Fault Monitoring Overview

Cisco© Prime Infrastructure 3.1
Fault Monitoring Overview Job Aid

© Copyright 2016 Cisco Systems, Inc. All rights reserved.
## Contents

### Basics

- Overview ................................................................................................................................. 1
- Introduction ............................................................................................................................ 1
- Skills ........................................................................................................................................ 2
- Network Operator ................................................................................................................ 2
  - Proficient ............................................................................................................................ 2
- Terms ....................................................................................................................................... 2
- Events and Alarms .................................................................................................................. 2

### Monitoring Faults

- Monitoring Summary Alarm and Event Data ........................................................................ 3
  - Alarm, Event, and Syslog Summaries .................................................................................. 3
    - Application Banner Alarm Summary .................................................................................. 3
    - Metrics Alarm Summary Dashlets ..................................................................................... 7
    - Alarm, Event, and Syslog Summary Data ........................................................................... 9
    - Wireless-Specific Faults and Events ............................................................................... 12
- Monitoring Alarms on Maps ................................................................................................ 15
  - Wired Network Alarm Reporting on Topology Maps ....................................................... 15
  - Wireless Network Alarm Reporting on Site Maps ............................................................ 18
- Monitoring Detailed Alarms and Events Data ..................................................................... 22
- Monitoring Syslogs .............................................................................................................. 24
  - Overview ............................................................................................................................ 24
  - Applying Data Filters ......................................................................................................... 25
  - Monitoring Live Syslog Streams ....................................................................................... 27
  - Reviewing Historical Syslog Data ..................................................................................... 29

### Managing Alarm Reporting

- Overview ................................................................................................................................. 30
- Configuring Alarm Reporting in Alarm Policies ................................................................. 32

### Links

- To Product Information .......................................................................................................... 35
- To Training .............................................................................................................................. 35
- To Contact Us ......................................................................................................................... 35
Introduction

For all of the aspects of the system, Prime Infrastructure reports faults that might be affecting network accessibility, the user experience, or network performance. Network faults include errors, failures, or exceptional conditions on the network or its devices.

Fault monitoring includes collecting all of the syslog events, SNMP trap events, and system-generated events during device polling or when conditions prompt devices to send events to the system.

When conditions or series of events require more attention, for example, key performance indicator values moving outside of their operational thresholds, the system reports that information by using alarms.

Because conditions can return to acceptable, or normal, states without manual intervention, a situation might require more intensive monitoring only. Or, when you see more emergent situations, you can respond to alarms to help mitigate or avoid network issues or downtime.

Administrators configure back end alarm, event, and syslog reporting and clearing behaviors and severities in Administration.
Because fault reporting is a key monitoring feature and can escalate critical changes, Prime Infrastructure reports that information in many areas of the application.

This job aid introduces you to the areas of the application that report aggregated and detailed fault data, including events, alarms, and syslog messages, and to the key method that you use to manage alarm reporting.

### Skills

**Network Operator**

To perform fault monitoring tasks, you need the following experience.

**Proficient**

- Prime Infrastructure user interface navigation and behaviors
- Networking concepts and practical networking experience

### Terms

**Events and Alarms**

An event is a separate incident occurring on the network or on a device at a distinct point in time and includes those incidents that indicate a return to acceptable, or normal, conditions.

An alarm is the method of escalation that the system uses to report that a single event, or a series of correlated events, requires more or immediate attention.

The system references its events and alarms catalog to associate events to alarms and to indicate the severity of incident conditions. When an alarm is active and a new event of the same type occurs from the same source, the system associates that event with the active alarm.

**Note:** For more information on event and alarm concepts, refer to the Cisco Prime Infrastructure 3.1 User Guide.
Monitoring Faults

Monitoring Summary Alarm and Event Data

Alarm and event reporting is a key method by which Prime Infrastructure alerts you to changing conditions on the network and its devices that might require additional monitoring or more immediate attention.

The system reports summary alarm and event information:

- In the Alarm Summary list.
- On metrics and dashboard dashlets.

Alarm, Event, and Syslog Summaries

Application Banner Alarm Summary

To call attention to alarms that are occurring, the system provides an alarm indicator on the application banner.

To open the list of alarms:

- Click the alarm indicator.
The banner indicator displays the total number of alarms of the highest severity that are currently active for the categories that you enabled in your user preferences.

The list contains all of the alarm categories that you have enabled in your preferences and their associated numbers of alarms based on severity level.
To review all of the alarms that are currently active for a category:

- In the **Alarm Summary** list, click a category link.

The **Alarms** page opens and lists all of the alarms that are currently active for the category, and the **Alarm Summary** list remains open.
To review all of the alarms of a specific severity in a category:

- In the **Alarm Summary** list, in the category row, click a severity number link.

![Alarm Summary screenshot](image)

The **Alarms** page opens and lists all of the alarms in the category and of the severity that you selected, and the **Alarm Summary** list remains open.

![Alarms page screenshot](image)

To review all alarms:

- Below the **Alarm Summary** list, click **View Details**.

![View Details button](image)
The **Alarm Summary** closes and the system opens the **Alarms** page.

---

**Metrics**

**Alarm Summary Dashlets**

On the **Network Summary** dashboard, on the **Overview** and **Incidents** tabs, in the **Metrics** section:

- The **Alarm Summary** dashlet summarizes the number of critical, major, and minor active alarms.
- The **Rogue Alarms** dashlet summarizes rogue access points that are connecting to the network.

---

**Note:** The color-coding of each severity in the dashlets changes from green to the severity level indicator color, such as red for critical alarms, when alarms of that severity are occurring.
To review alarm details, in the dashlet, in the severity category:

- Click the number link.

The **Alarms** page opens and lists all of the alarms in the category and of the severity that you selected.

![Alarm Summary](image)

![Alarms Page](image)
Alarm, Event, and Syslog Summary Data

For an overview of fault and event metrics and alarms, refer to the Network Summary | Incidents dashboard.

You can review:

- Alarms organized by count or type.
- Events organized by type.
- Syslogs organized by severity or type.
- The senders that are sending syslogs most often.
To navigate to a page that presents detailed alarm, event, or syslog information:

- Beside the dashlet title, click **View Details**.

The **Syslog Watch** dashlet indicates the type of syslog that it is actively reporting in a link below the zoom tool. You can change the reported syslog type based on your specific monitoring needs.

To indicate the type of syslog that you need to monitor:

- On the dashlet tool bar, click **Edit**, in the **Syslog Type** drop-down list, select the category of syslogs that you need to monitor, and then click **Save**.
To review the list of syslogs that a category is reporting:

- Below the Zoom tool, click the category list.

The system navigates to the Syslog Viewer page | Historic tab. The Show drop-down list indicates the filter that is active.
Wireless-Specific Faults and Events

For an overview of wireless-specific fault and event metrics and alarms, refer to the Wireless | Security dashboard.
On the **Wireless | Security** dashboard page, dashlets report alarms related to:

- Rogue, or unauthorized, access points.
- CleanAir security, which indicates devices that pose potential security risks in the shared wireless spectrum.
- Network attacks detected by a Cisco Adaptive Wireless Intrusion Prevention System (adaptive wIPS).
- Management Frame Protection (MFP) attacks, which report the numbers of attacks on 802.11 management messages that are passed among access points and clients, which can indicate various types of attack attempts.
To review alarm details, in a dashlet table:

- Click the number link.

The system navigates to the **Alarms** list, which is filtered to report the related alarms.
Monitoring Alarms on Maps

Wired Network Alarm Reporting on Topology Maps

Topology maps display alarms that are occurring on the wired portion of the network that the map represents and associates them to the devices or links that are generating the alarms.

Network topology and data center maps are organized in similar layouts and provide similar tools.

Note: For more information on data center topology concepts and maps, refer to the Wired Network Summary Data Overview job aid.

When reviewing alarms on a location group level, the group icon displays the most severe alarm level occurring at the location, which helps you to recognize potential problem areas on the network.

Color-coded indicators illustrate alarm severity.
On the network topology or data center map, to evaluate alarms that are occurring at a network location:

- On the map, click the location icon, and then click **Drill Down Group**.

The map refreshes to display the devices at the location and their relationships to each other.
To evaluate the alarms that are occurring on a device:

- On the map, click the device icon, and then click **View 360**.

The **360° View** pop-up window opens. You can review performance statistics and alarm details, navigate to detailed device data, or take action on the device.

**Tip:** When you are evaluating alarms on a network topology map, you also can refer to the **Alarm Summary** list.

In the list, you can navigate to a list of the alarms based on their severity levels.

*Continued on next page…*
Or, you can open a separate browser window that lists all of the alarms indicated in the summary.

Wireless Network Alarm Reporting on Site Maps

Wireless site maps display alarms that access point radios are reporting in broad and more specific views.

To review alarms at a campus, building, or floor level:

- In the **Maps Tree View** list, expand a location entry, and then click the location that you want to see in detail.

  OR

- In the **Site Maps** list, click the location name link.

  The system opens the site, building, or floor view.
Campus / site views indicate alarms by using color-coded frames around buildings. The color code indicates the alarm of the highest severity occurring in the building.

On the Campus/Site View page, to review alarms at a building level:
- Click the location name link.
  - The system opens the Building View list, which displays each floor separately and includes a diagram of the floor and AP radio alarm overall status.

On the Building View page, to review alarms occurring on a floor:
- Click the diagram.
The system opens the **Floor View** page, which displays a visual representation of the wireless infrastructure overlaid on the floor’s layout. You can select the information that you want to see in the **Floor Settings** panel, such as:

- AP device locations and statuses.
- AP signal strength.
- Air quality.
- Interferers.
The map applies color code to the AP icons to indicate AP radio or AP device status.

To display AP radio or AP device status:

- In the Floor Settings panel, click the arrow beside Access Points, and then, in the AP Filter pop-up window, click the applicable Show option button.

The icon color coding indicates the most critical alarm severity level based on the status that you are monitoring.

In the following example, when monitoring the AP-Paris device status, the icon indicates that critical alarms are occurring on the device. When monitoring the same device’s radio status, the icon indicates that warning alarms are occurring for the radio.

To review all of the alarms that an AP device and radio are generating:

- Click the AP radio icon.

The system opens the 360° View pop-up window. You can see all of the radio and device alarms on the Alarms tab and take actions, as needed.
Monitoring Detailed Alarms and Events Data

The **Alarms and Events** page provides an alternate method for monitoring the network for potential issues, providing flexibility to monitor devices by:

- Their types or locations.
- Categories that system users have organized.
- Alarm severities.

Various application areas, including dashboards and maps, provide navigation to the **Alarms** pages.

When you use that navigation, the system filters the list based on the category and type of alarm that you clicked to access the page.

![Alarm Summary](image)
When you begin working to resolve conditions causing an alarm, you can acknowledge the alarm, or assign it to yourself or someone else for further investigation.

To assign an alarm to yourself or another system user for monitoring, evaluation, or troubleshooting:

- On the Alarms tab, select the alarm that requires attention, and then, in the Assign drop-down list, select the applicable assignment.

You also can define device groups to best support your monitoring tasks. For example, you might define a group that includes all of the devices that you monitor regularly.

You can define custom user groups on the Network Device Groups page.

Then, on the Alarms and Events page, you can select the group to filter the lists to display alarms, events, and syslogs for the devices in that group only.
Monitoring Syslogs

Overview

Devices generate syslog messages to report events and changes that are occurring on them. For certain device syslogs, Prime Infrastructure generates alarms by default.

In most cases, you need to use the syslog viewer to see all of the syslog messages that the system is receiving from devices. Monitoring incoming syslogs can help provide insight into device and network conditions in addition to those that are generating alarms.

You can review incoming syslogs on the **Syslog Viewer** page, which color codes message severity levels.

On the **Historic** tab, you can review asynchronous syslogs that the system captures when device events or changes occur.

On the **Live** tab, you can monitor incoming syslogs in real time for up to 10 devices that have debugging running, which can help you identify current or ongoing issues.
Applying Data Filters

The syslog viewer provides two filters on the Live and Historic syslogs tabs, located above and below the toolbar. When filter criteria are applied, the filter buttons display yellow color-coding.

The filter criteria change based on whether you have the Live or Historic tab active on the page.

**Important Note:** To help ensure that you are seeing the syslogs that you need, verify that the combination of filter settings includes them.

The filter criteria that you apply do not persist when you navigate away from the syslog viewer.

On the Live tab, you can select the location and device or devices for which you need to stream syslogs in real time.

On the Historic tab, you can display syslogs by location groups.
The **Show** drop-down list below the toolbar on each tab provides a second filter for the page data.

On the **Live** tab, you can filter incoming syslogs by severity level or configure specific filter criteria.

On the **Historic** tab, you can filter by syslogs by time period, severity level, or device condition.
Monitoring Live Syslog Streams

When debugging is running on a device for which Prime Infrastructure is a syslog receiver, the system immediately begins collecting the syslogs that the device generates and presenting them on the Live tab on the Syslog Viewer page.

This live streaming syslog feature supports reporting for up to 10 devices at a time.

Note: When devices are not generating syslogs, the page can appear blank.
You can configure the system to aggregate and report duplicate syslog messages as a single line item that totals the number of like messages that it is receiving, which can make it easier to review the messages in the list.

**Note:** When deduplicating messages, the system aggregates system messages on a system user level.

To report duplicate syslog messages as a single line item:

- On the toolbar, click **De-duplicate**.
  
The system adds the **Count** column and begins aggregating the same syslog messages automatically.
**Reviewing Historical Syslog Data**

On the **Historic** tab, you can review asynchronous syslogs that the system captures when device events or changes occur.

This information can provide insight into such network activities as configuration changes, high momentary error rates, or sustained abnormal conditions that other types of monitoring might not indicate.

**Tip:** By default, the system generates events based on a system-defined list of syslogs.

By using the **Custom Syslog Events** feature, you can configure the system to generate an event for a syslog that it is reporting or add a custom syslog for which you want the system to report an event.

When you save the event, the system begins reporting it the next time that it receives the associated syslog.

Configuring syslogs to report events can help support issue escalation for a network activity or condition and to meet business or operational requirements.
Managing Alarm Reporting

Overview

Prime Infrastructure identifies changing network conditions by collecting and evaluating events from network devices. When these events indicate conditions that are falling outside of operational thresholds, the system generates alarms in varying severities to bring attention to these situations.

To manage the alarms that the system reports, Prime Infrastructure provides default alarm policies associated with specific device types or components. These policies manage the types and severities of events that generate alarms and apply to device or port groups that system users can configure.

Note: Administrators can configure global settings that control back end alarm behaviors, such as the time intervals in which the system clears or drops alarms, or alarm display behaviors.

Alarm policies are a separate mechanism that allows you to control whether the system reports or suppresses specific alarms based on device type and device or port group, and applies to all areas of the application that report alarms.

Alarm policies report events that are occurring on the following device components or types:

- Device interfaces
- Wireless access points
- Wireless LAN controllers
- Layer 2 switches
- Wired infrastructure, which reports alarms related to physical component conditions, such as environment temperatures or fan conditions
By default, alarm policies apply to all of their configured events. You can manage alarm reporting behaviors by:

- Suppressing specific alarms or suppressing alarms on groups of devices or ports.
- Changing alarm severity levels.
- Configuring automated alarm clearing time periods.

By configuring the system to escalate only those alarms of importance to the enterprise helps system users to identify issues or take prompt action, as needed.

**Important Note:** When you configure alarm policies, those policies apply only to those devices or components that are available in the virtual domain in which you are working.

Other users working in the same virtual domain will see the alarm behaviors that you configure in the alarm policy.
Configuring Alarm Reporting in Alarm Policies

You can review alarm policy details to determine whether you want to make any changes.

To review alarm policy details:

- In the Alarm Policies list, click the Policy Name link.

The policy overview lists:

- The events included in the policy and the alarm severity level assigned to each event.
- The device or port groups, depending on the policy type, for which the system will generate alarms.
To edit policy details:

- Below the page title, in the page description or below the application banner, click **Edit Policy**.

For events, you can:

- Activate or suppress alarms.
- Change alarm severities.
- Configure the time interval in hours after which the system clears the alarm automatically.

**Tip:** For detailed information on what events are reporting, beside the page description, point to the information button, which opens a pop-up window that describes what each event is reporting.
For device or port groups, which are available based on the policy that you are configuring, you can select a category and activate or suppress alarms for all of the devices in that group.

Or, you can expand a category and activate or suppress a device type-specific alarm.

To apply the alarm policy configuration:

- Click **Save & Activate**. The alarm policy configuration applies immediately to the virtual domain in which you configured the policy.

**Important Note:** You can apply only one alarm policy to each event in a policy category. For example, in the **Interface** category, for a switch or router link down event, you can either activate or suppress the alarm, apply a single severity level, and configure a single automated alarm clearing time interval.
## Links

### To Product Information

- Visit the Cisco Web site to learn more about Cisco© Prime Infrastructure.
- Visit the Cisco Web site to review or download technical documentation.

### To Training

- Visit the Cisco Web site to access other Cisco© Prime Infrastructure learning opportunities.
- Visit the Cisco Web site to access learning opportunities for other Cisco products.

### To Contact Us

Send us a message with questions or comments about this job aid.