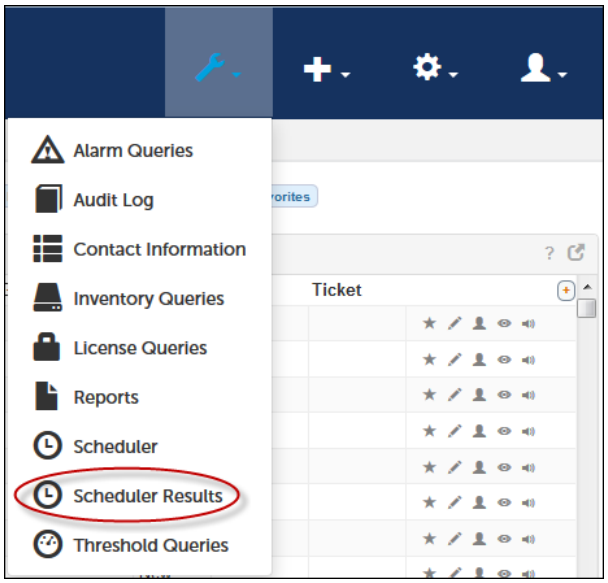
   Once the operation succeeds, the **On Demand Backup** panel displays a link to the backup file. The following is an example.

RETRIEVING ON-DEMAND BACKUP FILES

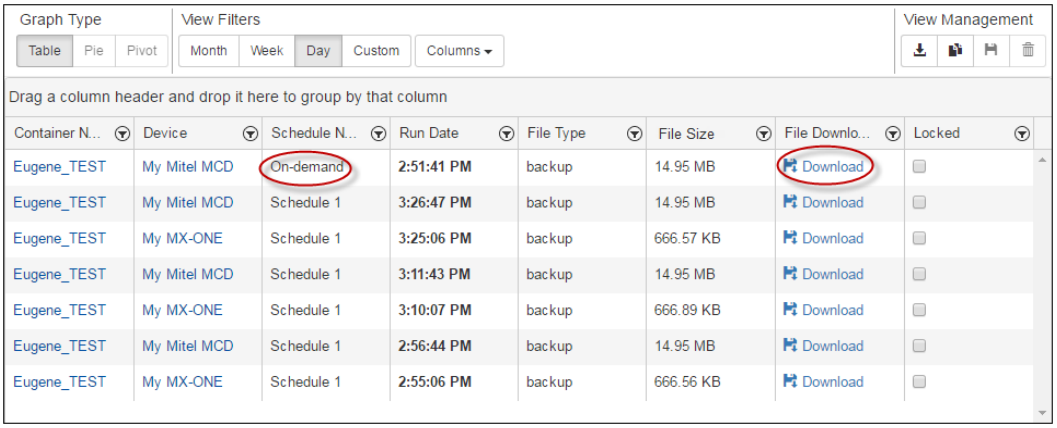
Use the **Completed Files** query to retrieve on-demand backup files.

Do the following steps:

1. Select **Scheduler Results** under the **Tools** icon.



By default the **Completed Files** query is displayed. The following is an example.



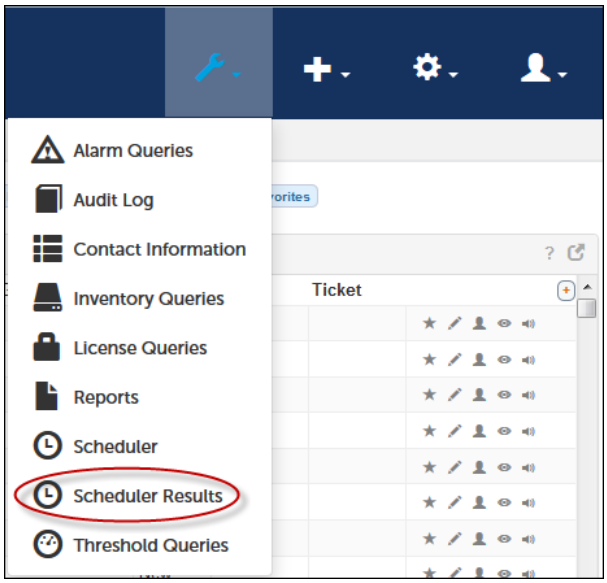
2. Locate the on-demand backup file of interest. Look for a file with a Schedule Name of **On-demand**. Click the **Download** link or **External Link** button to download the file to your local computer.
   For the backup name file convention, see "Performing an On-Demand Backup" on page 168.

LOCKING BACKUP FILES

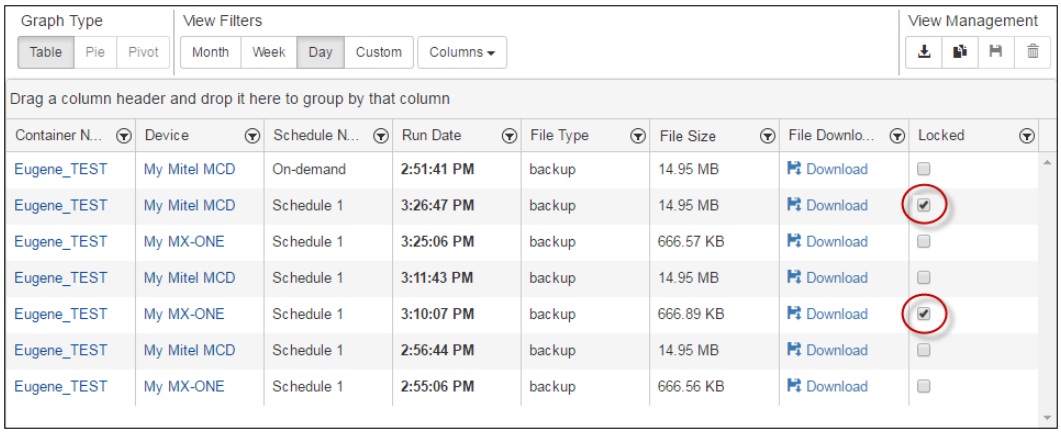
Use the **Completed Files** query to lock backup files. Locked files are retained indefinitely. For cloud-based installations, locking applies only to backup files stored in Mitel Performance Analytics secure offsite storage (Amazon S3). For on-premise installations, locking applies only to backup files stored in the local file system file store.

Do the following steps:

1. Select **Scheduler Results** under the **Tools** icon.



By default the **Completed Files** query is displayed. The following is an example.



2. Locate the backup file of interest. Click its associated **Locked** checkbox.
   You can lock up to five backup files per device.

ADVANCED USER OPERATIONS

Some specific configuration management tasks are complex for customers with MiVoice Business clusters and take a long time to complete. For example, moving a user from one MiVoice Business to another one, removing a user, or setting up and managing Busy Lamp Field (BLF) keys are time-consuming tasks.

The Advanced User Operations (AUO) tool greatly simplifies these tasks and reduces the time that it takes to complete these tasks. The AUO tool applies to MiVoice Business 7.0 and later.

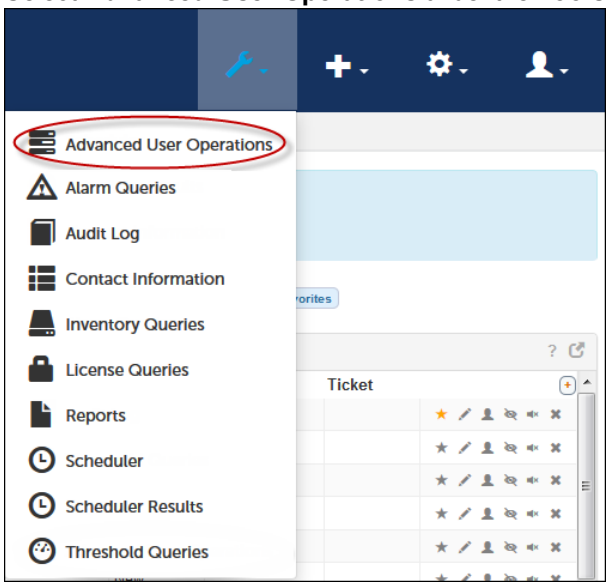
The Advanced User Operations tool helps to simplify the following scenarios:

- A user moves to a different location;
- A user leaves the company;

- The name of a user extension changes;
- A user changes departments within a company and thus the BLF needs to change;
- A complex BLF configuration setup.

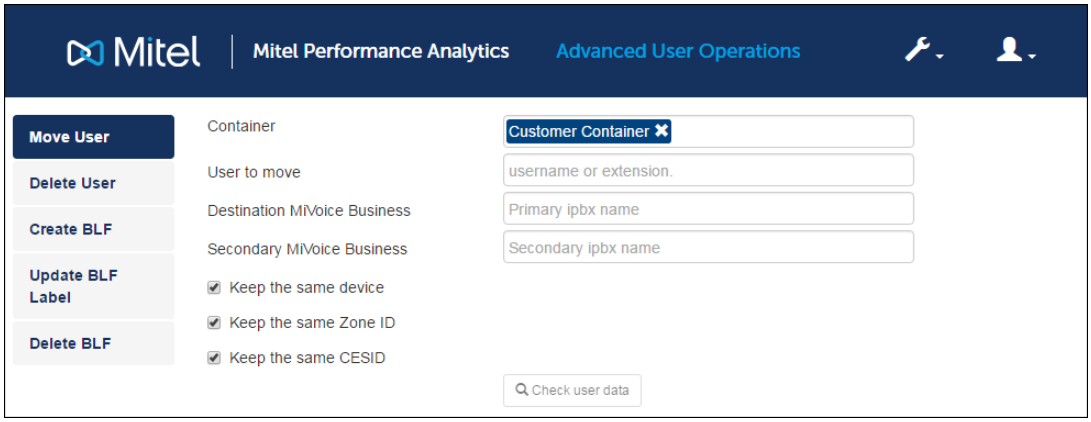
To access the AUO tool, do the following steps:

1. Select **Advanced User Operations** under the **Tools** icon.



The AUO tool opens and requests that you log in.

2. Supply your Mitel Performance Analytics credentials.
The main AUO panel is displayed.



For details on using the AUDO tool, refer to its online help.

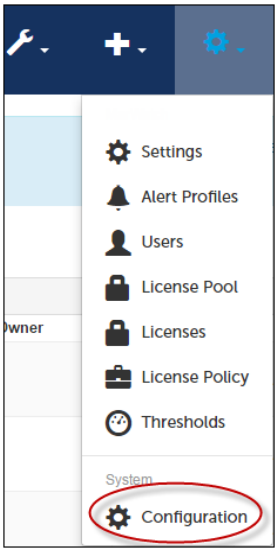
The AUO tool has the following menu items:

ICON	NAME	FUNCTION
	Tools	Use the **Dashboard** menu item to access the Mitel Performance Analytics dashboard. For devices, more and different tools may be displayed depending on the type of device.
	User	Use the menu items to: • Display online help • Display information about Mitel Performance Analytics • Log out of Mitel Performance Analytics

SYSTEM ADMINISTRATION PROCEDURES

Mitel Performance Analytics system administration is restricted to users with the **System Admin** permission.

To access the configuration window, select **System Configuration** under the **Settings** icon:

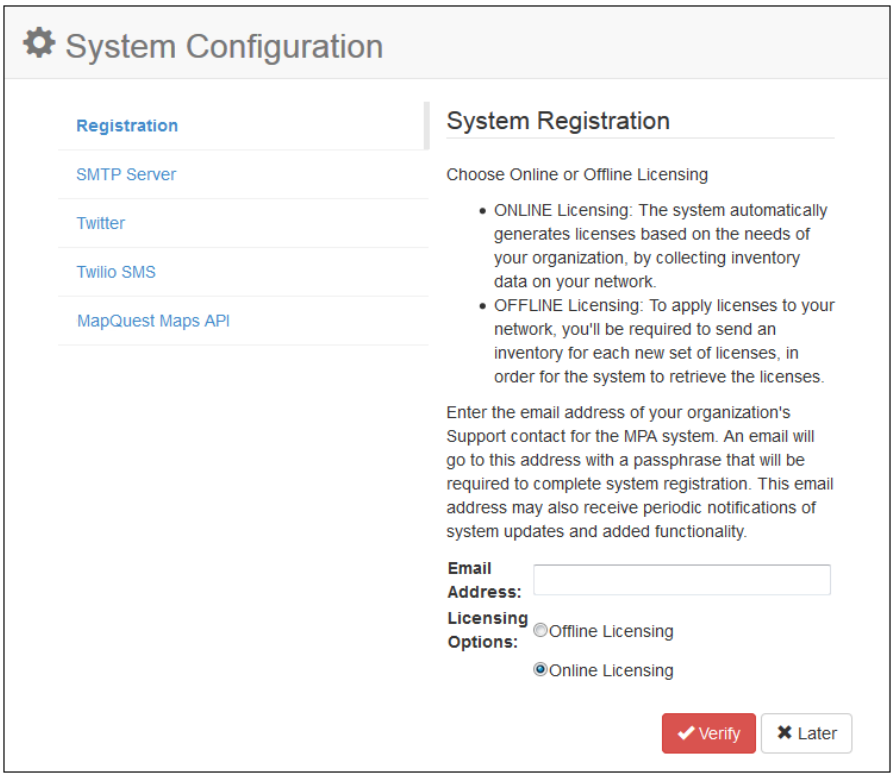


REGISTERING A SYSTEM

Licensed features do not operate until you register the Mitel Performance Analytics system and register a valid license IDs to a container; or manually perform licensing tasks. To register a license ID to a container, see "Registering a License ID to a Container" on page 175.

Do the following steps:

1. Initially, the **System Configuration** window displays the **System Registration** and **License Registration** panes.
   Note: The **License Registration** pane appears only after you have registered a Mitel Performance Analytics system.



2. In the **System Registration** pane, supply an email address. This can be any email address. Mitel Performance Analytics does not use the email address for any purpose other than sending a passphrase to complete the registration process.
3. Select your licensing option:
   - Online: This option automates all tasks related to licensing.
   - Offline: This option means you need to manually perform licensing tasks. Licensing tasks include uploading a license policy, uploading license files, and applying licenses. See "Mitel Performance Analytics Licensing" on page 100 for details.
4. Click **Verify**. A **Passphrase** field appears.
   Mitel Performance Analytics sends a passphrase at the previously specified email address.
5. When you receive the passphrase, enter it in the **Passphrase** field.
6. Click **Verify & Save**.
   The **System Registration** pane confirms you are now registered in the licensing and support server.

REGISTERING A LICENSE ID TO A CONTAINER

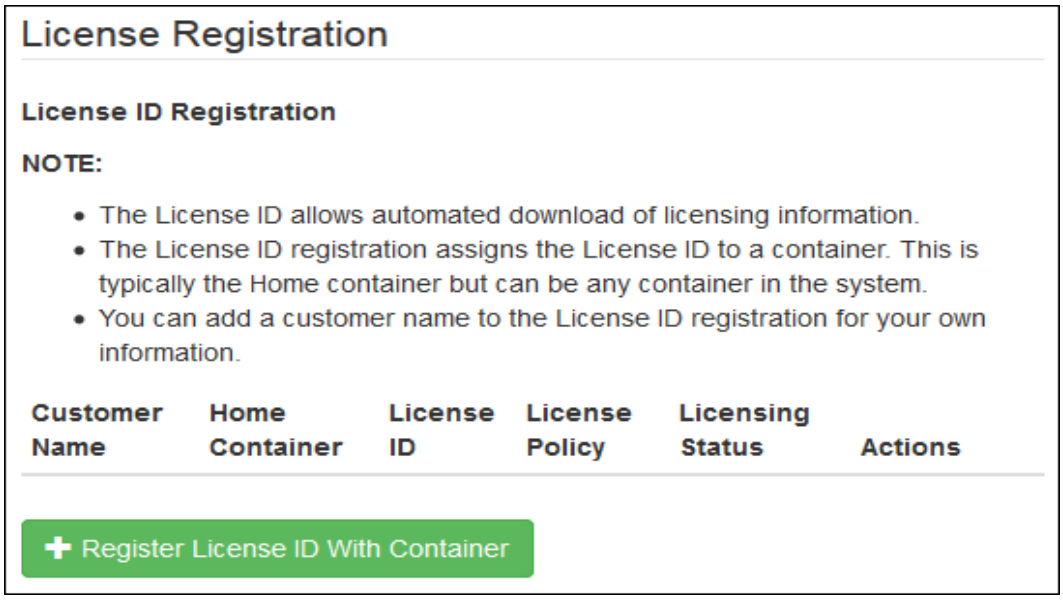
Licensed features do not operate until you register the Mitel Performance Analytics system and register a valid license ID to a container; or manually perform licensing tasks. To register the Mitel Performance Analytics system, see "Registering a System" on page 174.

Do the following steps:

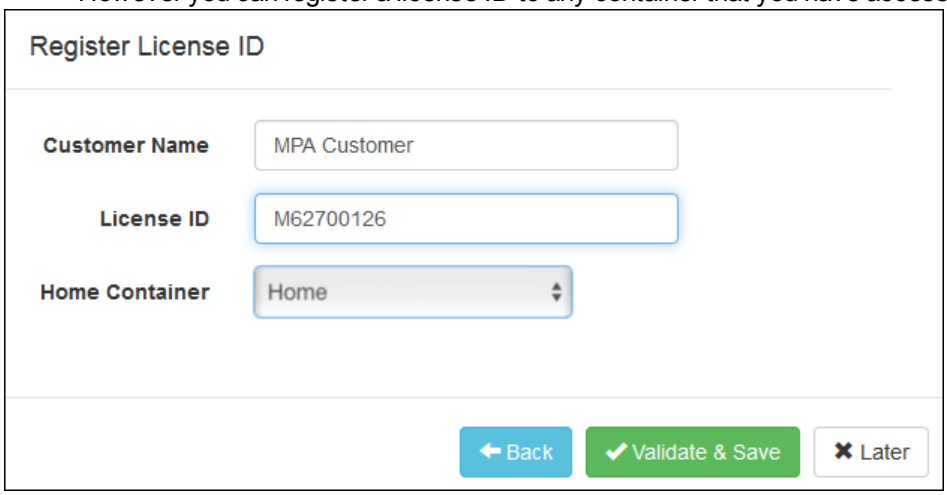
1. Open the dashboard of the topmost or root container and select **System Configuration** under the **Settings** icon:

The **System Configuration** window displays the **System Registration** and **License Registration** panes.

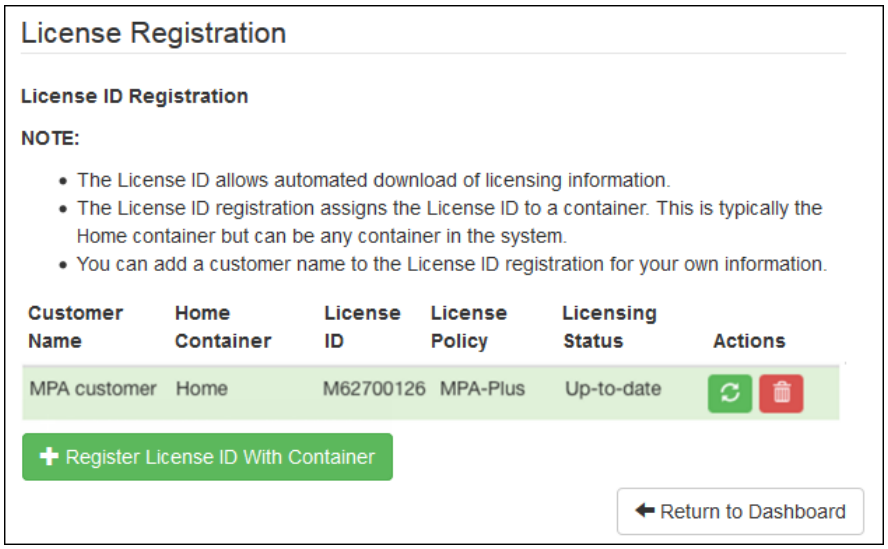
Note: The **License Registration** pane appears only after you have registered a Mitel Performance Analytics system.



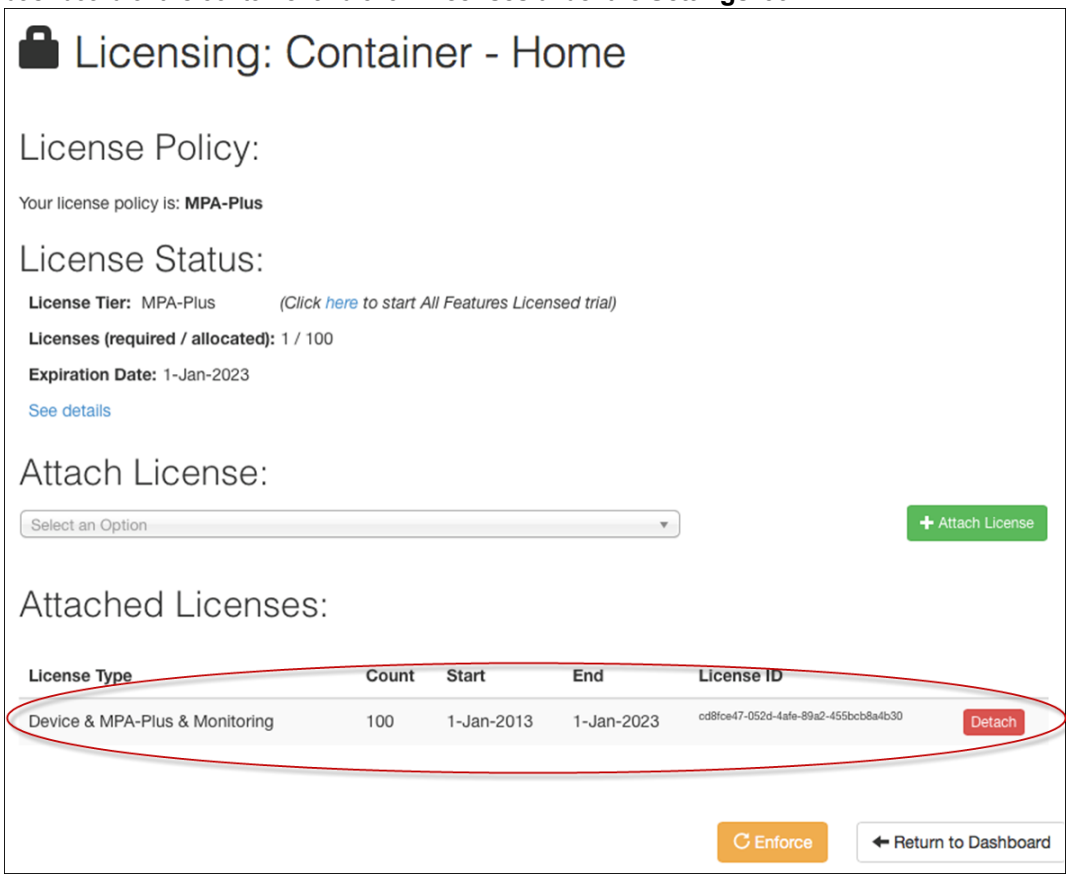
2. Click **Register License ID with Container**.
3. In the resulting screen:
   - Input a customer name.
   - Input the license ID: You are provided the license ID by your supplier once your order has been processed.
   - Use the dropdown list to choose the container that is associated with the license ID. In most cases, this is the home container for the Mitel Performance Analytics system. However you can register a license ID to any container that you have access to.



4. Click **Validate & Save**.
   Mitel Performance Analytics connects to the licensing server and download its licenses.



5. Confirm the license are downloaded and assigned to the expected container. Go to the dashboard of the container and click **Licenses** under the **Settings** icon.



REFRESHING ONLINE LICENSING

With online licensing, Mitel Performance Analytics automatically performs inventories, uploads license files as required, and applies licenses as required.

However, you can choose to manually trigger the online licensing process.

Do the following steps:

1. In the **License Registration** pane, identify the license ID that you want to trigger the online licensing process. Click the green **Refresh** icon.
   The system uploads a license policy to your system, performs an inventory, and then uploads and applies all licenses associated with that license ID.

RELEASING A LICENSE ID

A license ID can only be associated with a single Mitel Performance Analytics system or a single container. To move a license ID to a different system or container, you must first release it.

Releasing a license ID causes all of their licensing data to be removed the container; thus freeing the licenses to be re-associated with a different container or system.

Do the following steps:

1. In the **Licensing Registration** pane, identify the license ID that you want to release. Click the red **Trash** icon.
   The system removes of the licensing data from the container.

To register the license ID to a different system or container, see "Registering a License ID to a Container" on page 175

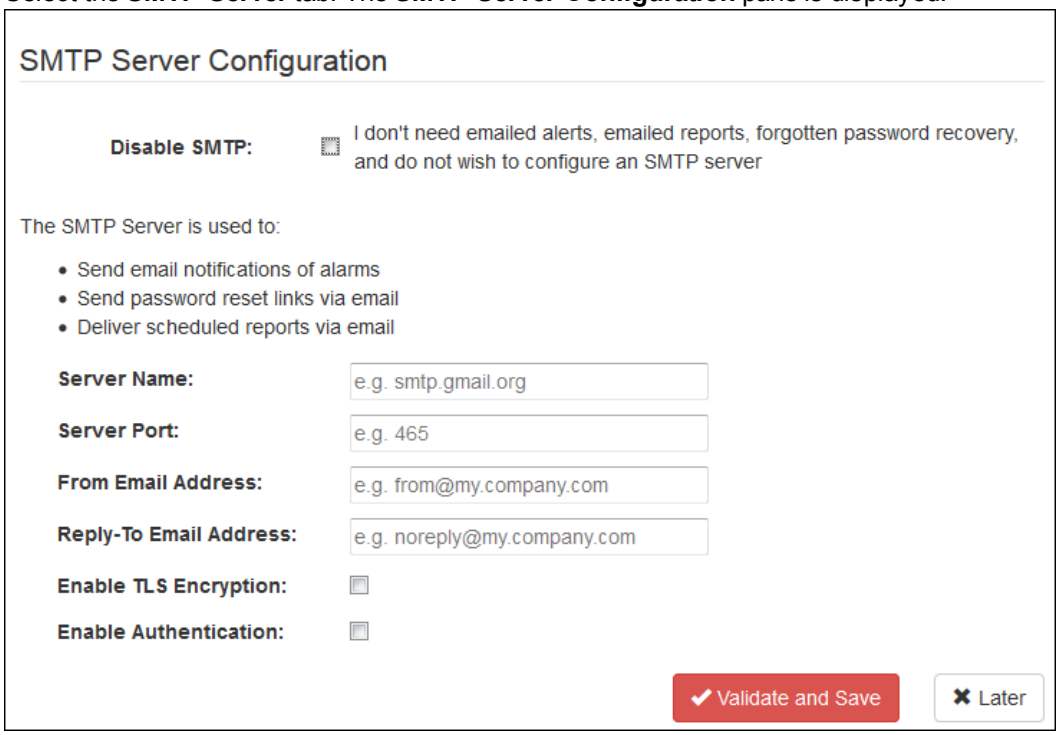
CONFIGURING THE SMTP SERVER

Use this procedure to update or correct SMTP server settings used by Mitel Performance Analytics to:

- Send email notification of alarms
- Send forgotten password reset links by email
- Deliver scheduled reports by email

Do the following steps:

1. Select the **SMTP Server** tab. The **SMTP Server Configuration** pane is displayed.



2. In the **SMTP Server Configuration** pane, enter the SMTP server configuration settings:
   - SMTP server name or address; for example, `smtp.gmail.com`
   - SMTP server port number; typically `25`, `465` or `587`
   - From email address; When Mitel Performance Analytics generates an email, it displays this email address as the originator.
   - Reply-to email address; Replies to a Mitel Performance Analytics-generated email are sent to this email address.
   - SMTP encryption; yes or no. Mitel recommends that you use encryption.
   - SMTP authentication; yes or no
   - STMP username and password (for authentication, if required)

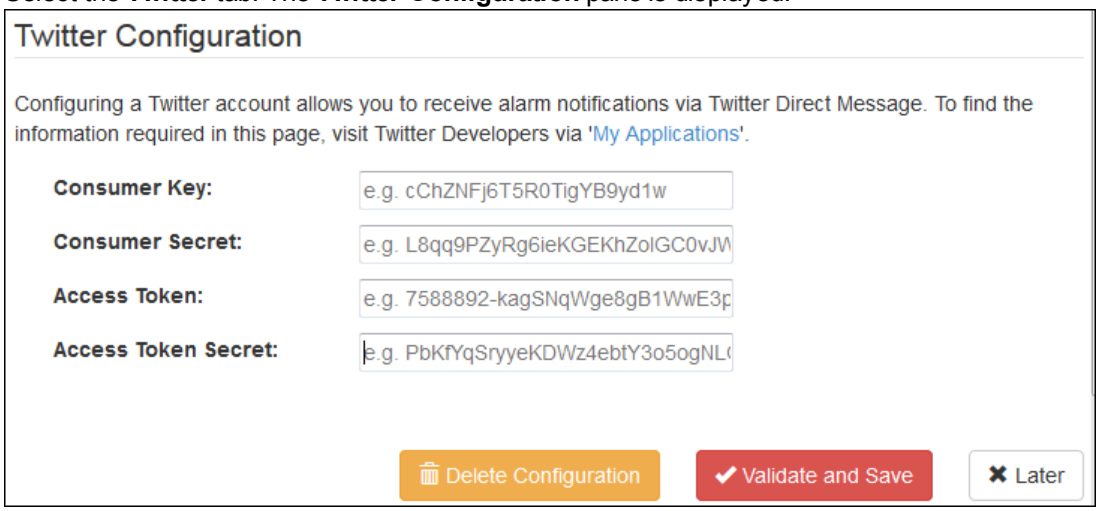
   You can also disable SMTP configuration thus avoiding reminders and notifications when you log in that the SMTP server has not been configured.
3. Click **Validate** and **Save**.

CONFIGURING A TWITTER ACCOUNT

Use this procedure to configure a Twitter account so you can receive alarm notification through Twitter.

Do the following steps:

1. Select the **Twitter** tab. The **Twitter Configuration** pane is displayed.



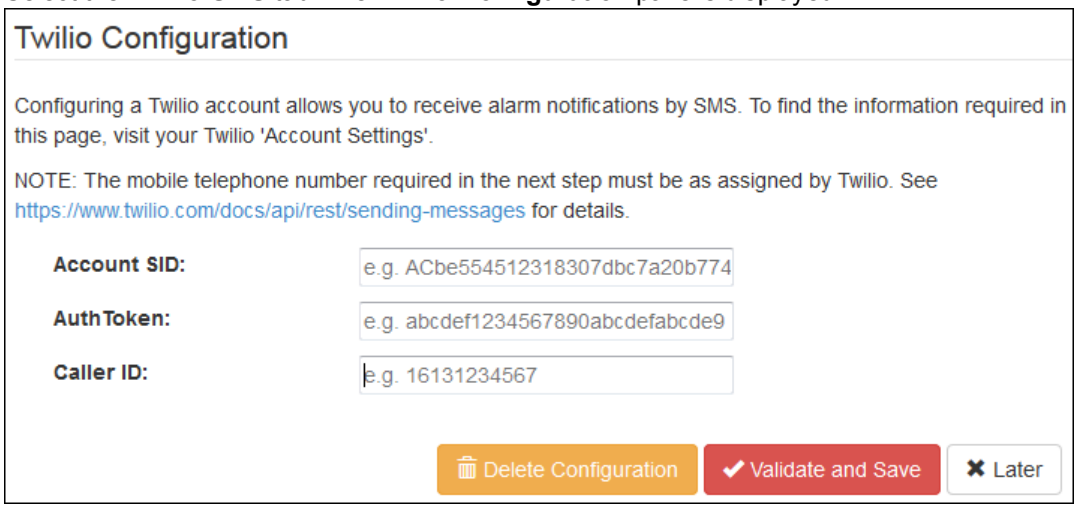
2. In the **Twitter Configuration** pane, enter your Twitter account data:
   - Consumer key
   - Consumer secret
   - Access token
   - Access token secret
3. Click **Validate** and **Save**.

CONFIGURING A TWILIO SMS ACCOUNT

Use this procedure to configure a Twilio SMS account so you can receive alarm notification through SMS.

Do the following steps:

1. Select the **Twilio SMS** tab. The **Twilio Configuration** pane is displayed.



2. In the **Twilio Configuration** pane, enter your Twilio account data:
   - Account SID

- AuthToken
- Caller ID

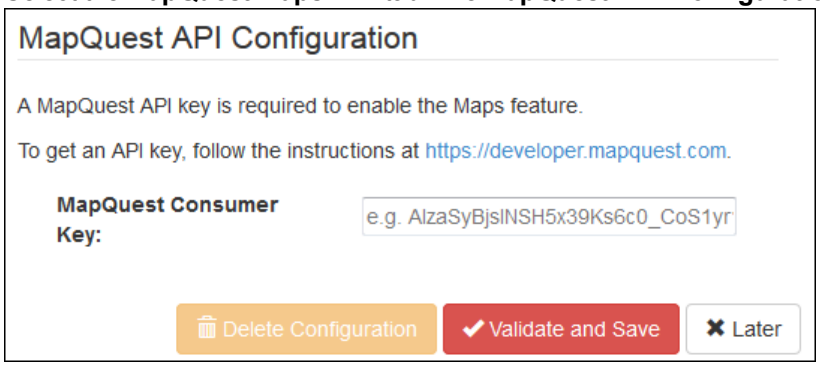
3. Click **Validate** and **Save**.

CONFIGURING A MAPQUEST MAPS API KEY

Use this procedure to configure a MapQuest Maps API key to enable dashboard maps and map coordinate lookup from street addresses.

Do the following steps:

1. Select the **MapQuest Maps API** tab. The **MapQuest API Configuration** pane is displayed.



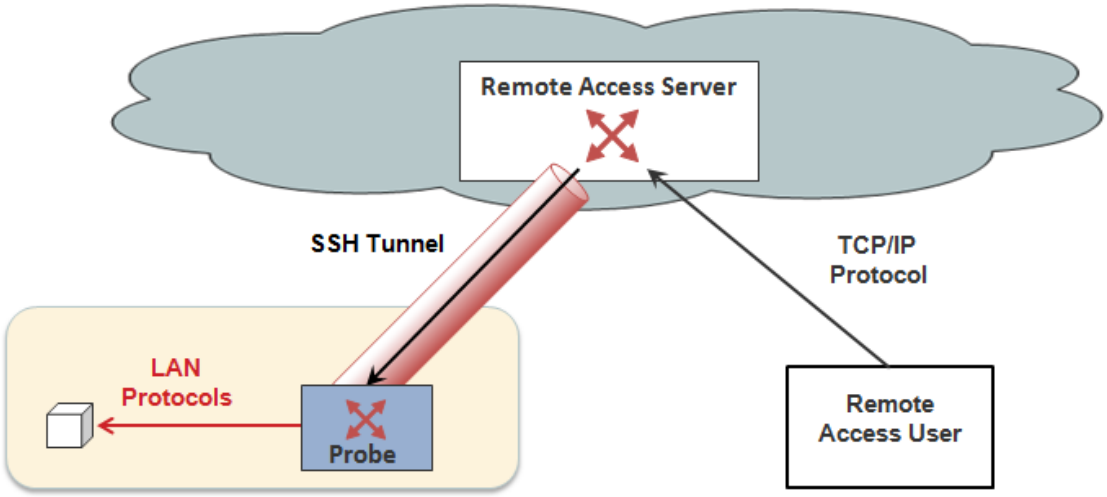
2. In the **MapQuest API Configuration** pane, enter your MapQuest Consumer API key.
3. Click **Validate** and **Save**.

MITEL PERFORMANCE ANALYTICS REMOTE ACCESS

With Mitel Performance Analytics Remote Access, you can connect to a remote monitored device or any other device on the customer LAN using any Internet connection, without the need for pre-installed VPNs or modems.

MITEL PERFORMANCE ANALYTICS REMOTE ACCESS ARCHITECTURE

The Probe establishes and maintains a persistent SSH connection to the Mitel Performance Analytics server.



When the Remote Access user requests a remote access connection to a device on the remote LAN, the sequence of actions is:

1. The user initiates a request using the Mitel Performance Analytics web interface. Only users who have specific remote access privileges are permitted to implement remote access.
2. All remote access requests are logged with user ID, LAN IP address, and time of request.
3. Mitel Performance Analytics checks the requested LAN address against the Probe's Remote Access Control settings. If the Remote Access Control settings allow it, the remote access request is allowed to proceed. If the Remote Access Control settings do not allow it, the remote access request is denied and the attempt is recorded in the audit log.
4. Mitel Performance Analytics sends a message to the Probe over the SSH connection requesting it to create an SSH Port Forward or "tunnel" for TCP/IP through the SSH connection, and to forward packets from this tunnel to the LAN IP address.
5. Mitel Performance Analytics "opens" a port on a publically reachable IP address for the Mitel Performance Analytics Remote Access server and listens for IP packets with a source IP address that is the same as the address of the PC that was used to request the remote access session.
6. If the source address matches, the Mitel Performance Analytics Remote Access server establishes a remote access session and forwards the IP packet from the user's PC through

the secure SSH Port Forward to the Probe. The Probe in turn forwards the packet to the remote LAN device.

7. Once the remote access session has been established, the Probe forwards IP packets it receives from the remote LAN device through the SSH Port Forward to the user's PC.
8. If the session is idle for a timeout period, typically 15 minutes, the SSH Port Forward is closed and the remote access server stops listening for incoming traffic from the user's PC.

ADVANTAGES OF MITEL PERFORMANCE ANALYTICS REMOTE ACCESS

Mitel Performance Analytics Remote Access provides a number of key advantages:

- There is generally no need to configure firewall rules at either the remote site or the reseller site, because Mitel Performance Analytics Remote Access uses outbound connections from the Probe using standard TCP/IP protocols.
- No VPN server or client software is required, either at the remote site or on the user's PC.
- Because no VPN software is required, there is no chance of VPN client conflict. Different customers may prefer different VPN clients and in most cases these different VPN clients cannot co-exist or operate at the same time on the user's PC.
- The Mitel Performance Analytics Remote Access service allows multiple simultaneous connections from the user's PC to different remote sites without having to worry about IP addressing conflicts. This is not possible using VPN technologies.
- The Mitel Performance Analytics Remote Access service manages all of the security tokens required to establish a secure remote connection, avoiding the need to maintain multiple lists of VPN access credentials.

REMOTE ACCESS CONNECTION SECURITY FEATURES

The Mitel Performance Analytics Remote Access service uses standard IP security mechanisms. The communication links are secure using industry standard encryption and authentication mechanisms.

- **System Authentication**: Mitel Performance Analytics uses a 2048-bit security certificate and authenticates all connection requests.
- **SSL**: All SSL sessions to Mitel Performance Analytics are encrypted and authenticated using RSA-2048 for key exchange and AES 128 for encryption.
- **SSH**: All SSH sessions are encrypted and authenticated using RSA-1024 with rotation for key exchange and AES 128 for encryption. Key Rotation is enabled generating a new key for each session.

REMOTE ACCESS CONTROL SETTINGS

Mitel Performance Analytics allows remote access controls on the Probe settings sheet. Users can configure the Probe to:

- Never allow port forwarding, thereby blocking all remote access capabilities
- Allow port forwarding only to those devices monitored by the Probe
- Allow port forwarding for all devices on the subnet the Probe is connected to, thereby allow remote access to device not monitored by the Probe

The **Remote Access** panel for the Probe provides information on all active remote access sessions.

SOURCE IP ADDRESS RESTRICTION

Mitel Performance Analytics accepts only incoming remote access packets with the source IP address of the user who requested the Remote Access session.

AUDIT LOG REMOTE ACCESS RECORDS

Mitel Performance Analytics maintains an Audit Log for all Remote Access sessions. The Audit Log records the Mitel Performance Analytics user name and address of the remote device.

USER IP PROTOCOL SECURITY

The link between the user's PC and the Mitel Performance Analytics system uses Internet connectivity for cloud-hosted Mitel Performance Analytics. Therefore, any traffic that is sent over this link is encrypted for security.

Mitel uses SSL/HTTPS for connection to Mitel Performance Analytics web portals with security provided by RSA-2048 for key exchange and AES 128 for encryption.

The following table lists commonly used TCP/IP protocols and their security levels:

PROTOCOL	SECURE	APPLICATION
HTTP	No	Web
HTTPS	Yes	Web
SCP	Yes	File Transfer
SFTP	Yes	File Transfer
SSH	Yes	Secure Session
Telnet	No	Terminal Session
FTP	No	File Transfer

Mitel cautions against the use of HTTP, Telnet and FTP when using Mitel Performance Analytics Remote Access because the segment of the connection between the user's PC and the Mitel Performance Analytics server is not secured.

CERTIFICATE WARNINGS

Because of the way that Mitel Performance Analytics provides remote access connections, users may receive certificate warnings when the connection is being established. This is completely normal and is not a cause for alarm.

REMOTE ACCESS PROCEDURES

The Mitel Performance Analytics Remote Access capability can be used to connect to any device on the remote LAN as long as the Remote Access Control settings do not restrict access. For details on Remote Access Control, see "Remote Access Control Configuration" on page 115.

Remote access is performed through the **Port Forwards** panel on the device dashboard. The **Port Forwards** panel is usually located at the bottom of the device dashboard.

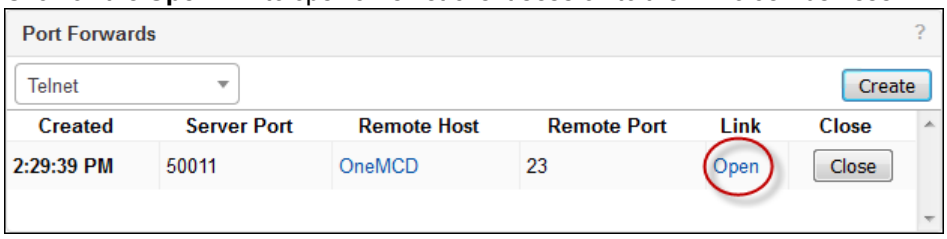
This section uses examples to illustrate how to use Mitel Performance Analytics Remote Access to connect to various devices using various protocols. The examples cover the following devices:

- MIVoice Business
- MiVoice MX-ONE
- MiCollab server
- MiVoice Office 250
- HP ProCurve switch
- Avaya IP Office System Status Application (SSA)
- PathSolutions Server

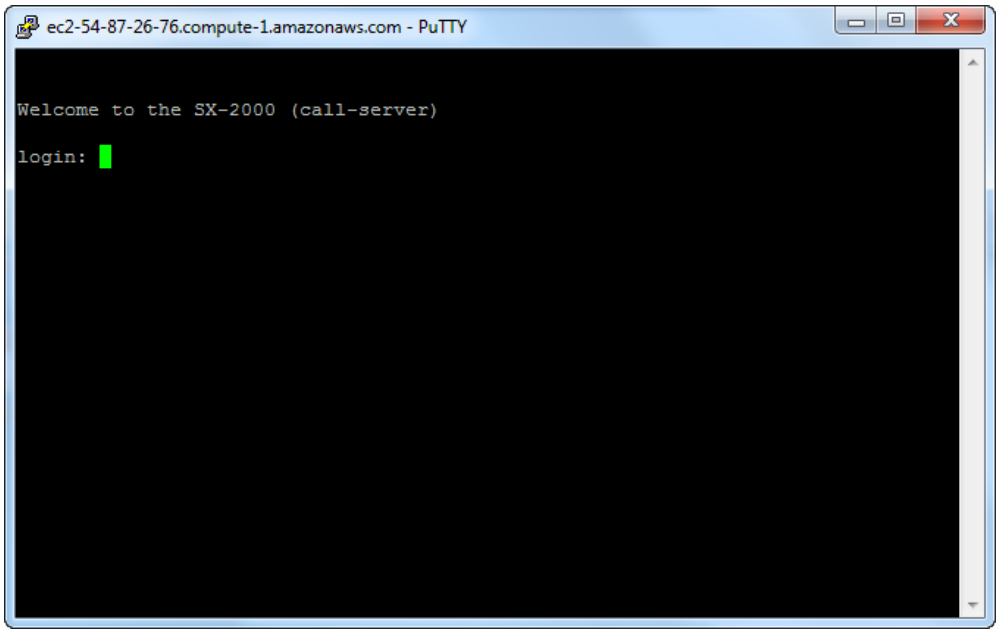
CONNECTING TO A MIVOICE BUSINESS USING TELNET

To use Mitel Performance Analytics Remote Access to connect to a MiVoice Business call server with the Telnet protocol, do the following steps:

1. Access the dashboard for the device you want to connect to.
2. From the **Port Forwards** panel, select **Telnet** from the protocol dropdown list or supply a non-default port number. If you choose **Telnet**, the remote access session uses default port 23.
3. Click on the **Create** button to create a port. The **Port Forwards** panel updates. The various table columns are populated.
4. Click on the **Open** link to open a Telnet client session to the MiVoice Business.



The Telnet session starts.

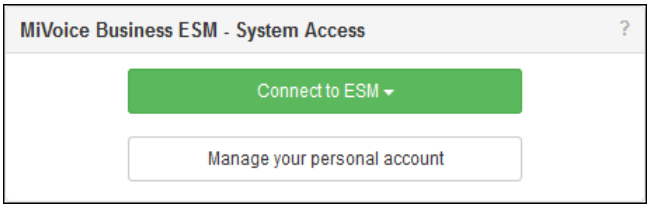


5. Enter your credentials to Telnet into the MiVoice Business.

Tip: You can use these instructions to connect to the MiVoice Business port 2002 to manage it.

CONNECTING TO MIVOICE BUSINESS ESM

Remote access to a MiVoice Business ESM is done through the **MiVoice Business ESM - System Access** panel.



General Considerations

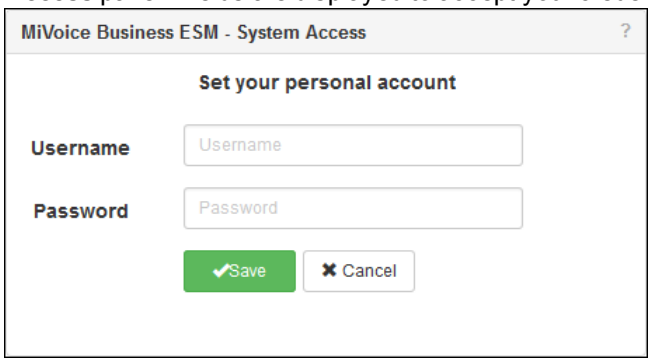
Consider the following when using this panel:

- The MiVoice Business/3300 must be monitored by a Probe for the **MiVoice Business ESM-System Access** panel to be present.
- To connect to a MiVoice Business ESM, you must use a supported browser and a private browsing session. If you attempt to connect with a public browsing session, you are provided a link to use once you open a private browsing session. To start a private browsing session, right-click on the provided link and choose the appropriate menu item, such as **Open Link in New Private Window** for Firefox.

Configuring your ESM Credentials

Do the following steps:

1. Click the **Manage your personal account** button on the **MiVoice Business ESM- System Access** panel. Fields are displayed to accept your credentials.



2. Enter your username and password, and click **Save**.

Once configured, the **MiVoice Business ESM- System Access** panel uses your credentials to start a session with the MiVoice Business ESM when you invoke that option.

Using a Shared Account

An administrator can configure a shared account from the device **Settings** page. See "MiVoice Business Device Configuration" on page 120 for details.

Once configured, all users with **Remote Access** and **Shared SSO Credentials** permissions can use the shared account to log into the MiVoice Business ESM. If configured, the shared account option is listed in the **Connect to ESM** button dropdown list. Users shared account users are not aware of the shared account password. Invoking the shared account option starts a session with the MiVoice Business ESM without displaying its login page.

Starting an ESM Session

To start an ESM session, choose a connection option from the Connect to ESM drop down list:

- Choose **Login page** to display the ESM login page. You can then use any credentials to start an ESM session.
- Choose **Personal account** to start an ESM session with the credentials configured with the **MiVoice Business ESM- System Access** panel. The ESM session starts without you having to supply credentials.
- Choose **Shared account** to start an ESM session with the preconfigured shared account. The ESM session starts without you having to supply credentials.

To start an ESM session, click **Connect to ESM**.

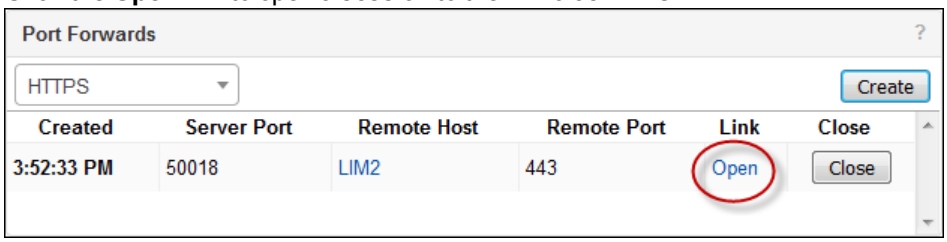
The Mitel ESM web interface does not support all Web browsers. If you are using a Web browser for Mitel Performance Analytics that is not supported by the ESM web interface, then the **MiVoice Business ESM- System Access** panel informs you of the issue and provides a link that you can use in one of the supported Web browsers to access ESM.

All attempts to access ESM are recorded in the audit log.

CONNECTING TO A MIVOICE MX-ONE

Do the following steps:

1. Access the dashboard for the device you want to connect to.
2. From the **Port Forwards** panel, select the desired protocol from the protocol dropdown list or supply a non-default port number.
3. Click the **Create** button to create a port. The **Port Forwards** panel updates. The various table columns are populated.
4. Click the **Open** link to open a session to the MiVoice MX-ONE.



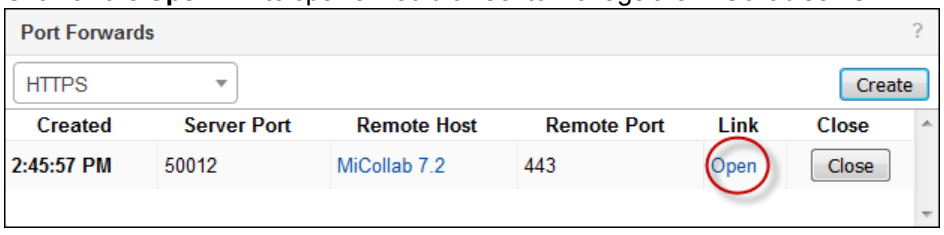
Either a MiVoice MX-ONE Provisioning Manager or Service Node Manager session is started, depending on what Mitel Performance Analytics is configured to monitor.

If you are using a Web browser for Mitel Performance Analytics that does not support the selected protocol (for example SSH or TFTP), then the **Port Forwards** panel informs you of the issue. Start a separate application that does support the selected protocol. Use the supplied **Server Port** to connect to the MiVoice MX-ONE.

CONNECTING TO A MICOLLAB SERVER USING HTTPS

To use Mitel Performance Analytics Remote Access to connect to a MiCollab server with the HTTPS protocol, do the following steps:

1. Access the dashboard for the device you want to connect to.
2. From the **Port Forwards** panel, select **HTTPS** from the protocol dropdown list or supply a non-default port number. If you choose **HTTPS**, the remote access session uses default port 443.
3. Click on the **Create** button to create a port. The **Port Forwards** panel updates. The various table columns are populated.
4. Click on the **Open** link to open a web browser to manage the MiCollab server.



The browser opens to the web page for the MiCollab server.

Some MiCollab server releases return the following error message:

"Your browser does not appear to support cookies or has cookie support disabled. This site requires cookies - please turn cookie support on or try again using a different browser. "

If you receive this message, do the following steps:

1. Open another browser window and navigate to the following URL: `http://msl-fix.marwatch.net/`
2. Log into the MiVoice Border Gateway or MiCollab again. You should be able to log in successfully.

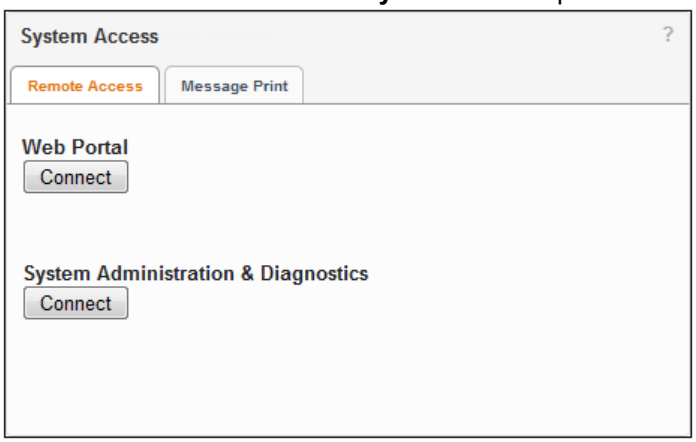
CONNECTING TO A MIVOICE OFFICE 250

Access to a MiVoice Office 250 is done by using the MiVoice Office 250 **System Access** panel and **Mitel System Administration and Diagnostics**.

The software version of **System Administration and Diagnostics** must match the software version of the target MiVoice Office 250 device.

Do the following steps:

1. Access the MiVoice Office 250 **System Access** panel.



2. Click **Connect** under **System Administration and Diagnostics**. A connection is created to the device.
3. Access the device using **Mitel System Administration and Diagnostics**:
   - Open the **Mitel System Administration and Diagnostics** tool.
   - Open the **Setup** > **Options** menu in the top right corner of the software.
   - Under the **Advanced** tab, ensure **Show IP** ports is selected.
   - Click **OK**.
   - Under the **System Connection** section, select **Add System Connection**.
   - Give the connection a name.
   - Enter the IP address from the Mitel Performance Analytics MiVoice Office 250 **System Access** panel to the **Onsite IP address / Hostname** field.
   - Enter the port value from the Mitel Performance Analytics MiVoice Office 250 **System Access** panel to the **Listening Port** field.
   - Click **Save connection**.
   - Click **System management tools** > **Launch DB Programming** on the application.

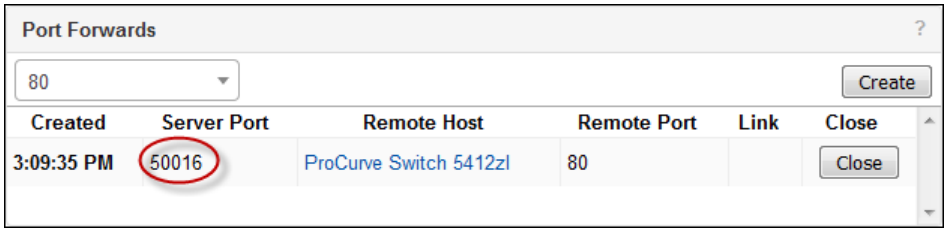
MiVoice Office 250 Web Portal

To access the MiVoice Office 250 web interface, click **Connect** under **Web Portal** on the MiVoice Office 250 **System Access** panel. A connection is created to the device. Click the resulting **Web Manager** link and the web manager page for the device appears.

CONNECTING TO AN HP PROCURVE SWITCH USING HTTP

To use Mitel Performance Analytics Remote Access to connect to an HP ProCurve switch with the HTTP protocol, do the following steps:

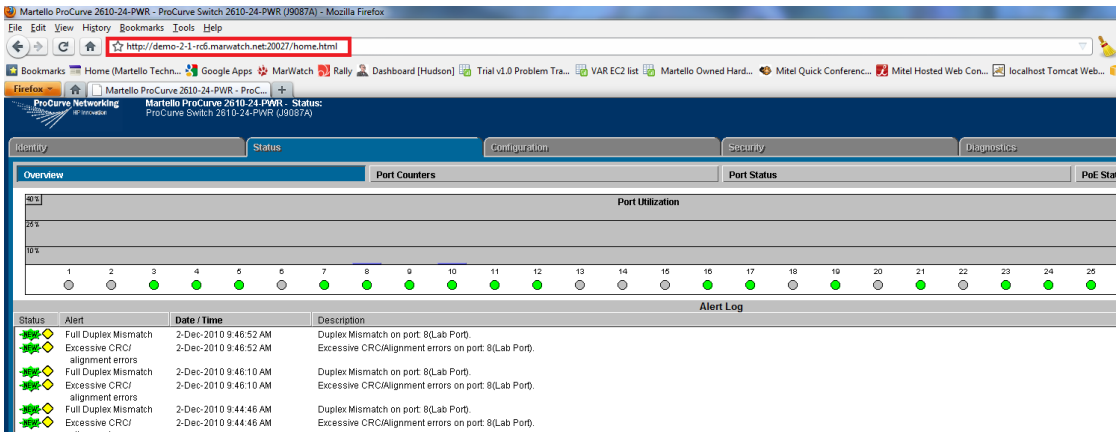
1. Access the dashboard for the device you want to connect to.
2. From the **Port Forwards** panel, the protocol dropdown list does not list HTTP. Enter the default HTTP port, **80**.
3. Click on the **Create** button to create a port. The **Port Forwards** panel updates. The various table columns are populated. Note the Server Port number. In the following example, it is **50016**.



4. Open your browser and input a URL using the following syntax: https://<MPA_FQDN>:<Server_Port>

   Note: The previous syntax statement uses HTTPS instead of HTTP because you need to HTTPS to access the Mitel Performance Analytics server. The Mitel Performance Analytics server then connects you to the Probe using SSH. Finally, the Probe connects to the ProCurve switch using HTTP.

   The browser opens to the embedded web page for the HP ProCurve switch. The following is an example.



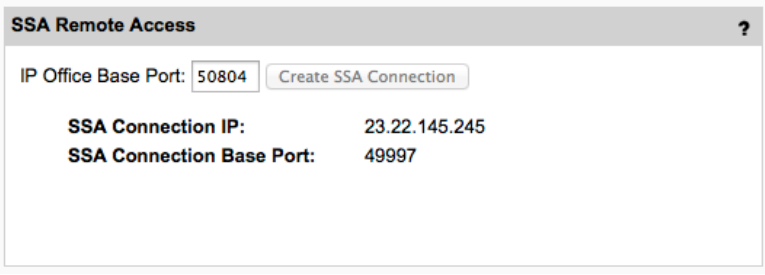
CONNECTING TO AN AVAYA IP OFFICE SSA

Mitel Performance Analytics supports remote access for the Avaya IP Office System Status Application (SSA).

Do the following steps:

1. Access the dashboard for the device you want to connect to.
2. Confirm the IP Office Base Port number. The default is 50804. If the system you want to connect to is using a different base port, enter the port number in the **IP Office Base Port** field in the **SSA Remote Access** panel.

3. Click **Create SSA Connection**
   Mitel Performance Analyticscreates a remote access connection to the IP Office system and provides a connection IP address and base port to use with the SSA application for the remote connection.



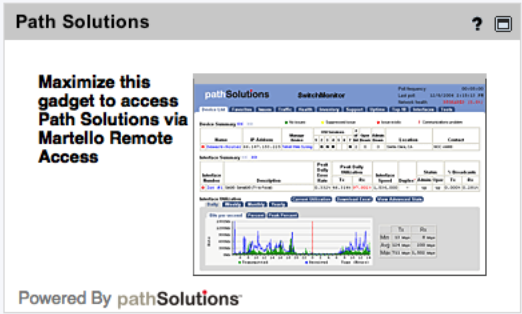
4. Open the Avaya SSA application.

5. Enter the SSA Connection IP address into the **Control Unit IP Address** field
6. Enter the SSA SSA Connection Base Port into the **Services Base TCP Port** field
7. Enter the User Name and Password.
8. Click on the **Logon** button
   Note: In some circumstances, Mitel Performance Analytics may return a hostname instead of an IP address for the SSA Connection IP address. Since the SSA application cannot accept a

hostname, convert the hostname to an IP address by using a service such as WhatIsMyIP (http://www.whatismyip.com/ip-tools/ip-address-host-name-lookup/).

CONNECTING TO A PATHSOLUTIONS SERVER

The **PathSolutions Remote Access** panel provides remote access to the PathSolutions server. Expanding the panel opens the web console for the PathSolutions server.



MONITORING REMOTE ACCESS USAGE

The audit log records remote access usage. See "Audit Log" on page 89 for details.

PROBE INSTALLATION

The Probe is software that runs on a host in the customer LAN or on a dedicated server appliance, the Probe Appliance. The Probe monitors customer devices and reports to Mitel Performance Analytics, as well as providing Remote Access to a customer LAN, if this capability is enabled.

Mitel Performance Analytics provides Probe installers for Windows, Red Hat Linux (and distributions based on this, such as CentOS and Mitel Standard Linux), installation as a blade on a Mitel MSL or MiCollab server, and installation as a virtual appliance.

This chapter describes how to install various types of Probes. For details on configuring Probes, see "Probe Configuration" on page 114.

HOST REQUIREMENTS

The Probe is designed to be lightweight and to impose minimal host requirements. Recommended host configurations are listed in the following table. The Probe is a Java application and requires the Oracle JRE or OpenJDK JRE Release 1.8, or later. Mitel recommends Java Release 1.8 release 40 or later. For MiVoice MX-ONE support, ensure the host uses Java Release 1.8, release 25 only.

NO. OF DEVICES TO MONITOR	CPU	RAM	DISK	JAVA ENVIRONMENT
< 10 monitored devices per Probe Appliance	ARM5, 1GHz	512 MB total	512 MB total	OpenJDK 1.8 or later.
< 10 monitored devices per host	Core2 Duo / i3 1 GHz or faster	256 MB Service, 512 MB Host	5 GB free space	Oracle Java Runtime Environment (JRE) 1.8 or OpenJDK 1.8 or later.
< 80 monitored devices per host	Dual Core i5, 2 GHz or faster	1 GB Service, 2 GB Host	20 GB free space	Oracle Java Runtime Environment (JRE) 1.8 or OpenJDK 1.8 or later.
≥ 80 monitored devices per host	Contact Mitel for engineering guidelines.			

PROBE CAPACITY

For users that have Mitel Performance Analytics installed on premise with their equipment, the Probe that is provided with your installation can monitor approximately 100 devices, assuming the monitored network consists of a variety of devices.

For service providers that have Mitel Performance Analytics installed in their data center, the system Probe that is provided with your installation can monitor approximately 100 devices, assuming the monitored network consists of a variety of devices. Every additional installed Probe can monitor a

medium sized network consisting of five routers and 10 MiVoice Business devices with automatic backup and SMDR gathering enabled.

For cloud based users, a single Probe can monitor a medium sized network consisting of five routers and 10 MiVoice Business devices with automatic backup and SMDR gathering enabled.

LAN CONNECTIVITY REQUIREMENTS

To provide monitoring and remote access, the Probe must be able to connect to the LAN devices.

The Probe uses the following IP protocols to communicate to devices it is monitoring:

APPLICATION	IP PROTOCOL AND PORT	IP SESSION SOURCE	IP SESSION DESTINATION
SNMP / Performance	UDP, port 161	Probe	Device
SNMP	UPD port 162	Device	Probe
HTTPS / Performance	TCP, port 443	Probe	Mitel Performance Analytics
HTTP	TCP, port 80	Probe	MiVoice Office 250
MiXML	TCP, port 443	Probe	MiVoice Business
SMDR	TCP, port 1752	Probe	MiVoice Business
SIP Endpoint Voice Quality	UDP, port 5060	SIP Endpoint	Probe
MiVoice Office 250 / Message Print	TCP, ports 4000, 44000	Probe	MiVoice Office 250
Avaya IP Office	TCP, port 50802 and ports in the range 50804 to 50813 (defaults, actual ports may range between 49152 and 65289 depending on IP Office services base port) UDP, ports 50794, 50798	Probe	Avaya IP Office
PathSolutions	TCP, port 8084 (default)	Probe	PathSolutions

APPLICATION	IP PROTOCOL AND PORT	IP SESSION SOURCE	IP SESSION DESTINATION
FTP / Backup	TCP, port 21	Probe	MIVoice Business
SSH / Performance	TCP, port 22	Probe	Device
Ping / Availability	ICMP Echo	Probe	Device

OTHER PROTOCOLS AND PORTS

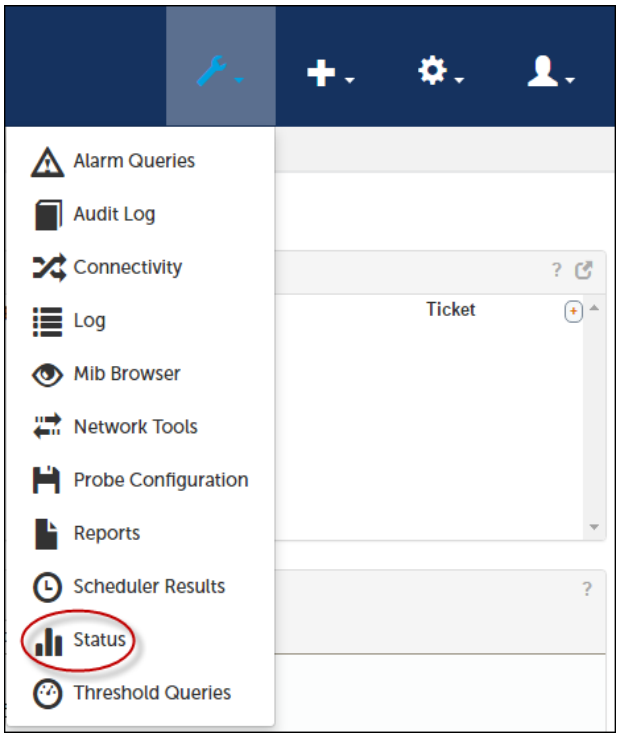
If the Probe is used for Remote Access, the Probe must have network connectivity to the LAN devices for the appropriate TCP/IP protocol and port used by the Remote Application.

RECEIPT OF SNMP TRAPS

To receive SNMP traps, the Probe must receive the SNMP packets. These are sent by default on port 162.

The Probe attempts to bind to port 162. If it cannot, it binds to port 1162 instead.

The **Probe Status** panel shows the port that the Probe has bound to. The **Probe Status** panel is available under the **Tools** icon of the Probe dashboard:



The following is a typical Probe Status panel:

Component	Message
ProbeConfig	Added: 8 Removed: 0 Updated: 0 LoadFail: 0
CheckForUpgrade	Last Modified: Mon Mar 30 21:33:10 UTC 2015
CollectorManager	Collecting 9 devices with 42 Collectors.
BufferingRemoteRrdUpdater	Buffer size: 0/2048, max age: -1, enqueued: 2552, sent: 2544, dropped: 0, errors: 0, permanent errors: 8, internal errors: 0, HWM: 38, retry later:0
MCDMiXMLCollector	Collecting for 4 MCDs
MBGCollector	Collecting VQ for 1 MBGs
ThreadPoolSNMPTaskRunner	Running 61 tasks, 0.15 Tasks/Second
SNMPTrapReceiver	Listening on port 162
FixedThreadPoolPingTaskRunner	Pinging 8 devices with 5 threads.

To ensure receipt of traps, configure the trap sender to send traps on the port the Probe has bound to.

INTERNET CONNECTIVITY REQUIREMENTS

For remote monitoring, the Probe must have continuous network access to the devices to be monitored and must have Internet access for HTTP/SSL on port 443 to the Mitel Performance Analytics server.

For other, optional services, the Probe connects to either customer specified servers (for file transfer) or to Mitel Performance Analytics servers for Mitel Performance Analytics cloud storage or Remote Access.

Note that the Probe always initiates IP connections; that is, all connections are outbound.

PROTOCOL OR APPLICATION	IP PROTOCOL AND PORT	IP SESSION INITIATOR	DESTINATION	COMMENT
HTTPS	TCP, port 443	Probe	Mitel Performance Analytics server(s)	Required for Remote Monitoring.
HTTPS	TCP, port 443	Probe	Mitel Performance Analytics Cloud File server(s)	Optional, Required for Mitel Performance Analytics Cloud File Storage.
FTP, FTPS Implicit	TCP, port 21	Probe	Customer-defined File server(s)	Optional, used for SMDR file transfer.

PROTOCOL OR APPLICATION	IP PROTOCOL AND PORT	IP SESSION INITIATOR	DESTINATION	COMMENT
SFTP	TCP, port 22	Probe	Customer-defined File server	Optional, used for SMDR file transfer.
FTPS Explicit	TCP, port 990	Probe	Customer-defined File server	Optional, used for SMDR file transfer.
SSH	TCP, port 50000	Probe	Mitel Performance Analytics server(s)	Required for Remote Access.
DNS	TCP and UDP, port 53	Probe	DNS server	Required to resolve host names or URLs to IP addresses.
NTP	UDP, port 123	Probe	NTP server	Required to synchronize Probe system time.

OTHER REQUIREMENTS

To install a Probe, you must have the **Probe Installer** administrative permission. See "User Permissions" on page 46.

PROBE SOFTWARE INSTALLATION PROCEDURES

All installers are available from the **Probe Configuration** panel.

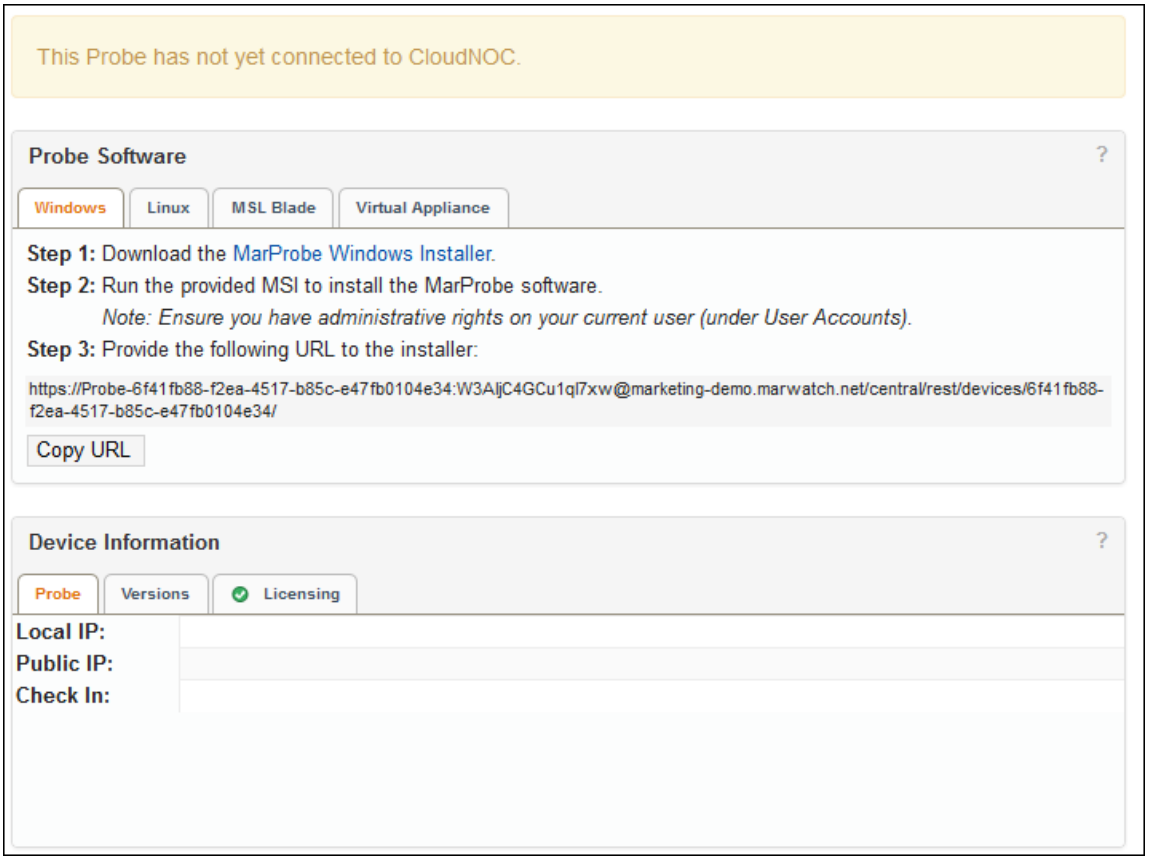
For both Windows and Linux installations, the general procedure is:

1. Install the Probe software.
2. Start the Probe application (as a Windows service or Linux daemon).
3. Provide the Probe software with the appropriate Mitel Performance Analytics configuration URL to enable the Probe to connect to the correct Mitel Performance Analytics server and to uniquely identify itself to Mitel Performance Analytics.
   Note: To perform Step 3, you have the **Probe Installer** administrative permission.

The Probe software is available from the **Probe Configuration** panel available on the Probe dashboard. That means that you must have previously added the Probe device to a container.

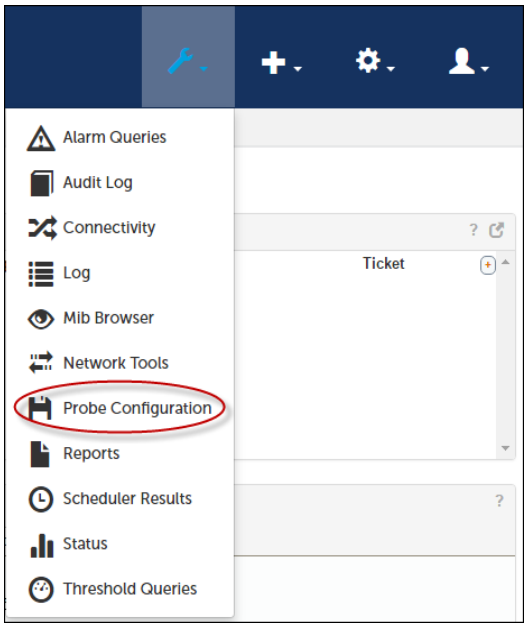
Before the Probe has connected to Mitel Performance Analytics, the Probe dashboard shows only two panels: the **Probe Configuration** panel and the **Probe Device Information** panel.

The following is a typical Probe dashboard before it has connected to Mitel Performance Analytics:



The Probe Dashboard shows only these two panels to highlight the fact that the Probe has not yet connected to Mitel Performance Analytics. Use the **Probe Configuration** panel to install the Probe software.

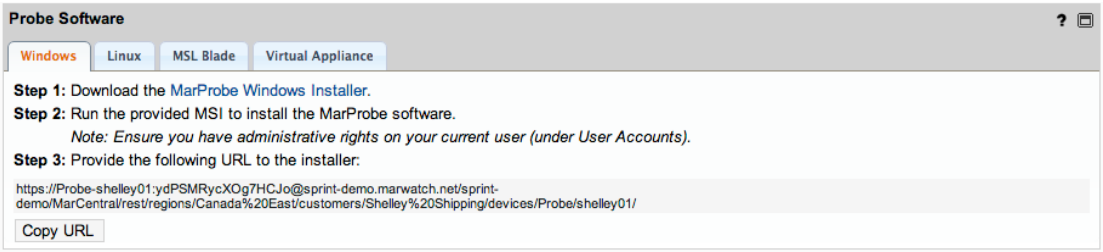
If a Probe is already connected to Mitel Performance Analytics, the **Probe Configuration** panel is available under the **Tools** icon of the Probe dashboard:



PROBE WINDOWS INSTALLATION

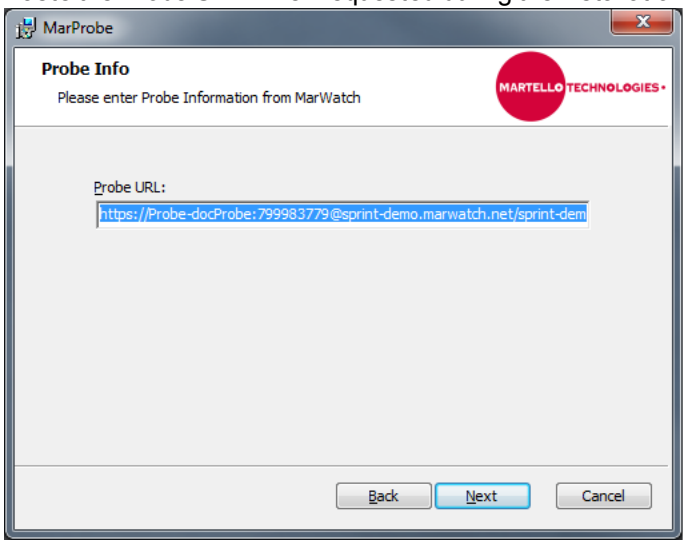
The Windows Installer runs on Windows (XP, Vista, 7) and Windows Server (2003 and Server 2008). To install the software on Windows:

1. Log into the Windows system using an account with administration privileges.
2. Go to the dashboard for the Probe you want to install.
3. Go to the **Probe Configuration** panel, select on the **Windows** tab and download the Probe installer to the Windows system.



4. Copy the Probe URL, either manually or by clicking the **Copy URL** button.
   Note: To do this step, you must have the **Probe Installer** administrative permission.
5. Run the Probe Windows installer.

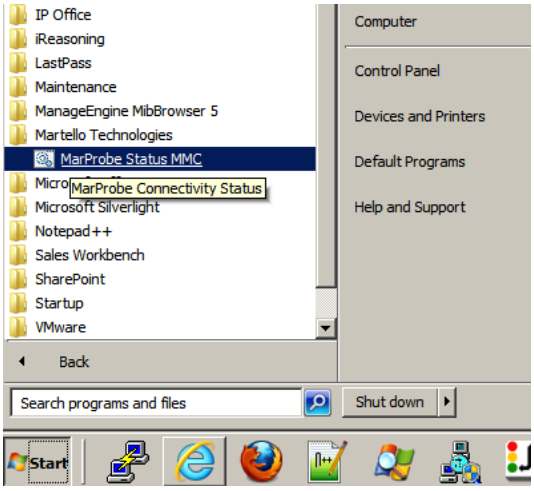
6. Paste the Probe URL when requested during the installation process.



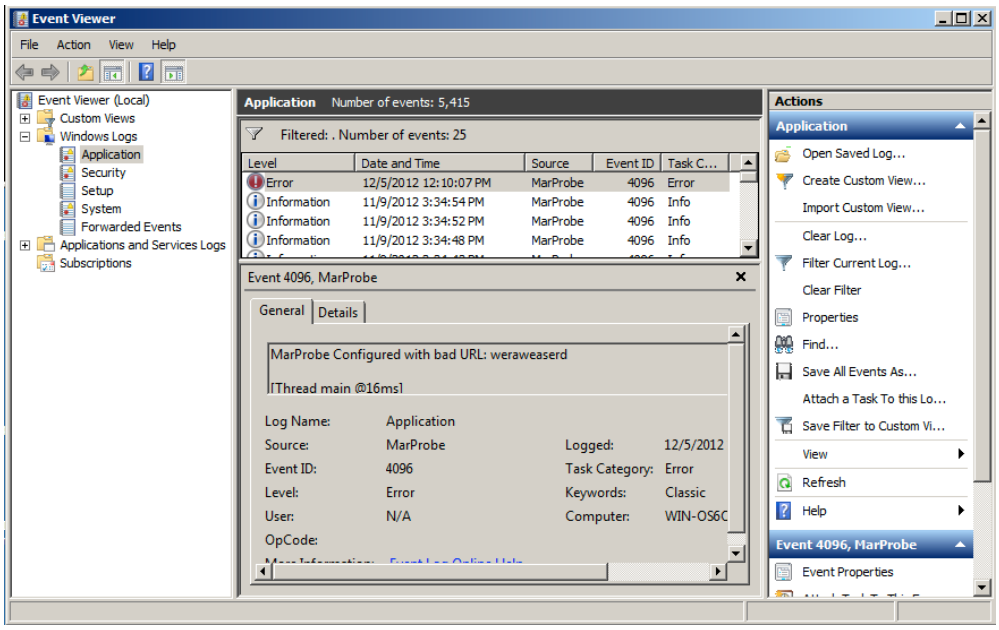
When the installer has finished, the Probe software is configured to run as a Windows service.

Confirm Installation

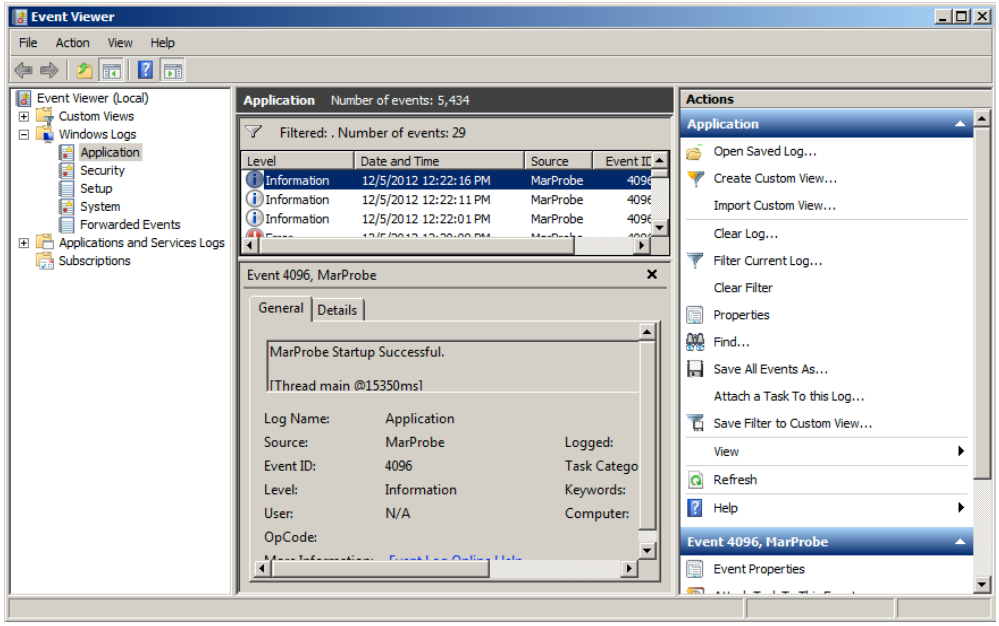
To confirm that the software is running, go to the Martello Technologies folder in the Start Menu, and click on the MarProbe Status MMC link.



This action opens the Microsoft Management Console and shows recent Windows events related to the Probe. In the following example, the Probe has been misconfigured with a bad URL. This condition is shown in the MMC Console.



To correct the URL, uninstall and reinstall the Probe software with the correct URL. This time, the MarProbe Status MMC command shows that the Probe startup has been successful.



In Windows XP, the MarProbe Status MMC Start menu item is replaced by MarProbe Status CMD. This option opens a Windows command line interface which shows the five most recent entries in the Windows System Log for the Probe.

For example, the results from the MarProbe Status CMD on a Windows XP computer with a system name of MRTCOMP-11:

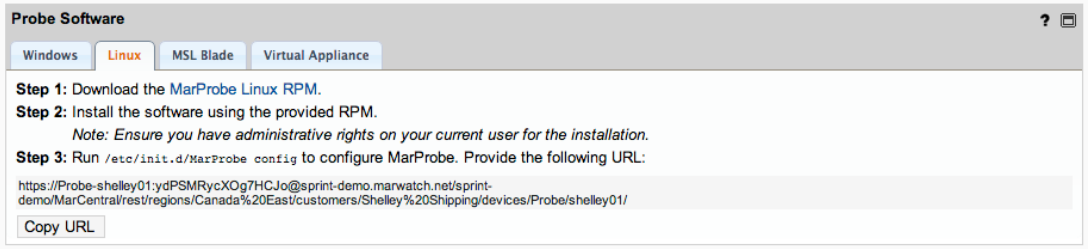
```
The default script host is now set to "cscript.exe".
Microsoft (R) Windows Script Host Version 5.7
Copyright (C) Microsoft Corporation. All rights reserved.


------------------------------------------------------------------------
-------
Listing the events in 'application' log of host 'MRTCOMP-11'
------------------------------------------------------------------------
-------
Type:         information

Event:        4096
Date Time:    12/05/2012 15:44:59
Source:       MarProbe
ComputerName: MRTCOMP-11
Category:     Info
User:         N/A
Description:  Remote Access Connected.  [Thread RemoteAccess Client
Initializing
 Thread @59443625ms]

Type:         information
Event:        4096
Date Time:    12/05/2012 14:31:43
Source:       MarProbe
ComputerName: MRTCOMP-11
Category:     Info
User:         N/A
Description:  Remote Access Connected.  [Thread RemoteAccess Client
Initializing
 Thread @55047297ms]

Type:         information
Event:        4096
Date Time:    12/05/2012 14:00:23
Source:       MarProbe
ComputerName: MRTCOMP-11
Category:     Info
User:         N/A
Description:  Remote Access Connected.  [Thread RemoteAccess Client
Initializing
 Thread @53167797ms]

Type:         information
Event:        4096
Date Time:    12/05/2012 13:37:33
Source:       MarProbe
ComputerName: MRTCOMP-11
Category:     Info
```

```
User:          N/A
Description:   Remote Access Connected.  [Thread RemoteAccess Client
Initializing
 Thread @51797656ms]
```

PROBE LINUX INSTALLATION

The Probe is supported on Red Hat Enterprise Linux or a derivative platform such as Fedora, CentOS or Mitel Standard Linux.

1. Log into the Linux system using an account with administration privilege (root).
2. Go to the dashboard for the Probe that you want to install.
3. Go to the **Probe Configuration** panel, select the **Linux** tab and download the MarProbe RPM to the Linux system.



4. Copy the Probe URL, either manually or by clicking on the **Copy URL** button.
   Note: To do this step, you must have the **Probe Installer** administrative permission.
5. Open a terminal window.
6. Type `rpm -ivh <path_to_Probe_file/Probe_file_name>.rpm` to install the Probe, resulting in the following output:

```
[root@localhost ~]# rpm -ivh MarProbe-MarWatch-3.5.0.i386.rpm
Preparing... ########################################### [100%]
java version "1.6.0_22"
OpenJDK Runtime Environment (IcedTea6 1.10.4) (fedora-61.1.10.4.fc16-
i386)
OpenJDK Client VM (build 20.0-b11, mixed mode)
1:MarProbe ########################################### [100%]
================================
```

7. Type `/etc/init.d/MarProbe config` to configure the Probe and provide it with the Probe URL from the **Probe Configuration** panel:

```
[root@localhost ~]# /etc/init.d/MarProbe config

========== Martello Technologies MarProbe Configuration ==========

Enter Probe URL from MarWatch []:
https://Probe-shelley01:ydPSMRycXOg7HCJo@sprint-
demo.marwatch.net/sprint-
demo/MarCentral/rest/regions/Canada%20East/customers/Shelley%20Shipping
/devices/Probe/shelley01/
Writing config to /usr/local/martello/marProbe.conf... OK
```

8. Type `/etc/init.d/MarProbe start` to start the Probe.

```
[root@localhost ~]# /etc/init.d/MarProbe start
Starting MarProbe (via systemctl):  [ OK ]
```

9. To confirm that the software is running, type `ps -Af | grep MarProbe` to display the running Probe processes.

```
[root@localhost ~]# ps -Af | grep MarProbe
root 1873 1 0 10:18 ? 00:00:00 /usr/local/martello/bin/marProbe -debug
-pidfile /var/run/marProbe.pid -DmarProbe.logfile.prefix=/var/log/ -cp
/usr/local/martello/MarProbe-Fat.jar
com.martellotech.bootstrap.startup.JSVCDaemon https://Probe-
shelley01:ydPSMRycXOg7HCJo@sprint-demo.marwatch.net/sprint-
demo/MarCentral/rest/regions/Canada%20East/customers/Shelley%20Shipping
/devices/Probe/shelley01/
root 1874 1873 25 10:18 ? 00:00:00 /usr/local/martello/bin/marProbe -
debug -pidfile /var/run/marProbe.pid -
DmarProbe.logfile.prefix=/var/log/ -cp /usr/local/martello/MarProbe-
Fat.jar com.martellotech.bootstrap.startup.JSVCDaemon https://Probe-
shelley01:ydPSMRycXOg7HCJo@sprint-demo.marwatch.net/sprint-
demo/MarCentral/rest/regions/Canada%20East/customers/Shelley%20Shipping
/devices/Probe/shelley01/
```

Note: You can also download the Probe using the wget command from a terminal window:

```
[root@localhost ~]# wget
https://d3lno0et4zhxmw.cloudfront.net/MarProbe-MarWatch-3.5.0.i386.rpm
--2012-01-16 10:29:51-- https://d3lno0et4zhxmw.cloudfront.net/MarProbe-
MarWatch-3.5.0.i386.rpm
Resolving d3lno0et4zhxmw.cloudfront.net... 204.246.169.166,
204.246.169.191, 204.246.169.186, ...
Connecting to d3lno0et4zhxmw.cloudfront.net|204.246.169.166|:443...
connected.
HTTP request sent, awaiting response... 200 OK
Length: 898566 (878K) [application/x-rpm]
Saving to: “MarProbe-MarWatch-3.5.0.i386.rpm”

100%
[======================================================================
==================================================>] 898,566 3.07M/s
in 0.3s

2012-01-16 10:29:51 (3.07 MB/s) - “MarProbe-MarWatch-3.5.0.i386.rpm”
saved [898566/898566]
```

PROBE MSL BLADE INSTALLATION

The Probe software can be installed on an MSL server as an MSL blade.

Note: Mitel does not provide support or warranty for the Probe blade installation on an MSL server.

MSL Version Support

The Probe MSL blade is supported on MSL R9.3 and later.

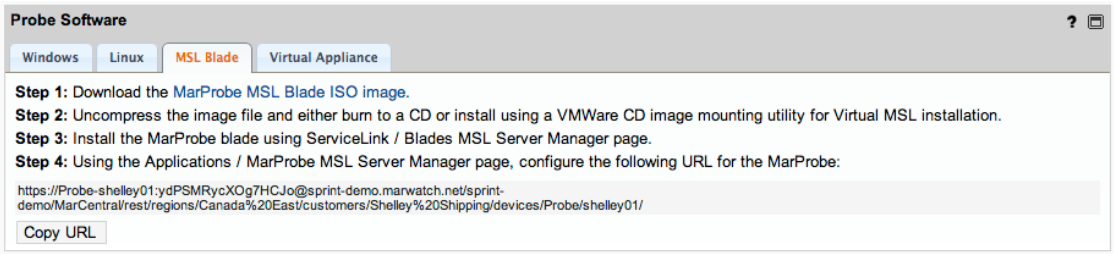
Blade Packaging

The blade is distributed as an ISO CD image file. The image file can be either burned to a CD or installed using a VMWare CD image mounting utility for Virtual MSL installation.

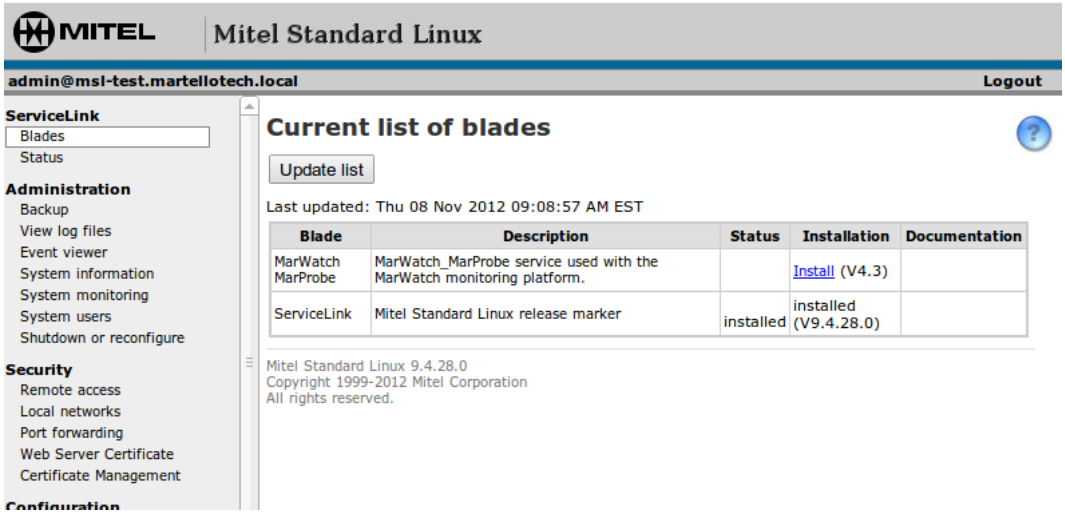
Installation

To install the Probe MSL blade:

1. Go to the dashboard for the Probe that you wish to install.
2. Go to the **Probe Configuration** panel, select the **MSL Blade** tab and download the MSL blade ISO image.

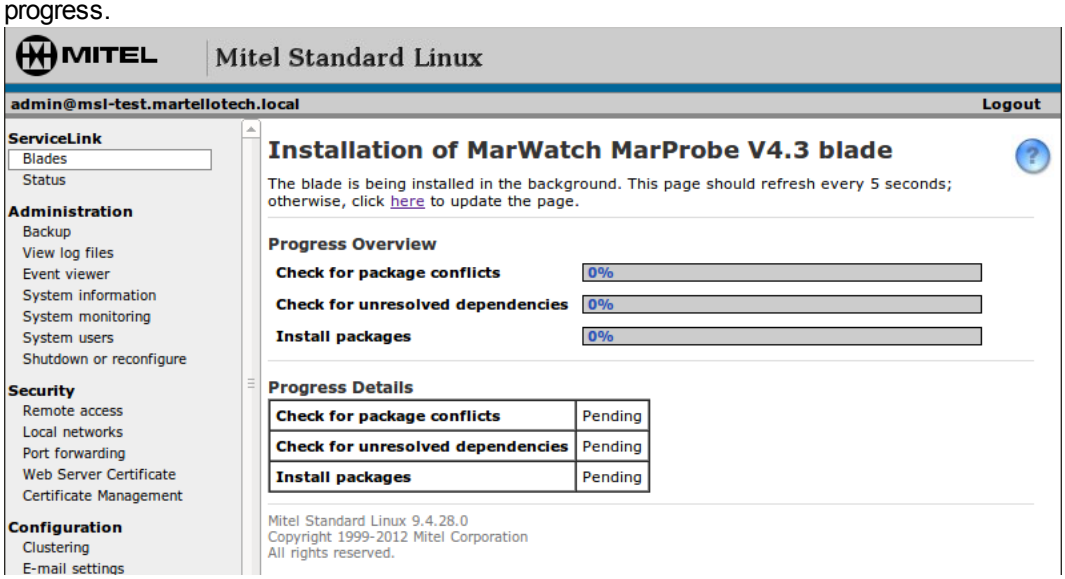


3. Copy the Probe URL, either manually or by clicking on the **Copy URL** button.
   Note: To do this step, you must have the **Probe Installer** administrative permission.
4. Open a Web browser and navigate to the MSL server manager URL (for example, http://<MSL_server_FQDN>/server-manager).
5. Log in to the MSL server manager interface.
6. If you are installing the blade from CD, insert the CD in the server CD ROM drive.
7. In the left navigation pane under **ServiceLink**, click **Blades**. The available list of blades is displayed.

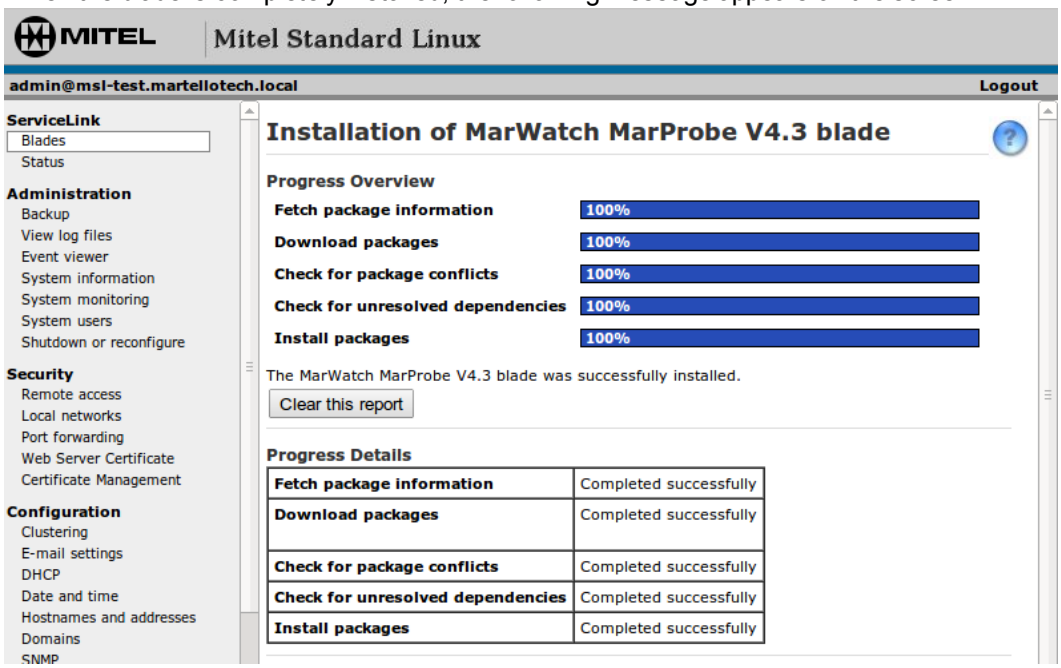


8. Click **Install**.
9. Review and accept the software license terms by clicking **Accept All Licenses**.

10. The installation process for the Probe blade begins. The installation screen shows installation progress.



11. When the blade is completely installed, the following message appears on the screen:



12. Click **Clear this report**.

This completes the Probe blade installation.

After the Probe blade installation is complete, the Probe service starts and is available for configuration.

PROBE MICOLLAB BLADE INSTALLATION

The Probe software can be installed on a MiCollab server as a blade.

Note: Mitel does not provide support or warranty for the Probe blade installation on a MiCollab server.

To manually install the Probe software downloaded from the Probe dashboard as a blade on a MiCollab server:

1. Start an SSH session to the MiCollab system. Log in as `root` with the admin password.
2. Put the ISO image from the Probe dashboard onto the `/root` directory of the MiCollab server using one of the following methods:
   - Download the ISO image to your local computer and then use SSH to copy the file to the MiCollab server.
   - Download the ISO image to your local computer and then put it on a USB memory stick.
   - Download the ISO image directly from the Mitel Performance Analytics server to the MiCollab server.
3. Mount the ISO image to the Linux system using the `mount -o loop` command.
4. Install the blade using the `install_blade -cdrom` command.
5. If your MiCollab is running MSL 10.3.31 or later, run the following command: `signal-event app-post-install`

Example – Copying a local ISO image using scp

This assumes the following:

- You have already downloaded the ISO image to your local computer.
- The ISO image file name is `Blade-MarWatch_MarProbe-5.0-r0SNAPSHOT.i386.iso.`
- The IP address of the MiCollab server is 10.10.5.10.

The `scp` command to copy from your local system to the MiCollab /root directory is:

```
scp Blade-MarWatch_MarProbe-5.0-r0SNAPSHOT.i386.iso
root@10.10.5.10:/root/
```

Example – Copying a local ISO image using WinSCP

This assumes the following:

- You have already downloaded the ISO image to your local computer.
- The ISO image file name is `Blade-MarWatch_MarProbe-5.0-r0SNAPSHOT.i386.iso.`
- The IP address of the MiCollab server is 10.10.5.10.

The procedure to copy from your local Windows machine to the MiCollab /root directory is:

1. Start the WinSCP application.
2. Connect to the MiCollab server.
3. Using the WinSCP GUI, drag the `Blade-MarWatch_MarProbe-5.0-r0SNAPSHOT.i386.iso` file to the target MiCollab `/root` directory.

Example – Direct download of the ISO image

This assumes the following:

- The URL of the Mitel Performance Analytics server is https://mycompany.com.
- You have not already downloaded the ISO image to your local computer.

The `wget` command to download the ISO image from the Mitel Performance Analytics server to the MiCollab `/root` directory is:

```
wget https://mycompany.com/ProbeSoftware/MarProbe-Installer.noarch.iso
```

Example – Mounting and Installing ISO Image When Using SSH

In this example, the ISO image file name is `Blade-MarWatch_MarProbe-5.0-r0SNAPSHOT.i386.iso`. The MiCollab is running MSL 10.3.31 or later.

The Linux commands to mount the ISO image and install the blade are:

```
mkdir /mnt/cdrom
mount -o loop Blade-MarWatch_MarProbe-5.0-r0SNAPSHOT.i386.iso
/mnt/cdrom
install_blade -cdrom Blade-MarWatch_MarProbe-5.0-r0SNAPSHOT.i386
signal-event app-post-install
```

Example – Mounting and Installing ISO Image When Using USB Stick

In this example, the USB stick's storage name is `sdd1` and the ISO image file name is `Blade-MarWatch_MarProbe-5.0-r0SNAPSHOT.i386.iso`. The MiCollab is running MSL 10.3.31 or later.

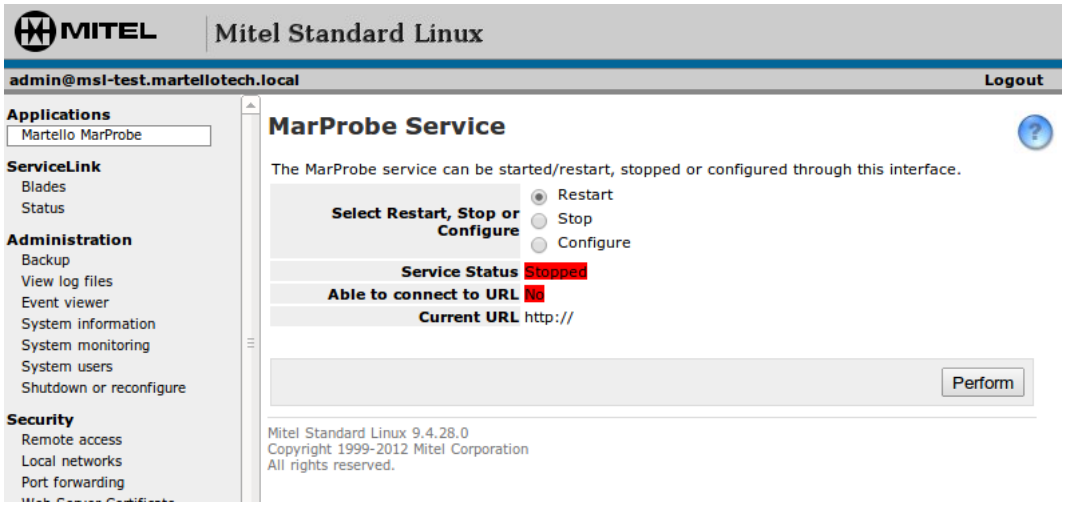
The Linux commands to mount the ISO image and install the blade are:

```
mkdir /mnt/usbflash
mount /dev/sdd1 /mnt/usbflash
cp /mnt/usbflash/Blade-MarWatch_MarProbe-5.0-r0SNAPSHOT.i386.iso /root/
mkdir /mnt/cdrom
mount -o loop Blade-MarWatch_MarProbe-5.0-r0SNAPSHOT.i386.iso
/mnt/cdrom
install_blade -cdrom Blade-MarWatch_MarProbe-5.0-r0SNAPSHOT.i386
signal-event app-post-install
```

Post Blade Installation Configuration

After installing the Probe blade, you must configure the Probe. You are presented with a new link in the Applications menu: Martello MarProbe.

Click the **Martello MarProbe** link to open the **MarProbe Application** Menu.



The web interface for the Probe service has three options; **Restart**, **Stop** and **Configure**. To perform an action, select an option and click the **Perform** button.

By default **Restart** is selected. It performs a restart of the Probe service. The **Stop** option forces the Probe service to stop. The **Configure** option is used to apply a Probe URL from the Mitel Performance Analytics device page for the Probe.

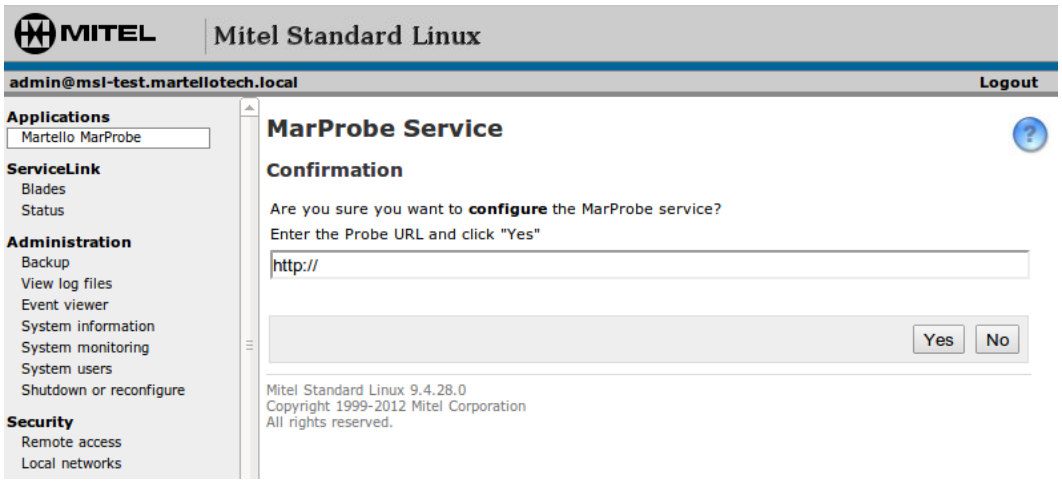
When the Probe service is initially installed, there is no Probe URL configured and the service is stopped.

Note: After installation or upgrade of the Probe blade, you may be unable to **Restart**, **Stop** or **Configure** the Probe service. This is a known MSL issue. The workaround is to quit the web browser, wait 15 minutes for all session timers to expire and try again.

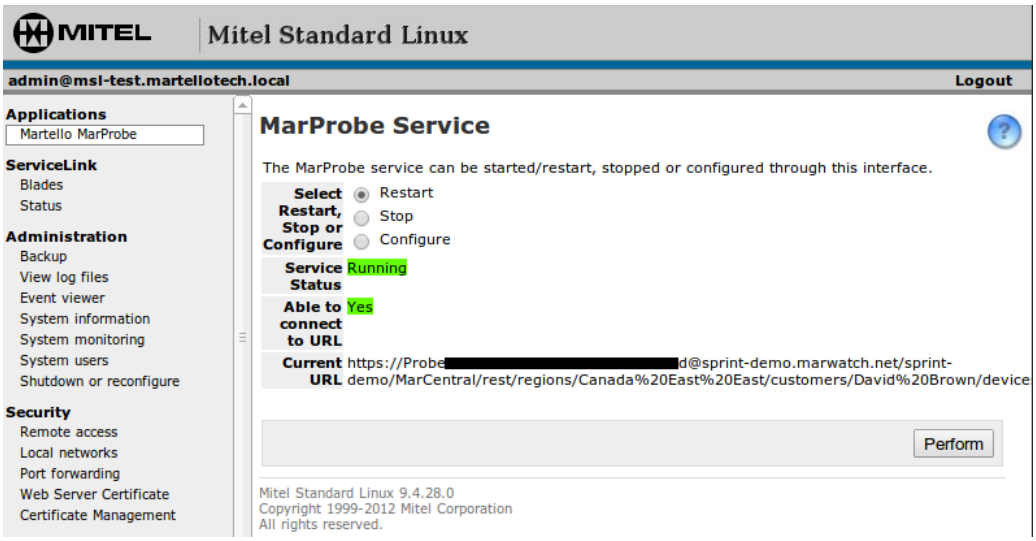
To configure a URL for the Probe service, select the **Configure** option and click **Perform**.

Enter the URL from the **Probe Configuration** panel in Mitel Performance Analytics into the Probe URL text box, and click **Yes**. This applies the URL to the system and the restarts the Probe service.

Note: To do this step, you must have the **Probe Installer** administrative permission.



After the service is restarted, the MarProbe Application interface shows the Probe service status and whether or not Mitel Performance Analytics is reachable from the Probe (that is, that the Probe can resolve the hostname in the URL and establish a connection to the Mitel Performance Analytics server identified by that hostname).



The Service Status shows the status of the Probe, either Running or Stopped.

If the MSL server can connect to the URL specified, the **Able to connect to URL** field shows Yes. If not, it shows No.

This feature facilitates troubleshooting connectivity issues by allowing arbitrary URLs to be tested, similar to pinging a server. For example, if http://www.google.com is entered as the configured URL, the MSL server attempts to retrieve the contents of http://www.google.com and report the result of that action.

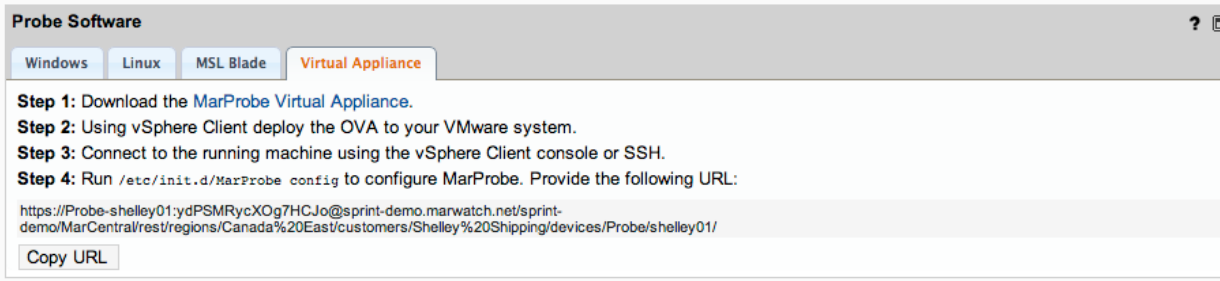
PROBE VIRTUAL APPLICATION INSTALLATION

The Probe can also be downloaded as a Virtual Appliance. The system provides a VMware OVA that can be installed as Virtual Machine. The Virtual Machine contains an Ubuntu 14.04 Linux installation with the Probe software preinstalled.

Before installing the Virtual Appliance, configure the memory and resource allocation for the VM so that it meets the RAM requirements shown in "Host Requirements" on page 193.

To install and configure the Virtual Appliance:

1. Go to the dashboard for the Probe that you wish to install.
2. Go to the **Probe Configuration** panel, select the **Virtual Appliance** tab and download the OVA file.



3. Install the OVA file according to VMware instructions.
4. Start the VM and connect to it using SSH or the VMware console.
5. Log in as `config` with password config.
   For the first log in, you are prompted to change passwords.
6. By default, the VM is configured to use DHCP. You can optionally change this setting to use static IP addressing. To do so, do the following steps:
   - Set a static IP address by running the following command and providing the following fields:
     Command: `sudo vi /etc/network/interfaces.d/eth0`
     Fields:

```
auto eth0
iface eth0 inet static
address <IP address>
netmask <network mask>
gateway <Gateway IP Address>
```

   - Press `Esc` and enter `:wq` to write and exit from the file.
   - Configure DNS server by running the following command and providing the following fields:
     Command: `sudo vi /etc/resolv.conf`
     Fields:

```
nameserver <DNS server IP Address 1>
nameserver <DNS server IP Address 2>
```

     Enter as many DNS server IP addresses as required.
   - Press `Esc` and enter `:wq` to write and exit from the file.
   - Bring up the network interface by running the following command:
     Command: `sudo ifdown eth0 && sudo ifup eth0`
7. Type `sudo /etc/init.d/marprobe config` to configure the Probe and provide it with the Probe URL from the **Probe Configuration** panel:
   Note: To do this step, you must have the **Probe Installer** administrative permission.

```
[root@localhost ~]# sudo /etc/init.d/marprobe config


========== Martello Technologies MarProbe Configuration ==========

Enter Probe URL from MarWatch []:
https://Probe-shelley01:ydPSMRycXOg7HCJo@sprint-
```

```
demo.marwatch.net/sprint-
demo/MarCentral/rest/regions/Canada%20East/customers/Shelley%20Shipping
/devices/Probe/shelley01/

Writing config to /usr/local/martello/marprobe.conf... OK
```

8. Type `sudo /etc/init.d/marprobe start` to start the Probe.

```
[root@localhost ~]# sudo /etc/init.d/marprobe start
Starting marprobe (via systemctl):  [ OK ]
```

9. To confirm that the software is running, type `sudo ps -Af | grep marprobe` to display the running Probe processes.

```
[root@localhost ~]# sudo ps -Af | grep marprobe
root 1873 1 0 10:18 ? 00:00:00 /usr/local/martello/bin/marprobe -debug
-pidfile /var/run/marprobe.pid -Dmarprobe.logfile.prefix=/var/log/ -cp
/usr/local/martello/marprobe-Fat.jar
com.martellotech.bootstrap.startup.JSVCDaemon https://Probe-
shelley01:ydPSMRycXOg7HCJo@sprint-demo.marwatch.net/sprint-
demo/MarCentral/rest/regions/Canada%20East/customers/Shelley%20Shipping
/devices/Probe/shelley01/
root 1874 1873 25 10:18 ? 00:00:00 /usr/local/martello/bin/marprobe -
debug -pidfile /var/run/marprobe.pid -
Dmarprobe.logfile.prefix=/var/log/ -cp /usr/local/martello/marprobe-
Fat.jar com.martellotech.bootstrap.startup.JSVCDaemon https://Probe-
shelley01:ydPSMRycXOg7HCJo@sprint-demo.marwatch.net/sprint-
demo/MarCentral/rest/regions/Canada%20East/customers/Shelley%20Shipping
/devices/Probe/shelley01/
```

10. If you need to configure the Linux system (IP address DNS, system name etc.), use standard Red Hat or CentOS instructions.
    These are available at: http://wiki.centos.org/FAQ/CentOS6

PROBE APPLIANCE INSTALLATION

The Probe Appliance is a small form-factor server with pre-installed Probe software. The Probe Appliance uses Debian Linux as its operating system.

The Probe Appliance has connectors for:

- Power, 110/240 VAC, 50/60 Hz
- Ethernet (10, 100, 1000 BASE-T)
- USB 2.0 type A

The Probe Appliance is shipped with:

- Standard US Power Cord
- Two-pin US Power Connector
- Ethernet Cable

The Probe Appliance must be configured for use with Mitel Performance Analytics. The configuration details for a Probe are entered in the property page for that Probe device and are visible on the device dashboard page for that Probe.

You must have the Probe configuration URL to configure a Probe.

PROBE APPLIANCE CONFIGURATION WITH SSH

Do the following steps:

1. Connect power and Ethernet to the Probe Appliance. The Probe Appliance uses DHCP to obtain its Ethernet address. To configure a Probe Appliance, you need to know its IP address.
2. The IP address can be obtained by scanning the network in which the Probe Appliance has been installed, and looking for devices with a MAC address that starts with `F0-AD-4E` or `00-50-43`.
3. Connect to the Probe using SSH to its IP address.
4. Login to the system as user `config` with password `config`. The first time you login to the system, it prompts you to change the shipped default password. The `config` user has sudo privileges.
   The following is an example of the password change dialog. (Note that IP addresses and Linux version numbers may be different. This is not significant).

```
Using username "config".
config@10.4.50.8's password:
You are required to change your password immediately (root enforced)
Linux marProbe 2.6.32-5-kirkwood #1 Sat Dec 11 05:09:52 UTC 2010
armv5tel
The programs included with the Debian GNU/Linux system are free
software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Jul 6 14:37:29 2011 from 10.4.50.7
WARNING: Your password has expired.
You must change your password now and login again!
Changing password for config.
(current) UNIX password:
Enter new UNIX password:
```

```
Retype new UNIX password:
passwd: password updated successfully
```

5. The system now terminates the SSH session. You need to reconnect and login as the user `config` with the password you have chosen.
6. Type `sudo /etc/init.d/marprobe config` to configure the Probe and provide it with the Probe URL from the **Probe Configuration** panel:
   Note: To do this step, you must have the **Probe Installer** administrative permission.

```
[root@localhost ~]# sudo /etc/init.d/marprobe config


========== Martello Technologies MarProbe Configuration ==========

Enter Probe URL from MarWatch []:
https://Probe-shelley01:ydPSMRycXOg7HCJo@sprint-
demo.marwatch.net/sprint-
demo/MarCentral/rest/regions/Canada%20East/customers/Shelley%20Shipping
/devices/Probe/shelley01/

Writing config to /home/marProbe/etc/marProbe.conf...
OK
MarProbe service is now restarting
Stopping MarProbe stopped PID=###
Starting MarProbe started PID=###
```

PROBE APPLIANCE CONFIGURATION WITH USB DRIVE

The Probe Appliance can also be configured using a USB drive. To configure the Probe Appliance, you need a USB drive formatted as FAT32 and the configuration URL supplied by the Mitel Performance Analytics Probe Status page.

Do the following steps:

1. Create a file called `marprobe.config.` on the root directory of the USB drive.
2. Edit the file to contain the following lines:
   ```
   url=
   force=
   ```
   Note: These options are case sensitive and must not contain quotation marks. After the `url=` option, enter the Probe configuration URL supplied by Mitel Performance Analytics. The file dates are used to determine if the configuration URL should be applied. This can be overridden by placing `YES` after the `force=` option. Any other value in the force option field is ignored. Also note that only the first `url` and `force` options are read.
3. Save the file in the root directory of the USB drive and eject it.
4. Insert the drive into the USB port of the Probe Appliance. The indicator LED on the top of the appliance starts to blink as data is being read from, and written to the USB drive. When the LED stops blinking, it is safe to remove the drive from the appliance.
   Note: If the LED does not blink, the USB drive is not being read properly.

STATIC IP ADDRESSING

The Probe Appliance can be optionally configured with a static IP address using the USB drive configuration method. The following additional configuration variables are supported in the marprobe.config file:

```
address_assignment={static|dynamic}
address={dotted quad ip address}
netmask={dotted quad mask}
gateway={dotted quad ip address}
dns1={dotted quad ip address}
dns2={dotted quad ip address}
```

If `address_assignment` is set to `static`, the rest of the variables are used to define the network interface configuration.

If `address_assignment` is set to `dynamic`, the default DHCP configuration is used.

The following is an example marprobe.config file:

```
address_assignment=static
address=10.0.10.25
netmask=255.255.255.0
gateway=10.0.10.1
dns1=10.0.10.2
dns2=10.0.10.3
```

It assigns IP address 10.0.10.25/24 with default gateway 10.0.10.1 and DNS server addresses 10.0.10.2 and 10.0.10.3 to the Probe Ethernet interface.

LOG COLLECTION

To assist in troubleshooting, the Probe collects log information. Mitel support may ask for these logs to assist in problem resolution. The logs can be accessed through SSH or using a FAT-formatted USB drive.

SSH LOG ACCESS

The logs are stored in the `/var/log/marprobe/` directory. This is accessible from the `config` user account.

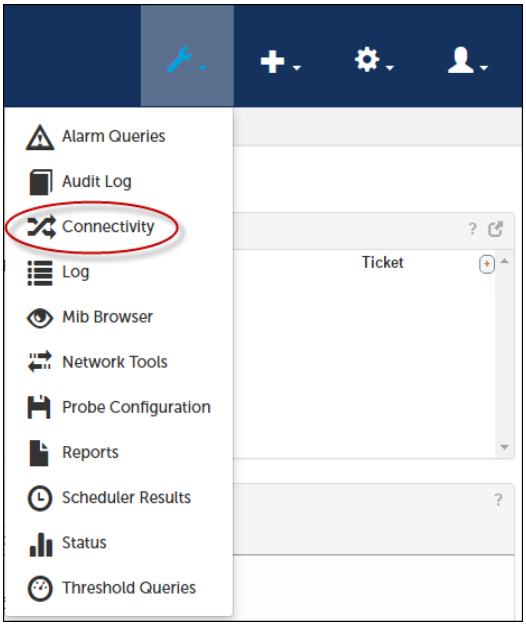
USB DRIVE LOG ACCESS

When a FAT formatted USB drive is connected to the Probe Appliance, the system automatically copies logs and configuration data to the USB drive.

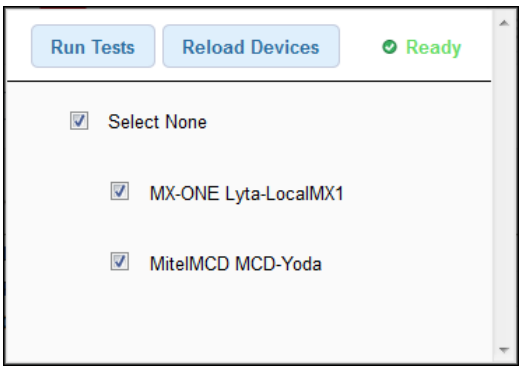
PROBE DEVICE CONNECTIVITY CHECK

The device connectivity check is used to verify that the Probe can establish connections to the devices it is configured to monitor.

The connectivity check is available under the **Tools** icon of the Probe dashboard:



The following is a typical connectivity check panel:

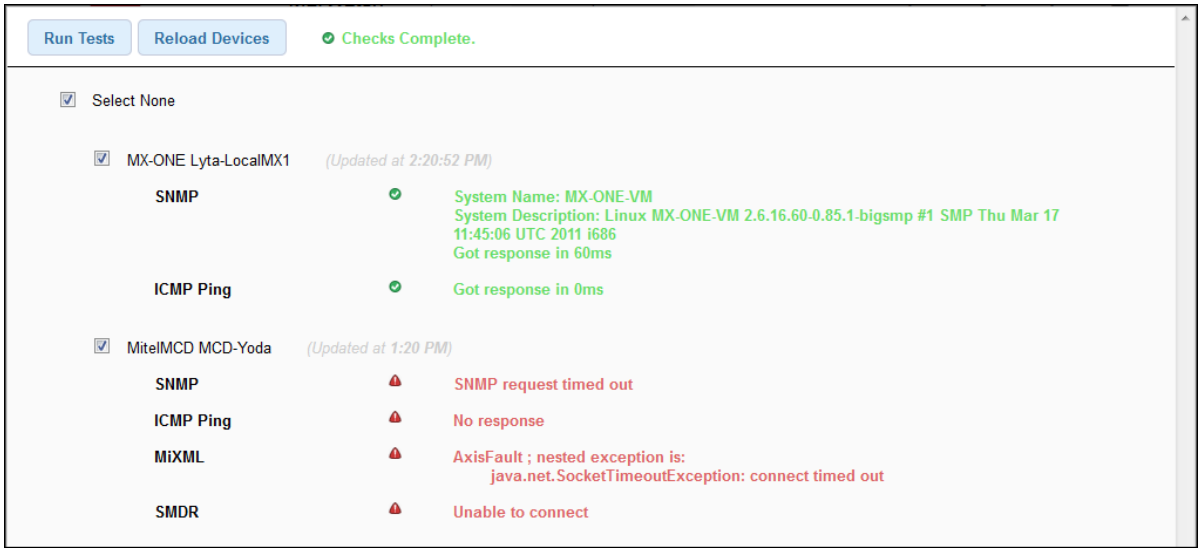


The checks verify both the IP network connectivity and the access credentials that have been configured for the device. The system runs this check for all of the connection protocols used by the device.

This capability can be used during installation to verify that local devices are properly configured and reachable from the Probe.

When a Device is created or edited, it can take up to 15 minutes for the configuration changes to propagate to the Probe. To check sooner, press the Reload Devices button to cause the Probe to request its configuration data from Mitel Performance Analytics.

The following is an example of the device connectivity check output.

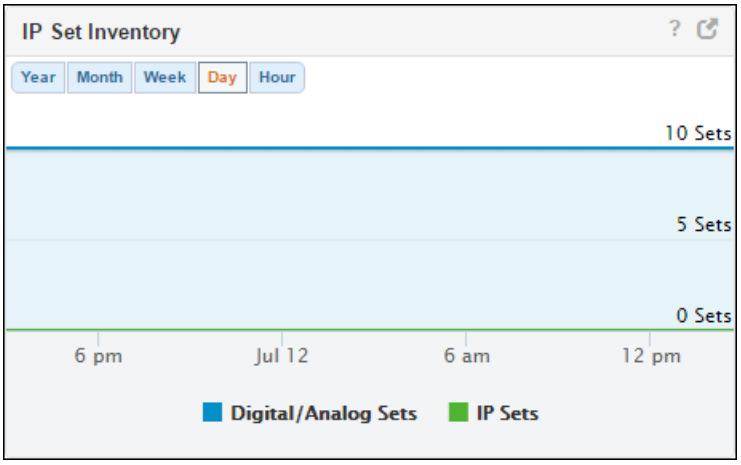


MITEL PERFORMANCE ANALYTICS DASHBOARD PANEL REFERENCE

The Mitel Performance Analytics web interface provides dashboard panels to display specific performance information for the devices contained within the dashboard context.

AVAYA IP OFFICE SET INVENTORY PANEL

Mitel Performance Analytics supports inventory monitoring for sets connected to an Avaya IP Office.



AVAYA IP OFFICE SET INVENTORY DEFAULT VIEW

The default view shows the total number of IP sets configured for the IP Office system by category, where the categories are:

- IP Sets: Avaya H.323/SIP or third party H.323/SIP sets
- Digital/Analog Sets: Avaya or third party digital or analog sets

AVAYA IP OFFICE SET INVENTORY EXPANDED VIEW

In its expanded view, the **Set Inventory** panel displays the following information about the sets connected to the Avaya Office system:

- **Name**: Short name assigned to set user.
- **Number**: Set directory number.
- **Device Type**: Set type.
- **Full Name**: Full name assigned to set user.
- **Port**: Logical port number for system port connected to set. Not applicable for IP sets. Note that the port number does not directly correspond to a physical card/port on the system.
- **Port Number**: The physical port on the card that connects to set. Not applicable for IP sets.
- **Module Number**: The module number for the card that connects to set. Not applicable for IP sets.
- **IP Address**: IP address for IP set. Not applicable for analog or digital sets.

- **MAC Address**: Hardware address that uniquely identifies the IP set. Not applicable for analog or digital sets.

The expanded view can be sorted on any column heading. Note that for an IP Office system with a large number of sets, this view can require some time to load.

Set Inventory Download

To download the set inventory to a .csv file, click on the icon.

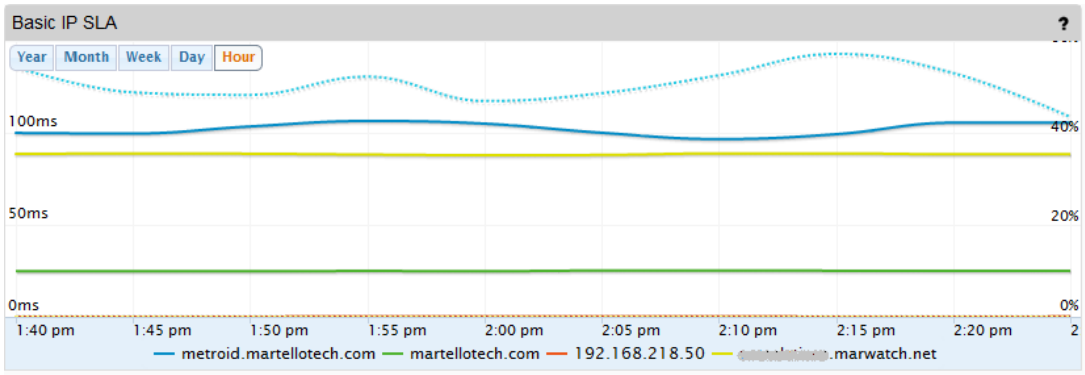
BASIC IP SLA PANEL

Mitel Performance Analytics supports basic IP SLA monitoring for up to four remote IP hosts (targets) from a Probe. The IP SLA graph provides Round Trip Time (RTT) and packet loss information to measure the quality of the network between the Probe and the target.

The **IP SLA** panel displays a graph of measured RTT and Packet Loss for up to four targets. There is a time scale selector which allows you to select Year, Month, Week, Day and Hour views of the data. Data for a target can be removed from the graph by clicking on the target name in the graph legend. By hovering over a graph line, you can show detailed information for any measurement.

To configure IP SLA Monitoring, refer to "Probe Configuration" on page 114.

Allow up to an hour for the **IP SLA** panel to display graph results. The following is an example of how the data is presented.



The following is a description of the displayed data:

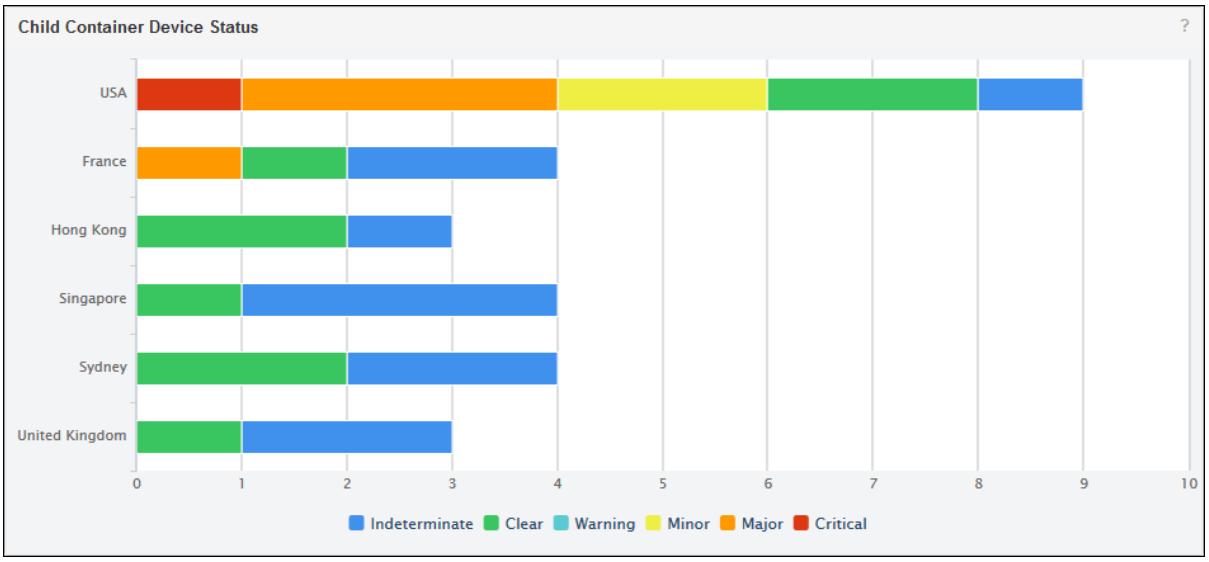
- **Round Trip Time (RTT)**: This is the average time for an IP packet to make a return journey from the Probe to the target. Mitel Performance Analytics uses ICMP Ping packets to make this measurement. For voice traffic RTT should be less than 300 ms. RTT depends on a number of factors:
  - Transmit time - the time it takes to send the ICMP test packet onto a network link. For fast links this time is negligible.
  - Propagation time - the time it takes for the ICMP packet to travel through the network. This is determined by the transmission speed in the network link and the physical length of the link.
  - Queueing time - if a network is busy, an intermediate network router may put IP traffic into a buffer and delay sending until the link is available.

- ICMP echo response time at the target - if the target is a network device such as a switch or router, the echo response time may be quite significant. Servers are typically far more responsive to ICMP pings.

- **Percentage Packet Loss**: This is the percentage of test packets sent to a target that were not received at the Probe. For voice networks packet loss should be less than 0.5%; for non voice IP traffic, packet loss should be less than 2%. Packet loss depends on a number of factors:
  - Network link occupancy
  - Firewalls that block ICMP ping
  - Target device type

CHILD CONTAINER DEVICE STATUS PANEL

This panel summarizes the alarm status in subcontainers in the current container. Information is displayed according to the subcontainer with the most severe alarms. Use this panel to quickly identify which subcontainers have devices with the worse alarms.



The previous example shows that the container has six subcontainers with devices generating alarms: USA, France, Hong Kong, Singapore, Sydney, and United Kingdom.

The USA subcontainer has the devices with the worse alarms. Of its nine devices:

- One device has critical alarms.
- Three devices have major alarms.
- Two devices have minor alarms.
- Two devices have cleared alarms.
- One device has indeterminate alarms.

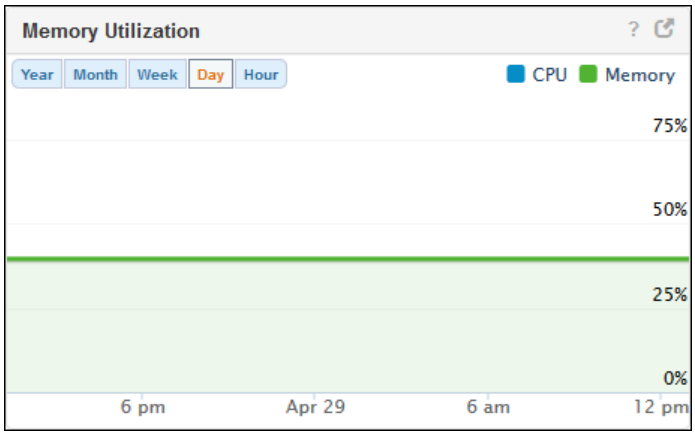
The France subcontainer has the next worse alarm count. Of its four devices:

- One device has major alarms.
- One device has cleared alarms.
- Two devices have indeterminate alarms.

Clicking on the subcontainer name listed on the left of the panel accesses the dashboard for that subcontainer.

CPU AND MEMORY UTILIZATION PANEL

This panel shows current and historical performance information for the memory and CPU utilization of the monitored device.



MEMORY UTILIZATION

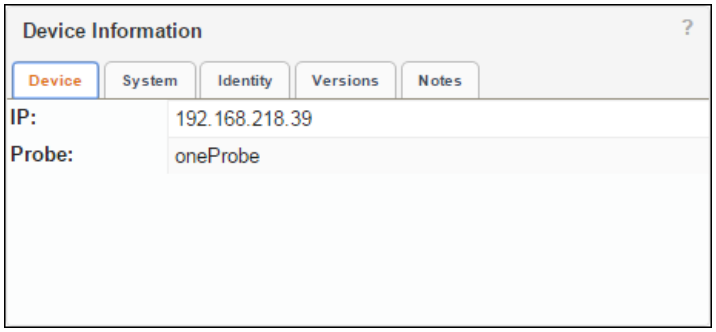
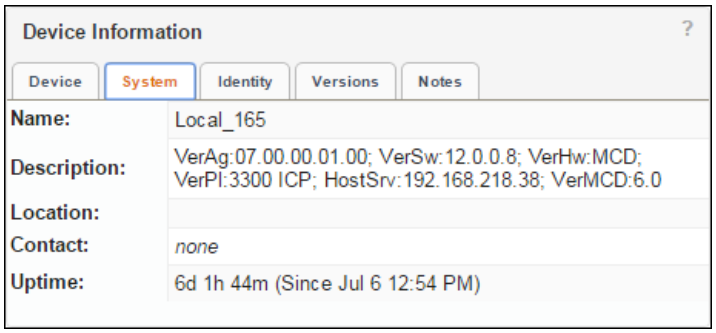
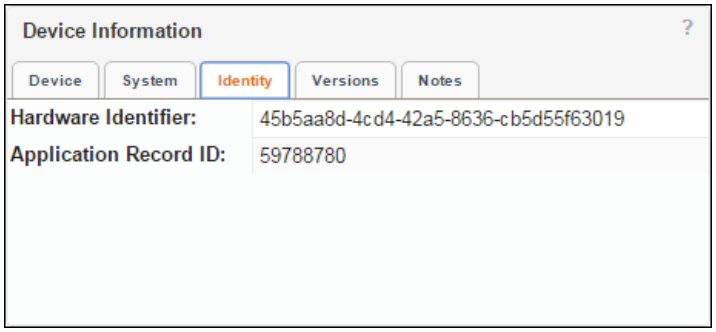
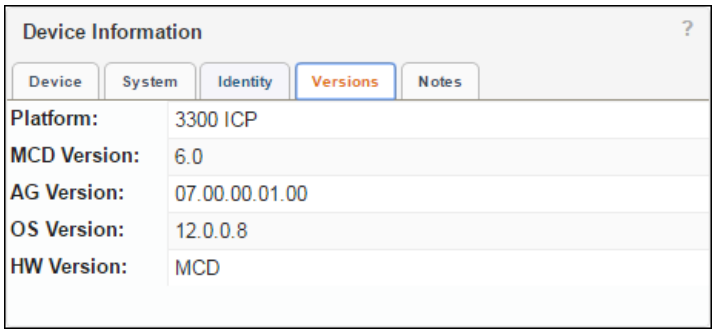
Utilization is displayed as a percentage of available memory. Increasing levels of memory utilization can be an indication that there is a memory leak in the software running on the monitored device. In general this should be less than 95% for embedded devices.

CPU UTILIZATION

Utilization is displayed as a percentage of available CPU. High levels of CPU utilization can indicate performance problems in the monitored device.

DEVICE INFORMATION PANEL

This panel shows information about the device being monitored. Depending on the device type, the panel displays a number of device information tabs.

TAB	DESCRIPTION	EXAMPLE
Device	Device IP Address and Probe used to monitor device (if applicable).	
System	Device information as reported by the device.	
Identity	3300 Hardware ID (if available) and MiVoice Business Application Record ID (if configured).	
Versions	Hardware inventory as reported by the device.	

TAB	DESCRIPTION	EXAMPLE
Notes	Text as entered in the Description field in the device's settings sheet.	

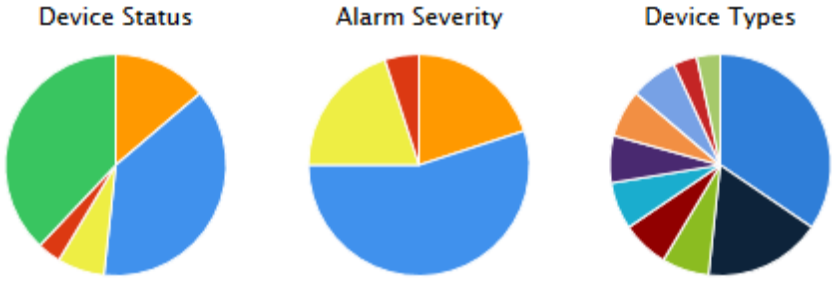
DEVICE INVENTORY PANEL

This panel's pie charts give a snapshot of the container's current network performance. All container alarms, equipment status', and device inventory are included.

The **Device Status** pie chart represents the ratio of status types critical, major, minor, warning, indeterminate, and clear from the total quantity of devices in inventory.

The **Alarm Severity** pie chart represents the ratio of alarm types: critical, major, minor, warning, and indeterminate. The alarms are taken from all devices.

The **Device Types** pie chart represents the ratio of devices types in inventory.



DISK USAGE PANEL

This panel shows the utilization of the file system(s) or disk(s) on the server. Utilization is displayed as a percentage of the total file size.

EVENT STREAM PANEL

This panel displays information on events generated by the monitored device.

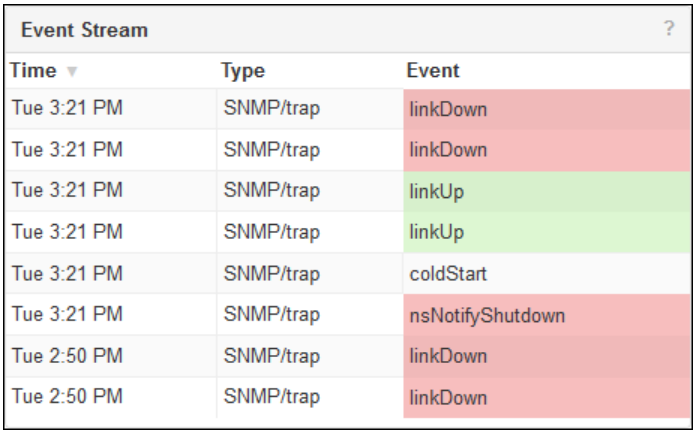
EVENT STREAM SUMMARY VIEW

The summary view displays the following information:

- **Time**: The date and time the event occurred.
- **Type**: Type of event; for example, an SNMP trap.

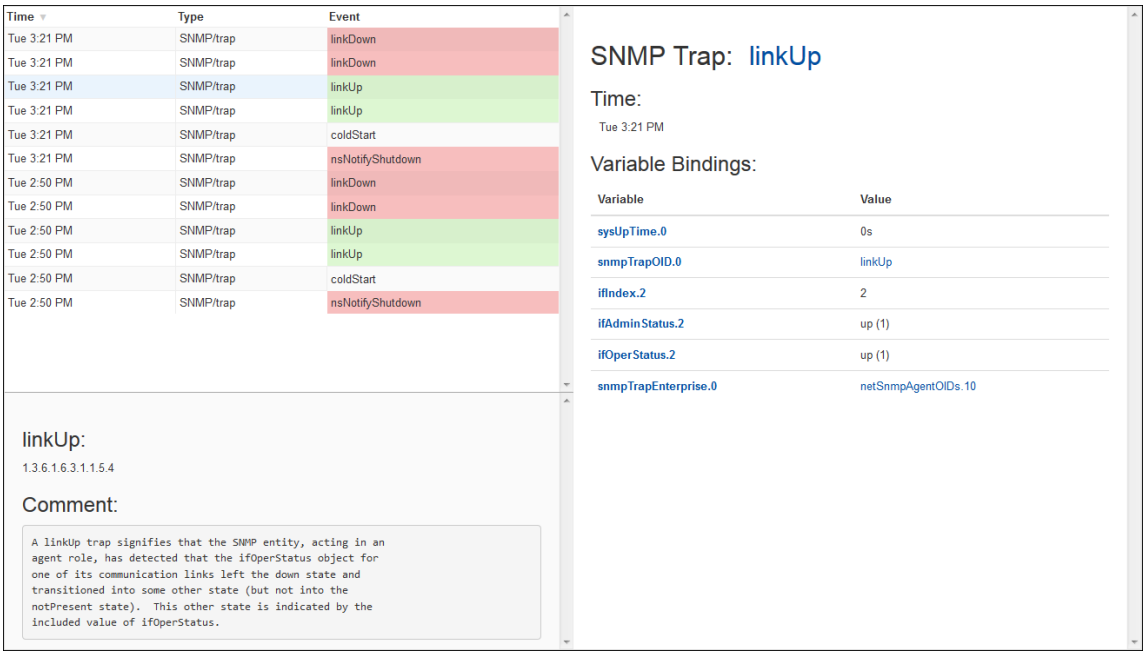
- **Event**: The name of the event; for example, **linkDown** or **coldStart**.

The following is a typical summary view.



EVENT STREAM DETAILED VIEW

Clicking on an event in the summary view displays a detailed view of that event. The following is a typical detailed view.

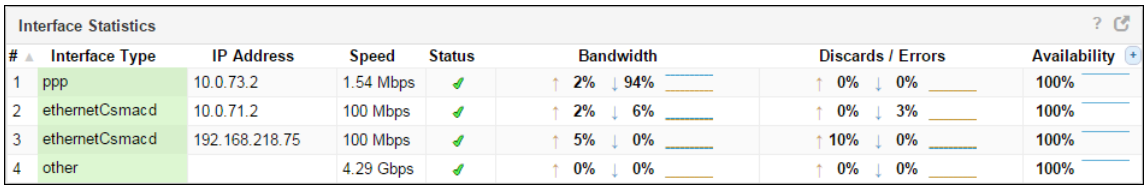


The information from the summary panel is shown in the top left area. Use it to select individual events. The selected event has a light blue background.

Detailed information about the selected event is shown in the area to the right. Clicking on any blue linked topic in the area to the right displays a description in the bottom left area, in the **Comment** box.

INTERFACE STATISTICS PANEL

This panel provides summary information about the physical and logical interfaces on a monitored device.



Interface rows are colored to indicate potential interface status:

- Red: likely trouble
- Orange: potential trouble
- Green: trouble unlikely

These color codes do not reflect alarm status. For details of the conditions under which they are applied, see "Interface Status Color coding" on page 230.

The table can be sorted by clicking on the column title. The following sections describe information presented in the table.

Clicking on the + icon to the right of the **Availability** column heading displays an additional **Description** column.

Interface Number Column

This is a reference number provided by the device.

Interface Type Column

This column describes the type of interface. Common values are:

- **ds1**: 1.5 Mbps serial interface
- **ds3**: 45 Mbps serial interface
- **e1**: 2.0 Mbps serial interface
- **ethernetCsmacd**: Ethernet interface
- **pppMultilinkBundle**: Multilink PPP (point-to-point protocol), in which multiple physical links are bonded to provide a single higher capacity logical link.

For a complete list, see http://www.iana.org/assignments/ianaiftype-mib.

Description Column

This is the interface description taken from the IF-MIB.

Note: For Cisco routers, the Description field may have a description containing unexpected alias names.

IP Address Column

This is the IP address associated with the interface.

Speed Column

This shows the interface speed in bits per second.

Status Column

The status icon shows the current interface status.

ICON	DESCRIPTION
	Interface is active
	Interface is down or there is a problem with the interface
	Interface is down and the administrative status is up

Bandwidth Column

This column shows summary information for bandwidth utilization per interface for the previous 60 minutes.

The up arrow shows uplink bandwidth utilization as percentage of link speed, most recent measurement.

The down arrow shows downlink bandwidth utilization as percentage of link speed, most recent measurement.

The Sparkline graphic shows trends for the uplink and downlink bandwidth utilization for the previous 60 minutes. Click on the Sparkline graphic for an expanded view of the 60 minutes.

Discards / Errors Column

The up arrow shows uplink discards as percentage of all packets, most recent measurement

The down arrow shows downlink discards, errors and unknown packets as percentage of all packets, most recent measurement.

The Sparkline graphic shows trends for the uplink and downlink discards and errors for the previous 60 minutes. Click on the Sparkline graphic for an expanded view of the 60 minutes.

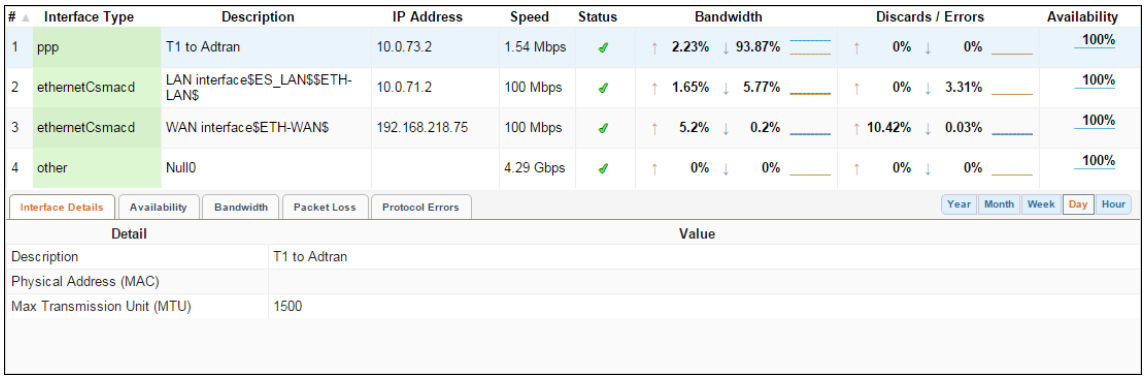
Note that discards and errors may be present for physical interfaces but not appear for logical interfaces. This is because the physical interface discards errored packets and does not present these to the logical interface.

Availability Column

This column shows summary information for the interface availability for the previous 60 minutes. The percentage displayed is the average availability over the last 60 minutes. The Sparkline graphic shows trends for the interface availability for the previous 60 minutes. Click on the Sparkline graphic for an expanded view of the 60 minutes.

INTERFACE STATISTICS EXPANDED VIEW

To get more detailed information on monitored device interface statistics, click on the **Expand** icon on the top right hand corner of the panel.



#	Interface Type	Description	IP Address	Speed	Status	Bandwidth	Discards / Errors	Availability
1	ppp	T1 to Adtran	10.0.73.2	1.54 Mbps	✓	↑ 2.23% ↓ 93.87%	↑ 0% ↓ 0%	100%
2	ethernetCsmacd	LAN interface$ES_LAN$$ETH-LAN$	10.0.71.2	100 Mbps	✓	↑ 1.65% ↓ 5.77%	↑ 0% ↓ 3.31%	100%
3	ethernetCsmacd	WAN interface$ETH-WAN$	192.168.218.75	100 Mbps	✓	↑ 5.2% ↓ 0.2%	↑ 10.42% ↓ 0.03%	100%
4	other	Null0		4.29 Gbps	✓	↑ 0% ↓ 0%	↑ 0% ↓ 0%	100%

Interface Details | Availability | Bandwidth | Packet Loss | Protocol Errors — Year | Month | Week | Day | Hour

Detail	Value
Description	T1 to Adtran
Physical Address (MAC)	
Max Transmission Unit (MTU)	1500

The expanded view displays the IP address (if assigned) of each interface and enables the display of more detailed interface performance statistics.

Interface Selection

Select an interface by clicking on the Interface row in the upper part of the window.

Historical Data

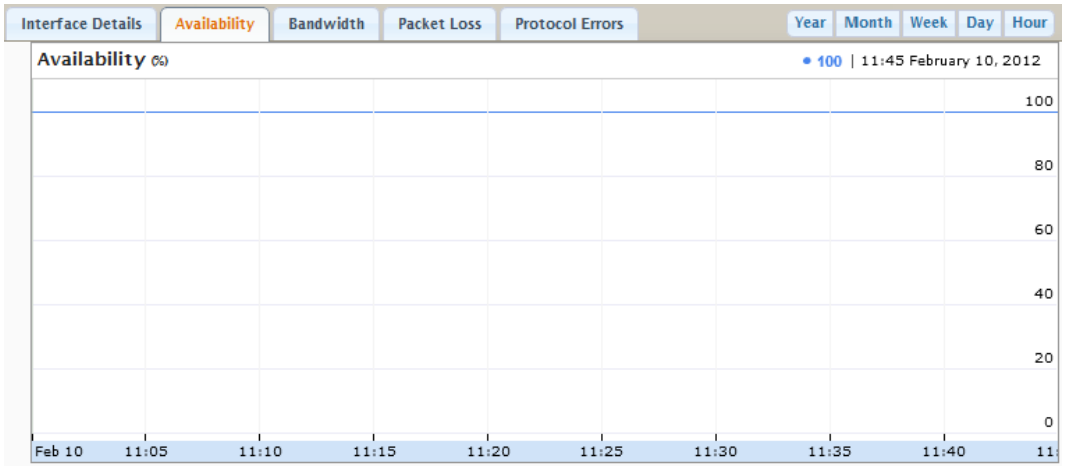
To examine historical interface statistics, click on one the time scale buttons (Year, Month, Week, Day, or Hour).

Interface Details Tab

This tab shows additional information for the selected interface. For the Ethernet interface in the previous example, the tab shows the MAC address and MTU.

Availability Tab

This tab shows percentage interface availability over time. For a given interface, this is either 0% (unavailable) or 100% (available).



Bandwidth Tab

This tab shows the following interface statistics:

- **Transmit Bandwidth (Uplink)**, in bits per second
- **Receive Bandwidth (Downlink)**, in bits per second

- **Discarded Packet Rate**, in packets per second. Packet discards are generally the result of buffer overflow and are an indicator of link congestion.
- **Interface Speed**, in bits per second. The interface speed is generally fixed except for a Multi-Link PPP logical interface, where the bandwidth is determined by the number of available physical interfaces assigned to the PPP interface. Note that polling occurs every hour, so the speed graph does not display data in the hour view.

Packet Loss Tab

When selecting an interface to view additional data, be sure to select a time view as well.

This tab displays:

- **Discards Out**, in packets per second. Outbound packet discards are generally the result of buffer overflow and are an indicator of link congestion.
- **Discards In**, in packets per second. Inbound packet discards are generally caused by framing errors or malformed packets and typically indicate a physical layer issue.
- **Queue Length**, in packets. This measures the transmit queue / buffer. High queue values indicate congestion on the interface.
- **Unknown Packets**, in packets per second. This measures unknown protocol packet received at the interface. These are rarely present in wide-area networks (WANs); in local-area networks (LANs) they typically indicate a non-IP protocol being received on an IP-interface.

Protocol Errors Tab

This tab displays:

- **Errors Out**, in packets per second. This measures the total rate of packets that could not be transmitted due to errors.
- **Errors In**, in packets per second. This measures the total rate of all errored packets received at the interface, whether errored packets or unknown protocols. In WAN links, this is generally an indication of a physical layer problem.

INTERFACE STATUS COLOR CODING

Mitel Performance Analytics applies color coding to the interface summary rows to assist in quickly identifying potential troubles. The color codes are:

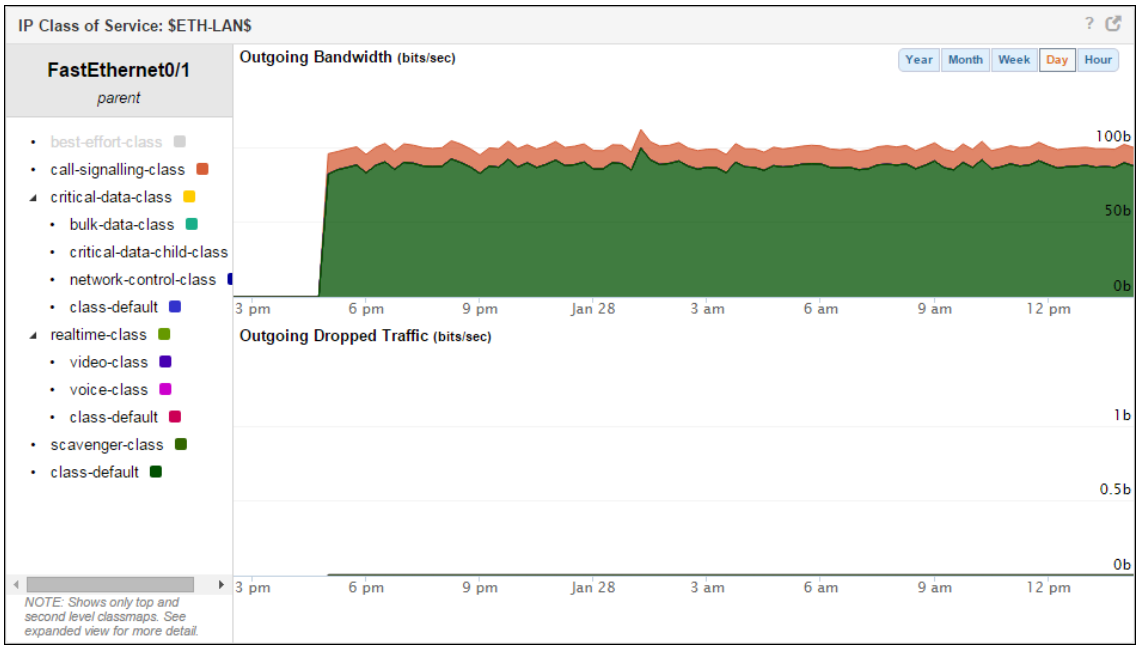
- Red: Likely Trouble. Any of the following conditions are met:
  - Operational status is down and the admin status is up
  - Percentage inbound discards exceeds 3%
  - Percentage inbound errors exceeds 3%
  - Percentage outbound discards exceeds 3%
  - Percentage outbound errors exceeds 3%
  - Percentage bandwidth utilization exceeds 75%
- Orange: Potential Trouble. Any of the following conditions are met:
  - Admin status is in down mode or test mode
  - Operational status is up for 5 minutes or less
  - Percentage inbound discards exceeds 1%
  - Percentage inbound errors exceeds 1%
  - Percentage outbound discards exceeds 1%
  - Percentage outbound errors exceeds 1%
  - Percentage inbound unknown protocol packets exceeds 3%
  - Percentage bandwidth utilization between 50% and 75%
- Green: Trouble Unlikely. None of the red or orange display criteria are met.

IP CLASS OF SERVICE PANEL

The **IP Class of Service** (CoS) panel provides information about the class-based congestion management of voice and data IP traffic sent from a monitored device.

Mitel Performance Analytics supports monitoring of Cisco and Adtran routers configured with class-based traffic management.

For Cisco routers, Mitel Performance Analytics provides an IP COS panel for each router interface as well as nested COS statistics.



CLASS-BASED TRAFFIC MANAGEMENT

Class-based traffic management is a form of congestion management typically used to manage bandwidth allocation on WAN links. Class-based traffic management uses the concepts of:

- Traffic classes based on match criteria, which may include protocol type, Access Control Lists (ACLs), and input interfaces.
- Class map policies that define how different traffic classes are prioritized under congestion.
- Service policies that define which interfaces the class map policies are applied to.

For details on Cisco class-based traffic management, refer to Cisco Quality of Service Overview at www.cisco.com. For details on Adtran class-based traffic management, search for article number 1617: *Configuring Quality of Service (QoS) in AOS* from the Adtran Knowledge Base.

CLASS NAME AND DIFFERENTIATED SERVICES CODE POINT (DSCP)

The IP COS panel provides details about the class name and the DSCP applied to outbound traffic by class, if available. DSCP marking is commonly used to indicate the MPLS class of service that IP packets are assigned to.

SUMMARY VIEW TRAFFIC MONITORING GRAPHS

The summary view panel header shows the name of the router interface providing the displayed statistics. In the previous example, the router interface name is **$ETH-LAN$**.

For Cisco routers, the right of the panel shows the first two levels of nested COS statistics. To display further levels, access the expanded view. See “"Expanded View Nested COS Traffic Monitoring Graphs" on page 232.

Click on a statistic name to show or hide the statistics on the graphs. Hidden statistics are grayed out.

The two traffic monitoring graphs are **Outgoing Bandwidth by Class of Service** and **Outgoing Dropped Traffic by Class of Service**.

Outgoing Bandwidth by Class of Service

This graph shows a stacked graph of all outbound traffic in bits per second, by traffic class. Note that this does not include traffic which has been dropped because of network congestion. The colors indicate the traffic class as defined in the router. The class name and DSCP (if assigned) are indicated in the legend.

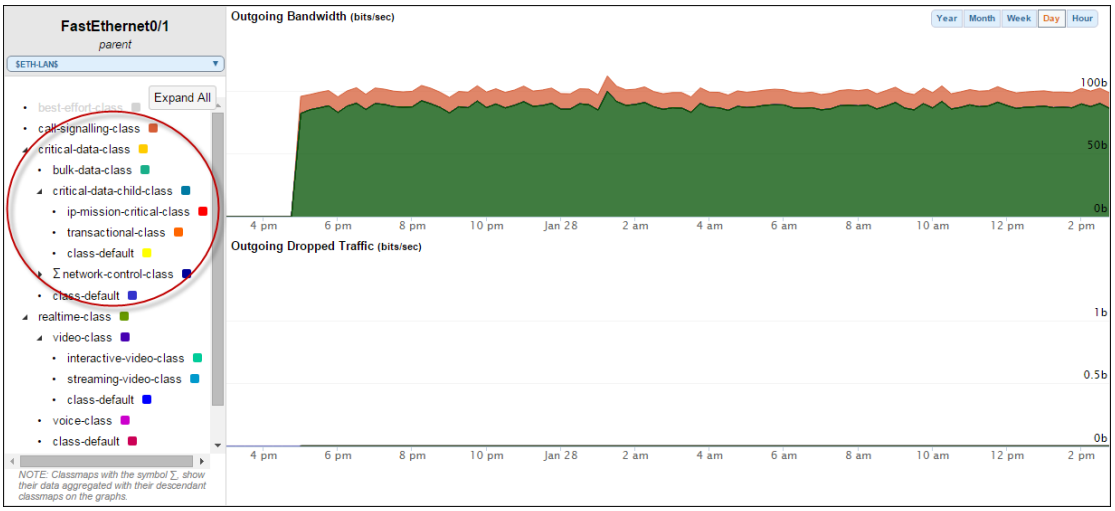
Outgoing Dropped Traffic by Class of Service

This graph shows a line graph of discarded traffic in bits per second, by traffic class. In normal operation, this should remain at zero. Discarded traffic indicates network congestion. The default view is for the previous 60 minutes. To view historical COS information, click on the time scale buttons.

EXPANDED VIEW NESTED COS TRAFFIC MONITORING GRAPHS

Use the expanded view of the IP COS panel to show nested COS statistics.

The **Sigma** icon (Σ) indicates that a lower level of policy exists. Click on it to expand the display and show the statistics of that lower level.



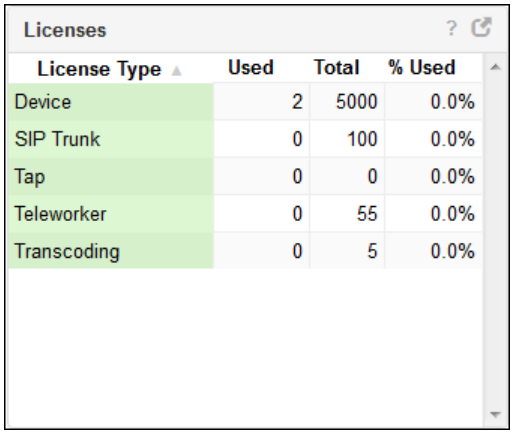
Use the **Expand All** button to display the full set of lower policies and their associated statistics.

For Cisco routers, use the drop-down box to select which interface to display statistics.

LICENSES PANEL

The **Licenses** panel is available on device dashboards. It displays a list of the different types of licenses found on the device along with how many are currently in use.

License types are highlighted to indicate use levels.



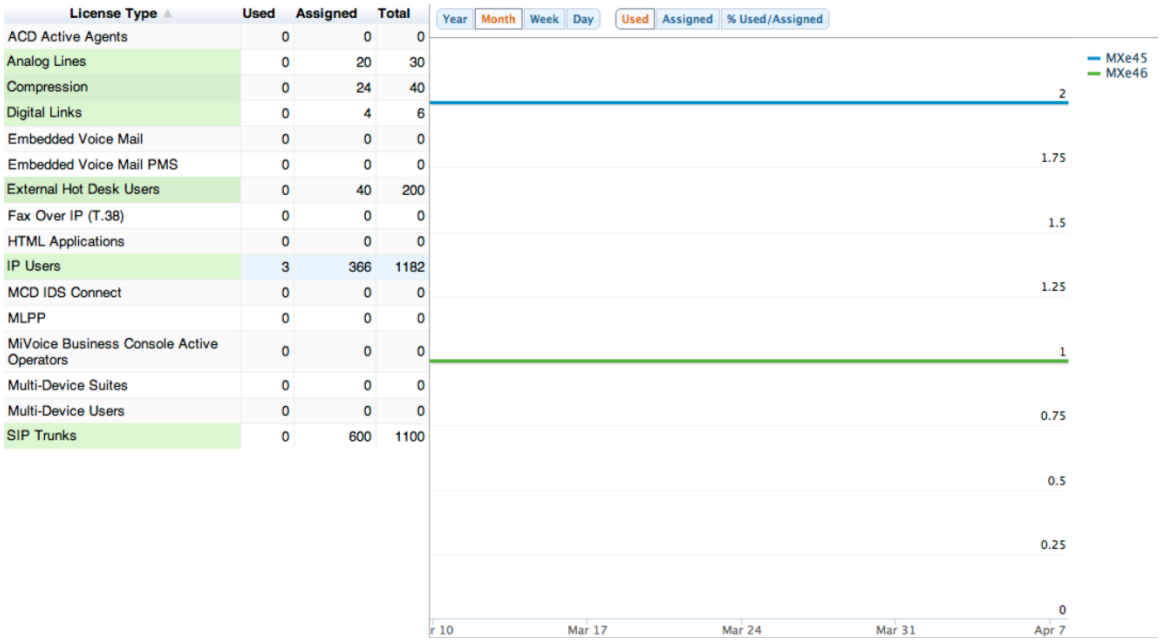
Licenses

License Type	Used	Total	% Used
Device	2	5000	0.0%
SIP Trunk	0	100	0.0%
Tap	0	0	0.0%
Teleworker	0	55	0.0%
Transcoding	0	5	0.0%

When the panel is expanded it displays a graph, showing the history of license utilization on this device.

To toggle, hide, or show the license consumption, click on the device name. This is useful in viewing license consumption by device over time.

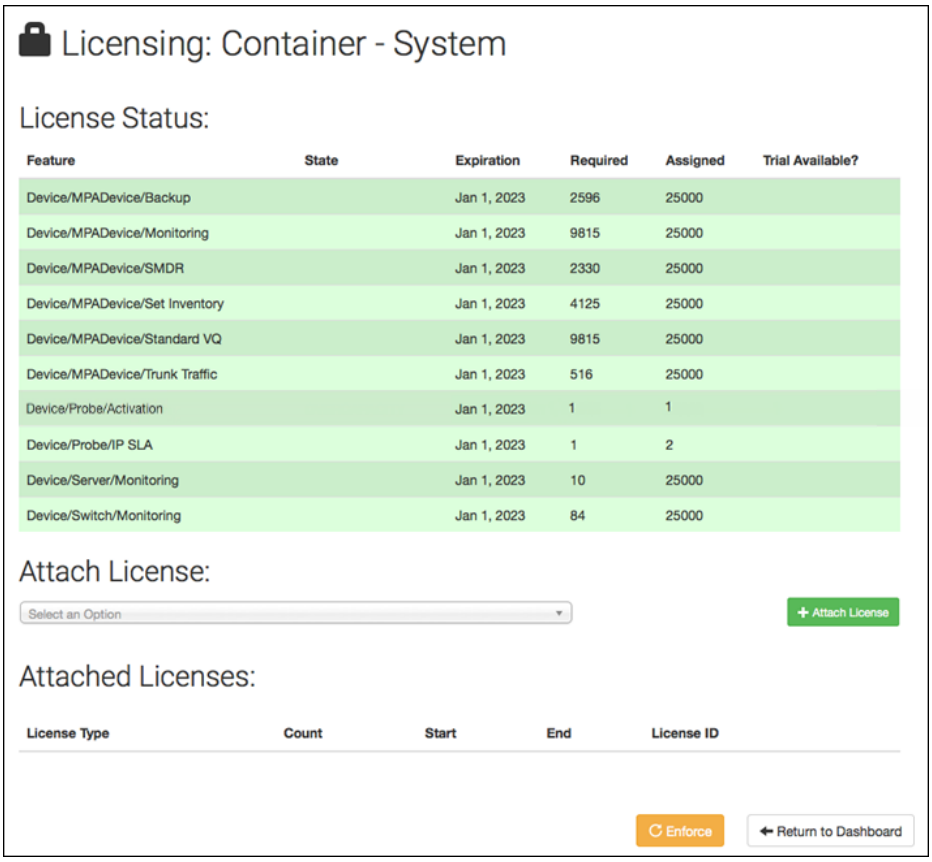
To toggle hide or show the license consumption by license type, click on the license name in the graph legend.



License Type	Used	Assigned	Total
ACD Active Agents	0	0	0
Analog Lines	0	20	30
Compression	0	24	40
Digital Links	0	4	6
Embedded Voice Mail	0	0	0
Embedded Voice Mail PMS	0	0	0
External Hot Desk Users	0	40	200
Fax Over IP (T.38)	0	0	0
HTML Applications	0	0	0
IP Users	3	366	1182
MCD IDS Connect	0	0	0
MLPP	0	0	0
MiVoice Business Console Active Operators	0	0	0
Multi-Device Suites	0	0	0
Multi-Device Users	0	0	0
SIP Trunks	0	600	1100

LICENSING PANEL

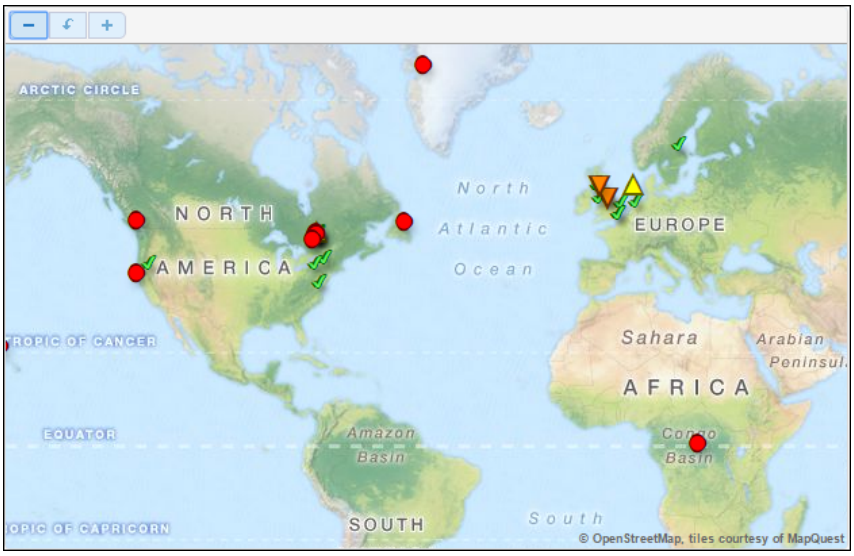
The Licensing panel is displayed when you select Licenses under the **Settings** icon.



The top part indicates the status of the licenses for this device or container. The middle part allows you to attach more licenses. The bottom part lists the currently attached licenses.

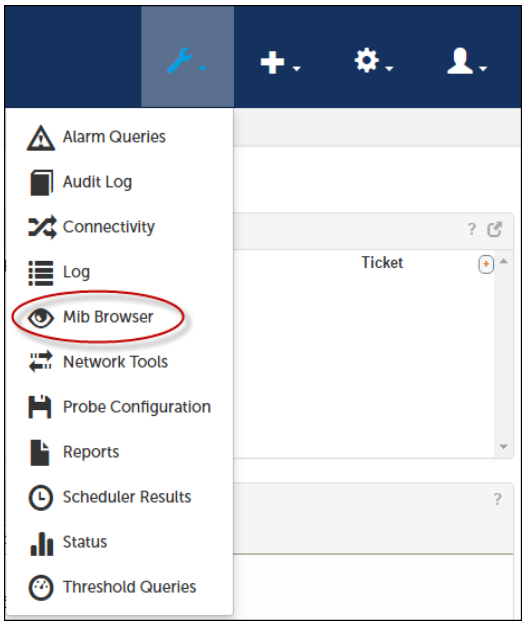
LOCATION MAP

The **Location Map** displays all containers being monitored globally. The container icon represents their current status. To narrow in on a particular site, click the appropriate icon.



MIB BROWSER

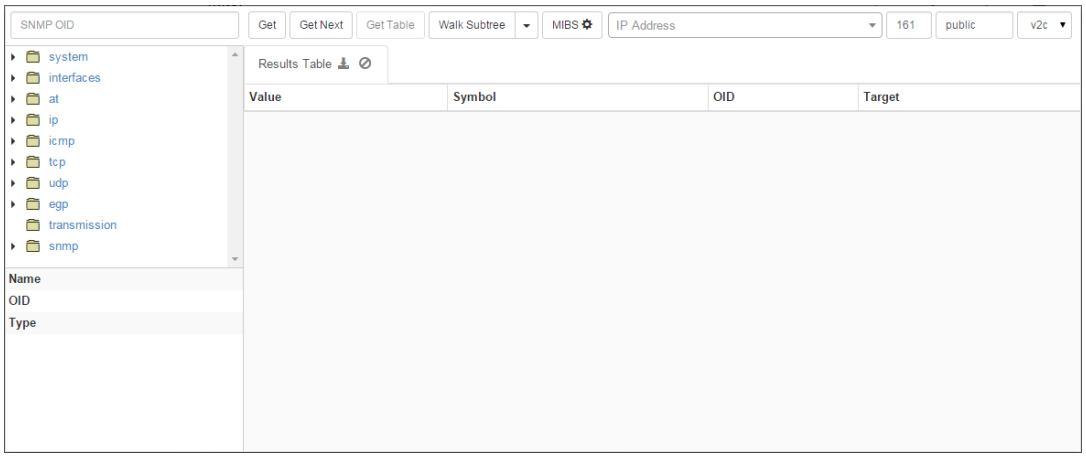
The **MIB Browser** is used to diagnose SNMP-enabled network devices and applications on the customer network. When applicable, it is available under the **Tools** icon of the dashboard. The following is an example for a Probe:



The MIB Browser can access certain devices only. If invoked from a device dashboard, the MIB Browser can access that device only. If invoked from a Probe dashboard, the MIB Browser can access any device that the Probe can reach.

To use the MIB browser:

1. Access the MIB Browser.



If applicable, following fields are prefilled with default values. These defaults vary depending on the device configuration. Typically the defaults are:

- SNMP port is set to **161**
- SNMP community string is set to **public**
- SNMP version is set to **v2c**

- MIB is set to **RFC1213-MIB**, with the object tree to the left displaying the correct objects

2. Optionally change the default settings.
   To change the MIB in use, click on the **MIBs** button to show available MIBS. Use the **Search MIBs** field to quickly search the available MIBs for the one you want. The Mitel Performance Analytics MIB browser is delivered many publically available MIBs. When satisfied, click **Confirm** to return to the MIB browser.

   If the Mitel Performance Analytics MIB browser does not contain the MIB you want, see “"Adding MIBs" on page 236.

   If you are accessing the MIB Browser from a Probe select the device from the **IP Address** dropdown list. If you are accessing the MIB Browser from a device, the IP Address dropdown list is prefilled with device IP address.
3. Select an object from any of the displayed object tree.
4. Click **Get** or **Get Table** as required to fetch the data.

A new tab is created for table queries. The tab is labeled with the OID and the system host name.

Result tabs contain icons that allow you to:

- Refresh the results
- Clear the results
- Download the results. Results are downloads as a .csv file.
- Rotate the results; that is, for tables swap columns for rows
- Close the tab

Clicking on any heading in the results of a table query highlights the object in the MIB object tree.

In addition, the MIB browser has buttons that allow you to:

- **Get** the **Next** object on the device
- Walk a Subtree

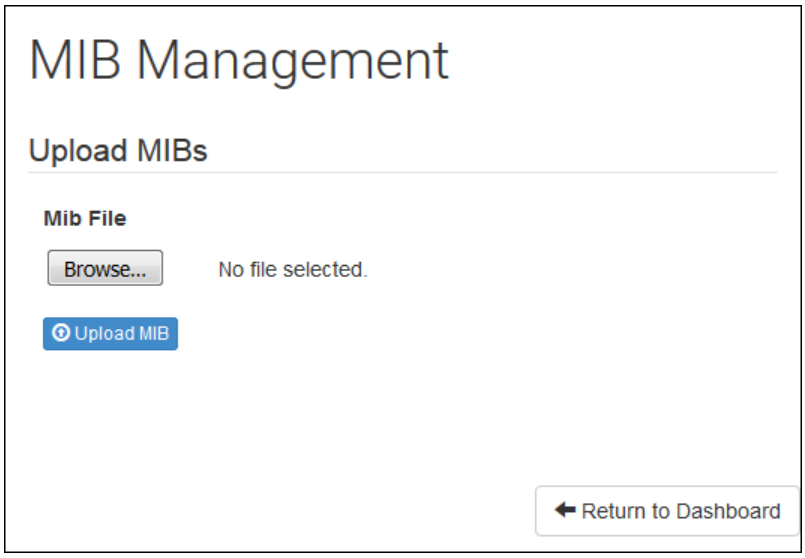
ADDING MIBS

The Mitel Performance Analytics MIB browser is delivered many publically available MIBs. If it does not contain the MIB you want, you can add the MIB to the MIB browser.

Note: You need a special permission to add a MIB. See “"User Permissions" on page 46.

Do the following steps:

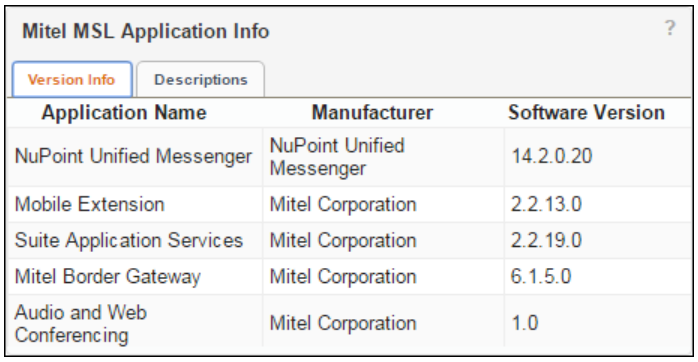
1. Access the MIB Browser.
2. Click the **MIBs** button.
3. Click the **Load MIBs** button.
   The **MIB Management** window is displayed.



4. Click the **Browse** button.
5. Navigate to the MIB and select it.
6. Click the **Upload MIB** button.
   Mitel Performance Analytics responds indicating it has successfully uploaded the MIB or informs you if it has issues uploading the MIB.
7. Click the **Return to Mib Browser** button.

MITEL MSL APPLICATION INFO PANEL

The **Mitel MSL Application Info** panel displays information on the applications that have been installed and are running on the blades of an MSL server.

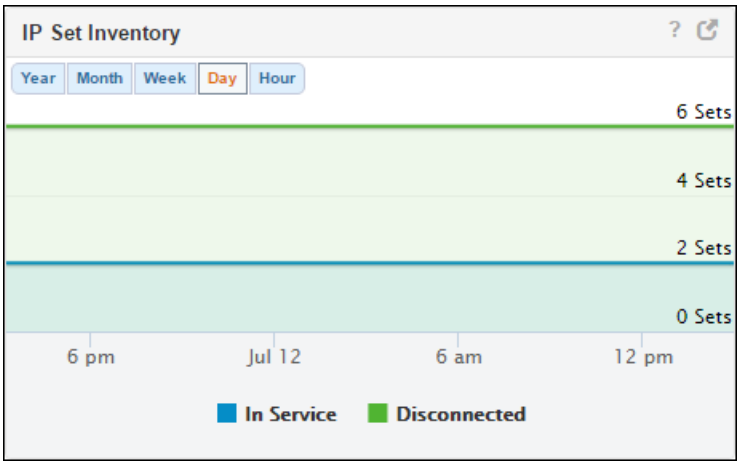


Application Name	Manufacturer	Software Version
NuPoint Unified Messenger	NuPoint Unified Messenger	14.2.0.20
Mobile Extension	Mitel Corporation	2.2.13.0
Suite Application Services	Mitel Corporation	2.2.19.0
Mitel Border Gateway	Mitel Corporation	6.1.5.0
Audio and Web Conferencing	Mitel Corporation	1.0

Details include application name, manufacturer, version, and description.

MIVOICE BORDER GATEWAY IP SET INVENTORY PANEL

Mitel Performance Analytics supports inventory monitoring for sets connected to a MiVoice Border Gateway.



DEFAULT VIEW MBG IP SET INVENTORY

The default view shows the total number of IP sets configured for the MiVoice Border Gateway by status, where the statuses are:

- In Service: IP set is connected and enabled
- Disconnected: IP set is enabled but disconnected
- Redirected: IP sets connected to alternate MiVoice Business

Click the graphic legend labels (**In Service**, **Disconnected**, or **Redirected**) to display or hide a set of data.

EXPANDED VIEW MBG IP SET INVENTORY

In its expanded view, the **Set Inventory** panel displays the following information about the sets connected to the MiVoice Border Gateway system:

- **State**: Identifies the state of the set, as described previously.
- **Enabled**: IP set admin status on MiVoice Border Gateway, True or False.
- **Connected**: Connection status, True or False.
- **Device ID**: MAC address of IP set (if known).
- **Device DN(s)**: DN(s) assigned to the IP set.
- **Device Type**: Type of IP set (if known).
- **Current ICP**: Name of current ICP for the IP set. Generally, Current ICP and Configured ICP are the same.
- **Configured ICP**: Name of default ICP for the IP set. Generally, Current ICP and Configured ICP are the same.
- **Type**: MiNet Client or SIP Client.
- **Most Recent IP Address**: IP address of record for the IP set.

The expanded view can be sorted on any column heading. For a MiVoice Border Gateway with a large number of sets, this view can require some time to load.

Set Inventory Download

To download the set inventory to a .csv file, click on the icon.

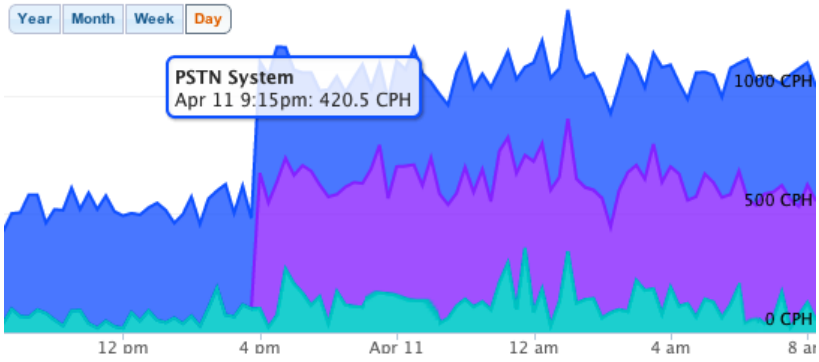
MIVOICE BORDER GATEWAY TRUNK UTILIZATION PANEL

The **Trunk Utilization** panel for MiVoice Border Gateway shows the performance of all of the SIP trunk groups in the MiVoice Border Gateway system. There are two areas in the **Trunk Utilization** panel: SIP Trunk Call Rates and SIP Trunk Utilization.

Click on the graphic legend labels at the bottom of the panel to display or hide the data of individual trunks.

SIP TRUNK CALL RATE

This area shows the call rate for all trunk group calls in the system in 15-minute intervals.

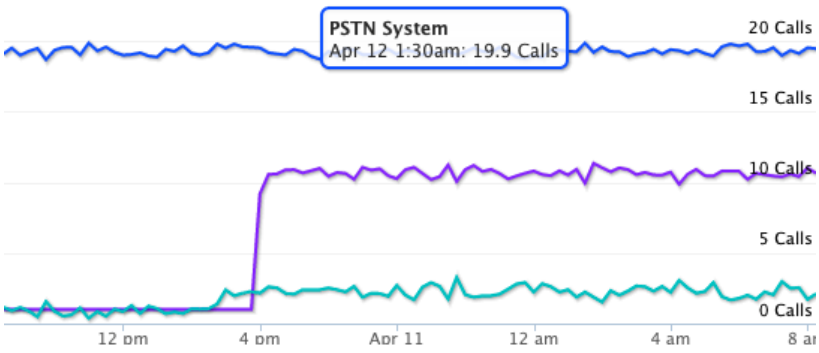


The area shows a stacked bar chart of all SIP trunk calls in the MiVoice Border Gateway, both inbound and outbound. Trunk groups are identified by their MiVoice Border Gateway SIP trunk names.

For more details, hover the mouse over a graph point. The graph displays the trunk name, time and date, and call rate for that data point.

SIP TRUNK GROUP UTILIZATION

To provide information per trunk group, the second area shows SIP trunk utilization by SIP trunk.

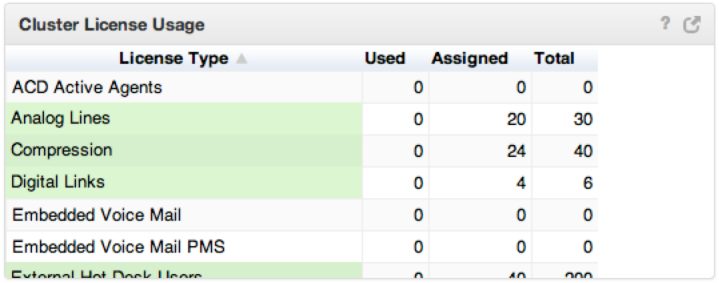


This graph shows maximum SIP trunk group utilization per 15-minute interval.

MIVOICE BUSINESS CLUSTER LICENSE USAGE PANEL

This panel displays a list of the different types of licenses found on the MiVoice Business cluster, along with how many are currently in use in the Cluster. Note that this information panel is displayed only on MiVoice Business call servers which are the Designated License Manager (DLM).

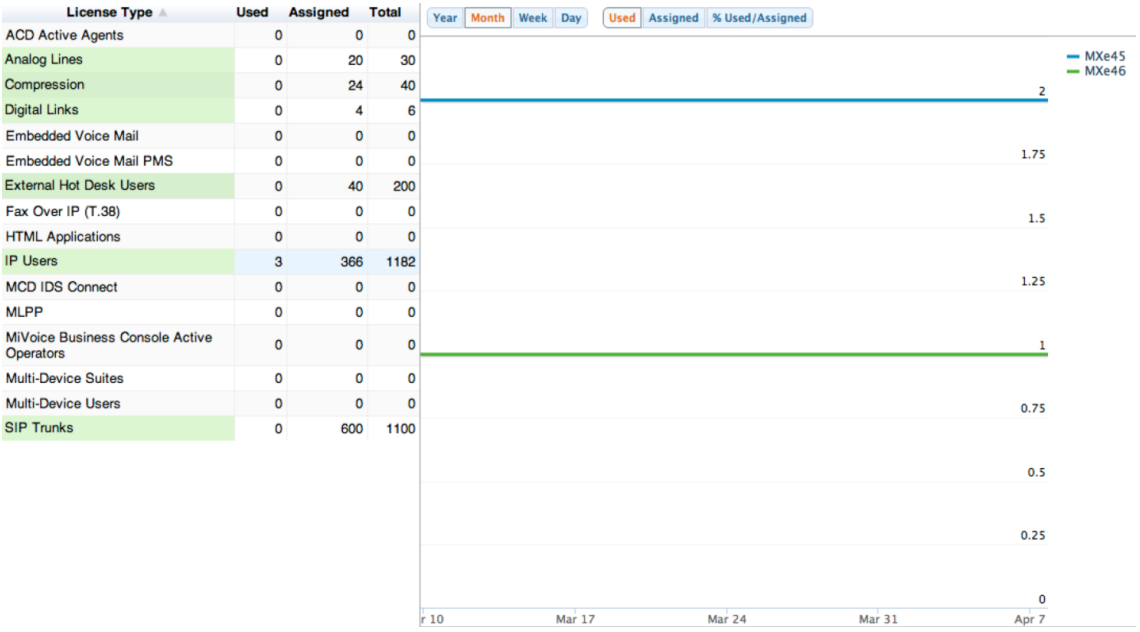
License types are highlighted to indicate utilization levels.



License Type	Used	Assigned	Total
ACD Active Agents	0	0	0
Analog Lines	0	20	30
Compression	0	24	40
Digital Links	0	4	6
Embedded Voice Mail	0	0	0
Embedded Voice Mail PMS	0	0	0
External Hot Desk Users	0	40	200

When the panel is maximized it displays a graph, showing the history of license utilization in the cluster by license type and MiVoice Business.

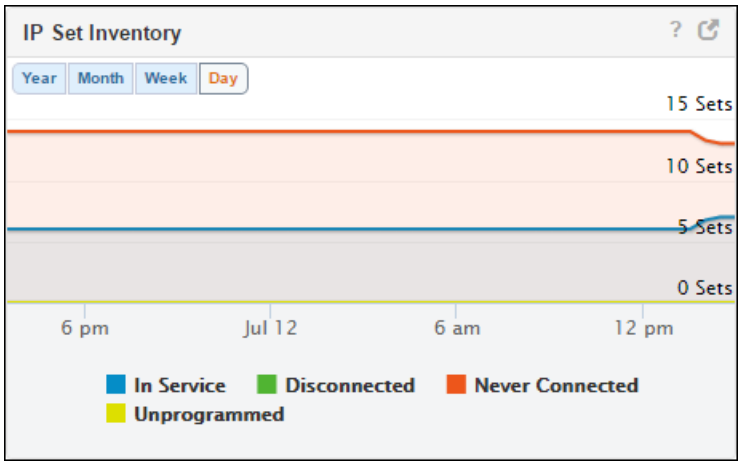
To toggle, hide, or show the license consumption, click on the MiVoice Business name in the graph legend. This is useful in viewing license consumption by MiVoice Business over time.



License Type	Used	Assigned	Total
ACD Active Agents	0	0	0
Analog Lines	0	20	30
Compression	0	24	40
Digital Links	0	4	6
Embedded Voice Mail	0	0	0
Embedded Voice Mail PMS	0	0	0
External Hot Desk Users	0	40	200
Fax Over IP (T.38)	0	0	0
HTML Applications	0	0	0
IP Users	3	366	1182
MCD IDS Connect	0	0	0
MLPP	0	0	0
MiVoice Business Console Active Operators	0	0	0
Multi-Device Suites	0	0	0
Multi-Device Users	0	0	0
SIP Trunks	0	600	1100

MIVOICE BUSINESS IP SET INVENTORY PANEL

Mitel Performance Analytics supports inventory monitoring for IP sets connected to a MiVoice Business.



DEFAULT VIEW MIVOICE BUSINESS IP SET INVENTORY

The default view shows the number of IP sets connected to the MiVoice Business by state, where the possible states are:

- In Service: Set has set up a TCP/IP connection and has been programmed.
- Disconnected: Set has been programmed and then disconnected from the LAN.
- Never Connected: Set has been programmed but has not been connected to the LAN.
- Unprogrammed: Set is connected to the LAN but has not been programmed.

Click the graphic legend labels (**In Service**, **Disconnected**, **Never Connected**, or **Unprogrammed**) to display or hide a set of data.

EXPANDED VIEW MIVOICE BUSINESS IP SET INVENTORY

In its expanded view, the **Set Inventory** panel displays the following information about the sets connected to the MiVoice Business:

- **Name**: Set user name.
- **Number**: Set prime directory number.
- **Device Type**: Set type.
- **State**: Identifies the state of the set, as described previously.
- **MAC Address**: Displays the hardware address that uniquely identifies the set. MAC addresses are not supported for SIP devices.
- **IP Address**: IP address of the set.
- **Subnet**: IP subnet for the set.
- **Gateway**: Default gateway for the set.
- **VQ Stats**: Indicates if voice quality statistics reporting is enabled for the set.
- **Primary ICP**: Displays the name or IP address of the set's local controller in a single-node environment or its primary controller (if programmed in the Network Elements form) in a resilient environment. If neither the name nor IP address is available, Unknown displays, indicating a problem with the controller.

- **Secondary ICP**: Applies to resilient environments only; the field is blank for single-node environments and for non-resilient Sets. If neither the name nor IP address is available, Unknown displays, indicating a problem with the controller.
- **Hardware Version**: The hardware version of the set (if available).
- **Software Version**: The software version of the set (if available).

The expanded view can be sorted on any column heading. Note that for a MiVoice Business with a large number of sets, this view can require some time to load.

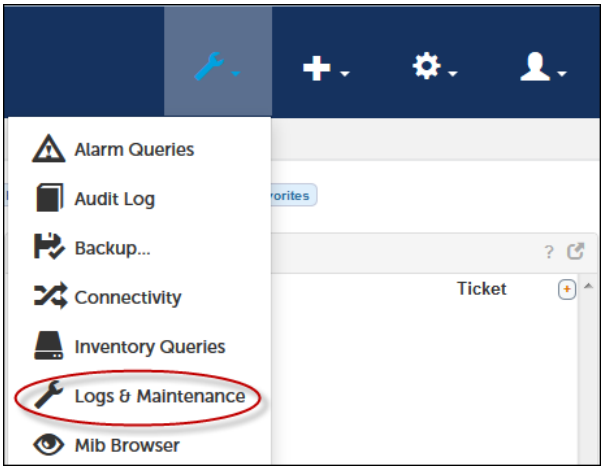
Set Inventory Download

To download the set inventory to a .csv file, click on the icon.

MIVOICE BUSINESS LOGS AND MAINTENANCE PANEL

This panel give you access to MiVoice Business maintenance and software logs. You can also send maintenance commands to the MiVoice Business.

Access this panel from device dashboard of a MiVoice Business. Select **Logs & Maintenance** under the **Tools** icon.



MIVOICE BUSINESS NODE LICENSING USAGE PANEL

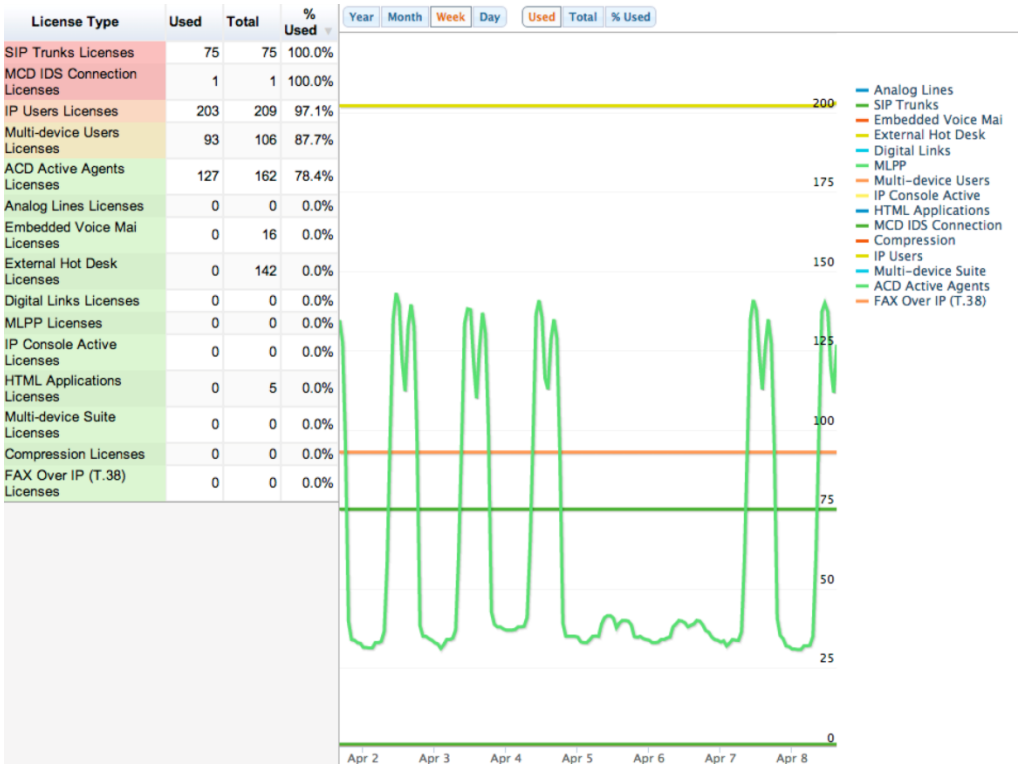
This panel displays a list of the different types of licenses found on the MiVoice Business device, along with how many are currently in use.

License types are highlighted to indicate utilization levels.

Node License Usage

License Type	Used	Total	% Used
SIP Trunks Licenses	75	75	100.0%
MCD IDS Connection Licenses	1	1	100.0%
IP Users Licenses	203	209	97.1%
Multi-device Users Licenses	93	106	87.7%
ACD Active Agents Licenses	127	162	78.4%
Analog Lines Licenses	0	0	0.0%
Embedded Voice Mai Licenses	0	16	0.0%
External Hot Desk Licenses	0	142	0.0%
Digital Links Licenses	0	0	0.0%
MLPP Licenses	0	0	0.0%
IP Console Active Licenses	0	0	0.0%

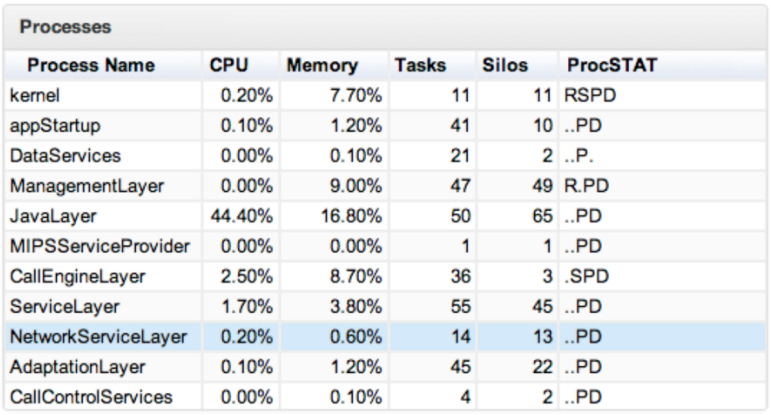
When the panel is expanded it displays a graph, showing the history of license utilization on this MiVoice Business.



To toggle, hide, or show the license consumption by license type, click the license name in the graph legend. This is useful in viewing license consumption by MiVoice Business over time.

MIVOICE BUSINESS PROCESSES TABLE

This panel is displayed for MiVoice Business release 7.0 and higher. The panel displays the MiVoice Business internal process status and resource utilization.



Processes

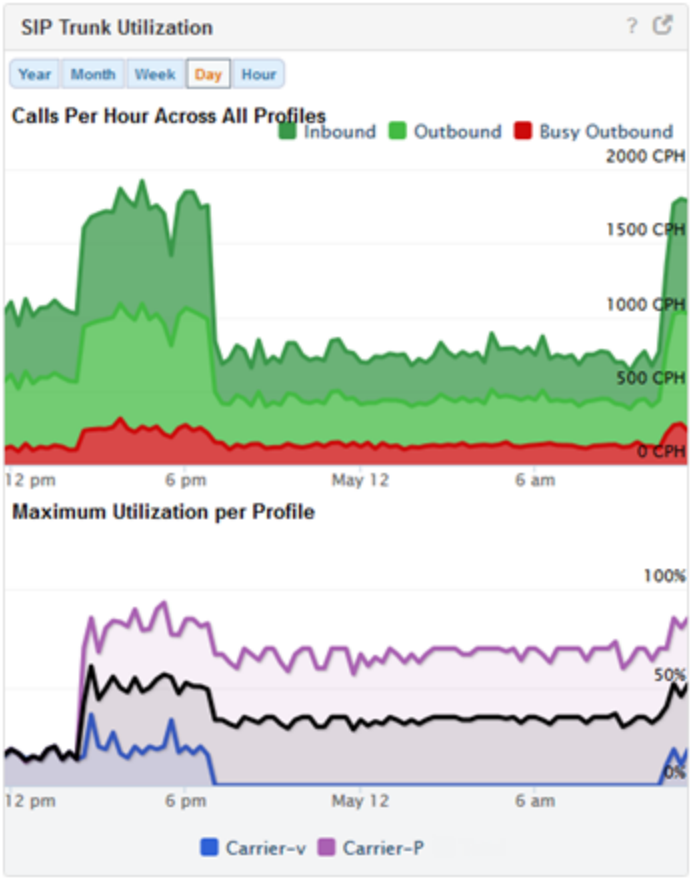
Process Name	CPU	Memory	Tasks	Silos	ProcSTAT
kernel	0.20%	7.70%	11	11	RSPD
appStartup	0.10%	1.20%	41	10	..PD
DataServices	0.00%	0.10%	21	2	..P.
ManagementLayer	0.00%	9.00%	47	49	R.PD
JavaLayer	44.40%	16.80%	50	65	..PD
MIPSServiceProvider	0.00%	0.00%	1	1	..PD
CallEngineLayer	2.50%	8.70%	36	3	.SPD
ServiceLayer	1.70%	3.80%	55	45	..PD
NetworkServiceLayer	0.20%	0.60%	14	13	..PD
AdaptationLayer	0.10%	1.20%	45	22	..PD
CallControlServices	0.00%	0.10%	4	2	..PD

The panel shows the following information for MiVoice Business processes:

- Task name
- Task % CPU utilization
- Task % memory utilization
- Number of tasks within the process
- Number of silos within the process
- Task summary: process contains tasks with the following status:
  - R=ready
  - S=suspended
  - P=pending
  - D=delayed

MIVOICE BUSINESS SIP TRUNK UTILIZATION PANEL

The **SIP Trunk Utilization** panel for MiVoice Business shows the performance of all SIP profiles in the MiVoice Business. There are two areas in the **SIP Trunk Utilization** panel: Call Rate and SIP Profile Trunk Utilization. Note that the MiVoice Business SIP trunk utilization data applies only to SIP trunks. Digital trunk utilization is reported on a different panel. See "MiVoice Business Trunk Utilization Panel" on page 246.



The trunk utilization metrics allow analysis of trunk capacity for actual traffic on the MiVoice Business. High numbers of busy outbound call attempts indicate that the trunk group is too small for the offered traffic. Low utilization shows that there is excess trunk capacity.

CALL RATE MIVOICE BUSINESS SIP TRUNKS

The **Call Rate** area shows the call rate for all SIP profiles in the system in 1-hour intervals (CPH). The area shows a stacked bar chart of:

- Inbound call rate (in dark green)
- Outbound call rate (in light green)
- Outbound busy call rate (in red)

Click the graphic legend labels (**Inbound**, **Outbound**, or **Busy Outbound**) to display or hide a set of data.

To convert to the number of call events per 15-minute interval, divide the hourly call rates by 4.

SIP PROFILE TRUNK UTILIZATION

SIP Profile Trunk Utilization area shows trunk utilization per SIP profile.

Utilization is defined as the maximum number of trunks in use per SIP profile (high water mark), expressed as a percentage of the number of trunks in each SIP profile.

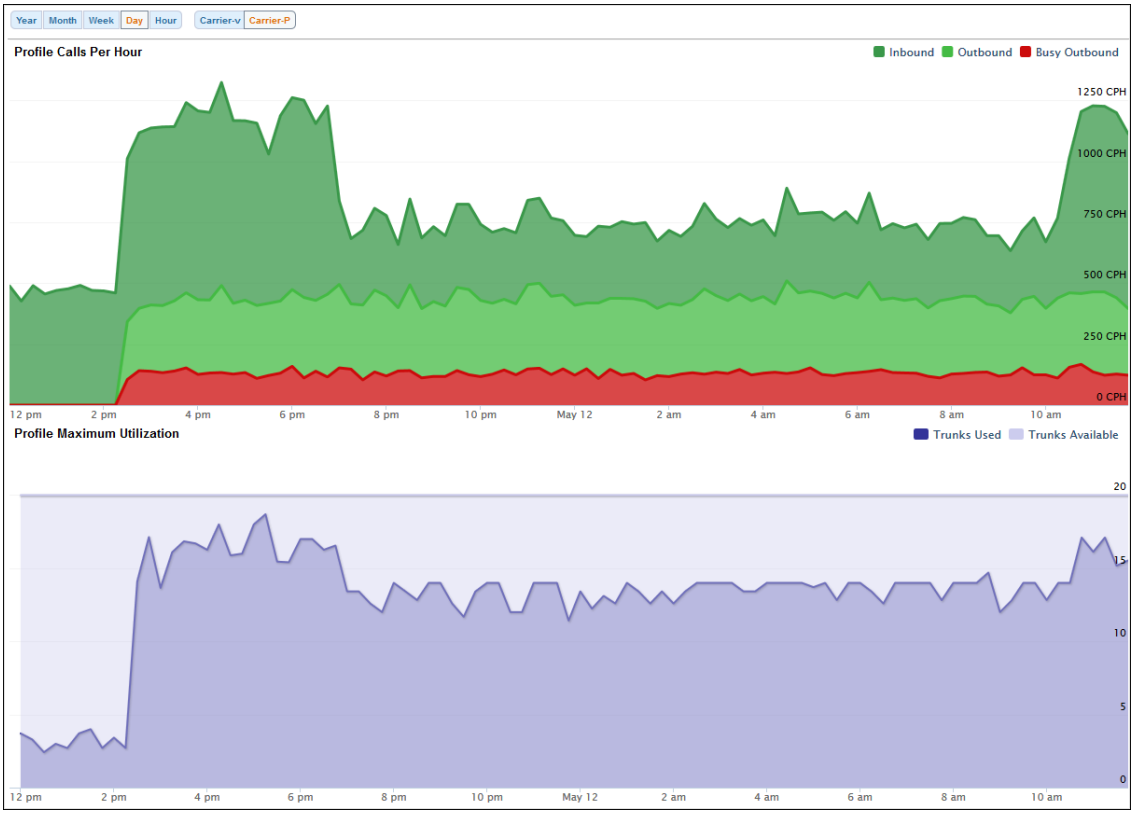
SIP profiles are identified by their name.

INDIVIDUAL SIP PROFILE TRUNK METRICS

The expanded view provides more detailed, individual SIP profile metrics. Traffic usage is expressed in CCS (hundred call seconds). Note that 1 Erlang = 36 CCS.

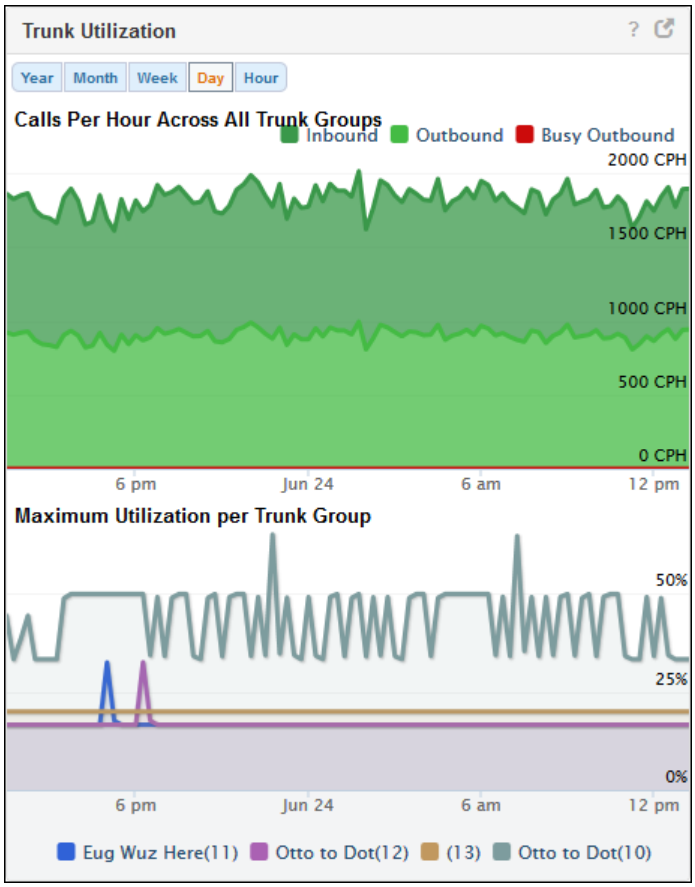
Available metrics are:

- Inbound, outbound and outbound busy call rates (calls per hour)
- Maximum number of trunks used (number)



MIVOICE BUSINESS TRUNK UTILIZATION PANEL

The **Trunk Utilization** panel for MiVoice Business shows the performance of all digital trunk groups in the MiVoice Business / 3300 ICP System. There are two areas in the **Trunk Utilization** panel: Call Rate and Trunk Group Utilization. Note that the MiVoice Business/3300 ICP trunk utilization data applies only to digital trunks. SIP trunk utilization is reported on a different panel. See "MiVoice Business SIP Trunk Utilization Panel" on page 244.



The trunk utilization metrics allow analysis of trunk capacity for actual traffic on the MiVoice Business/ 3300 ICP. High numbers of busy outbound call attempts indicate that the trunk group is too small for the offered traffic. Low utilization shows that there is excess trunk capacity.

CALL RATE MIVOICE BUSINESS TRUNKS

The **Call Rate** area shows the call rate for all trunk group calls in the system in 1-hour intervals (CPH). The area shows a stacked bar chart of:

- Inbound call rate (in dark green)
- Outbound call rate (in light green)
- Outbound busy call rate (in red)

Click the graphic legend labels (**Inbound**, **Outbound**, or **Busy Outbound**) to display or hide a set of data.

To convert to the number of call events per 15-minute interval, divide the hourly call rates by 4.

TRUNK GROUP UTILIZATION

The **Trunk Group Utilization** area shows trunk utilization per trunk group.

Utilization is defined as the maximum number of trunks in use per trunk group (high water mark), expressed as a percentage of the number of trunks in each trunk group.

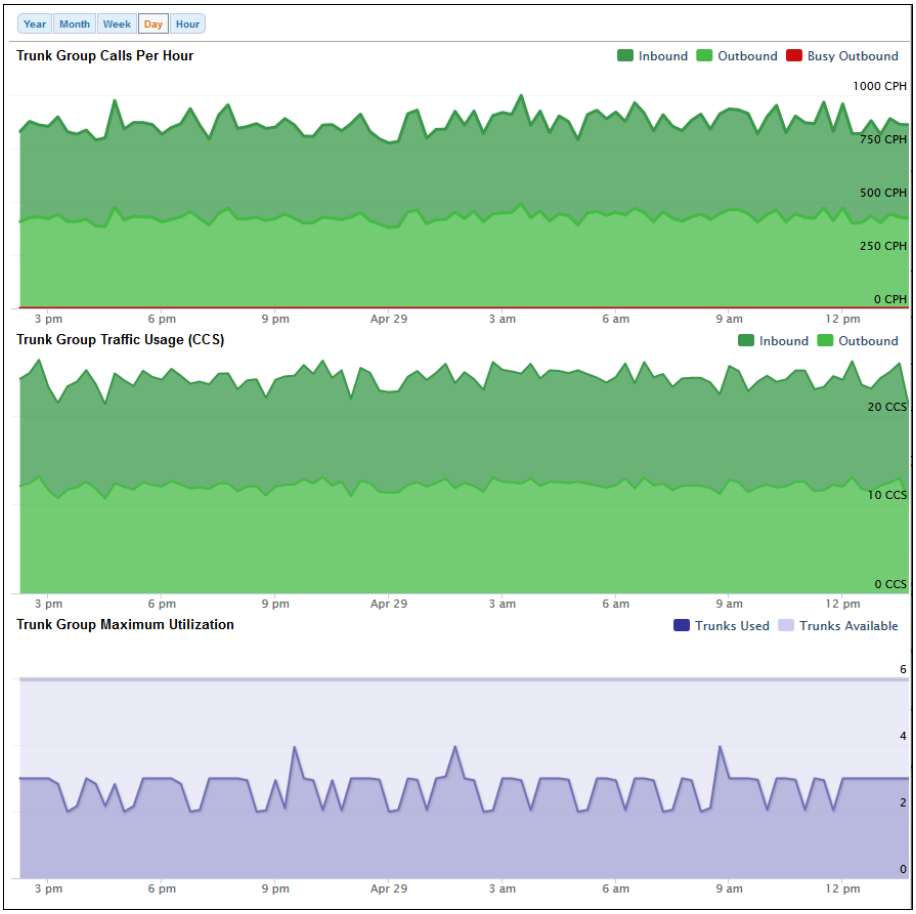
Trunk groups are identified by trunk group number and by trunk group label (if available).

INDIVIDUAL TRUNK GROUP METRICS

The expanded view provides more detailed, individual trunk group metrics. Traffic usage is expressed in CCS (hundred call seconds). Note that 1 Erlang = 36 CCS.

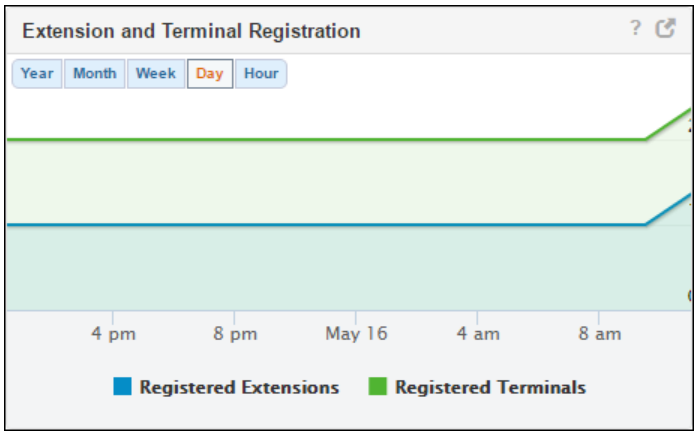
Available metrics are:

- Inbound, outbound and outbound busy call rates (calls per hour)
- Outbound and outbound traffic (CCS)
- Maximum number of trunks used (number)



MIVOICE MX-ONE EXTENSION AND TERMINAL REGISTRATION PANEL

Mitel Performance Analytics supports inventory monitoring for the extensions and terminals that are registered with a MiVoice MX-ONE.



Click the graphic legend labels (**Registered Extensions** or **Registered Terminals**) to display or hide a set of data.

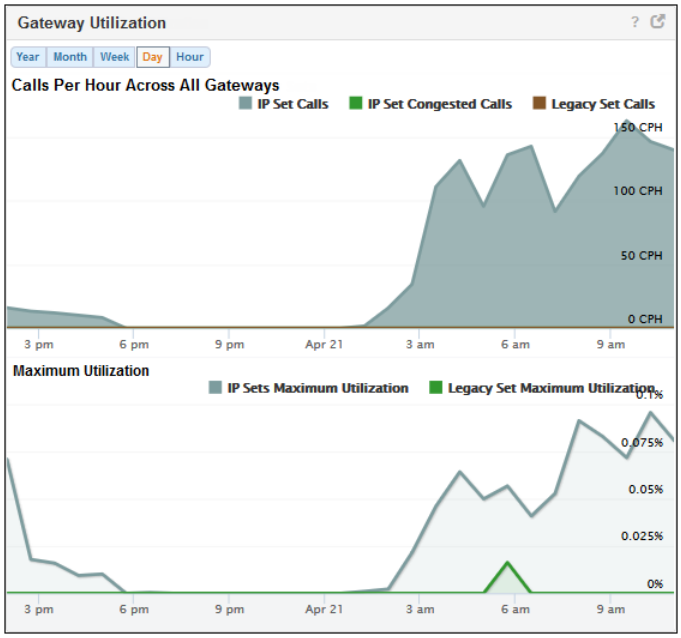
EXPANDED VIEW MX-ONE EXTENSION AND TERMINAL REGISTRATION

In its expanded view, the **Extension and Terminal Registration** panel displays the results of an **MiVoice MX-ONE Extensions** query. See "Inventory Queries" on page 79 for details.

MIVOICE MX-ONE GATEWAY UTILIZATION PANEL

The **Gateway Utilization** panel for MiVoice MX-ONE shows the performance of all configured IP (digitial) and legacy (analog) sets in the MiVoice MX-ONE. You can selectively display the data from either IP sets or legacy sets, or both.

There are two areas in the **Gateway Utilization** panel: Call per Hour Across All Gateways and Maximum Utilization.



CALL PER HOUR ACROSS ALL GATEWAYS

The **Call per Hour Across All Gateways** area shows the call rate for all sets in the system in 1-hour intervals (CPH). The area shows a stacked bar chart of:

- IP set call rate (in dark gray)
- IP set congested call rate (in dark green)
- Legacy set call rate (in brown)

Click the graphic legend labels (**IP Set Calls**, **IP Set Congested Calls**, or **Legacy Set Calls**) to display or hide a set of data.

To convert to the number of call events per 15-minute interval, divide the hourly call rates by 4.

MAXIMUM UTILIZATION

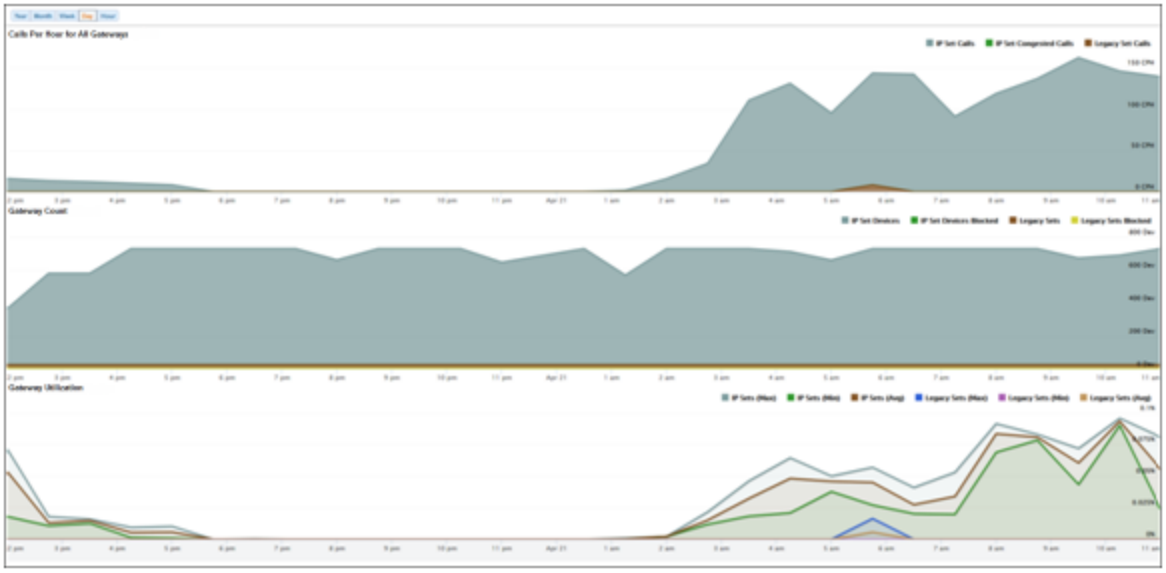
The **Maximum Utilization** area shows the maximum utilization for IP sets and legacy sets.

Utilization is defined as the number Erlangs divided by the number of sets in use.

DETAILED METRICS

The expanded view provides more detailed metrics:

- Call rate for all gateways (calls per hour)
- Gateways and blocked gateways (number)
- Maximum, minimum and average gateway utilization

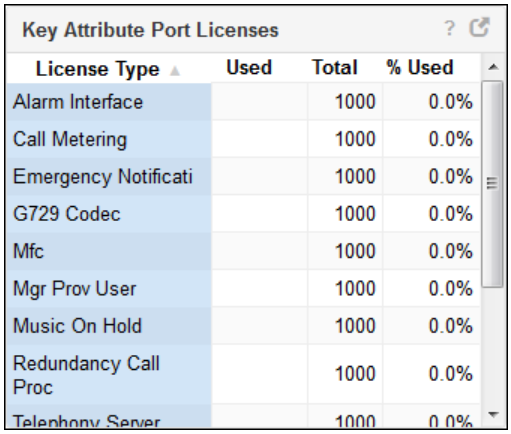


MIVOICE MX-ONE KEY ATTRIBUTE PORT LICENSES PANEL

The MiVoice MX-ONE **Key Attribute Port Licenses** panel displays a list of the different types of MiVoice MX-ONE port attribute licenses on the device along with how many are now in use.

License types are highlighted to indicate utilization levels.

The following is a typical panel.

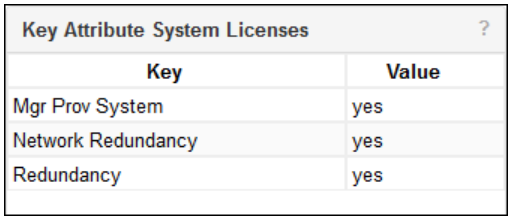


See also "Licenses Panel" on page 232.

MIVOICE MX-ONE KEY ATTRIBUTE SYSTEM LICENSES PANEL

The MiVoice MX-ONE **Key Attribute System Licenses** panel displays a list of the different types of MiVoice MX-ONE system attribute licenses found on the device and whether they are enabled or not.

The following is a typical panel.



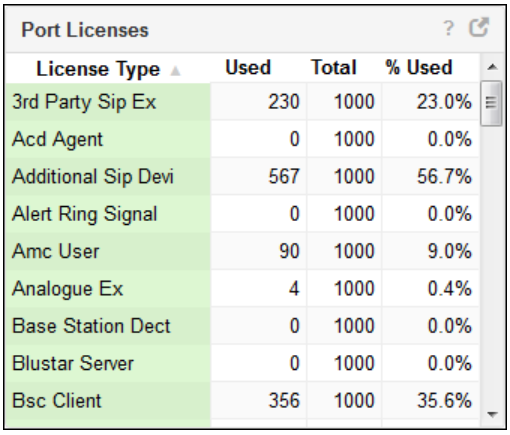
See also "Licenses Panel" on page 232.

MIVOICE MX-ONE PORT LICENSES PANEL

The MiVoice MX-ONE **Port Licenses** panel displays a list of the different types of MiVoice MX-ONE port licenses found on the device along with how many are currently in use.

License types are highlighted to indicate utilization levels.

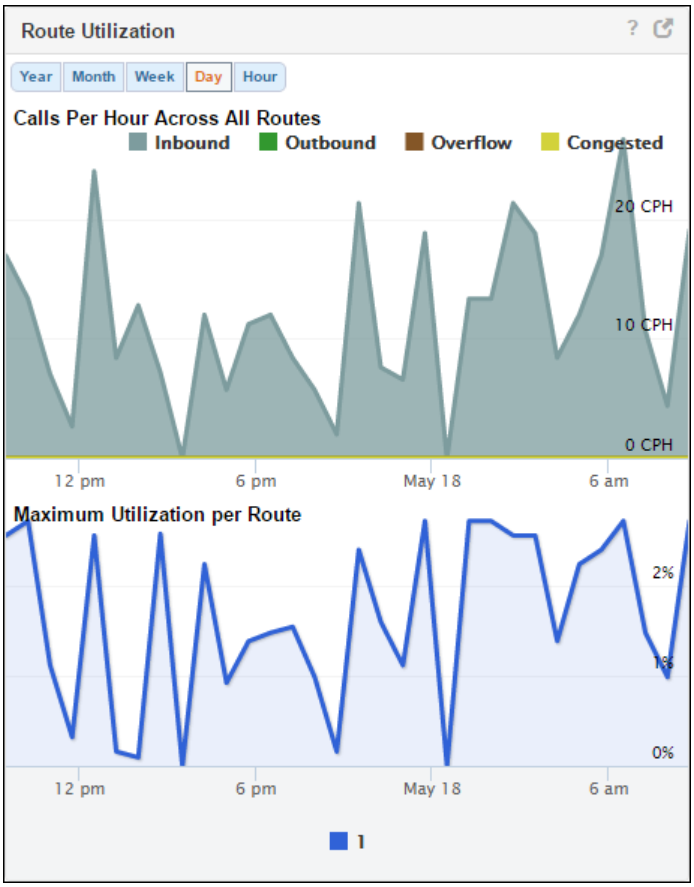
The following is a typical panel.



See also "Licenses Panel" on page 232.

MIVOICE MX-ONE ROUTE UTILIZATION PANEL

The **Route Utilization** panel for MiVoice MX-ONE shows the performance of all configured routes in the MiVoice MX-ONE. There are two areas in the **Route Utilization** panel: Call Rate and Maximum Utilization per Route.



The route utilization metrics allow analysis of route capacity for actual traffic on the MiVoice MX-ONE. High numbers of busy outbound call attempts indicate that the route is too small for the offered traffic. Low utilization shows that there is excess route capacity.

CALL RATE MX-ONE ROUTE UTILIZATION

The **Call Rate** area shows the call rate for all routes in the system in 1-hour intervals (CPH). The area shows a stacked bar chart of:

- Inbound call rate (in dark gray)
- Outbound call rate (in dark green)
- Overflow call rate (in brown)
- Congested call rate (in yellow)

Click the graphic legend labels (**Inbound**, **Outbound**, **Overflow**, or **Congested**) to display or hide a set of data.

To convert to the number of call events per 15-minute interval, divide the hourly call rates by 4.

MAXIMUM UTILIZATION PER ROUTE

The **Maximum Utilization per Route** area shows utilization per route.

Utilization is defined as the number Erlangs divided by the number of channels in use per route.

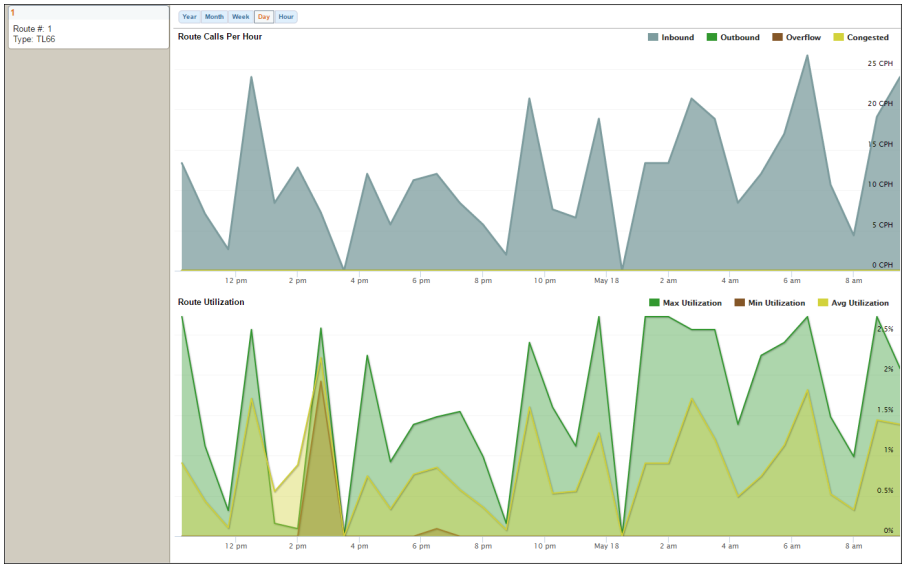
Routes are identified by their route ID.

INDIVIDUAL ROUTE METRICS

The expanded view provides more detailed, individual route metrics. Individual routes are listed to the left. Selecting a route displays its data on the right.

Available metrics are:

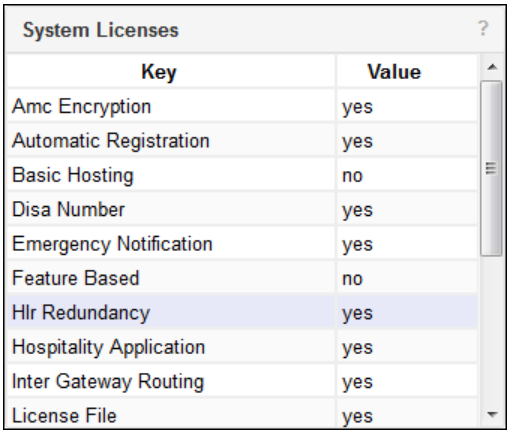
- Inbound, outbound, overflow, and congested call rates (calls per hour)
- Maximum, minimum, and average route utilization (number)



MIVOICE MX-ONE SYSTEM LICENSES PANEL

The MiVoice MX-ONE **System Licenses** panel displays a list of the different types of MiVoice MX-ONE system licenses found on the device and whether they are enabled or not.

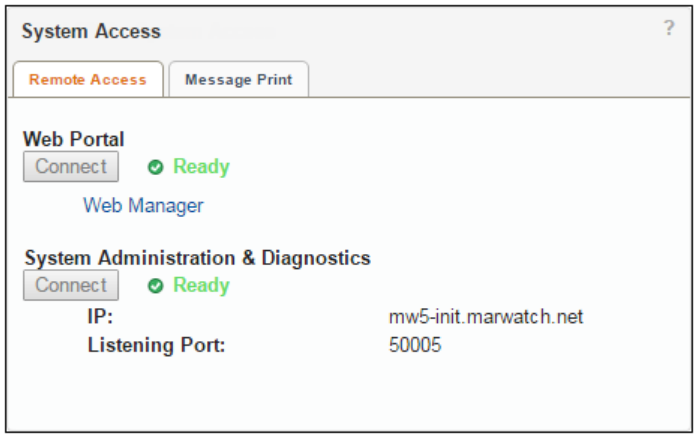
The following is a typical panel.



See also "Licenses Panel" on page 232.

MIVOICE OFFICE 250 SYSTEM ACCESS PANEL

The MiVoice Office 250 **System Access** panel provides access to various Mitel **System Administration and Diagnostics** functions.



REMOTE ACCESS TAB

Refer to "Connecting to a MiVoice Office 250" on page 189.

MESSAGE PRINT TAB

The **Message Print** tab provides access to the MiVoice Office 250 call processing **Message Print** logs.

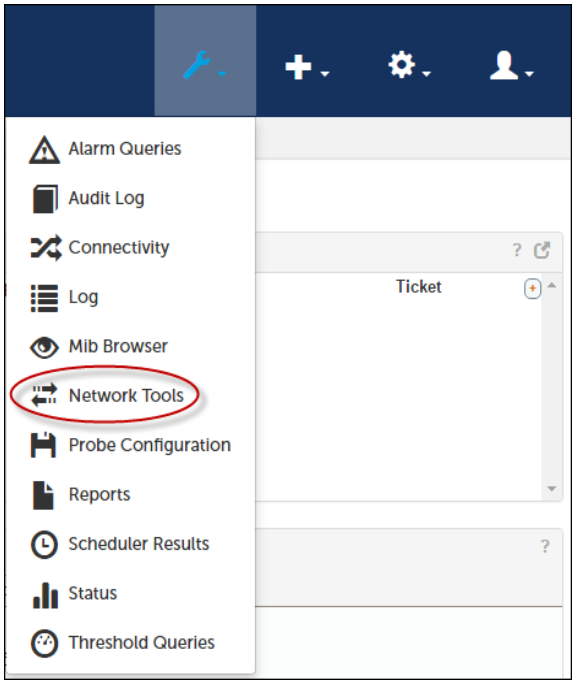
The tab shows the most recent log messages received by the system. To update the message list press the **Update** button.

For more information about message print messages, refer to the Mitel *Message Print Diagnostics Manual*.

NETWORK TOOLS PANEL

The **Network Tools** panel provides several tools for basic network troubleshooting. The tools are executed through Mitel Remote Access on the customer network where the Probe is installed.

When applicable, it is available under the **Tools** icon of the dashboard. The following is an example for a Probe:

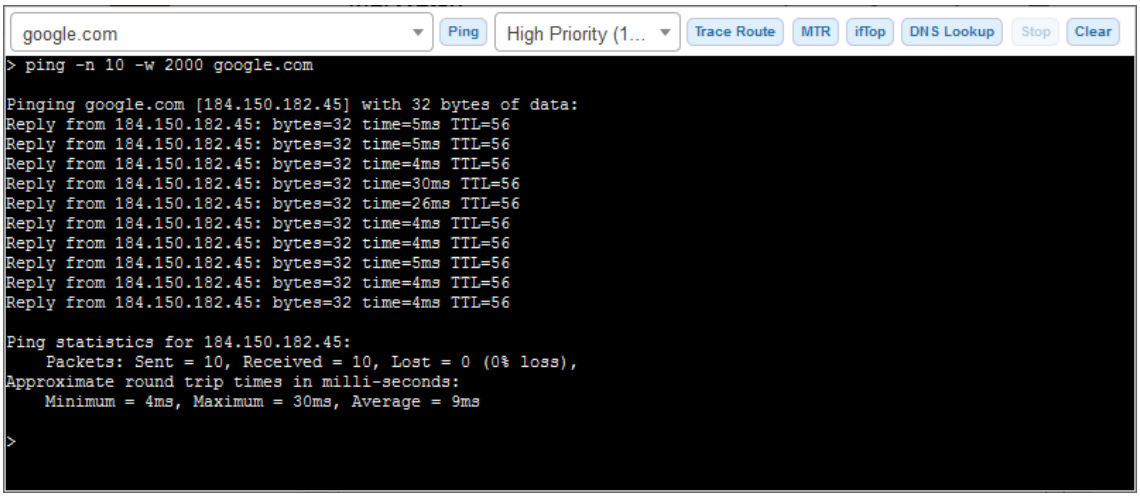


PING TOOL

This tool is used to check for the presence of an active connection on the customer network. To test if a host can be reached on the network, enter its hostname or IP address in the text field. Then, click the **Ping** button to get your result.

You can optionally specify the Type of Service (ToS) setting for the Ping packets to better mimic real VoIP traffic. The ToS setting ranges from 0 (Best Effort) to 184 (High Priority). The default is 0 (Best Effort).

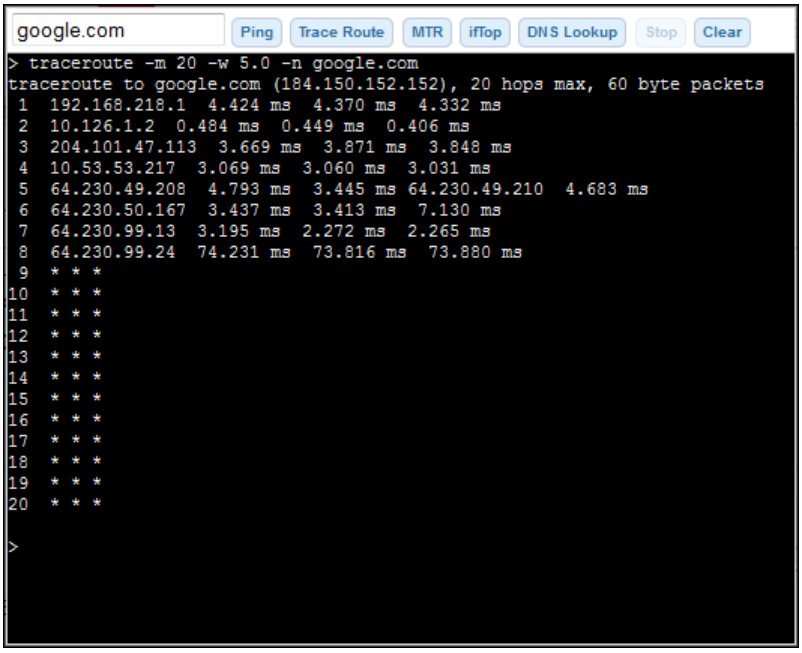
The Ping tool includes response time for insight into latency and network congestion.



TRACE ROUTE TOOL

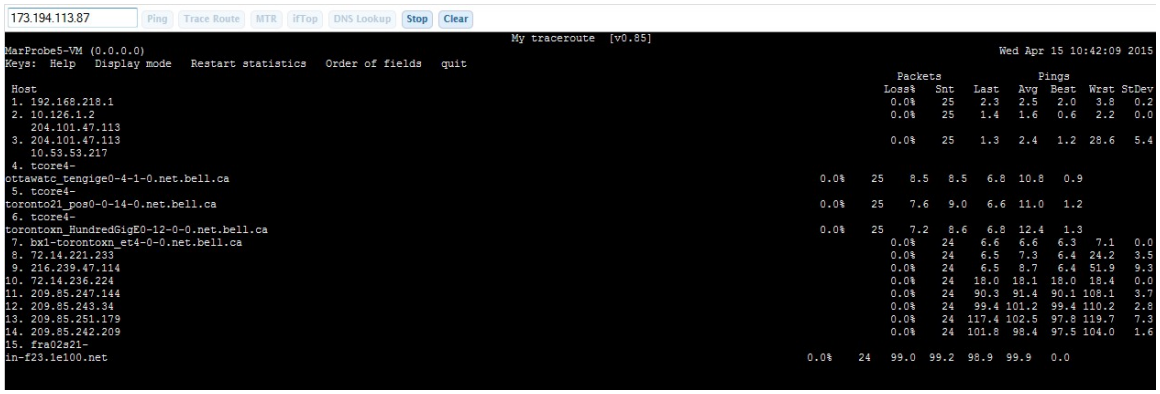
This tool includes response time for insight into latency and network congestion.

To determine the response time, type the destination hostname or IP address in the text field. Then, click the **Trace Route** button to plot the path taken to reach the host.



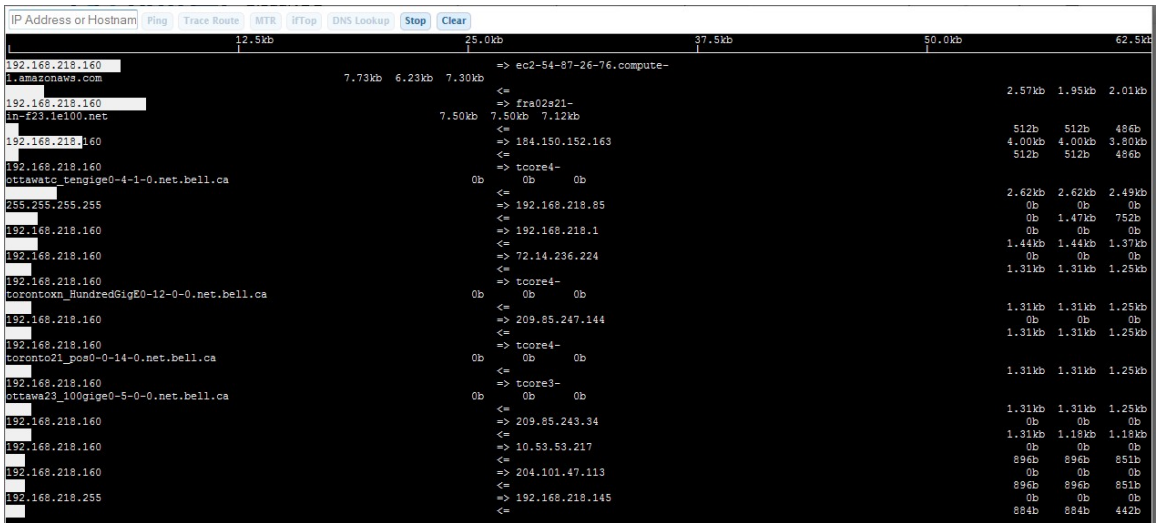
MTR TOOL

This tool combines Ping and Trace Route for greater insight into delays, location of packet loss, and average time from point to point.



IFTOP TOOL

The ifTop tool displays all traffic visible at the probe.

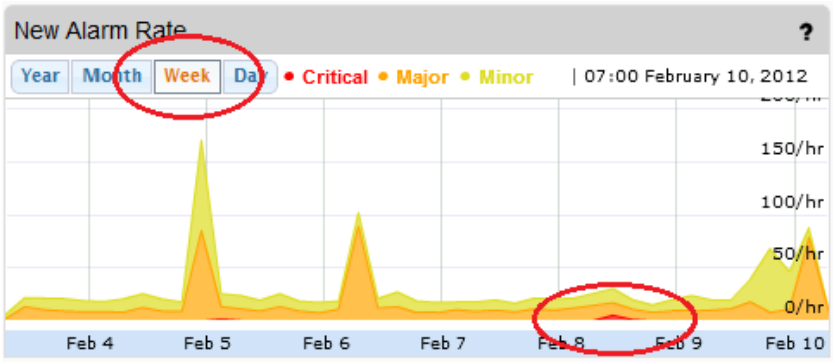


DNS LOOKUP TOOL

This tool is used to determine the IP address of a host on the network. Type the host name or the domain name in the text field. Then, click the **DNS Lookup** button to retrieve the IP address of the host or domain name.

NEW ALARM RATE PANEL

The **New Alarm Rate** panel shows the rate of alarm generation. Views may be selected by Hour, Day, Week, and Year. Note that if there are few alarms they may not be visible if the time scale is set to the yearly view. In the following example, the small blip of red at the bottom indicates that there are relatively few critical alarms during the indicated week view.



ON-DEMAND BACKUP PANEL

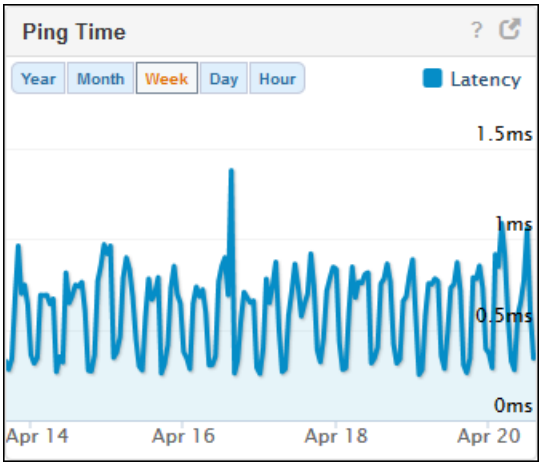
Use the **On Demand Backup** panel to do on-demand backups of MiVoice Business and MiVoice MX-ONE devices. See "On-Demand Backups" on page 168.

PING TIME PANEL

The **Ping Time** panel displays the round trip time for an ICMP ping packet sent from the Mitel Performance Analytics server or Probe to the monitored device. For an on-net device, this time is recorded from the Mitel Performance Analytics server to a remote device. For an off-net device, this time is recorded from the Probe because it monitors the device.

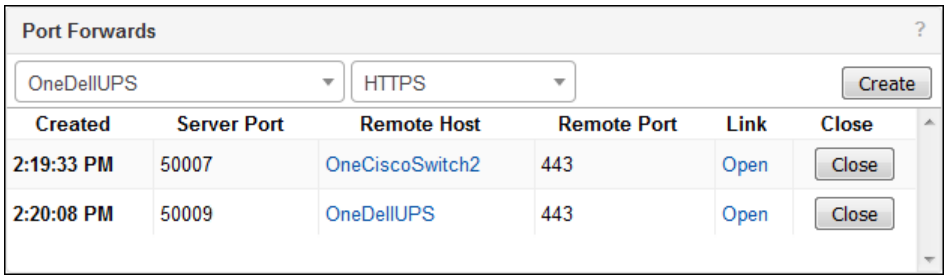
Ping time is displayed in milliseconds. Mitel Performance Analytics sends an ICMP ping to the monitored device at regular intervals, typically every five minute (3,600 seconds). Ping time is used to monitor:

- IP availability: the monitored device can be reached from the Mitel Performance Analytics server
- Device responsiveness: the monitored device must actively respond to each ping message
- Delay: ping time is an estimate of the round-trip delay from the Mitel Performance Analytics server to the monitored device



PORT FORWARDS PANEL

The **Port Forwards** panel allows you to create a remote access session to a device.



On the device dashboard of a Probe, the **Port Forwards** panel allows you to select the device or IP address to create a session to. From a Probe dashboard, you can reach any device monitored by the Probe.

On all other device dashboards, the panel allows you to pick the protocol to use. By default, you can create a session only to the particular device of that device dashboard.

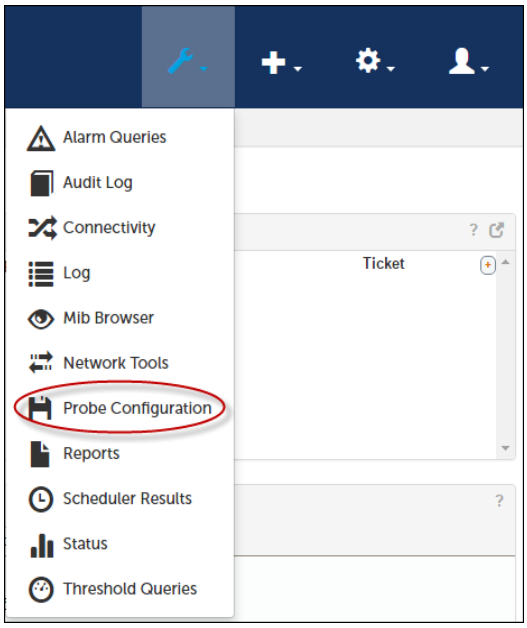
For details, see "Mitel Performance Analytics Remote Access" on page 182.

PROBE CONFIGURATION PANEL

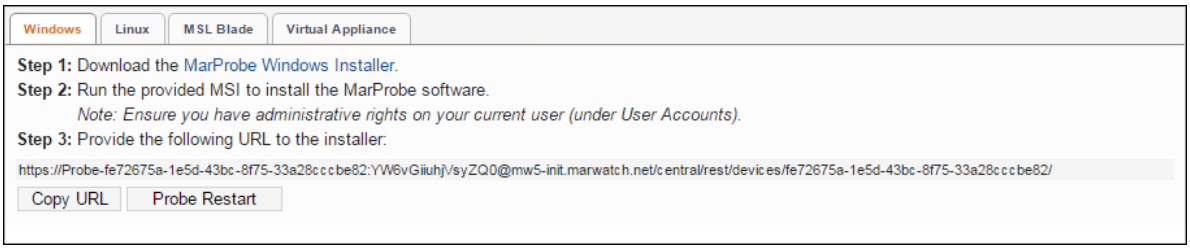
The **Probe Configuraton** panel provides software download and custom URLs for Probe installation. It also provides the **Probe Restart** button.

Note: The **Probe Restart** button is used under some troubleshooting circumstances. Do use this function without first consulting Technical Support.

To access this panel you need the **Probe Installer** privilege. The panel is available under the Tools icon of the Probe dashboard:



The following is a typical Probe Configuration panel:

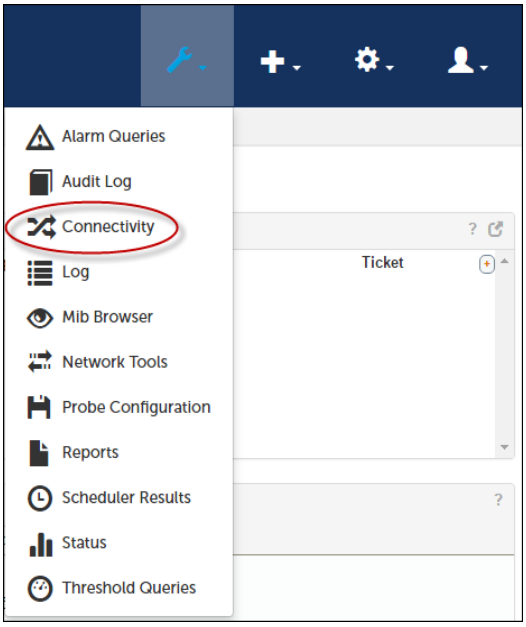


Each tab contains instructions to download the installation files for a Probe for that platform. For details, refer to "Probe Installation" on page 193.

PROBE CONNECTIVITY PANEL

The **Probe Connectivity** panel allows you to verify that the Probe can establish connections to the devices it is configured to monitor.

The **Probe Connectivity** panel is available under the **Tools** icon of the Probe dashboard:



For details, refer to "Probe Device Connectivity Check" on page 215.

PROBE JVM PANEL

This panel is only displayed if the **Collect JVM Stats** option has been selected on the Probe settings sheet and is intended for debugging purposes. The **Probe JVM** panel is accessed under the **Tools** icon on the Probe dashboard.

PROBE STATUS PANEL

This panel is only displayed if the **Collect Probe Status** option has been selected on the Probe settings sheet and is intended for debugging purposes. The **Probe Status** panel is accessed under the **Tools** icon on the Probe dashboard.

Component	Message
ProbeConfig	Added: 8 Removed: 0 Updated: 0 LoadFail: 0
CheckForUpgrade	Last Modified: Mon Mar 30 21:33:10 UTC 2015
CollectorManager	Collecting 9 devices with 42 Collectors.
BufferingRemoteRrdUpdater	Buffer size: 0/2048, max age: -1, enqueued: 2552, sent: 2544, dropped: 0, errors: 0, permanent errors: 8, internal errors: 0, HWM: 38, retry later:0
MCDMiXMLCollector	Collecting for 4 MCDs
MBGCollector	Collecting VQ for 1 MBGs
ThreadPoolSNMPTaskRunner	Running 61 tasks, 0.15 Tasks/Second
SNMPTrapReceiver	Listening on port 162
FixedThreadPoolPingTaskRunner	Pinging 8 devices with 5 threads.

PROCESSES PANEL

The **Processes** panel displays information on all of the software processes running on the monitored device, including:

- Process name
- CPU utilization
- Memory allocated to the process

The following is a typical **Processes** panel.

Processes

Process Name	CPU	Memory
System Idle Process	96.44%	24 KB
System	0.01%	208 KB
smss.exe	0.00%	488 KB
svchost.exe	1.31%	736.52 MB
csrss.exe	0.00%	4.59 MB
wininit.exe	0.00%	1.33 MB
winlogon.exe	0.00%	1.45 MB
services.exe	0.00%	5.93 MB
lsass.exe	0.04%	6.51 MB
lsm.exe	0.00%	3.18 MB

Note that there can be a very large number of processes running on a server. The **Processes** panel aggregates processes with the same name. For example, multiple instances of Apache would be shown as a single Apache process. You can sort the panel columns to identify heavy CPU and memory processes.

REMOTE ACCESS RPC PANEL

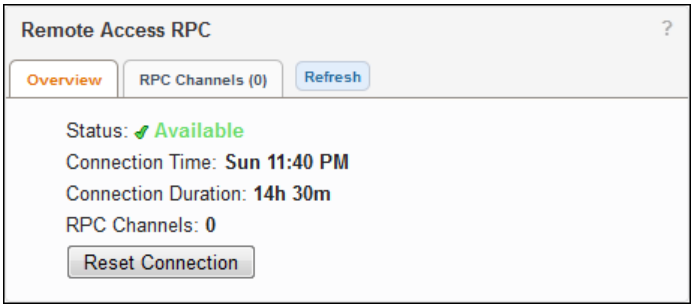
This panel is available for Probes only. It displays information about the Probe and Remote Procedure Call (RPC) Channels currently being used through remote access. This panel also allows the creation and testing of RPC Channels to devices on the network.

RPC OVERVIEW TAB

This tab shows the following information:

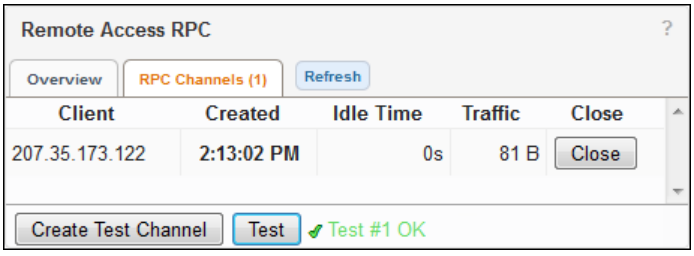
- **Status**: Displays whether remote access is available or unavailable
- **Connection Time**: Displays the day and time remote access was initiated
- **Connection Duration**: Display the up-time of the remote connection

- **RPC Channels**: Displays number of RPC channels open



RPC CHANNELS TAB

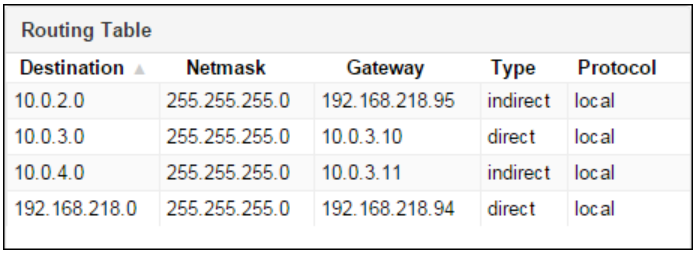
This tab shows how many Remote Procedure Call (RPC) channels are currently open. **Network Tools** use RPC channels to perform Trace Route, Ping, and DNS look ups.



You can also create a test channel to check if Remote Access functions correctly. This can be done by clicking the **Create Test Channel** button and then the **Test** button.

ROUTING TABLE PANEL

This panel is available for monitored Router devices. It displays the device's routing table.



SDS ERROR RATE PANEL

This panel is displays the rate at which System Data Synchronization (SDS) errors was detected by a MiVoice Business operating as part of a cluster.

SERVICE SETS PANEL

This panel shows a list of monitored services and their status. This panel is available for the following devices types: MX-ONE Application Server, MiVoice Call Recording, MiContact Center Business, Generic Server, Red Box Call Recorder, and InnLine Voice Mail.

Services are grouped into Service Sets and are presented in Service Set Views. Mitel Performance Analytics provides Service Sets for each supported device based on the expected services for that device type:

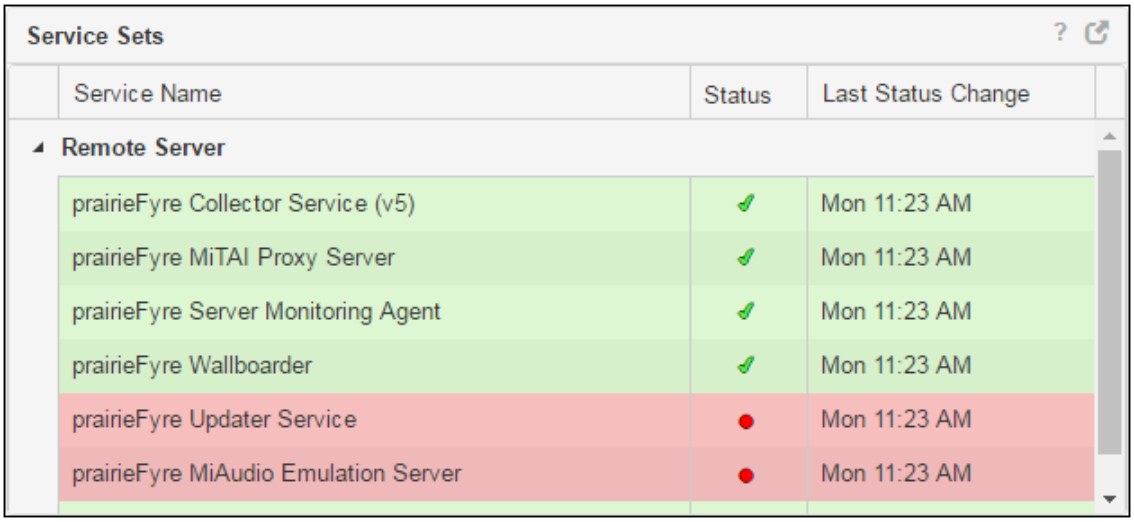
- Most device types have a single Service Set.
- The MX-ONE Application Server can have up to four Service Sets depending on your configuration choices: **ACS Media Server Services**, **CMG Services**, **inAttend Services**, and **MiCollab AM Services**. See "Configuring Mitel Performance Analytics for MX-ONE Application Server" on page 119.
- The MiContact Center Business can have up to four Service Sets depending on your configuration choices. See "Configuring Mitel Performance Analytics for Mitel Contact Center Business" on page 138.

Mitel Performance Analytics provides a default Service Set View for each supported device type except for the Generic Server. For the Generic Server, you must create an initial Service Set View based on its default **All Services** Service Set.

You can create, save and share your own custom Service Sets and Service Set Views by expanding the panel. Custom Service Set Views can contain only one Service Set.

SERVICE SETS SUMMARY VIEW

The following is a typical summary view showing of a MiContact Center Business showing the default **Remote Server** Service Set.

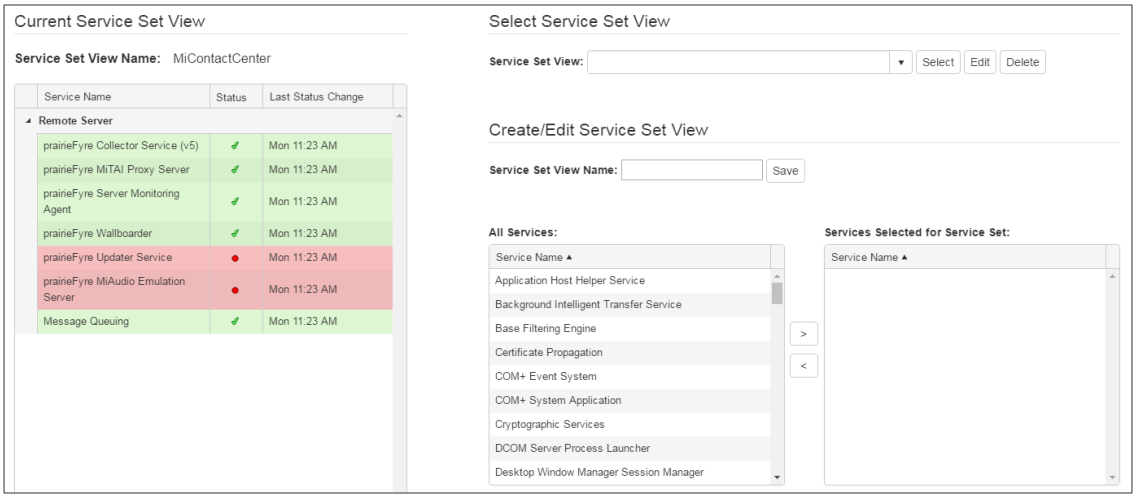


The **Service Sets** panel uses the following status icons:

ICON	COLOR	MEANING
	Red	The service is required and either is not installed or not operating.
	Blue	The service is not required. The service is not installed or not operating.
	Green	The service is functioning properly.

SERVICE SETS EXPANDED VIEW

To manage Service Set Views, click on the **Expand** icon on the top right hand corner of the panel.

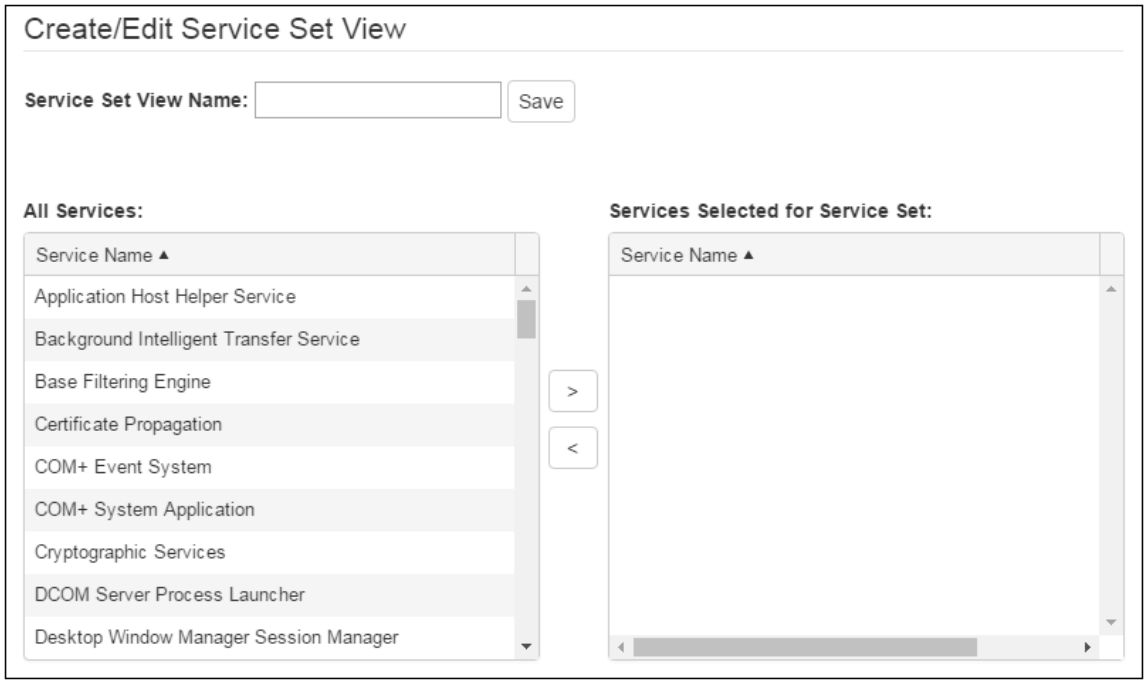


The left side of the expanded view shows the Service Set View and Service Set currently displayed in the panel summary view. The right side allows you to select and create Service Set Views.

A Service Set View is owned by the user who created it. Only that user can modify or delete it. Views are associated with the container where the owner logs in. Views are shared with anyone who can access that container or any subcontainer.

CREATING A CUSTOM SERVICE SET AND SERVICE SET VIEW

Use the **Create/Edit Service Set View** area to the right of the expanded panel.



Custom Service Set Views can contain only one Service Set.

Do the following steps:

1. Enter the name of the new Service Set View.
2. Select the services to include in the new Service Set from the left list. Use click, shift-click, and ctrl-shift-click as required.
3. Move the selected services to the right list.
4. Click Save.
   The **Service Set** panel displays the new Service Set View and the new Service Set.

CHANGING THE SERVICE SET VIEW IN USE

Use the **Select Service Set View** area in the top right of the expanded panel.

Do the following steps:

1. Choose a **Service Set View** from the dropdown list.
2. Click **Select**.
   The **Service Set** panel displays the new Service Set View.

EDITING A SERVICE SET VIEW

Use the **Select Service Set View** area in to top right of the expanded panel to select the Service Set View and the **Create/Edit Service Set View** area to modify it.

Only the owner of a Service Set View can edit it. You cannot edit the default Service Set Views. You can create your own Service Set View based on one of the default views.

Do the following steps:

1. Choose the **Service Set View** you want to modify from the dropdown list.
2. Click **Edit**.
   The bottom **Service Set** panel displays the Service Set of the selected Service Set View.
3. Modify the services in the Service Set as required. Use click, shift-click, and ctrl-shift-click as required to select the services. Move them from either list as required.
4. Click **Save**.
   The **Service Set** panel displays the newly modified Service Set View and Service Set.

DELETING A SERVICE SET VIEW IN USE

Use the **Select Service Set View** area in the top right of the expanded panel.

Only the owner of a Service Set View can delete it. You cannot delete default Service Set Views.

Do the following steps:

1. Choose the **Service Set View** from the dropdown list.

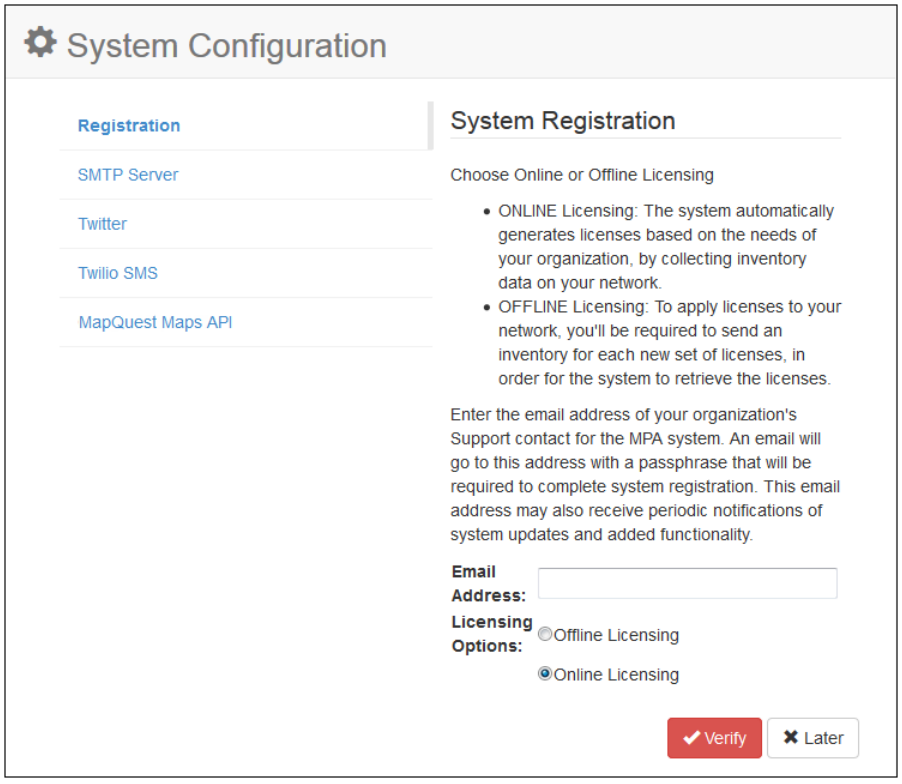
2. Click **Delete**.
3. When asked, confirm your intent.
   The Service Set View and associated Service Set are deleted.

SYSTEM CONFIGURATION PANEL

Use this panel to:

- Register your Mitel Performance Analytics system and enter a license ID for each customer to automate all tasks related to licensing
- Update or correct SMTP server settings used by Mitel Performance Analytics to:
  - Send email notification of alarms
  - Send forgotten password reset links by email
  - Deliver scheduled reports by email
- Configure a Twitter account to receive Twitter notification of alarms
- Configure a Twilio SMS account to receive SMS notifications of alarms
- Supply a MapQuest Consumer key to enable dashboard maps and map coordinate lookup from street addresses

Access to this panel is restricted to users with **System Admin** privileges.

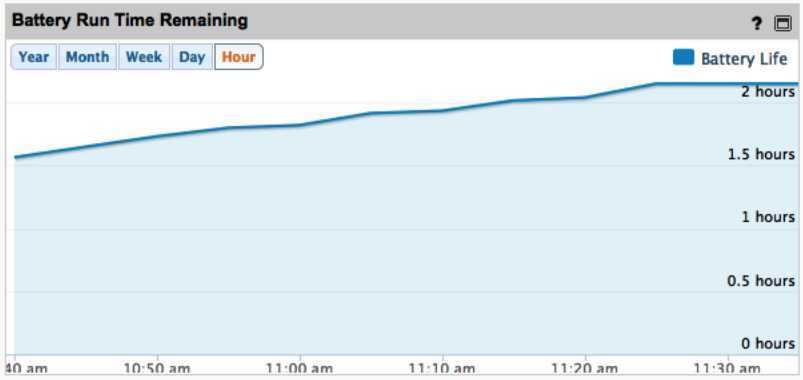


UNINTERRUPTIBLE POWER SUPPLY PANELS

The dashboard for UPS devices has a series of panels that provide current and historical information on alarms and performance of the UPS device. These panels are unique to UPS devices.

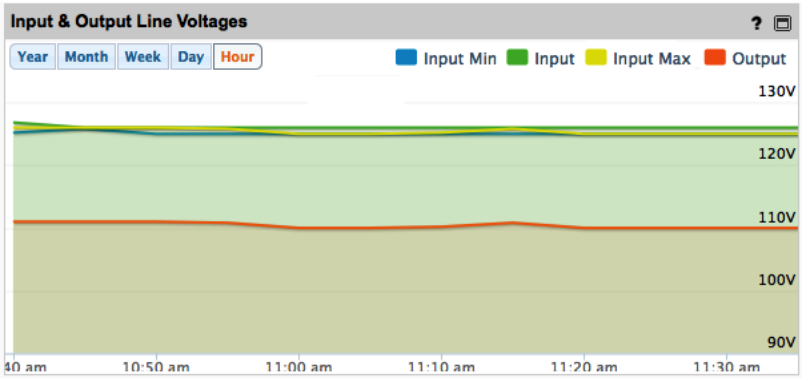
BATTERY RUN TIME REMAINING PANEL

This panel provides an estimate of the battery life of the UPS under current load conditions. In the previous example, the UPS is charging the battery and therefore the expected battery life under load is increasing.



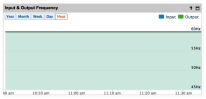
INPUT AND OUTPUT LINE VOLTAGE PANEL

This panel displays information on the voltage range at the UPS input and the UPS output voltage. The input voltage range covers a one minute period, sampled at five minute intervals.



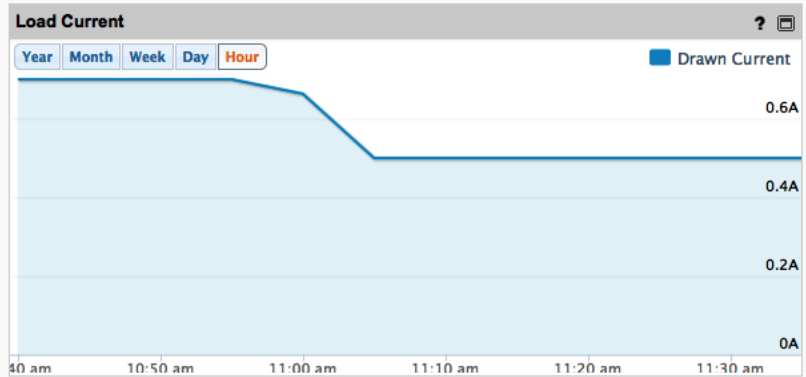
INPUT AND OUTPUT FREQUENCY PANEL

This panel shows the frequencies of the UPS input and output in Hz. If there is no input, the frequency is 0 Hz.



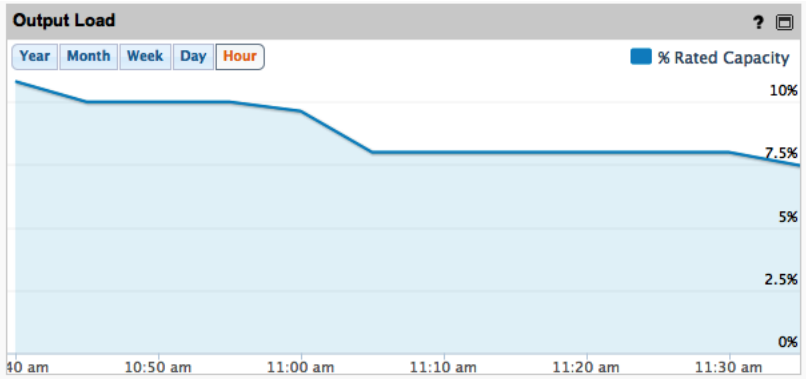
LOAD CURRENT PANEL

This panel shows the load current in Amps.



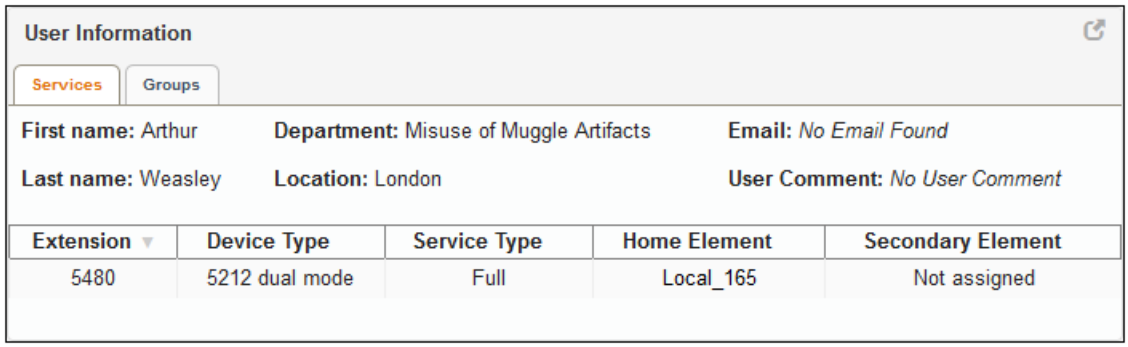
OUTPUT LOAD PANEL

This panel shows the UPS load as a percentage of rated capacity.



USER INFORMATION PANEL

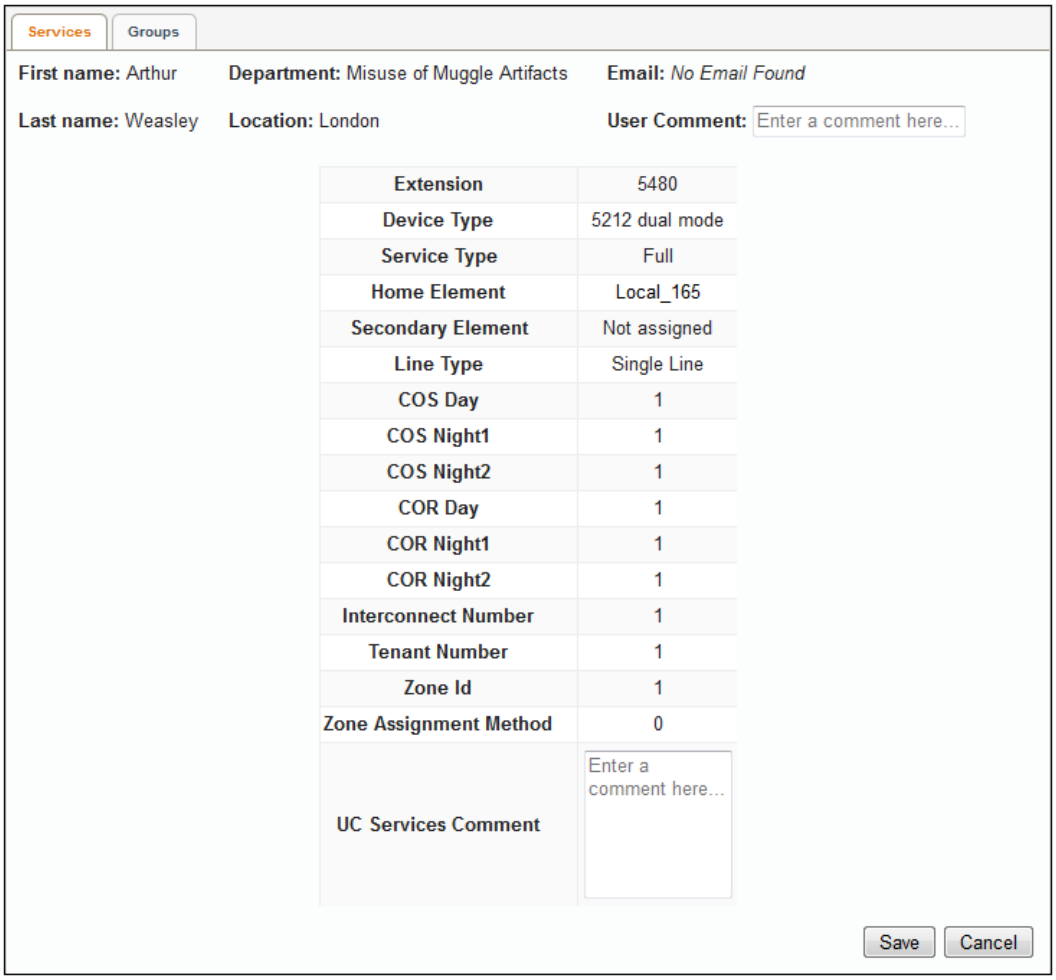
The **User Information** panel is displayed on IPT User dashboards. It provides a tabular summary of the services that the IPT user has, and the groups they belong. The following is an example.



Expand the panel to display additional details.

To enter a free-form comment on the IPT user or their UC services, do the following steps:

1. Expand the panel.
   By default, the **Services** tab is displayed. The following is an example.



2. From the **Services** tab, enter your comments in the provided fields.
3. Click **Save**.

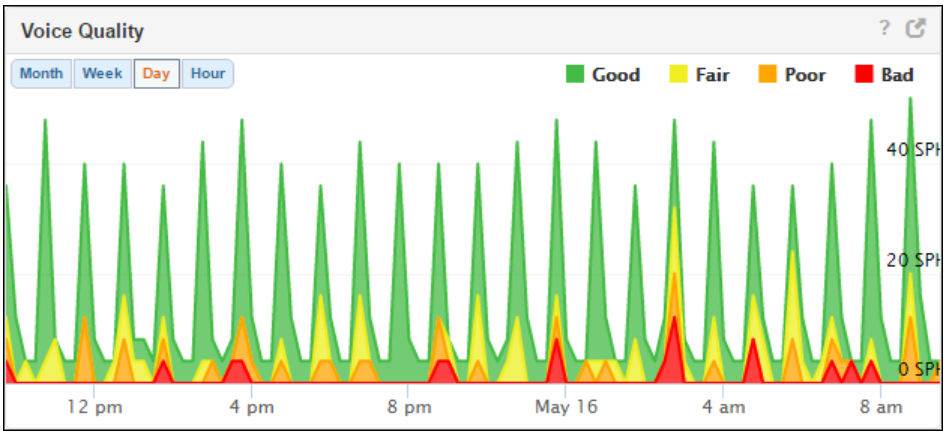
IPT user comments are visible on the **User Information** panel summary view and in the **MiVoice Business Users, Services & Sets** inventory query.

UC Services comments are visible on the **Services** tab of the expanded view and in the **MiVoice Business Users, Services & Sets** inventory query.

VOICE QUALITY AND SIP VOICE QUALITY PANELS

The **Voice Quality** panel and the **SIP Voice Quality** panel provide a graphic view of the quality of the Voice over IP calls made on the IP communications device being monitored.

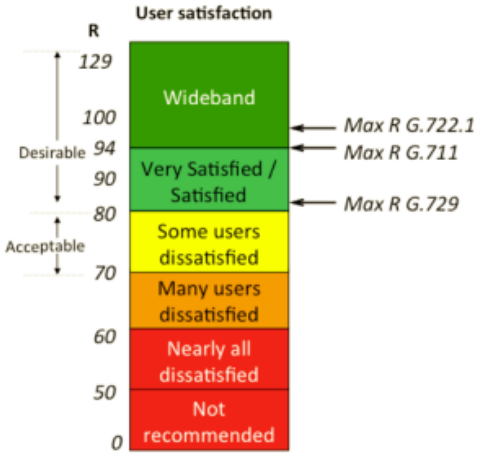
The **SIP Voice Quality** panel for a MiVoice Border Gateway has additional trunk data filter options.



Click on the graphic legend labels (**Good**, **Fair**, **Poor**, or **Bad**) to display or hide a set of data.

R VALUE

Mitel Performance Analytics uses the Extended E-model to estimate the received voice quality for VoIP calls. The E-model is based on ITU-T Recommendation G.107. The primary output of the E-model calculations is a scalar quality rating value known as the R value. The R scale ranges from 0 (bad) to a maximum of 129 (excellent). The range for R is 6.5 to 93.4 for narrowband codecs (G.729 and G.711) to a theoretical maximum of 129 for wideband codecs (G722.1).



DEFAULT VIEW VOICE QUALITY AND SIP VOICE QUALITY

The default view shows a recent time window with the number of sessions per hour, color coded as in the previous graphic to indicate R value for a call.

If the quality of a call varies over its duration, the color code is based on the worst R value measured during the call.

If there are multiple devices reporting voice quality performance to the dashboard, the **Voice Quality** panel and the **SIP Voice Quality** panel combine all of the voice quality information to show aggregate voice quality.

COLOR CODING FOR VOICE QUALITY AND SIP VOICE QUALITY

The voice quality information is color coded to enable rapid identification of trends. Mitel Performance Analytics uses the following thresholds.

		R VALUE	
COLOR	VOICE QUALITY	FROM	TO
Green	Good	80	93.2
Yellow	Adequate	70	80
Orange	Poor	60	70
Red	Bad	0	60

For good quality VoIP, the R value should be 80 or better. An R value less than 70 indicates poor audio quality and less than 60 is generally unusable.

EXPANDED VIEW VOICE QUALITY AND SIP VOICE QUALITY

The expanded view provides more detailed voice quality data. This view shows two graphs as follows:

The upper graph shows call rate by voice quality over time, color coded as in the main panel view.

The lower graph shows the range of R values for all calls in five-minute intervals with lines indicating worst, average and best R value for the five-minute interval.

The average R value is the time average of R value measurements for a call.

For MiVoice Business, Minet sets and for MiVoice Border Gateway R8 and earlier Minet sets, R values are reported every 100 seconds and at the end of a call.

For MiVoice Border Gateway R9 and later, R values are reported at 5-second intervals.

Voice Quality Call Filtering

The **Voice Quality** panel and the **SIP Voice Quality** panel provide a filtering capability to see VQ information only for calls from a particular IP subnet, calls to an IP subnet or calls made by an extension range.

- **DN:** Directory number such as 3204, or range such as 32__.
- **Source IP:** IP Address, or a subnet using CIDR notation.
- **Destination IP:** IP Address, or a subnet using CIDR notation.
- **R Value**: Minimum and maximum R values.

After filling out filter options click the search button. The graph changes to reflect only the calls that meet the filter criteria.

Call filtering applies only when the **Voice Quality** panel is displayed from a device dashboard; not a container dashboard.

Voice Quality Data Export

The export button generates a .csv file containing voice quality information about individual calls, based on the time range selected and selected filter options. The .csv file contains the directory number, start time, call length, R-Factor, IP addresses, codec, delay, jitter, and packet loss.

MIVOICE BORDER GATEWAY OPTIONS

When appearing on the dashboard of a MiVoice Border Gateway, the **SIP Voice Quality** panel has a **Teleworker** or **SIP Trunk** button allowing you to select the type of trunk to display Voice Quality data. If you select **SIP Trunk**, additional buttons let you show or hide selected data: **Near End**, **Far End**, **LAN**, or **WAN**. Individual trunks are identified at the bottom of the panel. Click on a trunk name to show or hide the data for that trunk.

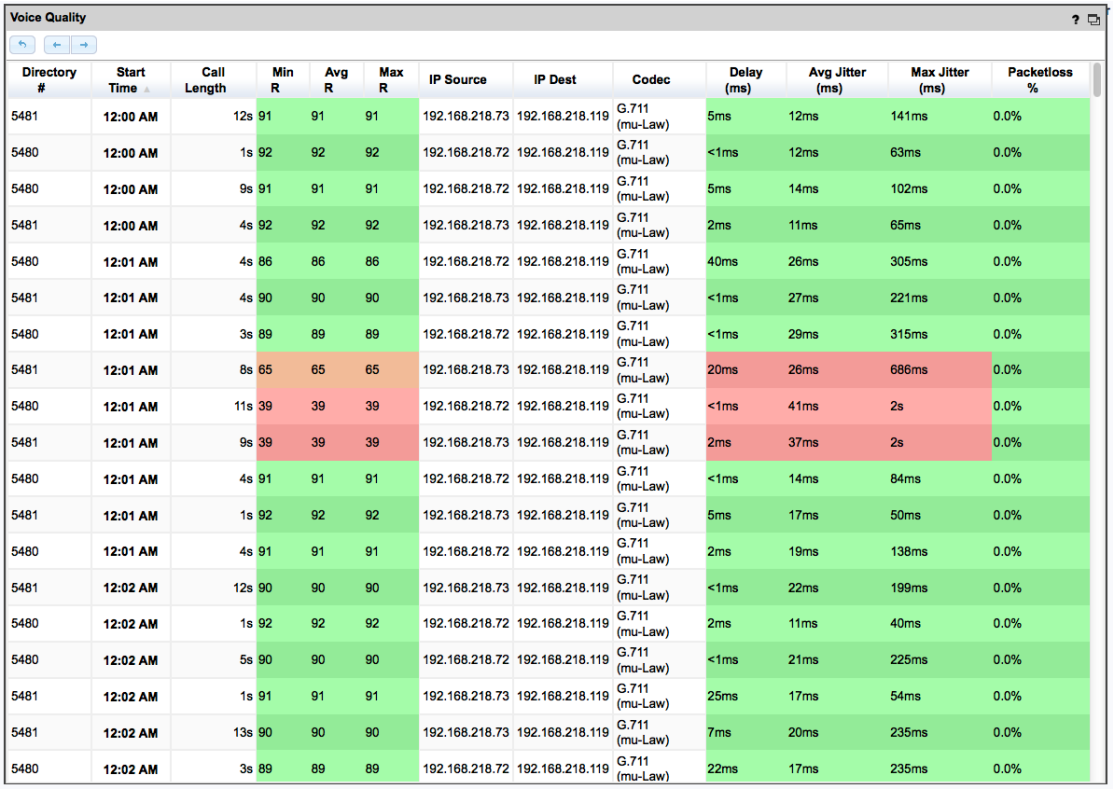
As well, the expanded view lists the available trunks. Selecting a single or multiple trunks displays the related data.

DETAILED VOICE QUALITY INFORMATION

To display detailed voice quality records, click on the R value range graph. The system displays details of all calls made in a one-hour interval around the time on which you clicked. This information may take some time to display if the number of calls is high.

The system shows the received voice quality by call with directory number, start time, call length, minimum, average and maximum R-Factor, IP addresses, codec, delay, jitter, and packet loss.

The system uses color highlighting to indicate good, poor and bad voice quality, and highlights likely contributing factors to abnormal voice quality.



Voice Quality

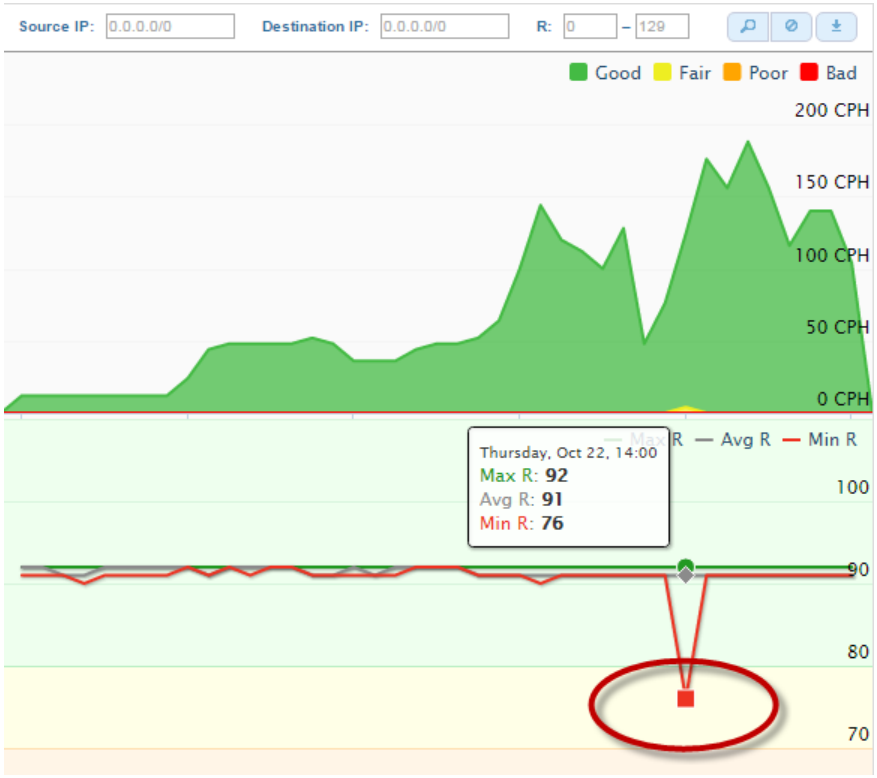
Directory #	Start Time	Call Length	Min R	Avg R	Max R	IP Source	IP Dest	Codec	Delay (ms)	Avg Jitter (ms)	Max Jitter (ms)	Packetloss %
5481	12:00 AM	12s	91	91	91	192.168.218.73	192.168.218.119	G.711 (mu-Law)	5ms	12ms	141ms	0.0%
5480	12:00 AM	1s	92	92	92	192.168.218.72	192.168.218.119	G.711 (mu-Law)	<1ms	12ms	63ms	0.0%
5480	12:00 AM	9s	91	91	91	192.168.218.72	192.168.218.119	G.711 (mu-Law)	5ms	14ms	102ms	0.0%
5481	12:00 AM	4s	92	92	92	192.168.218.73	192.168.218.119	G.711 (mu-Law)	2ms	11ms	65ms	0.0%
5480	12:01 AM	4s	86	86	86	192.168.218.72	192.168.218.119	G.711 (mu-Law)	40ms	26ms	305ms	0.0%
5481	12:01 AM	4s	90	90	90	192.168.218.73	192.168.218.119	G.711 (mu-Law)	<1ms	27ms	221ms	0.0%
5480	12:01 AM	3s	89	89	89	192.168.218.72	192.168.218.119	G.711 (mu-Law)	<1ms	29ms	315ms	0.0%
5481	12:01 AM	8s	65	65	65	192.168.218.73	192.168.218.119	G.711 (mu-Law)	20ms	26ms	686ms	0.0%
5480	12:01 AM	11s	39	39	39	192.168.218.72	192.168.218.119	G.711 (mu-Law)	<1ms	41ms	2s	0.0%
5481	12:01 AM	9s	39	39	39	192.168.218.73	192.168.218.119	G.711 (mu-Law)	2ms	37ms	2s	0.0%
5480	12:01 AM	4s	91	91	91	192.168.218.72	192.168.218.119	G.711 (mu-Law)	<1ms	14ms	84ms	0.0%
5481	12:01 AM	1s	92	92	92	192.168.218.73	192.168.218.119	G.711 (mu-Law)	5ms	17ms	50ms	0.0%
5480	12:01 AM	4s	91	91	91	192.168.218.72	192.168.218.119	G.711 (mu-Law)	2ms	19ms	138ms	0.0%
5481	12:02 AM	12s	90	90	90	192.168.218.73	192.168.218.119	G.711 (mu-Law)	<1ms	22ms	199ms	0.0%
5480	12:02 AM	1s	92	92	92	192.168.218.72	192.168.218.119	G.711 (mu-Law)	2ms	11ms	40ms	0.0%
5480	12:02 AM	5s	90	90	90	192.168.218.72	192.168.218.119	G.711 (mu-Law)	<1ms	21ms	225ms	0.0%
5481	12:02 AM	1s	91	91	91	192.168.218.73	192.168.218.119	G.711 (mu-Law)	25ms	17ms	54ms	0.0%
5481	12:02 AM	13s	90	90	90	192.168.218.73	192.168.218.119	G.711 (mu-Law)	7ms	20ms	235ms	0.0%
5480	12:02 AM	3s	89	89	89	192.168.218.72	192.168.218.119	G.711 (mu-Law)	22ms	17ms	235ms	0.0%

TROUBLESHOOTING VOICE QUALITY ISSUES

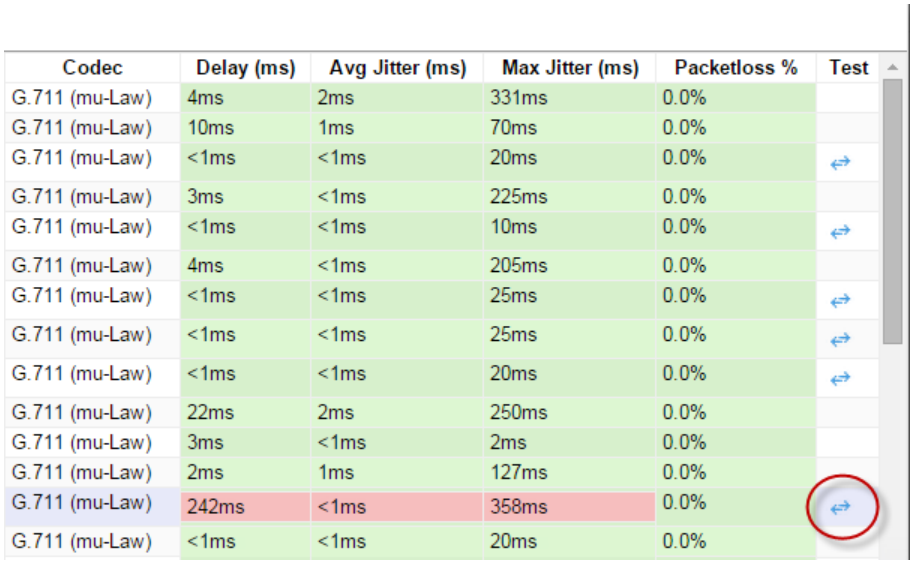
A Mitel Performance Analytics user with Remote Access privileges can run Trace Route from an IP set on a MiVoice Business system. This helps administrators determine possible voice quality issues. When the test is run, Trace Route executes using the source and destination IP addresses of a specific call. The Trace Route packets are tagged and marked the same as RTP packets and are sent on the phone's VLAN.

To run Trace Route for a specific IP call, do the following steps:

1. From a MiVoice Business or MiVoice Border Gateway dashboard, access the **Voice Quality** panel. Click on the areas of bad voice quality. The following is an example.



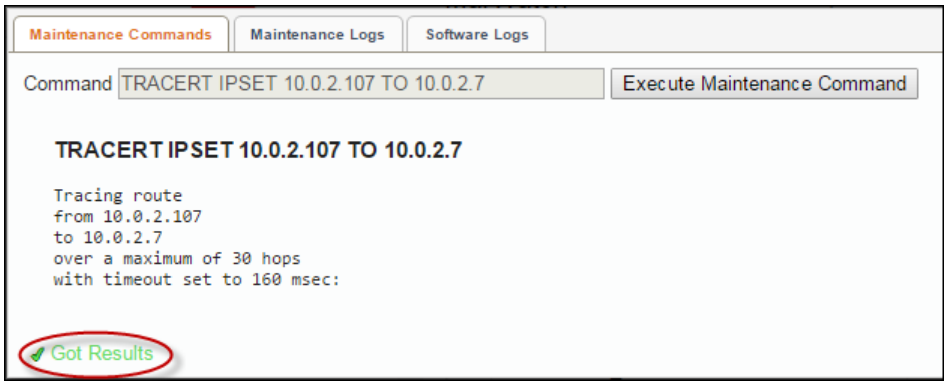
The expanded view is displayed.



Codec	Delay (ms)	Avg Jitter (ms)	Max Jitter (ms)	Packetloss %	Test
G.711 (mu-Law)	4ms	2ms	331ms	0.0%	
G.711 (mu-Law)	10ms	1ms	70ms	0.0%	
G.711 (mu-Law)	<1ms	<1ms	20ms	0.0%	⇄
G.711 (mu-Law)	3ms	<1ms	225ms	0.0%	
G.711 (mu-Law)	<1ms	<1ms	10ms	0.0%	⇄
G.711 (mu-Law)	4ms	<1ms	205ms	0.0%	
G.711 (mu-Law)	<1ms	<1ms	25ms	0.0%	⇄
G.711 (mu-Law)	<1ms	<1ms	25ms	0.0%	⇄
G.711 (mu-Law)	<1ms	<1ms	20ms	0.0%	⇄
G.711 (mu-Law)	22ms	2ms	250ms	0.0%	
G.711 (mu-Law)	3ms	<1ms	2ms	0.0%	
G.711 (mu-Law)	2ms	1ms	127ms	0.0%	
G.711 (mu-Law)	242ms	<1ms	358ms	0.0%	⇄
G.711 (mu-Law)	<1ms	<1ms	20ms	0.0%	

2. For a call with bad voice quality, click the **Test** icon in the **Test** column.
   The **Test** column appears only if you have Remote Access privileges. The **Test** icon appears only for calls from a MiVoice Business call server.

   Clicking the **Test** icon starts the test and displays the results.



The test status is displayed in the lower left corner of the panel.

To run the test for a different set of IP addresses, update arguments in the **Command** field and click the **Execute Maintenance Command** button. Mitel Performance Analytics allows you to update the command arguments, but not the command itself.

VOICE QUALITY FOR VOICE OVER IP TECHNICAL BACKGROUND

Voice quality for Voice over IP is mainly determined by IP network quality and codec.

Mitel Performance Analytics calculates an R value voice quality rating using the ITU-T wideband E-Model (see ITU-T G.107, G.107.1, and G.113). The R value is based on measurements of the IP network performance, as follows:

- Total Receive Delay = Codec Delay + Network Delay + Jitter Buffer Delay
- Probability of Packet Loss
- Burst Ratio
- Codec Type

The following tables show how R value is affected by codec type, receive delay, and packet loss.

G.711 is the standard 64 Kbps codec. G.729 is more bandwidth efficient, 8 Kbps, and more tolerant of packet loss. G.722.1 is a wideband audio codec, 32 Kbps and has a high tolerance for packet loss.

G.711 **R value**

	Delay ms	0	50	75	100	125	150	175	200	225	250	275	300
Packet Loss	0.00%	93	93	93	93	93	93	92	90	87	84	81	78
	0.25%	88	88	88	88	88	88	87	85	82	79	76	73
	0.50%	83	83	83	83	83	83	82	80	77	74	71	69
	0.75%	79	79	79	79	79	79	78	76	73	70	67	64
	1.00%	75	75	75	75	75	75	74	72	69	66	63	61
	1.25%	72	72	72	72	72	72	71	69	66	63	60	57
	1.50%	69	69	69	69	69	69	68	66	63	60	57	54
	1.75%	66	66	66	66	66	66	65	63	60	57	54	51
	2.00%	63	63	63	63	63	63	62	60	57	54	51	48
	2.25%	61	61	61	61	61	60	60	58	55	52	49	46
	2.50%	58	58	58	58	58	58	57	55	52	49	46	44
	2.75%	56	56	56	56	56	56	55	53	50	47	44	41
	3.00%	54	54	54	54	54	54	53	51	48	45	42	39

G.729 — **R value**

Packet Loss	Delay ms 0	50	75	100	125	150	175	200	225	250	275	300
0.00%	83	83	83	83	83	83	82	80	77	74	71	68
0.25%	82	82	82	82	82	82	81	79	76	73	70	67
0.50%	81	81	81	81	81	81	80	78	75	72	69	66
0.75%	80	80	80	80	80	80	79	77	74	71	68	65
1.00%	79	79	79	79	79	79	78	76	73	70	67	64
1.25%	78	78	78	78	78	78	77	75	72	69	66	63
1.50%	77	77	77	77	77	77	76	74	71	68	65	62
1.75%	76	76	76	76	76	76	75	73	70	67	64	61
2.00%	75	75	75	75	75	75	74	72	69	66	63	60
2.25%	74	74	74	74	74	74	73	71	68	65	62	59
2.50%	73	73	73	73	73	73	72	70	68	64	61	59
2.75%	73	73	73	73	72	72	71	69	67	64	61	58
3.00%	72	72	72	72	72	71	71	69	66	63	60	57

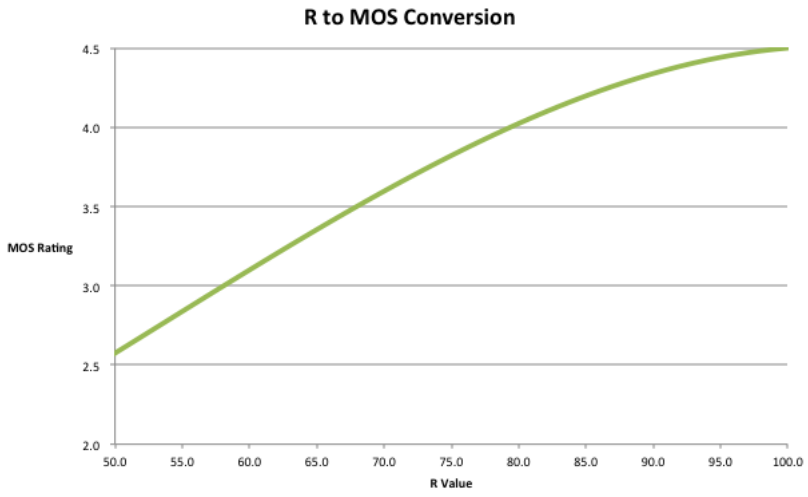
G.722.1 — **R value**

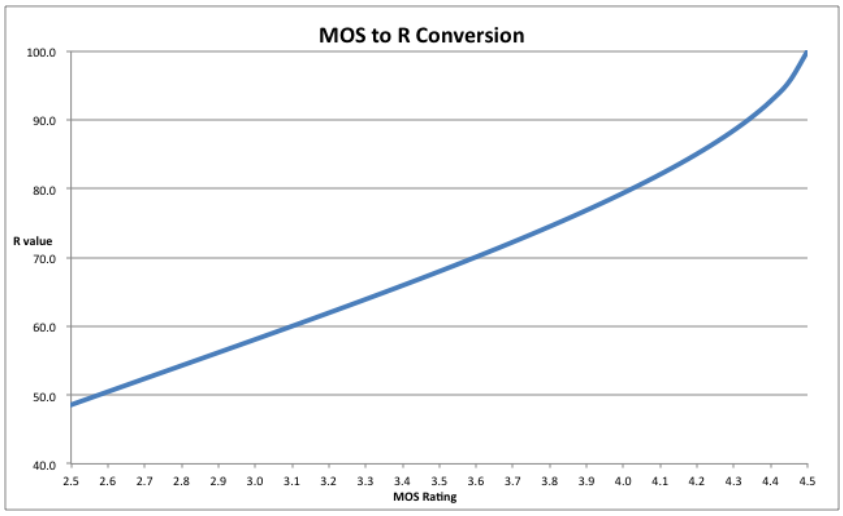
Packet Loss	Delay ms 0	50	75	100	125	150	175	200	225	250	275	300
0.00%	97	97	96	96	96	96	95	93	90	87	84	81
0.25%	94	94	94	93	93	93	92	90	87	84	81	78
0.50%	92	91	91	91	91	90	89	87	84	81	78	75
0.75%	89	89	88	88	88	88	87	85	82	79	76	73
1.00%	87	86	86	86	86	86	85	83	80	76	73	70
1.25%	85	84	84	84	84	84	83	80	77	74	71	68
1.50%	83	82	82	82	82	81	80	78	75	72	69	66
1.75%	81	80	80	80	80	80	79	76	74	70	67	64
2.00%	79	78	78	78	78	78	77	75	72	69	65	63
2.25%	77	77	77	76	76	76	75	73	70	67	64	61
2.50%	76	75	75	75	75	74	73	71	68	65	62	59
2.75%	74	74	73	73	73	73	72	70	67	64	61	58
3.00%	73	72	72	72	72	71	70	68	65	62	59	56

R Value and MOS Rating

Mean Opinion Score (MOS) rating can also be used to express perceived audio quality in telephony, however with the advent of wideband codecs, it is not generally possible to compare performance for both narrowband and wideband codecs using MOS Ratings.

For your information, the following graphs provide MOS rating conversion for common ranges of R values, for narrowband codecs only.





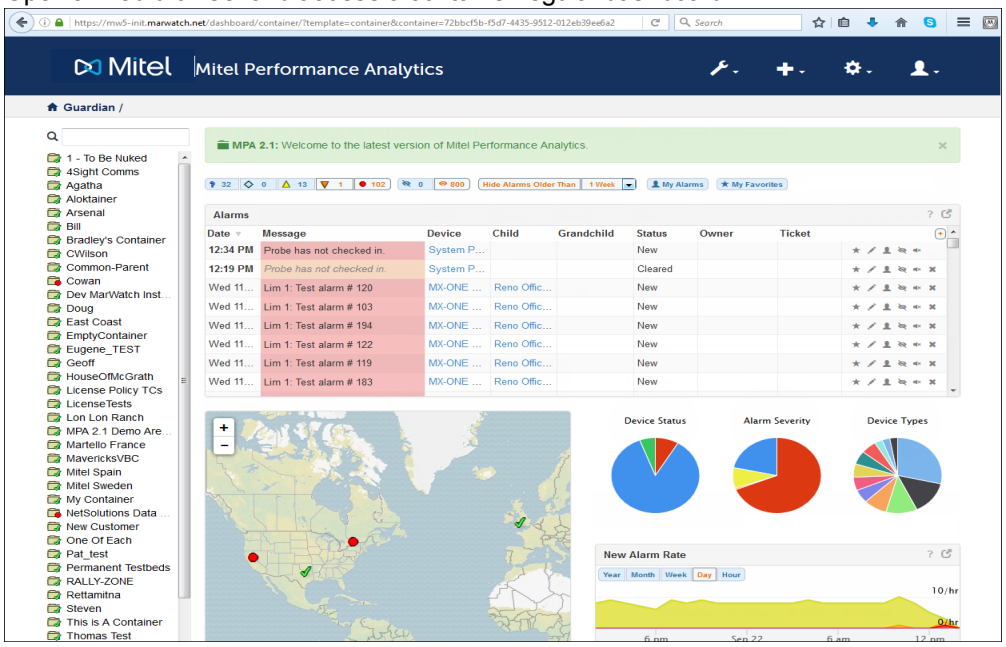
WIDESCREEN AND PROBLEM FINDER DASHBOARDS

A widescreen dashboard and a Problem Finder dashboard are available for use in a Network Operations Center (NOC) or data center. They provide an “at-a-glance” view of the map with filtered alarms for rapid detection and response. The Problem Finder dashboard is similar to the widescreen dashboard but has additional panels such as the **New Alarm Rate** panel and the **Voice Quality** panel.

Both the widescreen dashboard and the Problem Finder dashboard are read-only. You cannot perform configuration changes from them. For both dashboards, you can remain logged in for up to a year.

To access the widescreen dashboard or the Problem Finder dashboard:

1. Open a Web browser and access a container regular dashboard.



2. Note the expanded URL in the browser URL field. In the previous example, the expanded URL is:

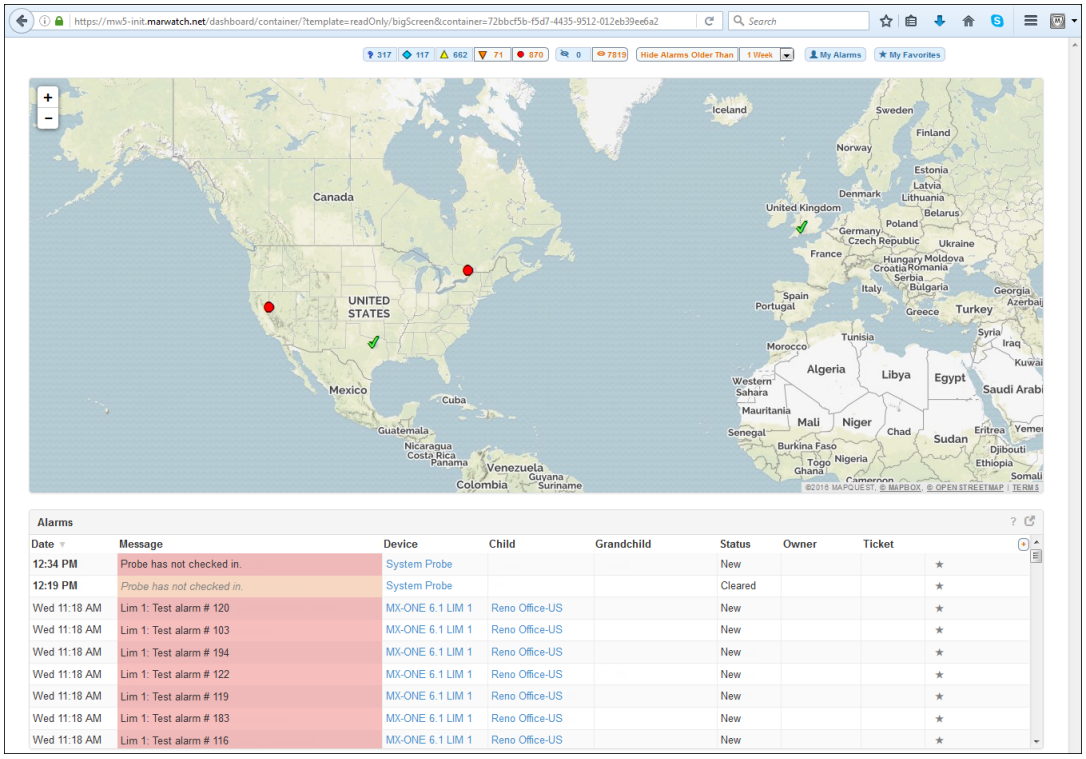
https://mw5-init.marwatch.net/dashboard/container/**?template=container**&container=72bbcf5b-f5d7-4435-9512-012eb39ee6a2

3. To access the widescreen dashboard, change the syntax of the expanded URL to use **?template=readOnly/bigScreen** instead of **?template=container**. For the URL from Step 2, the updated syntax is:

https://mw5-init.marwatch.net/dashboard/container/**?template=readOnly/bigScreen**&container=72bbcf5b-f5d7-4435-9512-012eb39ee6a2

In the previous example, only the highlighted section is different than the original URL in Step 2.

The widescreen dashboard is displayed.



To access the Problem Finder dashboard, change the syntax of the expanded URL to use **?template= readOnly/problemFinder** instead of **?template=container**. For the URL from Step 2, the updated syntax is:

https://mw5-init.marwatch.net/dashboard/container/**?template=readOnly/problemFinder**&container=72bbcf5b-f5d7-4435-9512-012eb39ee6a2

In the previous example, only the highlighted section is different than the original URL in Step 2.

The Problem Finder dashboard is displayed.

When you first access Mitel Performance Analytics, you see the dashboard of the top-level or root container. The dashboard URL may omit some elements required for widescreen or Problem Finder display. For example, the URL may only be:

https://lyta.marwatch.net/dashboard/container/

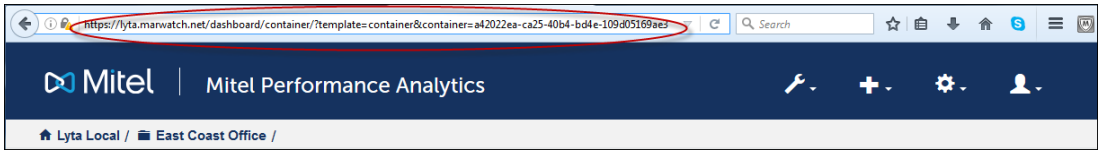
If you want to display the root container dashboard in widescreen or Problem Finder format, you must extend the URL for the root container to show all the required elements.

To display a root container in widescreen or Problem Finder format:

1. Access Mitel Performance Analytics.
   The URL of the root container omits some elements; for example:

   https://lyta.marwatch.net/dashboard/container/
2. Navigate to any subcontainer.
   The dashboard URL is populated with additional elements; for example:

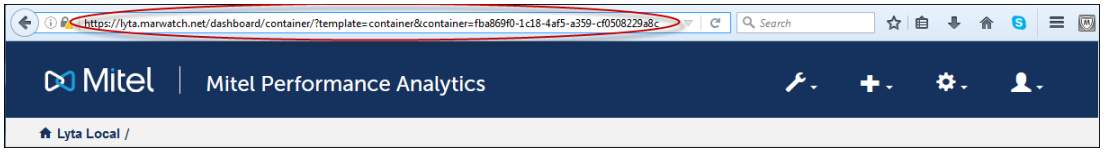
https://lyta.marwatch.net/dashboard/container/?template=container&container=a42022ea-ca25-40b4-bd4e-109d05169ae3



3. Return to the root container by selecting it from the breadcrumps at the top of the dashboard.

4. The dashboard URL is populated with the root container URL with all required elements; for example:

https://lyta.marwatch.net/dashboard/container/**?template=container**&container=fba869f0-1c18-4af5-a359-cf0508229a8c



5. Update the URL to use **?template=readOnly/bigScreen** or **?template=readOnly/problemFinder** as needed and as described previously.
   For example, to display the widescreen dashboard, change the URL from Step 4 to:

https://lyta.marwatch.net/dashboard/container/
?template=readOnly/bigScreen&container=fba869f0-1c18-4af5-a359-cf0508229a8c

In the previous example, only the highlighted section is different than the original URL in Step 4.

To display the Problem Finder dashboard, change the URL from Step 4 to:

https://lyta.marwatch.net/dashboard/container/
?template=readOnly/problemFinder&container=fba869f0-1c18-4af5-a359-cf0508229a8c

In the previous example, only the highlighted section is different than the original URL in Step 4.

APPENDIX 1: MITEL PERFORMANCE ANALYTICS ALARM MIB

This is the MIB describing the SNMP traps generated by Mitel Performance Analytics for alarm notifications.

```
MarWatch-MIB DEFINITIONS ::= BEGIN

IMPORTS
OBJECT-TYPE, OBJECT-IDENTITY, MODULE-IDENTITY, NOTIFICATION-TYPE,
enterprises, Integer32 FROM SNMPv2-SMI

TEXTUAL-CONVENTION, DateAndTime, DisplayString FROM SNMPv2-TC

MODULE-COMPLIANCE, OBJECT-GROUP, NOTIFICATION-GROUP FROM SNMPv2-CONF;

marWatchMibModule MODULE-IDENTITY
LAST-UPDATED "2013040200000Z"
ORGANIZATION "Martello Technologies"
CONTACT-INFO "support@martellotech.com"
DESCRIPTION  "Martello MarWatch MIB"

REVISION     "201202100000Z"    -- 10 Feb 2012
DESCRIPTION
"Initial Version"
::= { marWatchConformance 1 }

REVISION     "201304020000Z"    -- 11 April 2013
DESCRIPTION
"Add Device Dashboard URL to MarWatch Alarm information fields"
::= { marWatchConformance 1 }

martello  OBJECT IDENTIFIER ::= { enterprises 39275 }
marWatch  OBJECT IDENTIFIER ::= { martello 1 }
```

```
-- TEXTUAL CONVENTIONS


Status ::= TEXTUAL-CONVENTION
STATUS       current
DESCRIPTION  "Alarm Status Values"
REFERENCE    "RFC3877 Alarm MIB alarmModelState"
SYNTAX       INTEGER {
clear          (1),
indeterminate  (2),
warning        (3),
minor          (4),
major          (5),
critical       (6)
}



alarm                   OBJECT IDENTIFIER ::= { marWatch 1 }
marWatchConformance     OBJECT IDENTIFIER ::= { marWatch 100 }



-- NOTIFICATIONS


marWatchTraps OBJECT-IDENTITY
STATUS      current
DESCRIPTION "Definition point for MarWatch notifications."
::= { marWatch 0 }


marWatchAlarm NOTIFICATION-TYPE
OBJECTS { alarmId, alarmDevice, alarmComponent,
alarmCustomer, alarmNewStatus,
alarmStatusChangeTime, alarmDescription }
STATUS  current
DESCRIPTION
```

```
"This notification is generated whenever an alarm condition is detected
or cleared."

::= { marWatchTraps 1 }



-- ALARM


alarmTable OBJECT-TYPE
SYNTAX     SEQUENCE OF AlarmEntry
MAX-ACCESS not-accessible
STATUS     current
DESCRIPTION

"A list of alarm entries."

::= { alarm 1 }


alarmEntry OBJECT-TYPE
SYNTAX     AlarmEntry
MAX-ACCESS not-accessible
STATUS     current
DESCRIPTION

"Alarm object"

INDEX { alarmIndex }
::= { alarmTable 1 }


AlarmEntry ::= SEQUENCE {
alarmIndex                  Integer32,
alarmId                     OCTET STRING,
alarmDevice                 DisplayString,
alarmComponent              DisplayString,
alarmCustomer               DisplayString,
alarmNewStatus              Status,
alarmStatusChangeTime       DateAndTime,
alarmDescription            DisplayString
alarmURL                    DisplayString
}


alarmIndex OBJECT-TYPE
SYNTAX            Integer32 (1..65535)
MAX-ACCESS        not-accessible
STATUS            current
DESCRIPTION
```

```
"An index that uniquely identifies an entry in the alarm table."
::= { alarmEntry 1 }


alarmId OBJECT-TYPE
SYNTAX            OCTET STRING (SIZE (0..255))
MAX-ACCESS        read-only
STATUS            current
DESCRIPTION
"MarWatch Unique identifier for this Alarm"
::= { alarmEntry 2 }


alarmDevice OBJECT-TYPE
SYNTAX            DisplayString
MAX-ACCESS        read-only
STATUS            current
DESCRIPTION
"MarWatch Device Name"
::= { alarmEntry 3 }


alarmComponent OBJECT-TYPE
SYNTAX            DisplayString
MAX-ACCESS        read-only
STATUS            current
DESCRIPTION
"MarWatch Component Identifier"
::= { alarmEntry 4 }


alarmCustomer OBJECT-TYPE
SYNTAX            DisplayString
MAX-ACCESS        read-only
STATUS            current
DESCRIPTION
"MarWatch Customer Name"
::= { alarmEntry 5 }


alarmNewStatus OBJECT-TYPE
SYNTAX            Status
MAX-ACCESS        read-only
STATUS            current
DESCRIPTION
```

```
"New Status for this Device and Component"

::= { alarmEntry 6 }


alarmStatusChangeTime OBJECT-TYPE
SYNTAX            DateAndTime
MAX-ACCESS        read-only
STATUS            current
DESCRIPTION

"The time that Device and Component transitioned to this status"

::= { alarmEntry 7 }


alarmDescription OBJECT-TYPE
SYNTAX            DisplayString
MAX-ACCESS        read-only
STATUS            current
DESCRIPTION

"Textual description of Device and Component Status"

::= { alarmEntry 8 }


alarmURL OBJECT-TYPE
SYNTAX            DisplayString
MAX-ACCESS        read-only
STATUS            current
DESCRIPTION

"URL for Device Dashboard"

::= { alarmEntry 9 }



---- Conformance information--


marWatchCompliances OBJECT IDENTIFIER ::= { marWatchConformance 9 }
marWatchGroups      OBJECT IDENTIFIER ::= { marWatchConformance 10 }


-- Compliance Statements
marWatchCompliance MODULE-COMPLIANCE
STATUS current
DESCRIPTION

"The requirements for conformance to the MarWatch MIB."
```

```
MODULE -- this module

GROUP marWatchAlarmGroup
DESCRIPTION
"The MarWatch Alarm Group is optional."

GROUP marWatchNotificationGroup
DESCRIPTION
"The MarWatch Notification Group is optional."
::= { marWatchCompliances 1 }


marWatchNotificationGroup NOTIFICATION-GROUP
NOTIFICATIONS { marWatchAlarm }
STATUS        current
DESCRIPTION
"The MarWatch Alarm Group."
::= { marWatchGroups 1 }

marWatchAlarmGroup OBJECT-GROUP
OBJECTS {
alarmId,
alarmDevice, alarmComponent,
alarmCustomer, alarmNewStatus,
alarmStatusChangeTime, alarmDescription,
alarmURL
}
STATUS    current
DESCRIPTION
"The MarWatch Notification Group."
::= { marWatchGroups 2 }

END
```

APPENDIX 2: DEFINITION OF COMMON ALARMS

Mitel Performance Analytics presents a consolidated view of the alarms generated by the devices it monitors. Mitel Performance Analytics also generates its own alarms based on issues and events it detects.

The following sections describe common alarms that you may see on the Mitel Performance Analytics Alarms panel. Additional device alarms are possible. Refer to your device user documentation for details. For example, refer to Mitel MiVoice Business user documentation for details on MiVoice Business alarms.

PROBE ALARMS

The following alarms apply to the Probe.

“Probe has not checked in”

Alarm source: Mitel Performance Analytics

Description: The Probe assigned to this device has not checked in to the Mitel Performance Analytics server for some time.

Possible Cause: Probe may be powered off or blocked by network issues.

Notes: Use the Threshold panel to configure the elapsed time period.

“Off Net Collector Startup”

Alarm source: Mitel Performance Analytics

Description: Probe software restart.

“Connected from ###.###.###.###”

Alarm source: Mitel Performance Analytics

Description: A Probe Remote Access control channel was opened from specified IP address.

>“Disconnected from ###.###.###.###”

Alarm source: Mitel Performance Analytics

Description: The Probe Remote Access control channel from the specified IP address was closed.

“Checkin: RESTClientException: <URL>”

Alarm source: Mitel Performance Analytics

Description: An error occurred when the Probe attempted to verify its configuration.

“Restarting on new software version”

Alarm source: Mitel Performance Analytics

Description: A new version of the Probe software was detected and auto-downloaded.

“Time Sync threshold exceeded”

Alarm source: Mitel Performance Analytics

Description: The Probe's internal clock does not agree with the Mitel Performance Analytics server's clock.

Notes: This can affect timestamp of incoming alarms, and time when backups are triggered.

GENERIC ALARMS

The following alarms apply to all monitored devices.

“SNMP unreachable”

Alarm source: Mitel Performance Analytics

Description: The Probe cannot reach the device.

“Uptime threshold exceeded”

Alarm source: Mitel Performance Analytics

Description: Device is reporting uptime that is less than the configured threshold.

Possible Cause: Device likely rebooted recently

Notes: Use the Threshold panel to configure the uptime period. Alarm may be a false positive if triggered after approximately 498 days.

“Ping Packet Loss threshold exceeded”

Alarm source: Mitel Performance Analytics

Description: Probe has not been able to get a ping reply from the device for a configure time period. The device may be offline.

Notes: Use the Threshold panel to configure the time period.

"CPU threshold exceeded"

Alarm source: Mitel Performance Analytics

Description: Processor usage on the device is running high, possibly impacting performance.

Notes: Use the Threshold panel to configure the threshold.

"Memory Usage threshold exceeded"

Alarm source: Mitel Performance Analytics

Configurable through Thresholds screen

Description: Physical memory on the device may be running low, possibly impacting performance

Notes: Use the Threshold panel to configure the threshold.

"Probe not reporting"

Alarm source: Mitel Performance Analytics

Description: The Probe assigned to this device has not checked in to the Mitel Performance Analytics server for some time.

Possible Cause: Probe may be powered off or blocked by network issues.

"New device, information not yet available"

Alarm source: Mitel Performance Analytics

Only appears on newly created devices

Description: Mitel Performance Analytics has not yet collected information from the device.

"No probe configured"

Alarm source: Mitel Performance Analytics

Description: Device is configured, but there is no Probe assigned to monitor it.

"This Device is in maintenance mode."

Alarm source: Mitel Performance Analytics

Description: This alarm is for your information only. Mitel Performance Analytics is in maintenance mode for this device. All other alarms for this device are suppressed.

"Unlicensed Capability: xxxxxxxxx"

Alarm source: Mitel Performance Analytics

Description: An optional feature has been enabled for this device and the required license has not been applied yet.

MIVOICE BUSINESS ALARMS

The following alarms apply to MiVoice Business devices.

"x out of y SIP Link / Lines / Digital Links / ICP Comms unavailable."

Alarm source: Device

Description: Device has the indicate number of lines currently offline.

"x out of y Backup Failure unavailable."

Alarm source: Device

Description: Backup on the device has failed.

"x out of y VM Port Status unavailable."

Alarm source: Device

Description: Connection to the indicated number of Voicemail services has been lost.

"0 out of 1 SDS Sys Data unavailable."

Alarm source: Device

Description: Issue syncing data between cluster members.

"0 out of 1 Lic Violation unavailable."

Alarm source: Device

Description: Device is using some features or resources that are not supported by the Mitel license

"Missing set DN: xxxx, MAC xx:xx:xx:xx:xx:xx"

Alarm source: Mitel Performance Analytics

Description: The Set Inventory Disconnect Alarms feature is enabled. A handset connected to the MiVoice Business is offline.

"License _____ threshold exceeded"

Alarm source: Mitel Performance Analytics

Description: The indicated device alarm has exceeded the configured threshold (for example, 80% of total licensed SIP Trunks).

Notes: Use the Threshold panel to configure the threshold.

"Unable to retrieve data: Login operation failed in 3300"

Alarm source: Mitel Performance Analytics

Description: Probe attempted to log in to the MiVoice Business system to retrieve data, but failed.

Possible Cause: The device username and password was incorrectly configured in Mitel Performance Analytics.

"Voice Quality threshold exceeded"

Alarm source: Mitel Performance Analytics

Description: Recent calls have had poor quality.

Possible Cause: May indicate network or resource performance issues.

Notes: Use the Threshold panel to configure the threshold.

"Resiliency Failover from Admin, Cluster: _____ : 1."

Alarm source: Device

Description: Device failover has been triggered. Handsets are now reporting to the specified standby device.

MIVOICE BORDER GATEWAY ALARMS

The following alarms apply to MiVoice Border Gateway devices.

"Voice Quality threshold exceeded"

Alarm source: Mitel Performance Analytics

Description: Recent calls have had poor quality.

Possible Cause: May indicate network or resource performance issues.

Notes: Use the Threshold panel to configure the threshold.

"The connection to port 6810, the SRC Connector Port, was not successful. "

Alarm source: Mitel Performance Analytics

Description: The Probe needs to access the device on port 6810 to retrieve data.

Possible Cause: May indicate firewall issues or MBG misconfiguration. Enable the "Call Recording" option on the Server-Manager page to determine cause.

"MBG connectivity Alarm"

Alarm source: Device

Description: There is a connectivity alarm in the MBG alarm table that Mitel Performance Analytics cannot retrieve the full details.

"MBG status Alarm"

Alarm source: Device

Description: There is a Status alarm in the MBG alarm table that Mitel Performance Analytics cannot retrieve the full details.

"MiCollab Client Service status Alarm"

Alarm source: Device

Description: The MBG is part of a MiContactCenter Business platform. There is a Client Service alarm in the MBG alarm table that Mitel Performance Analytics cannot retrieve the full details.

"Minimum MOS threshold exceeded"

Alarm source: Device

Description: Recent calls have had poor quality.

Possible Cause: May indicate network or resource performance issues.

"SSH authentication failed"

Alarm source: Mitel Performance Analytics

Description: The Probe's attempt to log in to the device over SSH failed.

Possible Cause: The device username and password was incorrectly configured in Mitel Performance Analytics.

"License _____ threshold exceeded"

Alarm source: Mitel Performance Analytics

Description: The indicated device alarm has exceeded the configured threshold (for example, 80% of total licensed SIP Trunks).

Notes: Use the Threshold panel to configure the threshold.

"Commissioning Approval Pending for Certificate ID xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"

Alarm source: Mitel Performance Analytics

Description: The Probe has tried to authenticate with the MBG. Its certificate must be manually accepted from the Server-Manager page.

Remedial Action: Approve the Probe certificate using the MBG Server-Manager page. See "Accepting the Mitel Performance Analytics Certificate Request at the MiVoice Border Gateway" on page 130.

MICOLLAB ALARMS

The following alarms apply to MiCollab devices.

"ucserver status Alarm"

Alarm source: Device

Description: This MiCollab platform has a UC Server. There is a UC Server alarm in the MiCollab alarm table that Mitel Performance Analytics cannot retrieve the full details.

"MiCollab Client Service status Alarm"

Alarm source: Device

Description: This MiCollab platform has a client service. There is a client service alarm in the MiCollab alarm table that Mitel Performance Analytics cannot retrieve the full details.

"MBG connectivity Alarm"

Alarm source: Device

Description: This MiCollab platform has an MBG. There is an MBG connectivity issue reported in the MiCollab alarm table that Mitel Performance Analytics cannot retrieve the full details.

"SSH authentication failed"

Alarm source: Mitel Performance Analytics

Description: The Probe's attempt to log in to the device over SSH failed.

Possible Cause: The device username and password was incorrectly configured in Mitel Performance Analytics.

MICONTACT CENTER BUSINESS ALARMS

The following alarm applies to MiContactCenter Business devices.

"Windows Service Inactivity '_____' threshold exceeded"

Alarm source: Mitel Performance Analytics

Description: The named service is needed according to the Threshold panel. The named service has been inactive (stopped) for longer than configured in the Threshold panel.

Notes: Use the Threshold panel to configure the threshold.