MITEL PERFORMANCE ANALYTICS

RELEASE 3.0

SYSTEM DESCRIPTION

⋈ Mitel®

NOTICE

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

No part of this document can be reproduced or transmitted in any form or by any means - electronic or mechanical - for any purpose without written permission from Mitel Networks Corporation.

Trademarks

The trademarks, service marks, logos and graphics (collectively "Trademarks") appearing on Mitel's Internet sites or in its publications are registered and unregistered trademarks of Mitel Networks Corporation (MNC) or its subsidiaries (collectively "Mitel") or others. Use of the Trademarks is prohibited without the express consent from Mitel. Please contact our legal department at legal@mitel.com for additional information. For a list of the worldwide Mitel Networks Corporation registered trademarks, please refer to the website: http://www.mitel.com/trademarks.

Mitel Performance Analytics System Description
Release 3.0 - January 16, 2019

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 describes the Mitel Performance Analytics (MPA) monitoring system.

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
November 2, 2017	Mitel Performance Analytics R2.2 General Availability
January 16, 2019	Preliminary version for Mitel Performance Analytics R3.0.

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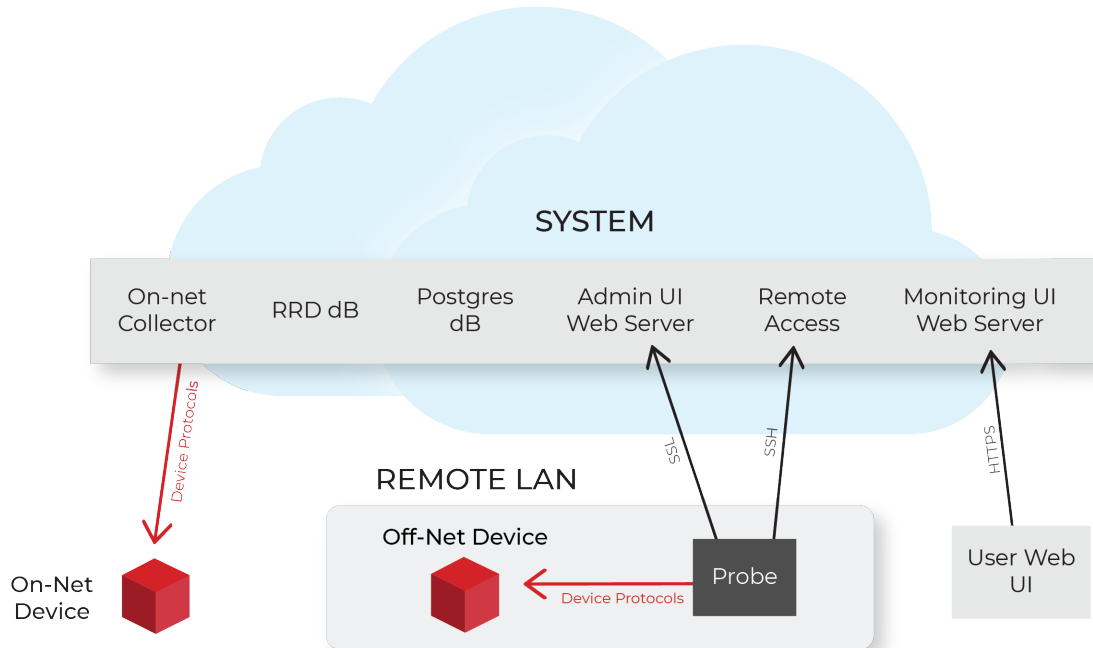
The various Mitel Performance Analytics components can run on a single or multiple servers, depending on capacity requirements.

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.
- It collects performance data and alarms from devices in the customer networks.
- It transfers performance data and alarm status to Mitel Performance Analytics.
- It enables secure remote access for the Mitel Performance Analytics user to the remote customer network.

For a detailed description of the **Probe**, see the *Mitel Performance Analytics Probe Installation and Configuration Guide*.

CAPABILITIES

Mitel Performance Analytics provides fault, inventory, and performance management for Mitel Networks Unified Communications systems, 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 with the standard with the Mitel Premium Software Assurance license provides:

- Support for a range of Mitel systems; see "Supported Devices" on page 10 for a complete list
- VoIP Quality monitoring and visualization for MiVoice Business, Mitel SIP sets, MBG (Teleworker and SIP trunk), MiVoice MX-ONE
- Cloud or on-premises packaging
- Real-time and historical fault and performance monitoring
- Alarm management tools (dashboards, alerting, views) and 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.
- Display of dynamic health status icons over user-supplied network diagram, with devices and containers arranged according to user preferences
- Monthly or on-demand customer reporting
- 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)
- IP SLA monitoring
- Simple deployment in remote customer networks with both software and hardware Probe available
- Supports multiple internationalized character sets for content entry into Mitel Performance Analytics
- 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
- Integrated remote access to customer networks (with Probe) in the cloud

Additional capabilities are available in Mitel Performance Analytics with the Mitel Premium Software Assurance Plus license, including the following:

- Emergency Response (ER) alarm monitoring and alerts for MiVoice Business and MiVoice Business EX
- Advanced User Operations (AUO) to simplify management configuration tasks across MiVoice Business clusters such as moving a user from one MiVoice Business to another one, removing a user, or setting up and managing Busy Lamp Field (BLF) keys
- Support for SNMP based third-party devices and applications
- Advanced user, set, and service inventory reporting for MiVoice Business, MiVoice Border Gateway, MiVoice Connect, and MiVoice MX-ONE
- Device and extension inventory for MiVoice Business, MiVoice Border Gateway, and MiVoice Connect

- IP set inventory for MiVoice Business and MiVoice Border Gateway
- Agent based network testing to assess, monitor and troubleshoot the availability, capacity, and performance of the network
- Collection and storage of SMDR records for MiVoice Business and MiVoice Office 250
- System wide backups, stored locally or in the cloud for MiVoice Business, MiVoice MX-ONE, and MiVoice Connect
- Trunk capacity reporting for MiVoice Business and MiVoice Connect
- Audio, web, and video port usage reporting for MiCollab (MSL)

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 enabled.

Mitel Performance Analytics is officially supported on:

- Firefox, Release 55.0 and later
- Chrome, Release 60.0 and later

Mitel Performance Analytics does work on Microsoft Edge, Release 16; however, it is not officially supported. Mitel Performance Analytics Mitel Performance Analytics does not work on Release 15 of Edge.

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

Important: Although Mitel Performance Analytics was never officially supported on Internet Explorer, as of Release 2.2, Mitel Performance Analytics no longer works on this browser. If you are using Internet Explorer, we recommended moving to one of the supported browsers to continue to take advantage of all of the features offered by Mitel Performance Analytics.

SUPPORTED DEVICES

Mitel Performance Analytics supports the following device types:

DEVICE	SUPPORTED VERSIONS
MX-ONE Application Server	
MiContact Center Business	Release 6.0 SP2 FP3, 7.1 SP2 PR1, and 8.1 or later
MiContact Center Enterprise	
MiContact Center Office	
MiVoice Office 250 CP systems	Release 6.3 or later
MiCollab	Release 7.1, 7.2, 7.2.2, and 8.0 FP1
MiVoice Border Gateway	Release 8.1 SP1, 9.2, 9.3, and 9.4
MiVoice Business, Mitel 3300, vMCD ICP systems	Release 7.0 SP1, 7.1 SP1, 7.2, and 8.0 SP2, 9.0
MiVoice Business EX	Release 9.0
MiVoice Business Multi Instance	
MiVoice Connect HQ Server	Version 32.0
MiVoice Connect Voice Switch	
MiVoice Connect Distributed Voice Server (DVS)	
MiVoice Connect Service Appliance	
Mitel Business Dashboard	
Mitel Open Integration Gateway	
Mitel Oria	
MiVoice MX-ONE	Release 6.0, 6.1 SP1, 6.2, 6.3 SP1, 7.0
MiVoice Call Recorder	Release 8.1 SP2, 9.0, 9.1
SIP DECT Open-Mobility Manager (OMM)	
SIP DECT Radio Fixed Part (RFP)	
Red Box Call Recorder	
Innovation InnLine Voice Mail Server	

DEVICE	SUPPORTED VERSIONS
Standard Servers (Windows and Linux)	
VMWare ESXi Server	Release 6, 6.5
Ethernet Switches (HP, Cisco, Dell, Avaya)	
Routers (Cisco and Adtran)	
PathSolutions Servers	
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
Elfiq Devices	
Basic IP Device	
Unipower Aspiro (PCC) 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.

Mitel Performance Analytics provides the monitoring capabilities listed in the following table.

DEVICE	SUPPORTED PERFORMANCE AND ALARM MONITORING
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
MiContact Center Business MiContact Center Enterprise MiContact Center Office	- System alarms - System information - System reachability and availability - Service availability monitoring for critical services - Performance metrics: CPU, memory, file system and interface statistics
MiVoice Office 250 CP systems	- System alarms - Inventory (system hardware, software information, hardware ID, app record) - System reachability and availability - License inventory - Performance metrics: CPU, memory
Mitel Business Dashboard	- System alarms - System information - System reachability and availability - Service availability monitoring for critical services - Performance metrics: CPU, memory, file system and interface statistics

DEVICE	SUPPORTED PERFORMANCE AND ALARM MONITORING
MiCollab, Mitel Standard Linux (MSL)	• System alarms • System information and Mitel service ID • System reachability and availability • MiCollab application 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

MiVoice Border Gateway	• System alarms
	• System information and Mitel service ID
	• System reachability and availability
	• MiCollab application inventory
	• License 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
	• Voice quality visualization charts
	• Performance metrics: CPU, memory, file system and interface statistics

MiVoice Business, Mitel 3300, vMCD ICP systems	• System alarms • Emergency Response (ER) alarms • System reachability and availability • Inventory (system hardware, software information, hardware ID, app record) • License inventory, node and cluster • Performance metrics: CPU, memory, interface statistics • Voice metrics: voice quality ratings by call (R factor) • Voice quality visualization charts • Digital trunk and SIP trunk utilization • IPT user data

DEVICE	SUPPORTED PERFORMANCE AND ALARM MONITORING
MiVoice Business EX	• System alarms • Emergency Response (ER) alarms • System reachability and availability • Inventory (system hardware, software information, hardware ID, app record) • License inventory, node and cluster • Performance metrics: CPU, memory, interface statistics • Voice metrics: voice quality ratings by call (R factor) • Voice quality visualization charts • Trunk utilization (SIP) • IPT user data
MiVoice Business Multi Instance	• System alarms • System information and Mitel service ID • System reachability and availability • Mitel MSL application inventory • Performance metrics: CPU, memory, processes, file system and interface statistics
MiVoice Connect HQ Server	• System information • System alarms • System reachability and availability • Voice quality visualization charts • Performance metrics: CPU, memory, file system and interface statistics • Extension inventory • License count • Trunk capacity reporting
MiVoice Connect Voice Switch, MiVoice Connect Distributed Voice Server (DVS), and MiVoice Service Appliance	• System alarms • System reachability and availability • Performance metrics: CPU, memory, file system and interface statistics

DEVICE	SUPPORTED PERFORMANCE AND ALARM MONITORING
Mitel Open Integration Gateway	• System alarms • System information and Mitel service ID • System reachability and availability • Mitel MSL application inventory • Performance metrics: CPU, memory, processes, file system and interface statistics
Mitel Oria	• System alarms • System information and Mitel service ID • System reachability and availability • Mitel MSL application inventory • Performance metrics: CPU, memory, processes, file system and interface statistics
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) • Performance metrics: CPU, memory, interface statistics • Voice metrics: SIP set voice quality ratings by call (R factor) over multiple interfaces • Voice quality visualization charts • IPT user data • Device and extension inventory • Extension and terminal registration • Route utilization • Gateway utilization
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

DEVICE	SUPPORTED PERFORMANCE AND ALARM MONITORING
SIP DECT Open-Mobility Manager (OMM)	• System alarms • System information • System reachability and availability • Performance metrics: CPU, memory, file system and interface statistics • Number of connected and configured gateways, devices and users • Whether the Locating License is enabled or not; whether the Messaging License is enabled or not; the number of connected and configured gateways.
SIP DECT Radio Fixed Part (RFP)	• System alarms • System information • System reachability and availability
Mitel Probe	• System information • Probe connectivity alarms • 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
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

DEVICE	SUPPORTED PERFORMANCE AND ALARM MONITORING
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

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 • System reachability and availability • System alarms • System Status Application (SSA) remote access • Interface performance monitoring • Server performance monitoring (Server Edition)

DEVICE	SUPPORTED PERFORMANCE AND ALARM MONITORING
Elfiq Devices	- System information - System reachability and availability - System alarms
Basic IP Device	- System information - System reachability and availability
Unipower Aspiro (PCC) Device	- System information - System reachability and availability - System alarms - Performance metrics: Voltage, Battery Current, Load Current, Rectifier Current, and Battery Temperature

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
  - MiVoice Business EX
  - MiContact Center Business
  - MiVoice Connect
  - 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
  - MiVoice Business EX
  - MiVoice Border Gateway
- Emergency Response (ER) alarms: MiVoice Business

MAP VIEW

Map view capabilities include:

- Shows customer locations with color coded location status
- Health status icons linked to the alarm filter

- Click on location to open container dashboard

NETWORK DIAGRAM VIEW

Network diagram view capabilities include:

- Displays device and container health status icons on any customer generated network diagram
- Health status icons linked to the alarm filter
- Click on device or container to show related alarms
- Click on alarm to display device or 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, emergency notification, 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)

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.

REPORTING

Mitel Performance Analytics provides optional reporting on device performance by customer.

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.

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

QUICK QUERIES

The on-demand quick queries are accessed from the **Network Data** menu. The container dashboard provides access to most queries. Some queries are available also from the dashboard of the device to which the query applies.

The following topics 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 time frame for the report. Additional queries can be configured with the **Reports** menu item.

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.
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.

QUERY NAME	DESCRIPTION
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.

BACKUP RESULTS

Mitel Performance Analytics provides the following queries for displaying backup information from scheduled and on-demand backups. The queries that are available depend on whether the query is run at the container or at the device level.

QUERY NAME	DESCRIPTION
Latest Backup Files (Container)	The latest backup file for each device in the container.
Failed Backups (Container)	Devices for which the most recent backup attempt has failed.
Managed Backup Files (Container)	All managed backup files for all of the devices within the container.
External Backup Files (Container)	All external backup files for all of the devices within the container.
All Backup Activity	• Container: All backup results for all devices within the container. • Device: All backup results for the device.
All Files (Device)	All backup files for the device.

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.

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.
Inventory of Customer Devices	List of customer devices in the container.
MiContact Center Licenses	Inventory of MiContact Center licenses
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. **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. **Note:** This query is only available with the Mitel Premium Software Assurance Plus license.
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.
Inventory of MiVoice Connect HQ Server Extensions	Lists details for MiVoice Connect HQ Server extensions, such as user name, email address, extension number, site, phone model, IP address, and more.
Probe Details	Lists detailed information about all Probes for use when troubleshooting; for example, the last time each Probe has checked in and the type of platform each Probe runs on

Note: By default, full inventory collection on MiVoice Business devices is performed daily at 5:00 am and 12:00 pm. If these times need to be changed, contact support@martellotech.com for assistance.

LICENSE QUERIES

Mitel Performance Analytics provides the following initial set of license queries. Additional queries can be configured with the **Reports** menu item.

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.
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 (Globally Unique Identifier).
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.
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.

ONLINE LICENSING SERVER UPLOADS

Mitel Performance Analytics requires certain information for licensing purposes. For offline licensing, you must manually do the following queries and send the results to Mitel before a license file is provided. With online licensing, the information is sent automatically. However, you may want to manually do the following queries to see what information is sent to Mitel.

QUERY NAME	DESCRIPTION
(Optional) Call Quality	If you have not opted out, the online licensing server collects aggregate, anonymous call quality information for all devices.
(Optional) Completed Schedules	If you have not opted out, the online licensing server collects the number and type of completed scheduled operations for each device type.
(Optional) User Actions	If you have not opted out, the online licensing server collects the number of audited actions taken by each user. User names are anonymized.
Container License States	The online licensing server collects whether or not each of your containers is properly licensed and the date when the container will become unlicensed.
Containers	The online licensing server collects an anonymized copy of your container hierarchy.
Device License States	The online licensing server collects whether or not each of your devices is properly licensed and the date when the device will become unlicensed.
Device Versions	The online licensing server collects the version information for all devices.
Devices	The online licensing server collects a copy of your devices including what type of device they are, which probe is monitoring them, and their unique ARID, hardware identifier or serial number.
Event Counts	The online licensing server collects the number of events that have been generated against each device in the last day.
Licensing Counts	The online licensing server collects a list of all items that your licenses may be based on as well as their corresponding counts.
Probes	The online licensing server collects an anonymized list of your probes including the last time they checked in and how many times they have restarted today.
User Counts	The online licensing server collects the number of users and active users as well as the number of unique email addresses that are receiving reports.

SCHEDULER RESULTS

Mitel Performance Analytics provides the following queries for use with the Operations Scheduler. The query results differ slightly depending on whether the query is run at the container or at the device level.

QUERY NAME	DESCRIPTION
All Scheduled Activity	• Container: Results of recent scheduled activities per device within the container. • Device: Results of recent scheduled activities for the selected device.
Schedule State	• Container: Per device timestamp of last success, last failure, and next execution. • Device: Timestamp of last success, last failure, and next execution for the selected device.
Success Rate	• Container: Per device and per schedule success rate. • Device: Per schedule success rate for the selected device.

SMDR FILES

Mitel Performance Analytics provides the following SMDR queries. The query results depend on whether the query is run at the container or at the device level.

QUERY NAME	DESCRIPTION
SMDR Files	• Container: All SMDR files for all devices within the container. • Device: All SMDR files for the device.

THRESHOLD QUERIES

Mitel Performance Analytics provides the following initial set of threshold queries. Additional queries can be configured with the **Reports** menu item.

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

VOICE QUALITY QUERIES

Mitel Performance Analytics provides the following initial set of Voice Quality (VQ) queries. Additional queries can be configured with the **Reports** menu item.

QUERY NAME	DESCRIPTION
Voice Quality by Hour of Day	Displays VQ metrics for the hours of the day. Metrics include the number and percent of good, fair, poor, or bad calls; the hour of the day they occurred, and the total number of calls.
Worst Performing DNs (#)	Displays the number of calls with bad or poor quality for the 10 worst directory numbers associated with a device.

QUERY NAME	DESCRIPTION
Worst Performing DNs (%)	Displays the percentage of poor quality calls for the 10 worst directory numbers associated with a device.
Worst Performing Devices (%)	Displays the number of calls with bad quality for the 10 worst devices in a container.

These queries and their associated charts are available for all device types that have their VQ data gathered.

ADVANCED FEATURES

Mitel Performance Analytics offers advanced features intended to simplify the management and maintenance of monitored devices and networks. To access these features, you must have the Mitel Premium Software Assurance Plus license.

SCHEDULED DEVICE GROUP OPERATIONS

Mitel Performance Analytics provides an Operations Scheduler to schedule operations on multiple devices at the same time.

Supported operations include:

- Backup:
    - MiVoice Business
    - MiVoice MX-ONE
    - MiVoice Connect HQ Server
    - MiVoice Connect Distributed Voice Server
- 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

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.

When you configure a scheduled operation, you specify the time period in which the Probe must execute the operation. The default time period is 3 hours; however, some operations may take longer than 3 hours to complete. If an operation is in progress and does not complete within the expected time, Mitel Performance Analytics indicates that the operation has failed. If the operation completes after the 3 hour time frame has elapsed, Mitel Performance Analytics updates the status and indicates that the operation is successful. If your device typically takes longer than the default time period to complete an operation, we recommend that you change the default time period to ensure that the status of the operation is accurate.

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.

REMOTE OFF-SITE BACKUP

Mitel Performance Analytics provides optional backup for MiVoice Business, MiVoice Connect, 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.

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.

EMERGENCY RESPONSE ALARMS

Mitel Performance Analytics provides optional emergency response alarms for MiVoice Business.

Mitel Performance Analytics listens for incoming Emergency Response (ER) SNMP traps from MiVoice Business devices. When such a trap is received, Mitel Performance Analytics acknowledges the trap by sending an SNMP Set message to the source MiVoice Business. Mitel Performance Analytics then generates a Major ER alarm that it displays its alarm list. The alarm message contains details about the emergency call, such as the extension that made the call and the time of the call. The ER alarm never expires and must be acknowledged by a Mitel Performance Analytics user.

When Mitel Performance Analytics sends an SNMP Set message to the source MiVoice Business following an incoming ER SNMP trap, it expects a response. If it fails to get the expected response, Mitel Performance Analytics tries again up to five times. If after five attempts it still does get the expected response, Mitel Performance Analytics generates an Indeterminate alarm. As with all Indeterminate alarms, it can expire.

All actions and events on ER alarms are tracked in a separate Emergency Call audit log.

Typical emergency response alarm actions include:

- Emergency call has been made.
- Alarm status has been updated to Forced Clear.
- Ticket has been assigned ticket number 4892.
- Alarm has been favorited.

TRUNK AND ROUTE CAPACITY ANALYTICS

Mitel Performance Analytics provides trunk capacity analytics for MiVoice Business and MiVoice Connect (HQ Server only) and route capacity analytics to MiVoice MX-ONE.

Trunk and route capacity analytics are viewed in the following ways in Mitel Performance Analytics:

- Schedule and run ongoing static reports that are emailed to recipients
- View and filter report data in a dashboard view

Trunk capacity analytics identify under and over utilized trunks for MiVoice Business (SIP and digital trunks) and MiVoice Connect (SIP trunks) as well as changes and trends in trunk usage over time.

Route capacity analytics identify under and over utilized routes for MiVoice MX-ONE as well as changes and trends in route usage over time.

The trunk and route capacity analytics show you important statistics including the grade of service (GoS) and trunk utilization over the busy hour, as well as recommendations to meet GoS targets, especially during the busy hour, which is the 60 minute window when the highest call rate occurred. This helps to identify if the trunks have enough capacity to keep dropped calls within an acceptable grade of service (1 to 2 %) and inform you if you have too much capacity during the busy hour.

Report dashboard views allow you to view and filter report data prior to sharing the report with other recipients. Specifically, you can:

- Filter the data to view different time-based scenarios.
- Change the Grade of Service value to see how capacity is affected.
- Group routes (Route Capacity only).
- Create and share a URL to the dashboard. The URL captures the dashboard at the specific point in time that the URL was created, so you can review how the data appeared then, not how it currently appears.
- Print the dashboard.

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.

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.

ADVANCED USER OPERATIONS

Mitel Performance Analytics provides an Advanced User Operations (AUO) tool for customers with MiVoice Business clusters.

The AUO tool greatly simplifies and reduces the time that it takes to complete tasks that are further complicated in a MiVoice Business clustered environment, such as moving users and devices across MiVoice Business nodes, deleting a user, or setting up and managing Busy Lamp Field (BLF) keys

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.

IPT USER DASHBOARD

Mitel Performance Analytics provides an IPT User Dashboard for MiVoice Business, MiVoice Connect, and MiVoice MX-ONE. This feature allows you to:

- View data for each user, including voice quality, for each call
- Investigate problems reported by users, or isolate problems to a particular user

MIVOICE BORDER GATEWAY VOICE QUALITY

Mitel Performance Analytics provides Voice Quality analytics for MiVoice Border Gateway SIP trunks. The analytics are displayed in the device dashboard panel, which provides a graphic view of the quality of the Voice over IP calls made on MiVoice Border Gateway for real-time identification of voice quality problems.

When appearing on MiVoice Border Gateway dashboard, the **SIP Trunk 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 dashboard view lists the available trunks. Selecting a single or multiple trunks displays the related data.

NETWORK TESTING

Mitel Performance Analytics provides optional agent based network testing for MiVoice Business, MiVoice MX-ONE, and MiVoice Connect systems that makes it easy to assess, monitor and troubleshoot the availability, capacity, and performance of the network.

The available network tests include:

- **SIP Call Test**: One or more test calls are made between two test agents and a PBX. Mitel Performance Analytics uses an internal SIP server to process these test calls. They are not made on the customer's telephony server.
- **Traceroute**: Traces the path that an IP packet takes from a test agent to an identified target. It lists all the routers it passes through until the target is reached, or fails and is discarded.
- **SIP Registration Test**: Attempts a SIP registration from a test agent to an identified SIP Registrar.
- **External Call Test**: A call is made from the test agent to an actual handset. It is recommended that a handset be configured with auto-answer in your network for testing purposes.

The tests are run between two endpoints. Depending on the type, the tests can be between two network agents or a network agent and a network endpoint such as a server, router, or switch. Alarms can also be set on the tests to ensure that any issues discovered are raised for review. See "Running Network Tests" on page 1 for details on running and scheduling network tests.

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.

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 12.

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.
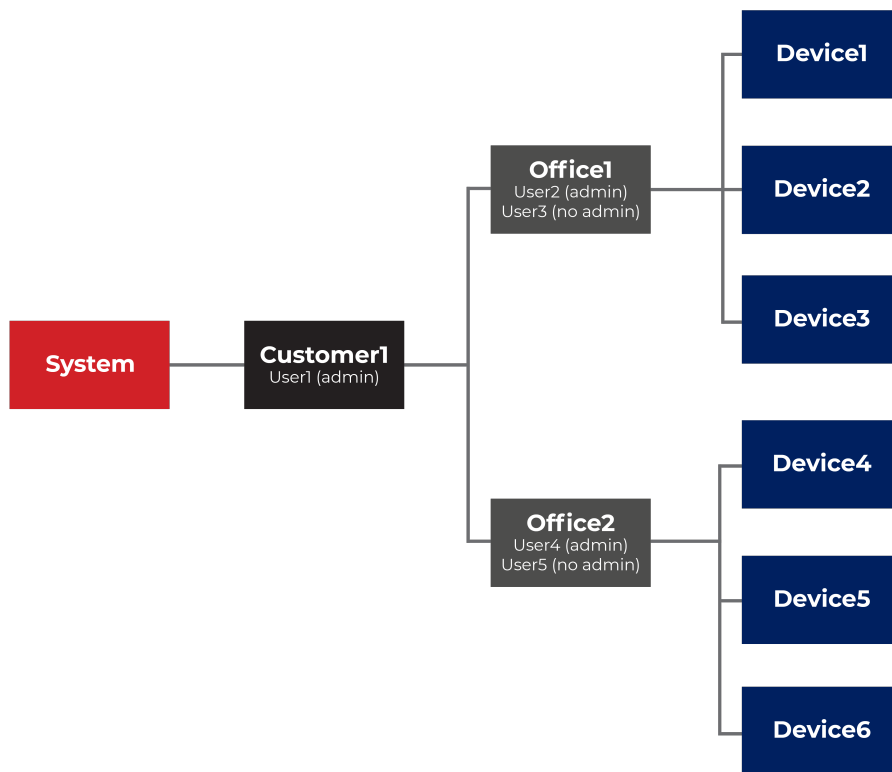
USERS

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.