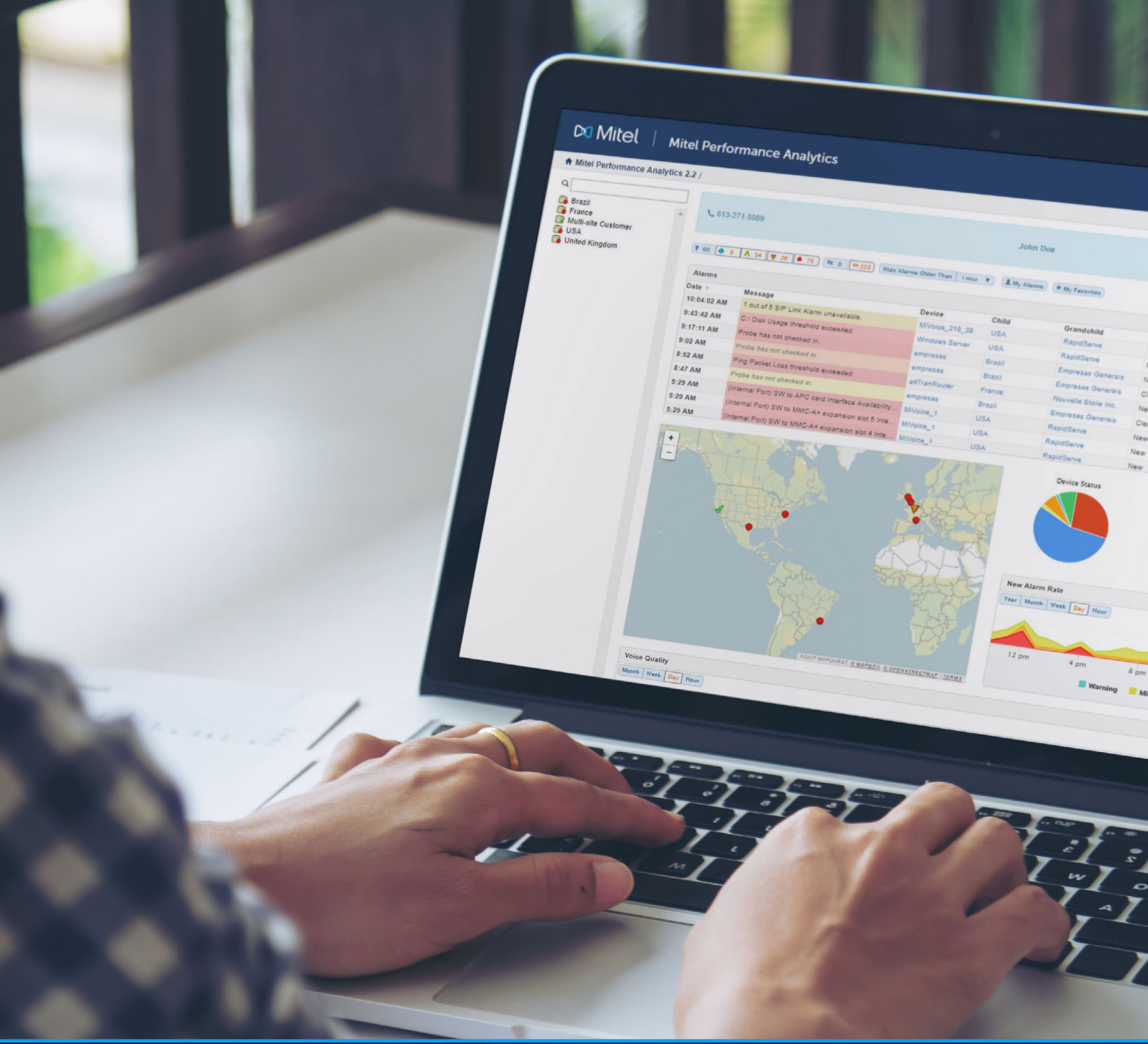


Making the Most of Alarms

Leverage the alarm management features of MPA to address network performance problems more effectively.

Mitel
Powering connections

Blueprint to Leverage Alarms and Alerts

Using Mitel Performance Analytics to leverage Alarms and Alerts.

Manage Alarm Fatigue

It's easy to get overwhelmed by alarms – either you are receiving too many, or the alarms you see are not relevant. Use alarm properties in MPA to manage the alarms you see - so you'll be PROACTIVE rather than REACTIVE in detecting and addressing problems on the network.

Set Thresholds

Configure performance thresholds to generate alarms when the thresholds are crossed. This gives you MORE control over the types of problems you are alerted to, and when and at what severity level.

Effective Alarm Management Eliminates Alarm Fatigue

Alarm Analytics

Customize your alarm management environment to help you see more easily the alarms that matter most to YOU. MPA learns 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.

Use Alarm Queries

MPA provides sets of pre-configured alarm queries to help you manage and track the alarms generated by MPA.

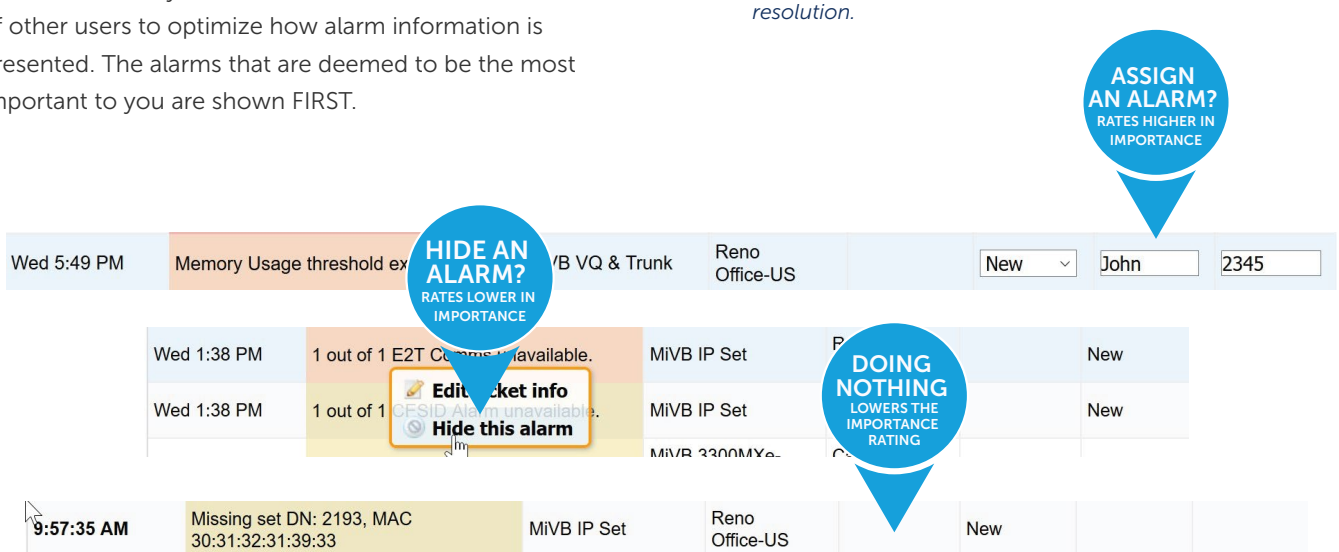
Alert Profiles Let You Manage Notifications

Configure Alert Profiles

Don't get lost in a sea of data. Alert profiles help you manage HOW, WHEN and to WHOM alerts are sent, to maximize their effectiveness. Notifications can be sent to an email address, to a desktop, by SMS, by Twitter Direct Message, or by a SNMP trap.

Why Use MPA?

- *Expertise in Mitel voice quality teamed with third-party device monitoring.*
- *Use alarms and alerts to manage network performance more proactively.*
- *Manage alarms effectively to see what's most important to you - for faster problem resolution.*



Alarm and Alert Management Best Practices

This white paper shows you how to use Mitel Performance Analytics (MPA) tools to manage alarms and alerts.

Overview

The purpose of this application note is to review those features of Mitel Performance Analytics (MPA) that help you manage alarms more effectively. Relevant and timely alarms are a key tool in managing network performance successfully. However, often network administrators are overwhelmed by alarms – either they receive too many, or the alarms they get aren't relevant to them. By setting up and using alarm properties to suit your needs, you'll find them more helpful in managing network performance, so you'll be more proactive than reactive in detecting and addressing problems on the network.

Alarm management capabilities covered in this application note include:

- Alarm Types and Severity
- Alarm Dashboard
  - * Alarm Filters
  - * Alarm Operations
- Threshold Alarms
- Alert Profiles
- Alarm Analytics
  - * Alarm Analytics Labels
  - * Alarm Analytics Data
  - * Time-Related Alarms
- Alarm Queries

Alarms Types

Mitel Performance Analytics (MPA) reports the following categories of alarms:

Device Alarms: Device alarms are those that are generated and reported by the devices and applications that MPA monitors. MPA receives the alarm information from the device or application and presents it on the Alarms panel.

Threshold Alarms: MPA monitors certain performance parameters in monitored devices and applications and is configured to generate alarms when thresholds are exceeded.

System Alarms: MPA generates alarms to indicate service problems. Some examples are "Incorrect Credentials to access a Device" and "Device SNMP or ICMP Unreachable".

Alarms are displayed on container, device and IPT user dashboards. Alerts are notifications of alarms. They are delivered to users as email, SMS, or TwitterTM direct messages; desktop notifications; or SNMP traps. Alerts are configured in alert profiles for specific alarm types and severities. For more information on setting up alert profiles, see the 'Configuring Alert Profiles' section of this Application Note.

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.
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 MPA 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.

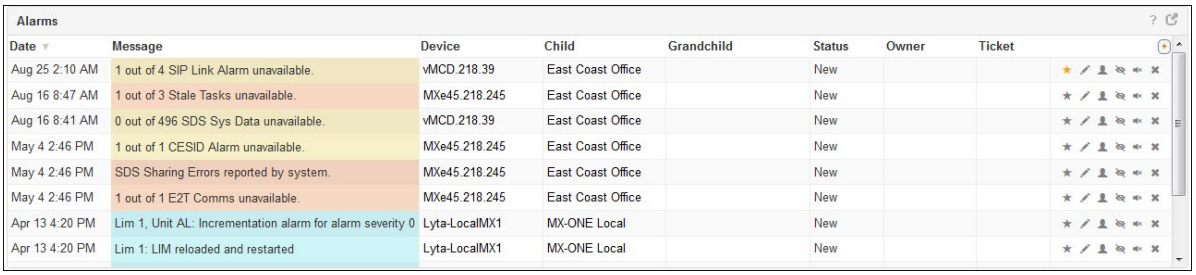
Mitel Performance Analytics

Performance management and analytics have become a strategic requirement for business communications. Monitoring and managing performance offers a better user experience, resulting in less downtime, and decreases the cost of support.

The Mitel Performance Analytics (MPA) software suite helps administrators manage enterprise deployments with multiple network nodes, while allowing partners to proactively detect and address performance issues on customer networks.

Alarms - Dashboard Display

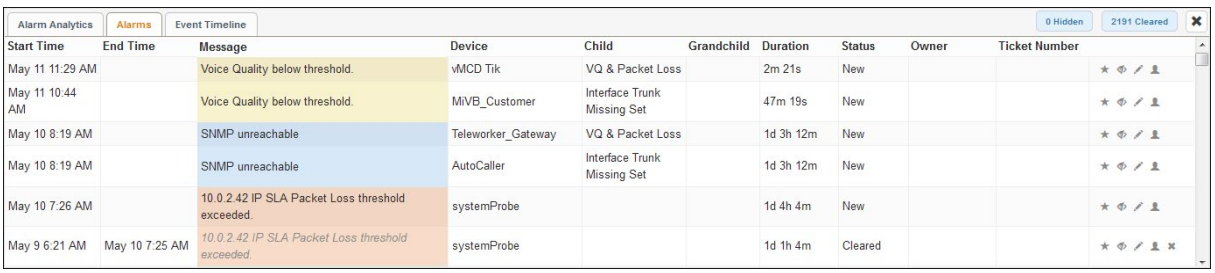
Alarms are front and centre in the MPA dashboard, making it easier to see problems happening on your network at-a-glance.



Date	Message	Device	Child	Grandchild	Status	Owner	Ticket
Aug 25 2:10 AM	1 out of 4 SIP Link Alarm unavailable.	vMCD.218.39	East Coast Office		New		
Aug 16 8:47 AM	1 out of 3 Stale Tasks unavailable.	MXe45.218.245	East Coast Office		New		
Aug 16 8:41 AM	0 out of 496 SDS Sys Data unavailable.	vMCD.218.39	East Coast Office		New		
May 4 2:46 PM	1 out of 1 CESID Alarm unavailable.	MXe45.218.245	East Coast Office		New		
May 4 2:46 PM	SDS Sharing Errors reported by system.	MXe45.218.245	East Coast Office		New		
May 4 2:46 PM	1 out of 1 E2T Comms unavailable.	MXe45.218.245	East Coast Office		New		
Apr 13 4:20 PM	Lim 1, Unit AL: Incrementation alarm for alarm severity 0	Lyta-LocalMX1	MX-ONE Local		New		
Apr 13 4:20 PM	Lim 1: LIM reloaded and restarted	Lyta-LocalMX1	MX-ONE Local		New		

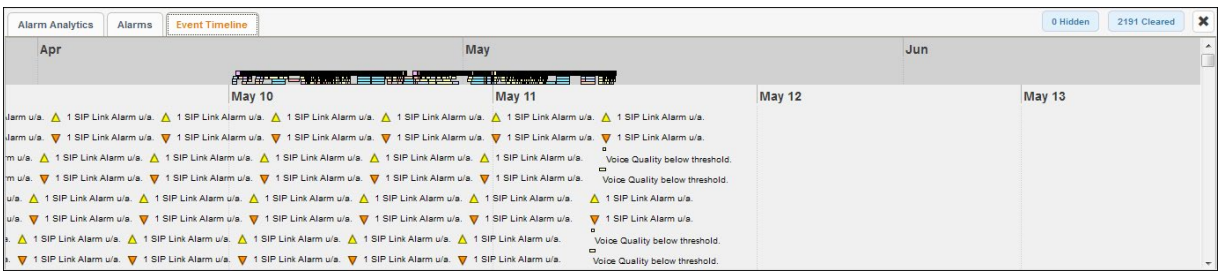
Expanding the Alarms panel displays tabs with specialized information:

- *The Alarm Analytics tab shows user-customized alarm information. Learn more in the 'Alarm Analytics' section of this Application Note.*
- *The Alarms tab shows an expanded view of the alarm panel with further detail on current and historical alarms as follows:*



Start Time	End Time	Message	Device	Child	Grandchild	Duration	Status	Owner	Ticket Number
May 11 11:29 AM		Voice Quality below threshold.	vMCD Tik	VQ & Packet Loss		2m 21s	New		
May 11 10:44 AM		Voice Quality below threshold.	MiVB_Customer	Interface Trunk Missing Set		47m 19s	New		
May 10 8:19 AM		SNMP unreachable	Teleworker_Gateway	VQ & Packet Loss		1d 3h 12m	New		
May 10 8:19 AM		SNMP unreachable	AutoCaller	Interface Trunk Missing Set		1d 3h 12m	New		
May 10 7:26 AM		10.0.2.42 IP SLA Packet Loss threshold exceeded.	systemProbe			1d 4h 4m	New		
May 9 6:21 AM	May 10 7:25 AM	*10.0.2.42 IP SLA Packet Loss threshold exceeded.*	systemProbe			1d 1h 4m	Cleared		

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



Alarms Filtering

The ability to filter alarms effectively makes it easier to see the problems that are most important to you. Device and container dashboards contain alarm filter buttons above the Alarms panel.

The filter buttons on the left display the number of Indeterminate, Warning, Minor, Major, Critical and Hidden alarms. Clicking a filter button controls whether or not those types of 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. 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 Management Options

Mitel Performance Analytics offers several alarm management options, to help you declutter your Alarms panel and focus on the alarms that you are most interested in.

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.

ICON	NAME	FUNCTION	FOR DETAILS SEE
★	Favorite	Mark the alarm as a favorite	See "Alarm Analytics"
✎	Edit	Edit related alarm information	See "Editing Trouble Management Information" in MPA Online Help.
👤	Assign	Assign alarm to me	See "Alarm Analytics"
🙈	Hide	Hide the alarm	Hiding an alarm increments the **Hidden** filter button located above the **Alarms** panel
👁	Unhide	Unhide or show the alarm	
🔇	Silence	Silence the alarm	Hides all present and future instances of a particular type of alarm, regardless of the type of device that generated it.
🔊	Unsilence	Unsilence the alarm	
✖	Acknowledge	Acknowledge or clear the alarm	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. Alarms that require an acknowledgment have an ✖ icon at the extreme right of the **Alarms** panel of a container dashboard and on the **Alarm Analytics** tab. If an alarm that requires acknowledgment occurs repeatedly, you can acknowledge any instance of that alarm and it applies to all of them.

Threshold Alarms

Mitel Performance Analytics allows you to configure performance thresholds to generate alarms when the thresholds are crossed. This gives you more control over the types of problems you are alerted to, and at what severity level.

Threshold alarms can have the following alarm severities:

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.

To configure thresholds, see 'Threshold Configuration' in the MPA Online Help.

Alert Profiles

Alerts are most effective when they don't get lost in a sea of data. Too many alerts often results in alarm fatigue, and can cause you to miss things that are important. Alert profiles help you manage how, when and to whom alerts are sent, to maximize their effectiveness.

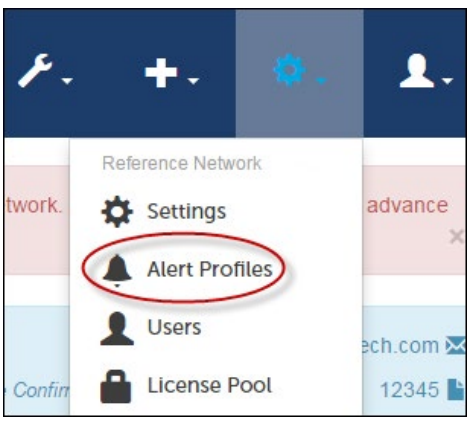
Alert profiles offer the ability to configure the system so it provides notification of an alarm when certain conditions are met. Multiple formats can be used for a single alarm. For instance, you can set up an alert profile so you are notified by email for all major and critical alarms during working 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 will fail with a logged error message. See "Configuring a Twitter Account" and "Configuring a Twilio SMS Account" in MPA Online Help.

Configuring Alert Profiles

To setup an alert profile, complete 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. Detailed instructions to help you are available in MPA Online Help.

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

Note: An SMTP server must be configured to use this functionality. See "Configuring the SMTP Server" in the MPA Online Help.

Desktop: Send notifications to your desktop

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

SMS: Sends an SMS or Text Message Alert

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" in the MPA Online Help.

Twitter: Sends a TwitterTM Direct Message Alert

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" in the MPA Online Help.

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.

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. Besides containing alarm information, the Alert emails summarize the overall status change for the device. The Digest option only applies to email notifications.

Alert Profile Type - Choose Between:

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.

Emergency Notification: All Emergency Response alarms are sent. See "Emergency Response Alarms" in the MPA Online Help.

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.

Alarm Analytics

Alarm Analytics allows you to customize your alarm management environment to help you more easily see the alarms that matter most to you. Mitel Performance Analytics learns 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.

Access Alarm Analytics by clicking the  icon in the top right corner of the Alarms panel to expand it and see its tabs.

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:

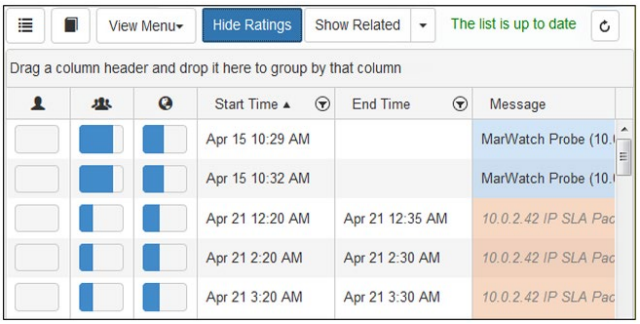
- *The alarm is assigned to you or someone else.*
- *The alarm is assigned a trouble ticket number or a trouble ticket is updated.*
- *You flag the alarm as a favorite.*
- *You click through to a sub-container or device from the Alarms panel of a parent container dashboard.*

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 ( ).



Managing Alarm Labels

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

You can subscribe to a label to tell MPA you are particularly interested in that label, similar to following a Twitter hashtag.

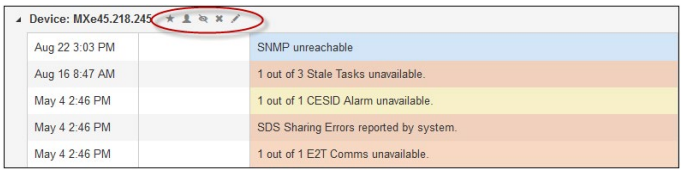
Use the Edit Alarm Information panel to:

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

Label operations require specific user permissions. See "User Permissions" in the MPA Online Help for more information. You can also find detailed instructions on how to manage alarm labels in 'Edit Alarm Information' in the MPA Online Help.

Managing Alarm Analytics Data

To make it easier to manage data and perform actions on groups of alarms, you can filter the alarm analytics tab, to show hidden or cleared alarms. You can also group alarms by device type or severity. Once alarms are grouped, you can perform operations that affect all the alarms that are in the group.



You can also create customized views of your alarm analytics panel and share them.

For detailed information and instructions on managing alarm analytics data and views, consult MPA Online Help.

Displaying Related Alarms

Alarm correlation can accelerate troubleshooting and get you to the source of a problem faster. One way to correlate alarms is by using the Show Related function, to display alarms that occurred at a similar time to an alarm of interest.

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.

For example, 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.

Alarm Queries

Mitel Performance Analytics provides the following initial set of pre-configured alarm queries to help you manage and track the alarms generated by MPA. Here are the query types:

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.

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.

The Alarm Queries can be accessed from the Tools icon, on the main MPA menu.

Learn More

The Mitel Performance Analytics (MPA) software suite helps administrators manage enterprise deployments with multiple network nodes, while allowing partners to proactively detect and address performance issues on customer networks. More information can be found at: mitel.com/mitelperformanceanalytics

Mitel
Powering connections

mitel.com

PG-300737-R1709-EN