Data Collection Concepts

Cisco© Prime Infrastructure 3.1

Job Aid

Copyright Page

Data Collection Concepts Job Aid

Contents

Basics

Overview

On initial installation, Cisco© Prime Infrastructure does not populate network data until it connects to and adds network devices to its inventory.

The system uses a variety of data collection methods based on data type, licensing, and the data collection functionality that is enabled based on network configuration to report data on:

- The device inventory and device configuration.
- Network and device performance metrics.
- Application usage and metrics.
- The wireless network.
- Clients and users detected on or using the network.
- Network and device faults and events.

This job aid introduces you to Prime Infrastructure data collection processes, which helps you to recognize how the system reports monitoring data, performance metrics, application usage, and faults and events, among other information.

Recognizing these processes also can help configurators and administrators ensure that system users see the data that they need for effective network monitoring and management.

Notes: For information on where the system reports data, refer to the Prime Infrastructure 3.1 overview job aids.

For information on data collection processes for the data center, refer to the Prime Infrastructure 3.1 **Data Center Monitoring Overview** job aid.

Skills

Network Operators, Configurators, and Administrators

To understand data collection concepts, you need the following experience.

Proficient

- Prime Infrastructure user interface navigation and behaviors
- Networking concepts
- Practical network management experience

Terms

Automonitoring Policies

Monitoring policies that begin collecting critical network and system health metrics after initial inventory data collection automatically

Note: For more information, refer to the **Automonitoring Policies** topic.

Device Discovery

A process that Prime Infrastructure uses to connect to and add new devices to its inventory

Device Profiling

A process that allows wireless LAN controllers to act as collectors of information that identify client types when clients are detected by the controller

Administrators must enable device profiling on wireless LAN controllers.

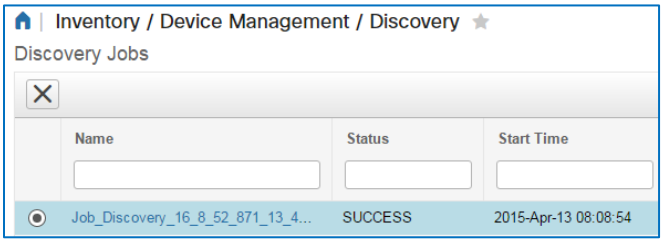
How Does Prime Infrastructure Collect…

Device Inventory and Device Data?

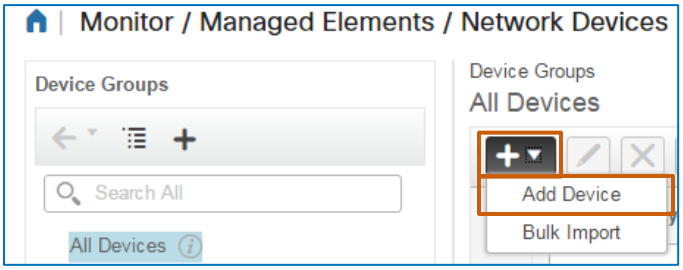
Initial Device Discovery

On initial installation, Prime Infrastructure does not populate network data until it connects to and adds network devices to its inventory. System users can use several methods to perform discovery, including:

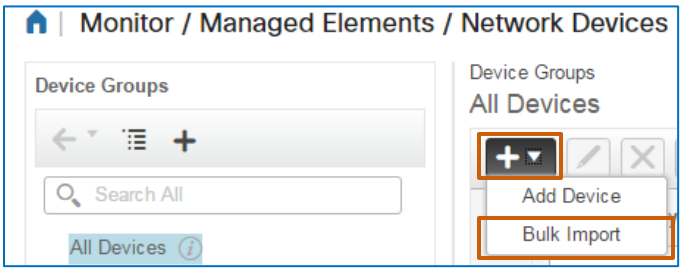
- Running device discovery jobs.



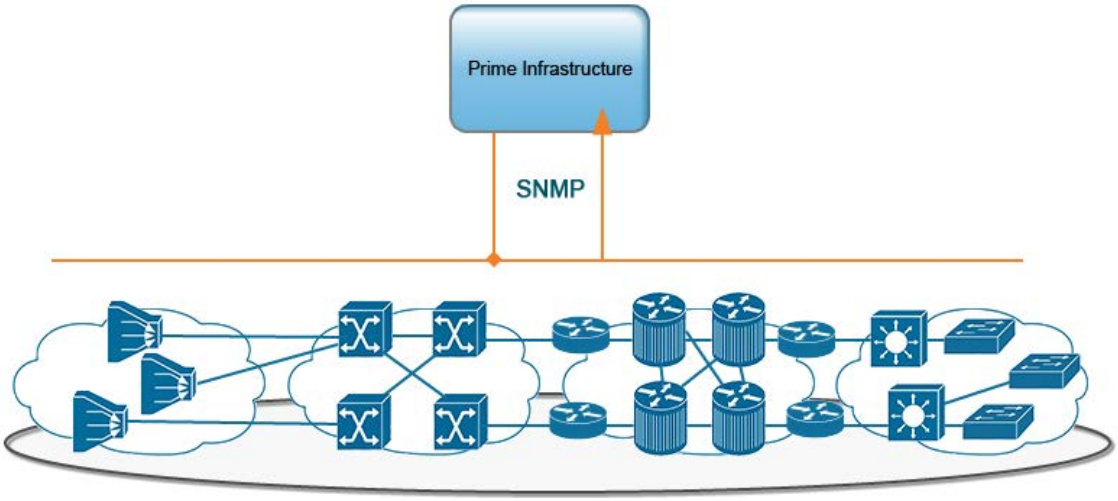
- Adding devices manually.



- Importing device information from another system or from a CSV file by using the bulk import feature.

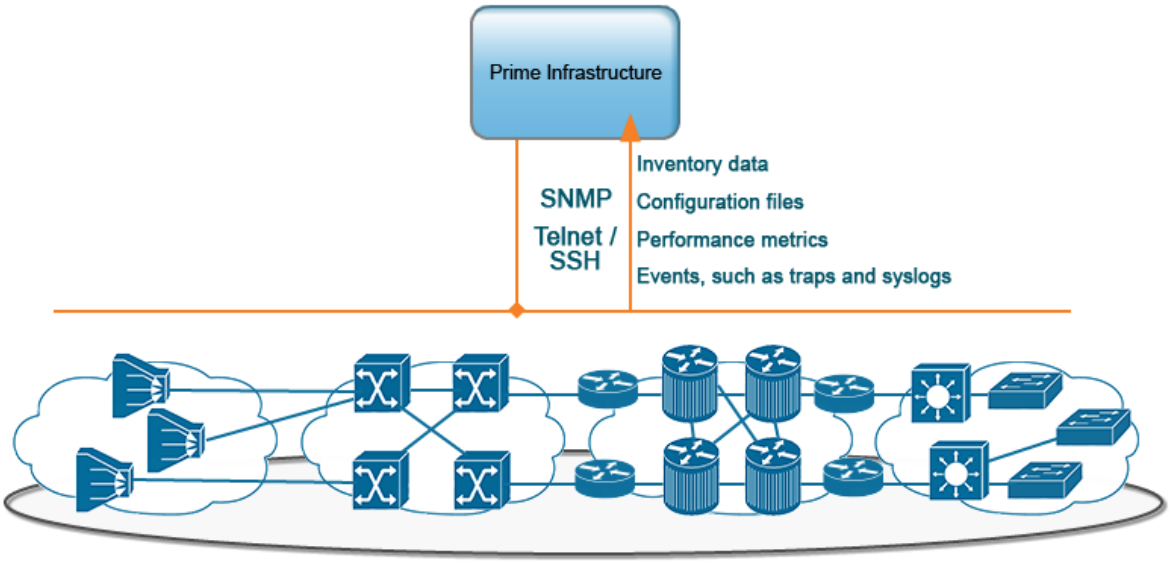


Prime Infrastructure performs device discovery by using the Simple Network Management Protocol (SNMP).



Initial data collection activity occurs after the device discovery process is completed. At that point, Prime infrastructure uses the SNMP and Telnet/SSH protocols to collect:

- Inventory data
  Including hardware and software components and information on the features and technologies that are active on the device.
- Configuration files
  Including the running and startup configurations, and the VLAN database configuration, if applicable.
- Performance metrics.
- Events, such as traps and syslogs.



Automonitoring Policies

After initial inventory data collection, the system begins collecting critical network and system health metrics by using the automated monitoring policies, referred to as automonitoring policies, which come with the system.

These automonitoring policies define the parameters and operational thresholds that the system will follow during data collection. By applying automonitoring policies, Prime Infrastructure does not require configuration to start collecting and reporting key health data.

Automonitoring policies report the device health metrics of:

- Routers.
- Switches.
- Hubs.

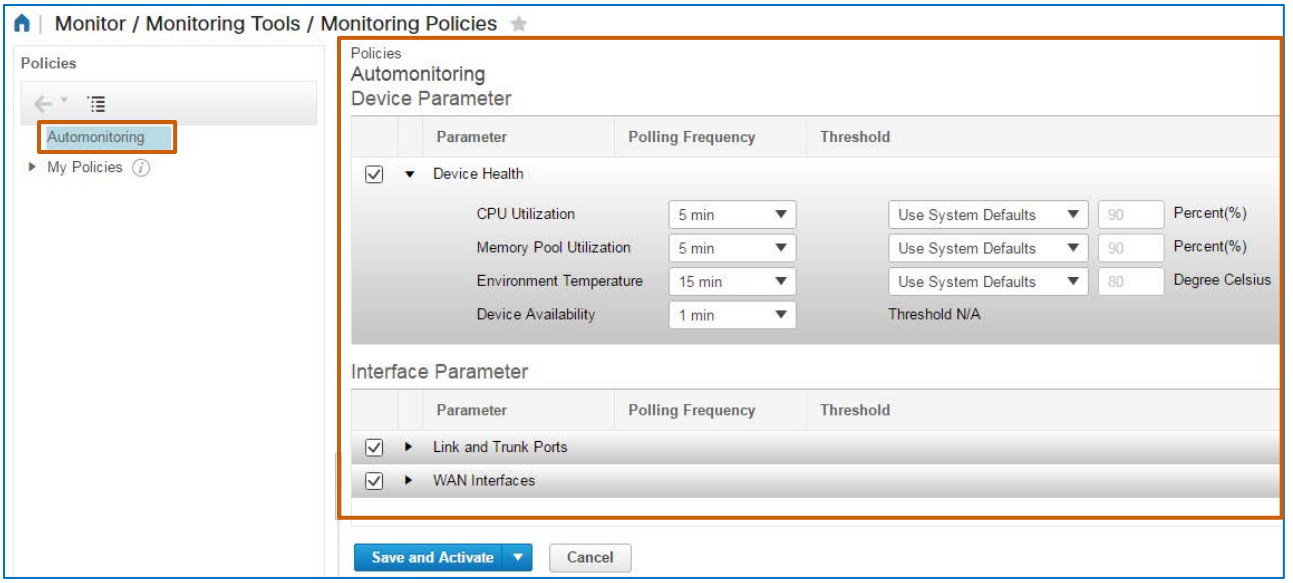
The interface health metrics of:

- Link and trunk ports.
- WAN interface groups.

Note: To begin collecting data on wireless LAN controllers, you need to add and activate a custom monitoring policy.

Based on the polling time intervals, or frequencies, defined in the policies, the system begins reporting the data that it is collecting.

System users can change the reporting thresholds and polling frequencies of automonitoring policy parameters to meet business or operational requirements.



The data that the automonitoring policies collect is available in various areas of the application, including:

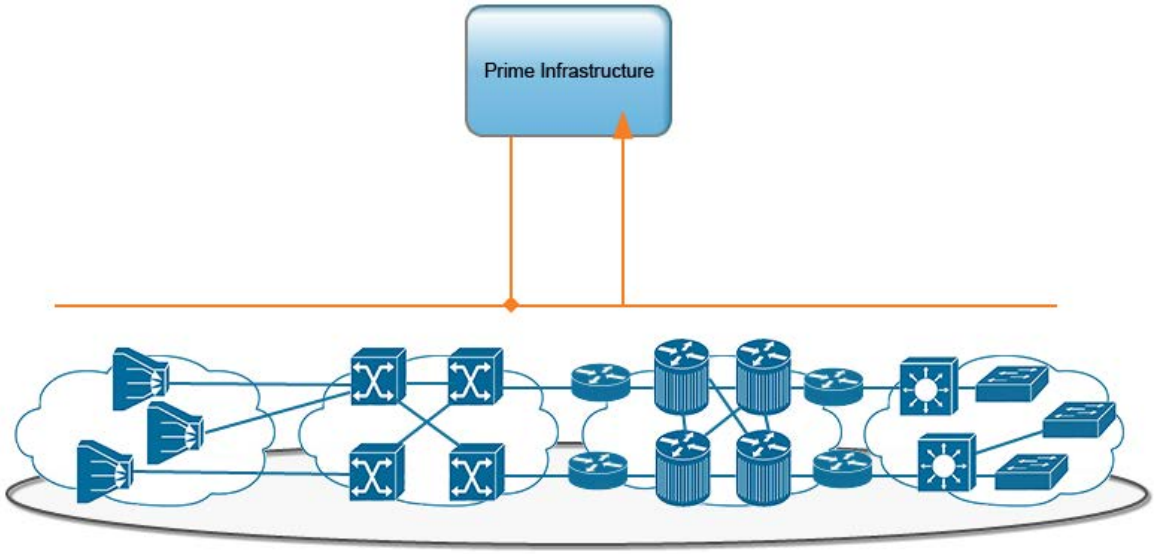
- Dashboards.
- Alarms and events.
- Reports.

Ongoing Device Polling

Device polling is the process by which the system continues to collect device data after initial device discovery.

Device polling uses the automated monitoring policies that the system activates during the device discovery process for data collection.

Polling also follows the custom monitoring policies that system users must configure to help ensure that Prime Infrastructure is collecting all of the data that is necessary to perform effective network monitoring and management.

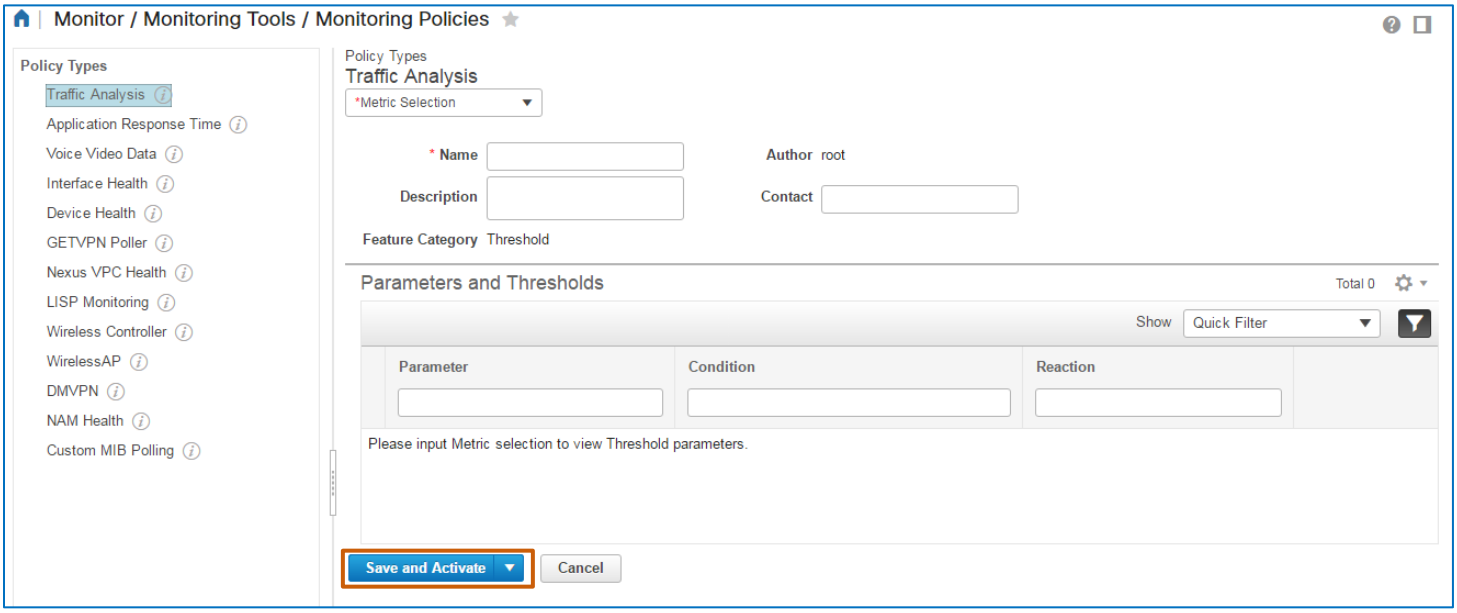


Additional Metrics, Data, and Changing Conditions?

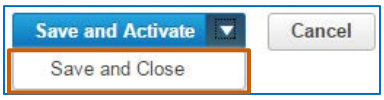
Custom Monitoring Policies

To begin collecting data that meets enterprise requirements, system users need to configure monitoring policies for all of the data categories for which they need information, such as application response time or voice and video data, for example.

Important Note: In addition to the data that automonitoring policies collect, Prime Infrastructure only collects data for custom monitoring polices that a system user has configured and activated.



Note: System users also can save custom monitoring policies and activate them later.



Key monitoring policies that you can configure include:

- Traffic analysis.
- Application response time.
- Voice and video.
- Interface health, in addition to the data that automonitoring policies collect.
- Device health, in addition to the data that automonitoring policies collect.
- Nexus Virtual Port Channel (VPC) health for Nexus, which monitors whether VPCs are configured correctly.
- Wireless LAN controllers.
- Wireless access points.

- Dynamic multi-point VPN metrics.
- Network analysis module (NAM) health metrics.
- Custom MIB polling, which collects third party device features, or Cisco devices and device group features, for which the system does not provide monitoring policy types.

Note: For information on how to configure custom MIB monitoring policies, refer to the **Cisco Prime Infrastructure 3.1 User Guide**.

In all monitoring policies, the parameters and thresholds that you define to collect statistics or report changing conditions are completely configurable.

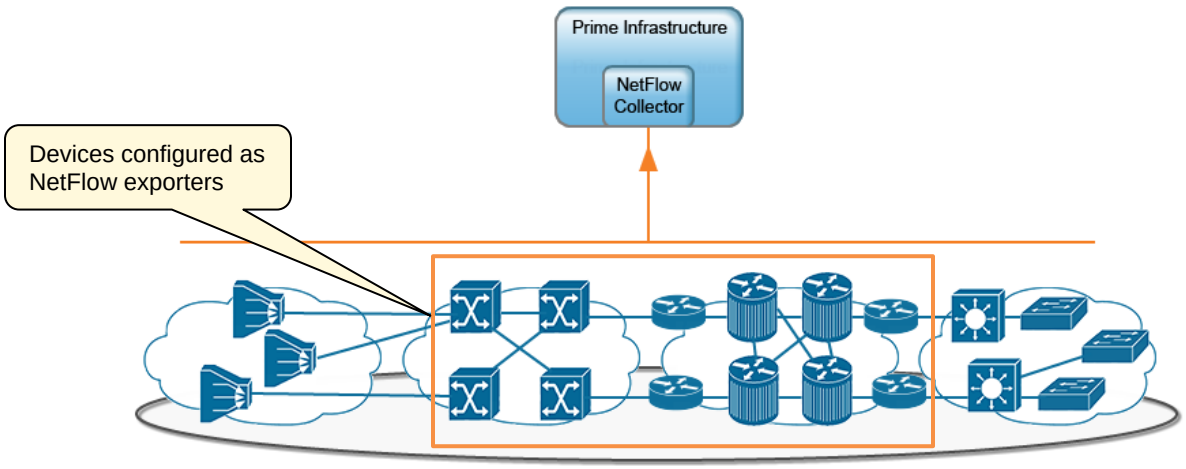
Application Traffic Data?

The NetFlow Protocol

Overview

Prime Infrastructure uses the NetFlow network protocol to collect IP traffic characteristics from devices, which indicate how and where application traffic is traversing the network.

To support NetFlow reporting, devices are configured as NetFlow exporters so that they can send data to Prime Infrastructure. The system then captures the information in its embedded NetFlow collector.



Ensuring Application Traffic Reporting in Dashlets

NetFlow data sources, including devices and interfaces, require NetFlow templates in order for Prime Infrastructure to report application and traffic data successfully.

NetFlow templates define the flow data that the data sources export automatically at defined intervals to Prime Infrastructure's NetFlow collector.

The collector then assembles, combines, and reports the flow data in various dashlets.

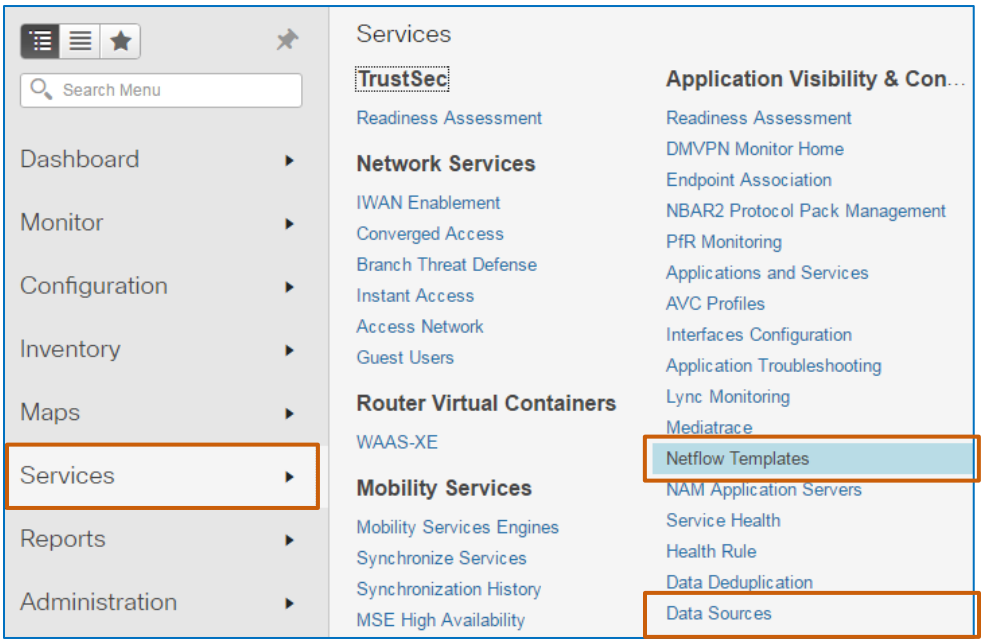
Important Note: For successful data reporting in dashlets, data sources must support NetFlow and have NetFlow templates configured for data exporting.

To determine whether a data source supports Netflow, refer to the technical documentation for that specific device.

When a dashlet is not reporting the data that you expect to see, you can:

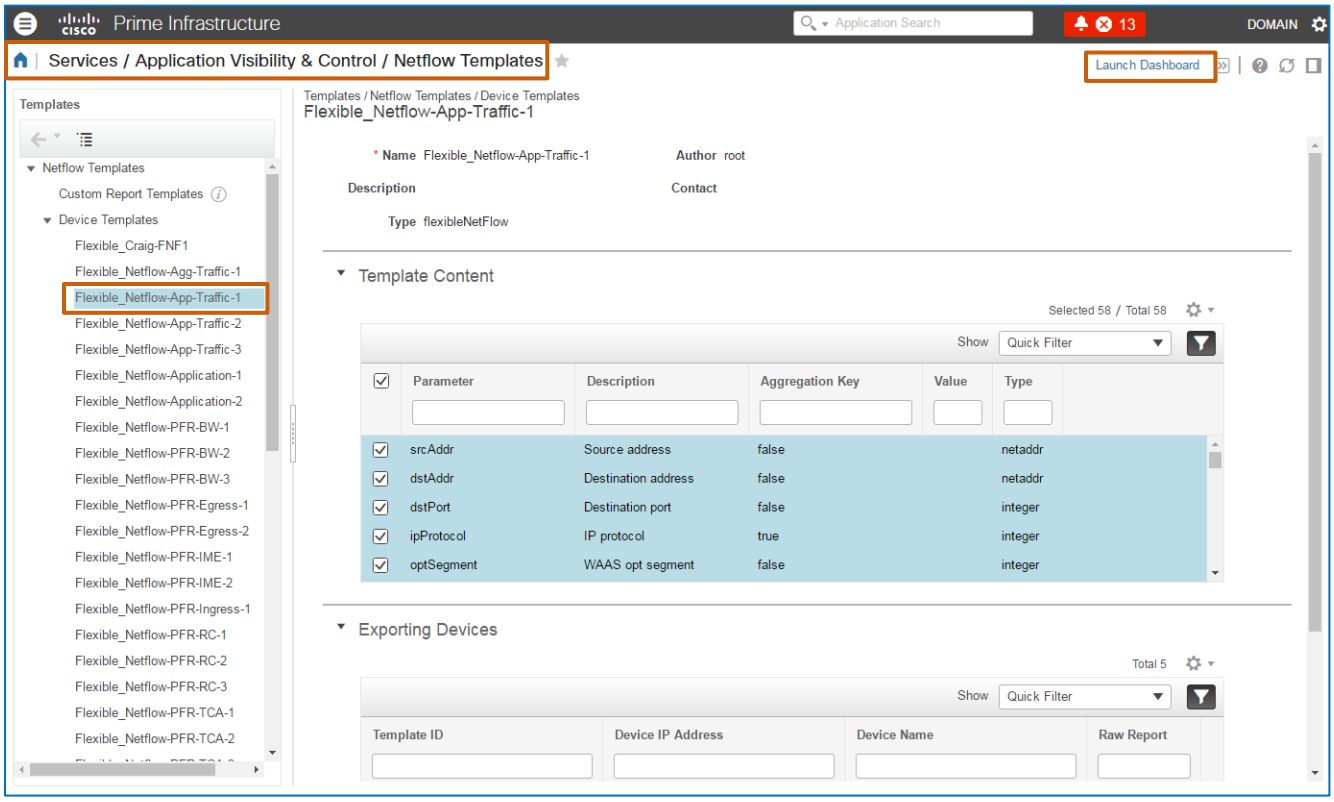
- Identify which NetFlow template collects the data that you need.
- Determine whether the template is available on the data source that you need.
- If the template is available on a device, determine whether the data source is sending that template, as expected.

The NetFlow template and data source information is available on the **Services** menu, under **Application Visibility & Control**.

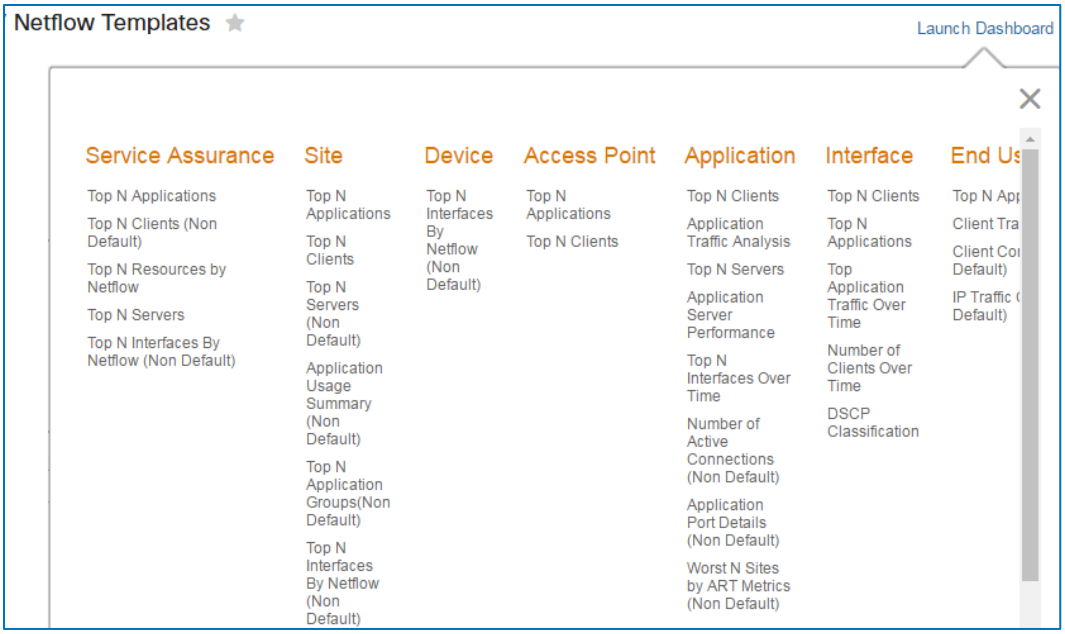


To identify which NetFlow template collects the data that you need:

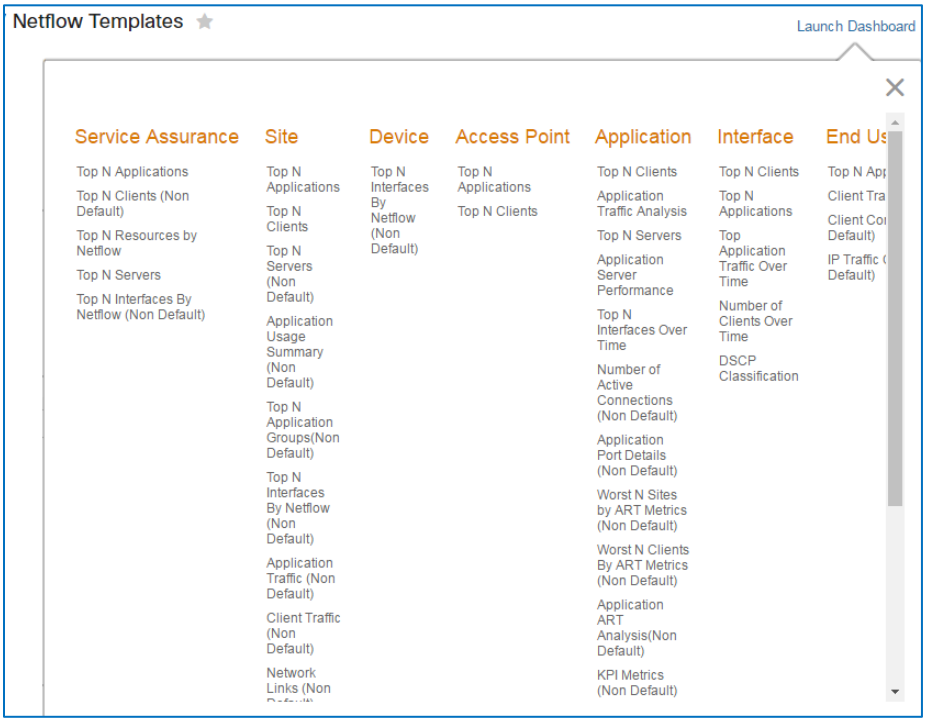
1. On the **Netflow Templates** page, in the **Templates** list, under **Device Templates**, select the template that you need to investigate.
2. Below the application toolbar, click **Launch Dashboard**.



The system opens a pop-up window that lists the dashlets, categorized by dashboard, that the template populates with data.

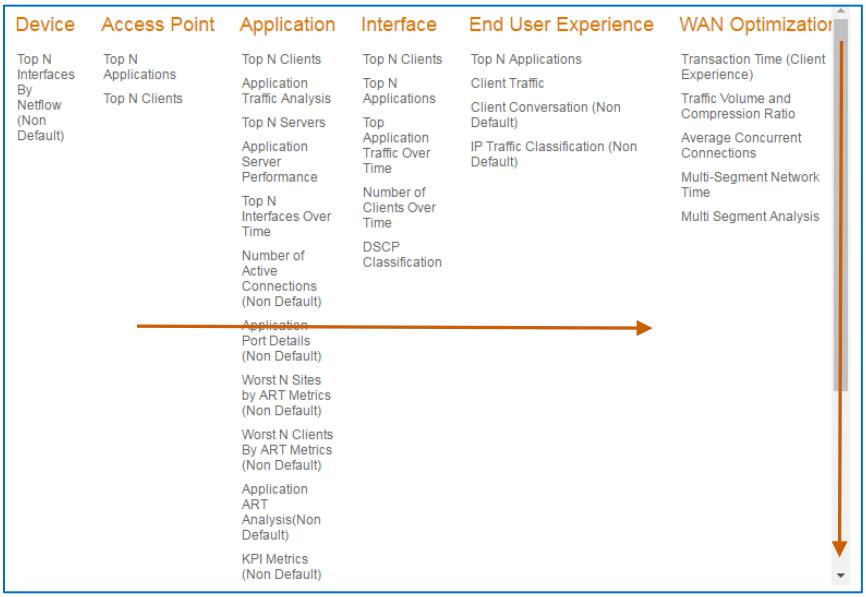


3. To identify the dashlet with missing data, in the pop-up window, review the lists of dashlets that the template populates.



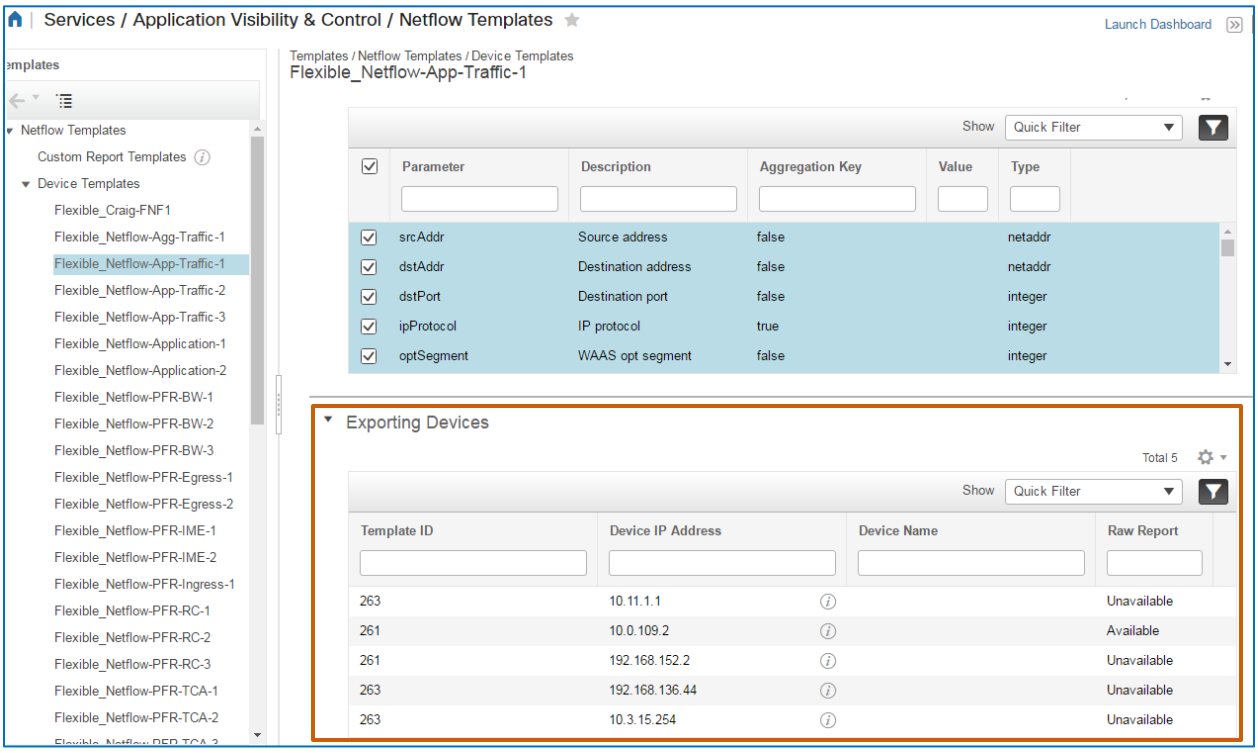
Tips: In the pop-up window, you can click a dashlet listing to navigate to the dashlet location.

To see additional categories of dashlets, in the pop-up window, drag the pointer to the right or scroll, as needed.



To determine whether the template is available on the data sources that you need:

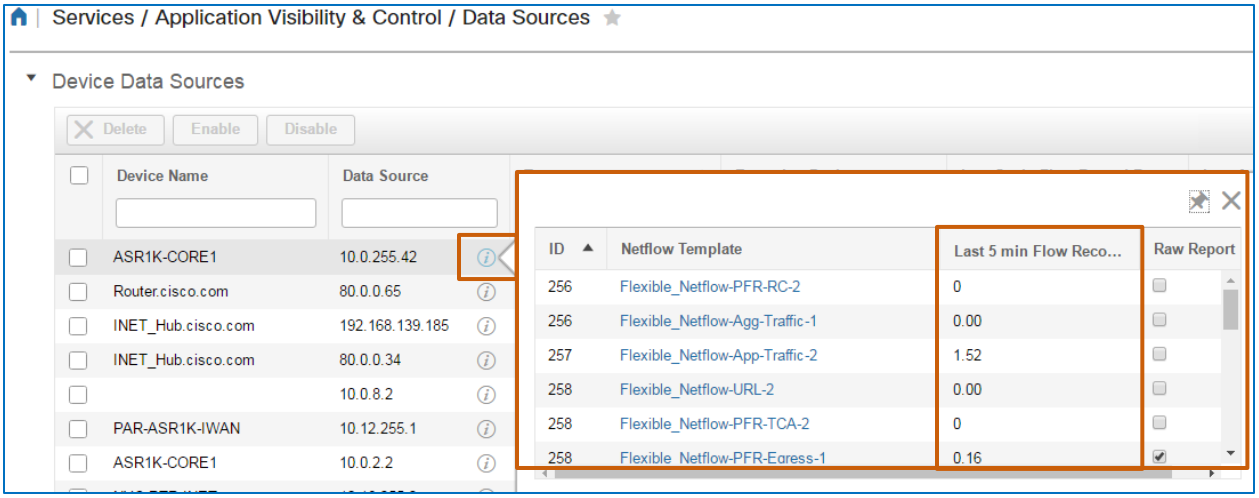
1. On the **NetFlow Templates** page, in the **Templates** list, under **Device Templates**, select the template that you need to investigate.
2. To determine whether the data source has the template, in the **Device Templates** page, under **Exporting Devices**, review the list of device IP addresses.



To determine whether the data source is sending the applicable template:

- On the **Data Sources** page, in the **Device Data Sources** list, find the data source, and then click the **Data Source** information button.

  The pop-up window lists each NetFlow template on the device and its last five minute flow record rate, which is populated with a record rate when the device is sending that template's data, as expected.



If no record rate appears in the **Last 5 min Flow Record** field, the associated template is not sending data. If you continue to see no data reporting over a period of time, you can evaluate the data source to determine whether:

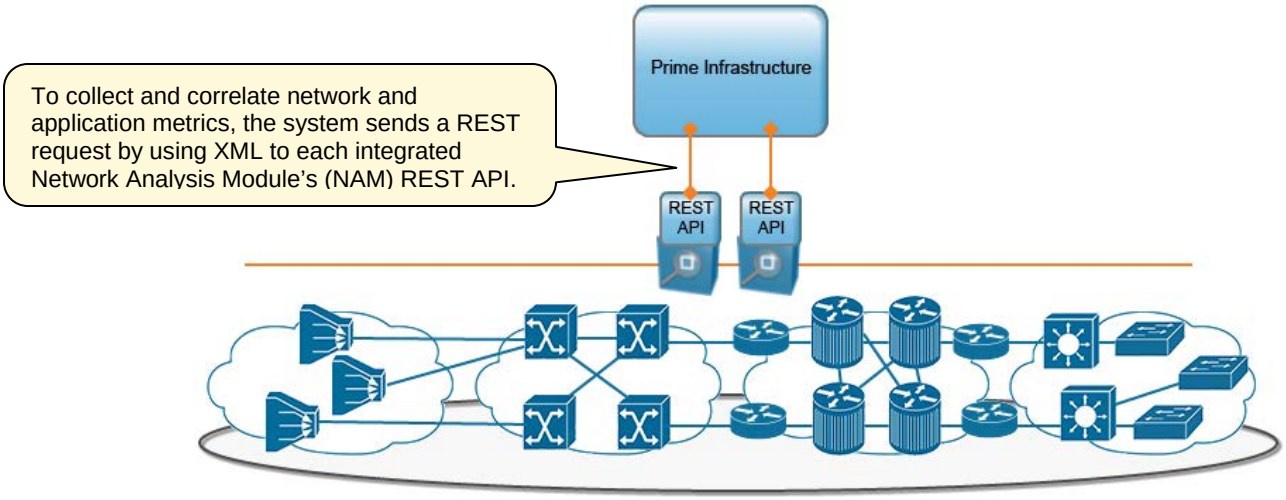
- The device supports NetFlow.
- The template is available on the device.
- The template is configured and is being sent by using NetFlow on the device.

Integrated Network Analysis Modules (NAMs)

Network Analysis Modules (NAMs) collect detailed traffic movement analysis data, including application response time and bandwidth usage metrics, which provides deeper insight into application traffic patterns and changing conditions.

When the network configuration integrates network analysis modules, or NAMs, Prime Infrastructure can collect and correlate network and application metrics calculated by the NAMs.

To collect data, the system sends a REST request by using XML to each NAM's REST API.



Network Based Application Recognition (NBAR) Technology

To recognize applications on which the system is reporting more easily, Prime Infrastructure uses the Network Based Application Recognition (NBAR) technology that is embedded in routers, controllers, and NAMs.

NBAR engines on these devices execute deep packet inspections (DPIs) to:

- Recognize applications.
- Send the system application identifiers and application metrics from routers, controllers, and integrated NAMs.

General Clients and Users Data?

The Device Profiling Process

Wireless LAN controllers perform the device profiling process to determine the type of client that is connecting to the network and whether the client has current security settings. It also determines whether client applications meet network access criteria.

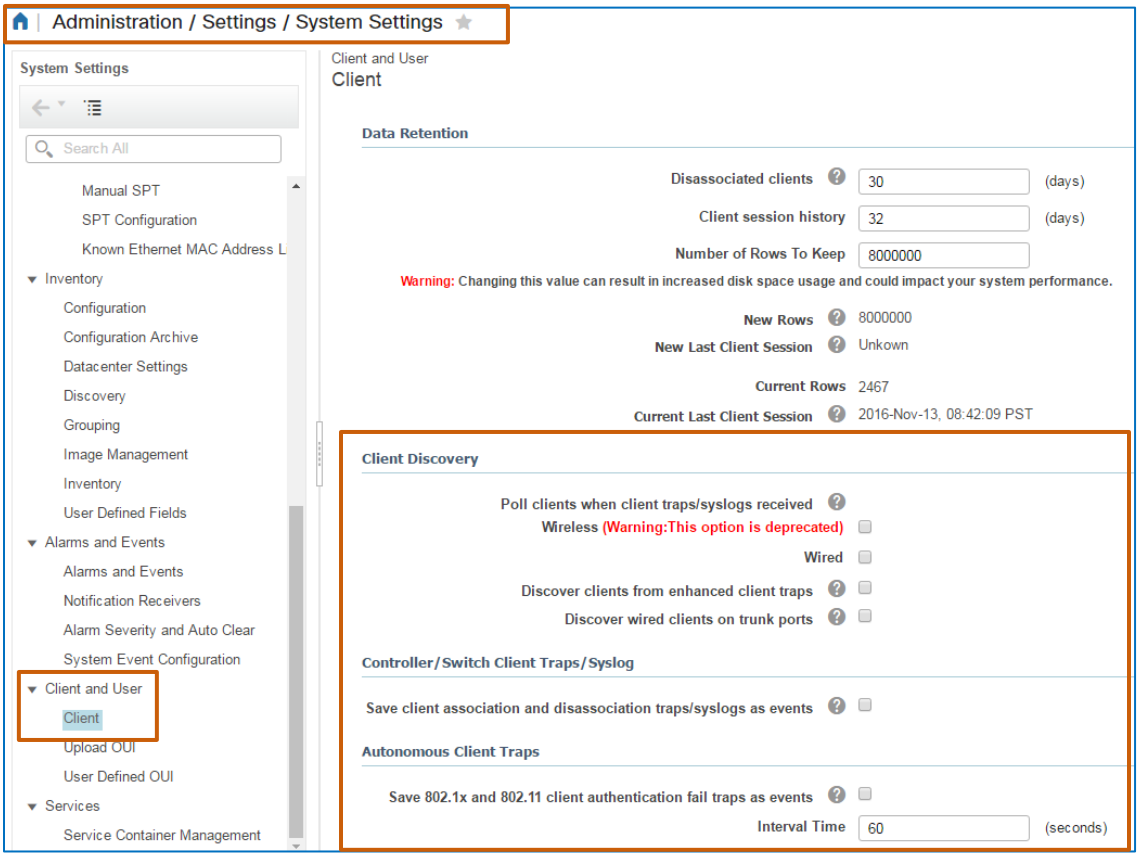
With this information, you can:

- Determine an end user's network session status.
- Identify possible problems with the end user's authentication or authorization for network access.
- Monitor and troubleshoot user applications and site bandwidth usage.

When integrated with Prime Infrastructure, Cisco Identity Services Engines (ISEs), which authenticate clients and endpoints, can perform device profiling, also.

When the network configuration includes an ISE, the engine associates the user to an authorization profile, which allows the user access to designated resources. In these cases, Prime Infrastructure also displays the authorization profile name that is associated with the user.

Administrators also can configure the system to collect client data when it receives a trap or syslog that indicates a client's association to or disassociation from a switch port, or when 802.1X client authentication fails.



Wireless Client and Mobility Data?

Wireless LAN Controllers and Cisco Mobility Services Engines (MSEs)

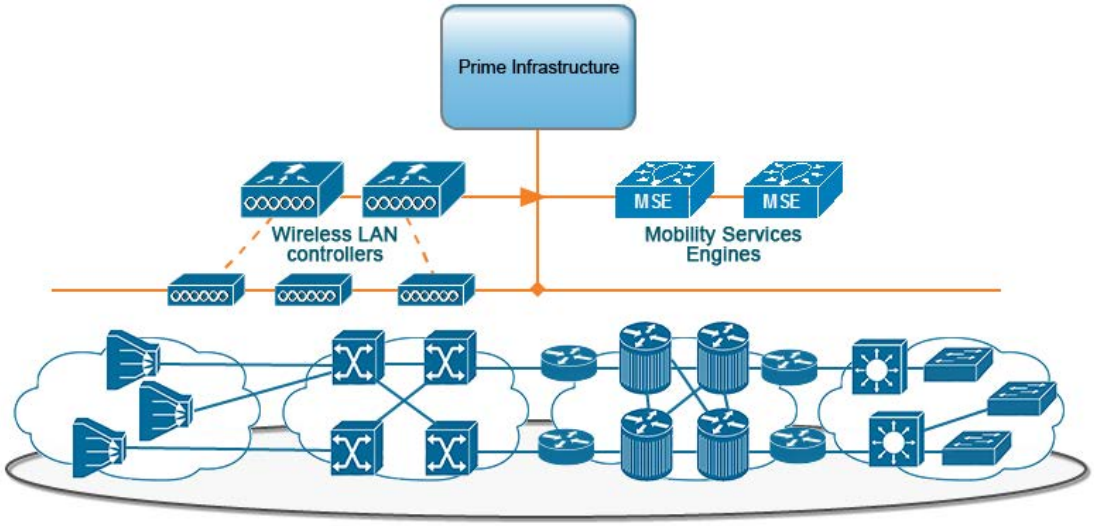
Prime Infrastructure reports detailed wireless network data through its integration with wireless LAN controllers and with Cisco Mobility Services Engines (MSEs).

Prime Infrastructure collects wireless LAN controller data, including data on the controller itself, and on the access points associated with the controller.

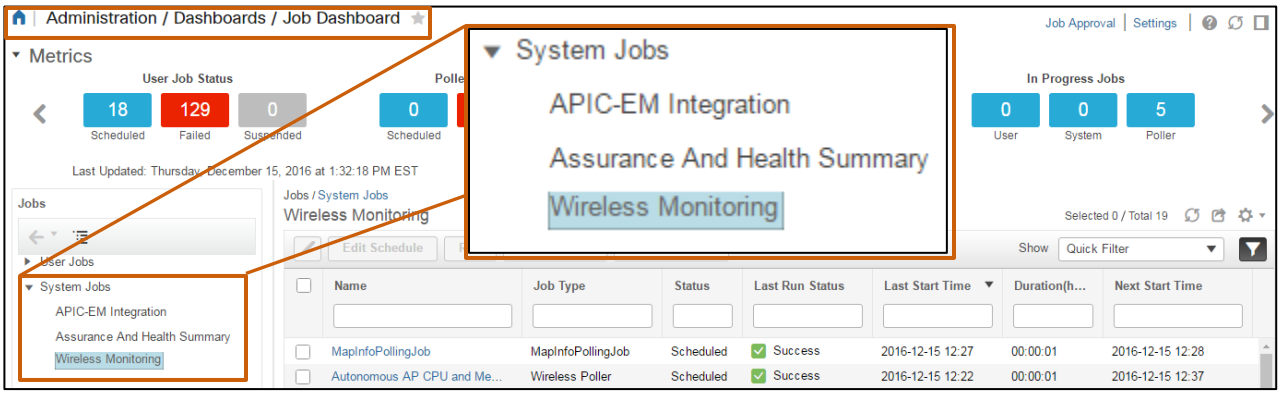
Wireless LAN controllers also forward the data that they collect from access points to Cisco Mobility Services Engines (MSEs).

The MSEs then provide various services to capture contextual and threat detection data about mobility clients and users for collection by Prime Infrastructure. This information provides you with valuable insight into the movement and behavior patterns of mobile devices and those who are using them.

For example, when monitoring or troubleshooting rogue APs or clients, you can use this information to track the client locations that the MSE services are detecting.



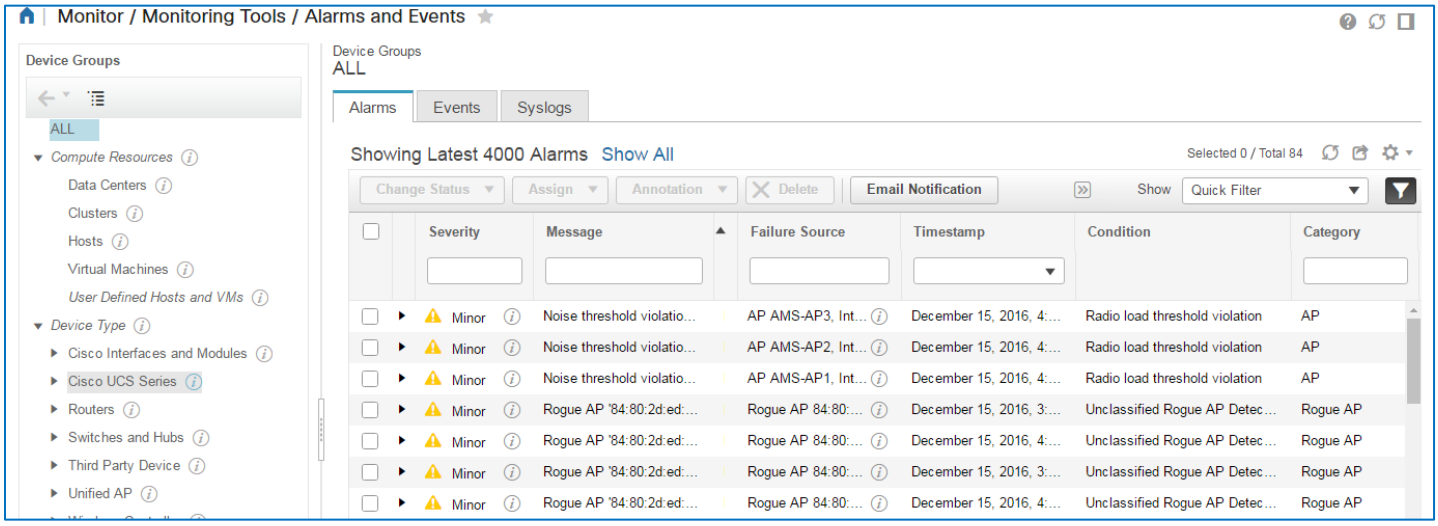
Prime Infrastructure primarily uses system jobs, accessible in the Administration area, to collect the data from wireless LAN controllers.



Faults and Event Data?

Monitoring Policies

Automonitoring and custom monitoring policies define the parameters and operational thresholds that the system uses to report data, including faults. When conditions fall outside of policy parameters or thresholds, the system can generate and report these conditions as alarms and events.



Alarm Policies

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.

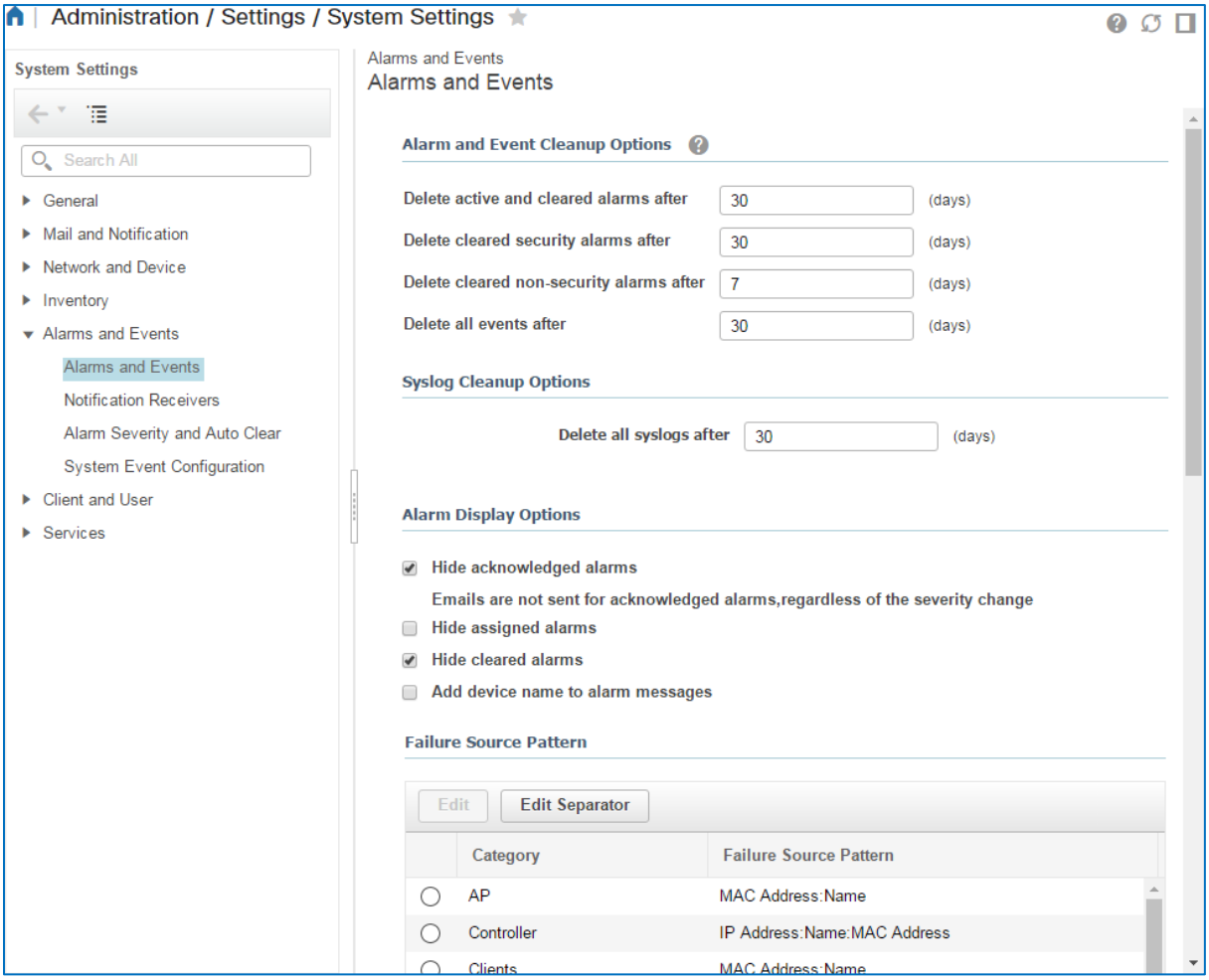
Note: For detailed information on the use and configuration of alarm policies, refer to the Cisco Prime Infrastructure 3.1 **Fault Monitoring Overview** job.

Administrative Settings

Overview

In Administration, you can configure the system settings that control the management and reporting behaviors of alarms. You also can configure the behaviors of the events and syslogs that form the basis for generating alarms, which provide detailed information.

Configuring these global settings is important for ensuring that the system is escalating issues and managing fault reporting based on operational and business requirements.



Collecting Fault Data in Northbound Systems

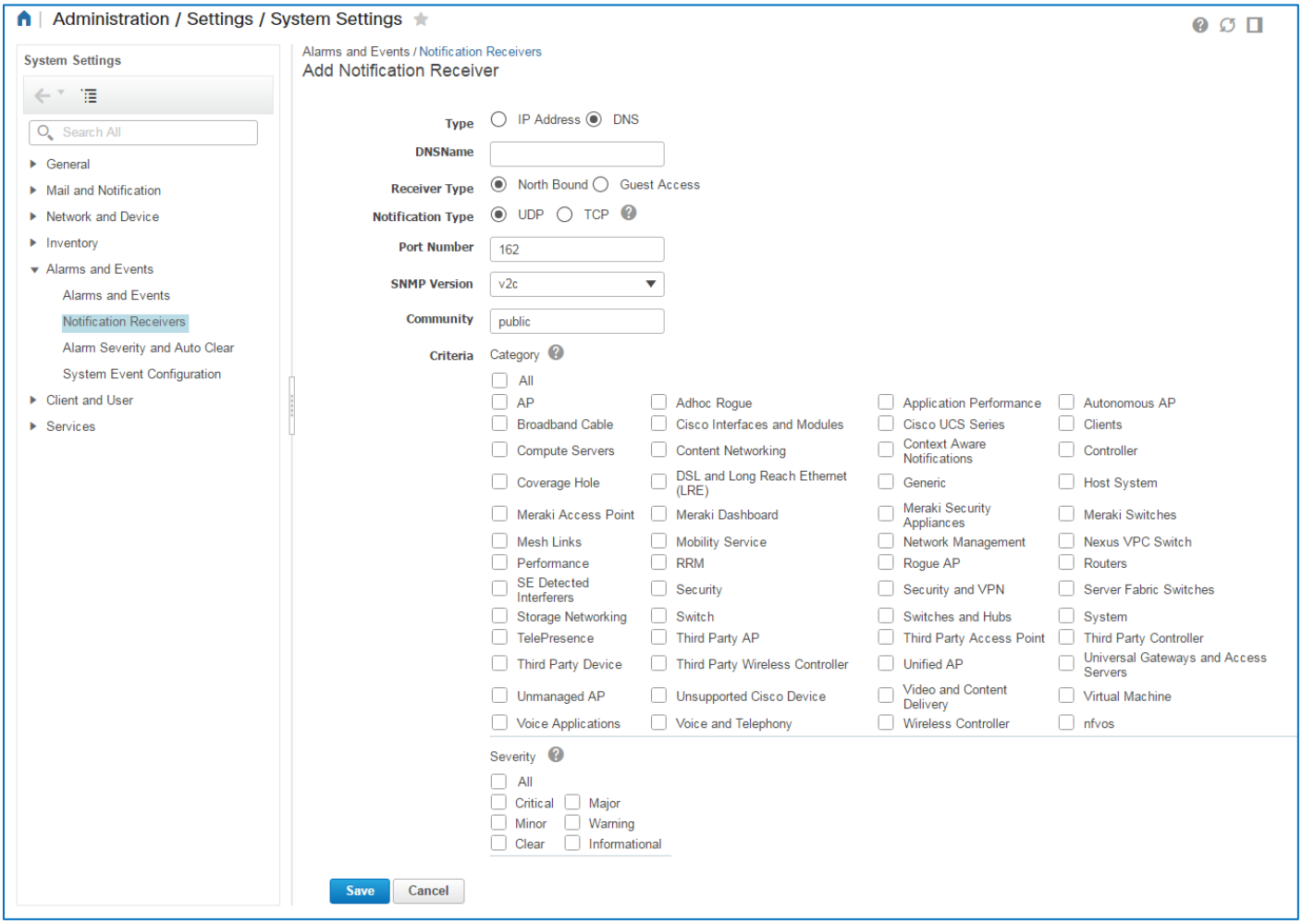
You can configure notification receivers so that northbound systems can receive data from Prime Infrastructure, including:

- Receiving alarms.
- Receiving events that are related to guest access activity, such as guest user accounts that are added, authenticated, or expired.

Forwarding these alarms or events help ensure that you are gathering the data that you need in the systems that you rely on for operational reporting and management activities.

In addition to configuring the forwarding details, you can configure one or more categories of events that you want to forward to the receiving system.

You also can configure the specific severity level or levels of the events that the system is forwarding.



Defining Alarm Severities and Behaviors

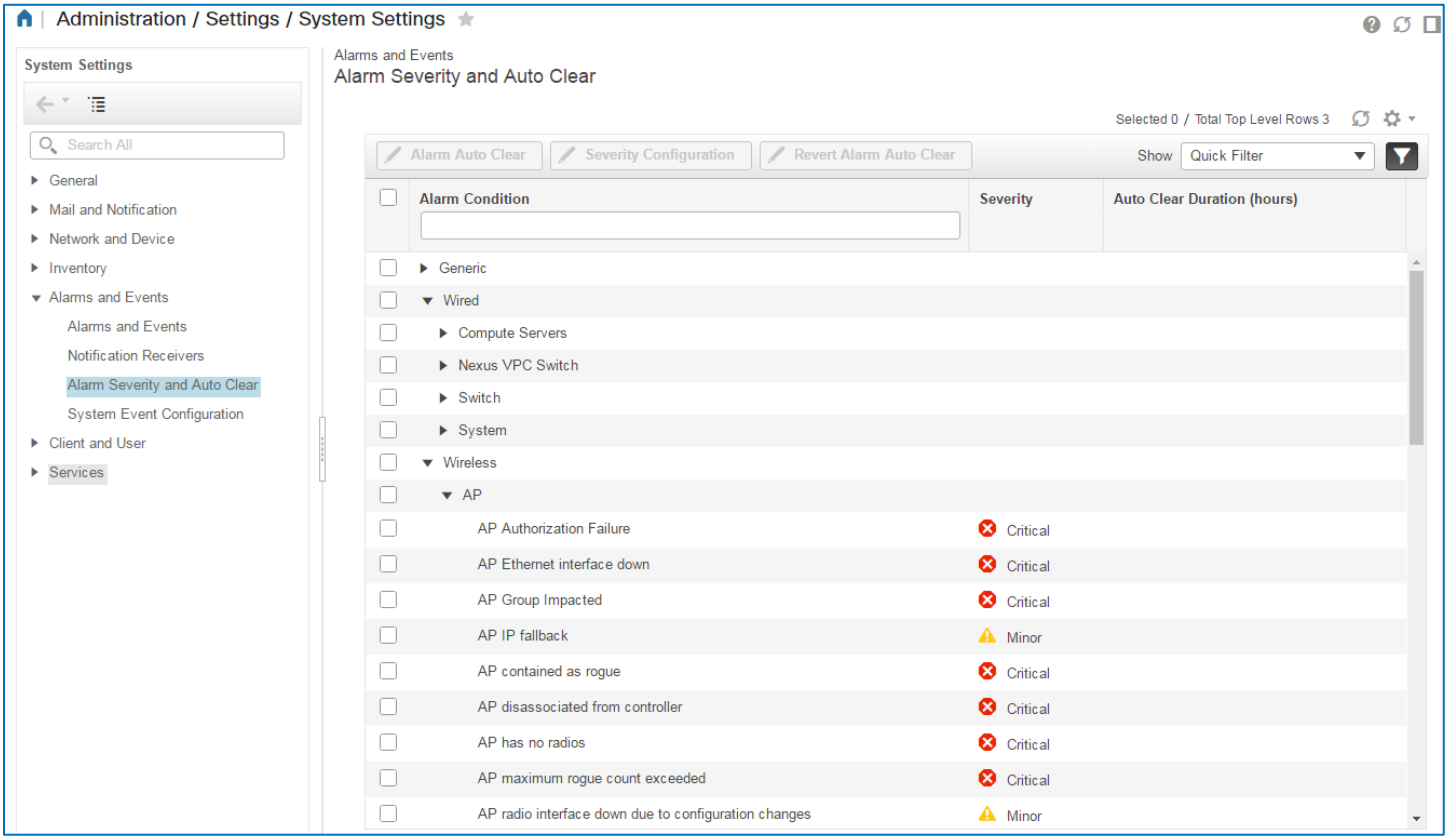
The system applies a default severity level to all of the alarms.

On the **Alarm Severity and Auto Clear** page, you can define the severity levels that the system applies to the alarms that it reports, and the time period that passes before the system automatically clears alarms.

When you change severity levels, you can return the alarm to its system default severity level.

You also can define the time period, in hourly increments, that passes before the system automatically applies a cleared status to an alarm, which overrides the global system default settings.

Note: When you change alarm settings, those changes apply to new alarms that the system generates and do not affect current or cleared alarms.



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

For information on where the system reports data, refer to the Prime Infrastructure 3.1 overview job aids.

For information on data collection processes for the data center, refer to the Prime Infrastructure 3.1 **Data Center Monitoring Overview** job aid.

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.

Note: Please send messages that address the content of this job aid or other training questions only.

Please follow your regular business process to request technical support or address technical or application-related questions.