Prime Infrastructure User Interface Reference

Cisco Prime Infrastructure is a web-based application. Tabs on the user interface are either specific to a particular Cisco Prime product or can be shared across multiple Cisco Prime products. The options on application tabs are displayed when you hover your cursor on the tab.

Note If any of your installed Cisco Prime products are not yet enabled through licensing, the tabs or options for those products are not activated.

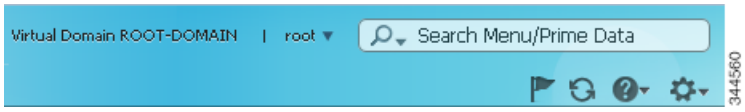
Prime Infrastructure UI Components

The Prime Infrastructure user interface components are visible on most of the pages.

Global Toolbars

Prime Infrastructure pages contain the following static global toolbar at the top right (see Figure A-1.)

Figure A-1 Global Toolbar—Top Right



- **Virtual Domain name**—Indicates the virtual domain to which you are assigned.
- **Login name**—Indicates your login name. Click the arrow to change your user preferences, change your password, or log out.

  Click the downward arrow next to your login name to switch to a different Prime Infrastructure view:

  – Lifecycle view, which is organized according to home, design, deploy, operate, report, and administer menus.

  - Classic view, which closely corresponds to the graphical user interface in Cisco Prime Network Control System 1.1 or Cisco Wireless Control System (WCS).

- **Search**—See Search Methods, page A-15.
- **Welcome**—Launches the Getting Started wizard, which provides guidance for getting started with setting up Prime Infrastructure.
- **Check for update**—Launches the Check for Update popup in the Software Update page. This icon appears until the update is installed into the server.
- **Refresh**—Refreshes the active page.
- **Help**—Launches Prime Infrastructure online help and learning modules.
- **Edit Dashboard**—Allows you to add, rename, and manage dashboards.

Prime Infrastructure pages contain the following static global toolbar at the bottom right.

Figure A-2 Global Toolbar—Bottom Right

- **Workflow Status**—Launches the workflow status summary window that displays the site maps, newly registered devices, and any failed wired and wireless workflows.
- **Support Cases**—Launches the TAC Services Request, where you can open a support request and gather critical information to be attached to the support case. See Opening a Support Case, page 21-2 for more information.
- **Alarm Browser**—Launches the alarm browser within the active page (bottom half of the page).
- **Alarm Summary**—Launches the alarm summary window, displaying all alarms and indicating the number of critical, major, and minor alarms.

Dashboards and Dashlets

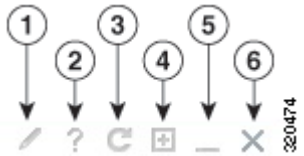
Dashboards display at-a-glance views of the most important data in your network. Dashboards contain *dashlets* that consist of visual displays such as tables and charts.

Note Adobe Flash Player must be installed before you can view the dashlets on a Prime Infrastructure dashboard.

Dashboards generally provide status and alerts, monitoring, and reporting information; a quick scan of a dashboard should let you know if anything needs attention. Use the filters at the top of the dashboards to specify the information that is displayed.

Dashboards contain dashlets that consist of visual displays such as tables and charts. You can drag and drop dashlets to any location in the dashboards. Hover your mouse cursor in any dashlet, and the following icons appear at the top-right corner of the dashboard.

Figure A-3 Dashlet Icons



1	Dashlet options include editing the dashlet title, refreshing the dashlet, or changing the dashlet refresh interval. (To disable refresh, uncheck Refresh Dashlet.)
2	Dashlet help includes a screenshot of the dashlet, a description, the data sources, and any applicable filters.
3	Refresh the dashlet.
4	Maximize the dashlet. A restore icon appears, allowing you to restore the dashlet to its default size.
5	Collapse the dashlet so that only its title appears. An expand icon appears.
6	Remove the dashlet.

Dashlet badges indicate which filters were applied when generating the contents of each dashlet (see Performing a Dashboard Filter, page A-9).

Figure A-4 Dashlet Badges

1	Network aware filter. Use this filter to collect data for all devices, wired devices, wireless devices, or a specific wireless SSID.
2	Site filter. Use this filter to collect data associated with an AP or a controller located at a predefined location.
3	Application filter. Use this filter to collect data based on a service, an application within a service, up to ten separate applications, or all applications.
4	Time frame filter. Use this filter to collect data for a preset time period, or you can specify a beginning and ending date.

You can customize the predefined set of dashlets depending on your network management needs. You can organize the information in user-defined dashboards. The default view comes with default dashboards and pre-selected dashlets for each.

Note

- The label "*Edited*" next to the dashlet heading indicates that the dashlet has been customized. If you reset to the default settings, the Edited label is cleared.
- When an upgrade occurs, the arrangement of dashlets in a previous version is maintained. Because of this, dashlets or features added in a new release are not displayed. Click the **Manage Dashboards** link to discover new dashlets.
- The horizontal and vertical scrollbars are visible if you zoom the dashlets. Reset the zoom level back to zero, or no zoom for viewing the dashlets without the scrollbars.

Adding Dashboards

To add a create a custom dashboard:

Step 1 Click the **Settings** icon and choose **Add New Dashboard**.

Step 2 Enter a name for the new dashboard, then click **Add**.

Step 3 Choose the new dashboard and add dashlets to it (see Adding Dashlets, page A-4).

Configuring Dashboards

After an upgrade, the arrangement of dashlets in the previous version is maintained. Therefore, dashlets or features added in a new release are not displayed. To display new dashlets, click the **Settings** icon and choose **Manage Dashboards**.

To restore a dashboard to the default settings:

Step 1 From the home page, click the **Edit Dashboard** icon.

Step 2 Click **Manage Dashboards**, choose a dashboard from the list, and click **Reset**.

Adding Dashlets

A subset of the available dashlets is automatically displayed in the dashboards. To add a dashlet that is not automatically displayed to a dashboard:

Step 1 Choose **Operate > Monitoring Dashboards > Detail Dashboards**.

Step 2 Display the dashboard to which you want to add the dashlet, click the gear icon on the global toolbar, then click **Add Dashlets**.

Step 3 Find the dashboard heading in the drop-down list; you can add any of the dashlets under that heading to that dashboard.

The following table lists the default dashlet options that you can add in your Prime Infrastructure home page.

Table A-1 Default Dashlets

Dashlet	Description
AP Join Taken Time	Displays the access point name and the amount of time (in days, minutes, and seconds) that it took for the access point to join.
AP Threats/Attacks	Displays various types of access point threats and attacks and indicates how many of each type have occurred.
AP Uptime	Displays each access point name and amount of time it has been associated.
Ad hoc Rogues	Displays ad hoc rogues for the previous hour, previous 24 hours, and total active.
Cisco Wired IPS Events	Displays wired IPS events for the previous hour, previous 24 hours, and total active.
Client	Displays the five most recent client alarms with client association failures, client authentication failures, client WEP key decryption errors, client WPA MIC errors, and client exclusions.
Client Authentication Type	Displays the number of clients for each authentication type.
Client Count	Displays the trend of associated and authenticated client counts in a given period of time.
Client Distribution	Displays how clients are distributed by protocol, EAP type, and authentication type.
Client EAP Type Distribution	Displays the count based on the EAP type.
Client Protocol Distribution	Displays the current client count distribution by protocols.
Client Security Events	Displays client security events within the previous 24 hours including excluded client events, WEP decrypt errors, WPA MIC errors, shunned clients, and IPsec failures.
Client Traffic	Displays the trend of client traffic in a given time period.
Client Troubleshooting	Allows you to enter a MAC address of a client and retrieve information for diagnosing the client in the network.
Clients Detected by Context Aware Service	Displays the client count detected by the context aware service within the previous 15 minutes.
Controller CPU Utilization (%)	Displays the average, maximum, and minimum CPU usage.
Controller Memory Utilization	Displays the average, maximum, and minimum memory usage as a percentage for the controllers.
Coverage Areas	Displays the list coverage areas and details about each coverage area.
Friendly Rogue APs	Displays friendly rogue access points for the previous hour, previous 24 hours, and total active.
Guest Users Count	Displays Guest client count over a specified time.

Table A-1 Default Dashlets (continued)

Dashlet	Description
Inventory Detail Status	Displays the Chart summarizing the status for the following device types: • Controllers • Switches • Autonomous APs • Radios • MSEs • Third Party Controllers • Third Party Access Points
Inventory Status	Displays the total number of client controllers and the number of unreachable controllers.
LWAPP Uptime	Displays the access point name and the amount of its uptime in days, minutes, and seconds.
Latest 5 Logged in Guest Users	Displays the most recent guest users to log in.
Mesh AP by Hop Count	Displays the APs based on hop count.
Mesh AP Queue Based on QoS	Displays the APs based on QoS.
Mesh Parent Changing AP	Displays the worst Mesh APs based on changing parents.
Mesh Top Over Subscribed AP	Displays the considered over subscribed APs.
Mesh Worst Node Hop Count2-28	Displays the Worst AP node hop counts from the root AP.
Mesh Worst Packet Error Rate	Displays the worst Mesh AP links based on the packet error rates of the links.
Mesh Worst SNR Link	Displays the worst Mesh AP links based on the SNR values of the links.
Most Recent AP Alarms	Displays the five most recent access point alarms. Click the number in parentheses to open the Alarms page which shows all alarms.
Most Recent Client Alarms	Displays the most recent client alarms.
Most Recent Mesh Alarms	Displays the most recent mesh alarms
Most Recent Security Alarms	Displays the five most recent security alarms. Click the number in parentheses to open the Alarms page.
Recent 5 Guest User Accounts	Displays the most recent guest user accounts created or modified.
Recent Alarms	Displays the five most recent alarms by default. Click the number in parentheses to open the Alarms page.
Recent Coverage Holes	Displays the recent coverage hole alarms listed by access point.
Recent Malicious Rogue AP Alarms	Displays the recent malicious rogue AP alarms.

Table A-1 Default Dashlets (continued)

Dashlet	Description
Recent Rogue Alarms	Displays the five most recent rogue alarms. Click the number in parentheses to open the Alarms page which shows the alarms.
Security Index	Displays the security index score for the wireless network. The security index is calculated as part of the 'Configuration Sync' background task.
Top APs by Client Count	Displays the Top APs by client count.
Unclassified Rogue APs	Displays unclassified rogue access points for the previous hour, previous 24 hours, and total active.
Client Count By Association/Authentication	Displays the total number of clients by Association and authentication in Prime Infrastructure over the selected period of time. • Associated client—All clients are connected regardless of whether it is authenticated or not. • Authenticated client—All clients are connected through a RADIUS or TACACS server. **Note** Client count includes autonomous clients. **Note** The wired clients connected to open ports are counted as authenticated although authentication did not really happen due to open policy. This is also applicable for the wireless clients connected to an OPEN WLAN. When two areas overlap, the color is blended in the dashlet.

Overriding a Dashlet Filter

You can change the filter settings for just one dashlet. For example, to change the time frame during which data is collected for a single dashlet from the default to 24 hours:

Step 1 Navigate to that dashlet and click **Dashlet Options**.

Step 2 Check the **Override Dashlet Time Filter** check box, choose **Past 24 Hours** from the **Time Frame** drop-down list, then click **Save And Close**.

The dashlet displays the last 24 hours of data. The label “Edited” next to the Time Frame dashlet badge with a red diagonal line over the badge indicates that the filter has been customized.

Creating Generic Dashlets

You can add a generic dashlet anywhere; it displays the values for all polled devices.

Before You Begin

You must create at least one custom template (for example, see Creating Custom SNMP Polling Templates, page 8-32).

To create a generic dashlet:

Step 1 Choose **Detail Dashboards > Device > Edit Dashboard > Add Dashlet(s)**.

Step 2 Find the Generic Dashlet and click **Add**. The Generic Dashlet appears on the dashboard.

Step 3 To edit the dashlet, hover your cursor over the Generic Dashlet and click **Dashlet Options**.

Step 4 Rename the dashlet.

Step 5 From the Template Name drop-down list, choose the custom template that you created, then click **Save**.

Filters

You can use the Filter feature to display specific information about the Prime Infrastructure interface. The Filter icon is provided wherever the data is displayed in a tabular format. The following types of filters are available:

- Quick Filter—See Performing a Quick Filter, page A-8
- Advanced Filter—See Performing an Advanced Filter, page A-8
- Dashboard Filter—See Performing a Dashboard Filter, page A-9

Performing a Quick Filter

This filter allows you to narrow down the data inside a table by applying a filter to a specific table column or columns. To apply different operators, use the Advanced Filter option (see Performing an Advanced Filter, page A-8).

To launch the quick filter, choose **Quick Filter** from the Filter drop-down list.

To clear the Quick Filter, click **Filter**.

Performing an Advanced Filter

This filter allows you to narrow down the data in a table by applying a filter using multiple operators such as Does not contain, Does not equal, Ends with, Is empty, and so on. For example, you can choose the filter pattern by table column names and the operator from the drop-down list. In addition, you must enter filter criteria based on the data available in the Prime Infrastructure database.

To launch advanced filtering, choose **Advanced Filter** from the Filter drop-down list.

Figure A-5 Advanced Filter

To save the filter criteria used in the Advanced filter:

Step 1 Enter the advanced filter criteria, then click **Go**. The data is filtered based on the filter criteria.

Step 2 After the data is filtered, click the **Save** icon.

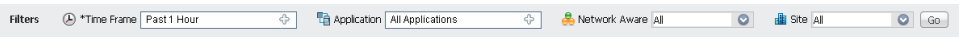
Step 3 In the Save Preset Filter dialog box, enter a name for the preset filter and click **Save**.

Performing a Dashboard Filter

The Filters toolbar allows you to narrow down the data that is displayed in all of the dashlets in a dashboard. Use this toolbar to filter the dashlets data by:

- Time frame—Select one of the preset options or create a custom time frame.
- Applications—Select a service, up to 10 individual applications, or all applications.
- Network Aware—Select wired, wireless, or all networks.
- Site—Select a site, unassigned sites, or all sites.

Figure A-6 Dashboard Filters Toolbar



To filter the data for all dashlets in a dashboard:

Step 1 Open a dashboard (for example, choose **Operate > Monitoring Dashboards > Detail Dashboards**).

Step 2 Change the settings in any of the **Filters** toolbar options, then click **Go**.

Data Entry Features

In addition to the check boxes, drop-down lists and data entry fields common in most user interfaces, Prime Infrastructure uses some specialized data-entry features. These features are designed to keep your view of the network as uncluttered as possible, while still making it possible for you to add, update, and save your settings when needed. These specialized data-entry features include:

- Anchored Fields, page A-9
- Edit Tables, page A-10
- Data Popups, page A-10

Anchored Fields

Anchored fields are recognizable by the plus sign (+) embedded in the field at the far right.

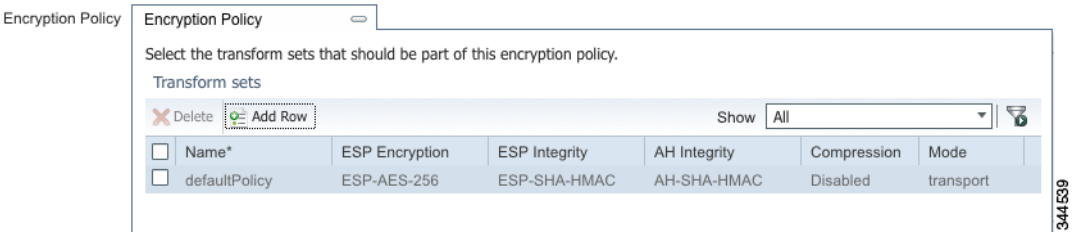
Figure A-7 Anchored Field

To use anchored fields:

Step 1 Click the anchored field's plus (+) button.

Step 2 With the associated data popup displayed (see Data Popups, page A-10), review or update the data as needed.

Figure A-8 Anchored Field with Popup



Step 3 When you are finished, click the anchored field's minus (-) button.

Edit Tables

Prime Infrastructure uses tables to display many kind of data, including lists of sites, devices, and events. The data is arranged in rows and columns, much like a spreadsheet.

An edit table differs from other tables in that you can add, edit, or delete the data it contains. Some edit tables also give you access to filters (see Filters, page A-8). Edit tables are often displayed in data popups that are triggered by check boxes or anchored fields.

Figure A-9 Edit Table

To use edit tables:

- To add a new row in the edit table:

  Click **Add Row**, complete the fields in the new row, and click **Save**.
- To delete one or more existing rows in an edit table:

  Click the row header check box (at the extreme left of each row), then click **Delete**.
- To update an entry in any field in any edit table row:

  Click the row header or on the field itself, edit the contents, then click **Save**.

Data Popups

A data popup is a window associated with a check box, anchored field (see Anchored Fields, page A-9), or other data-entry feature. It is displayed automatically when you select a feature, so you can view or update the data associated with that feature. In addition to containing check boxes, drop-down lists, and data-entry fields, data popups can also contain edit tables (see Edit Tables, page A-10).

To use a data popup:

1. Select the feature that triggers the data popup, such as an anchored field (see Figure A-7) or a check box (see Figure A-9).
2. With the associated popup displayed, view or update the fields as needed.
3. When you are finished, click anywhere outside the data popup. If you entered new information or changed existing information, your changes are saved automatically.

Common UI Tasks

You can perform the following actions from nearly any Prime Infrastructure window:

Changing Your Password

Step 1 Click the down arrow next to your username (at the top-right of the screen, to the left of the search field) and choose **Change Password**.

Step 2 Click the information icon to review the password policy.

Step 3 Enter a new password as directed and click **Save**.

Changing Your Active Domain

Step 1 Hover your mouse cursor on the Virtual Domain and click the icon that appears to the right.

Step 2 Choose a domain from the list of domains of which you are a member.

Monitoring Alarms

At the bottom of the Cisco Prime Infrastructure window, hover your mouse cursor on Alarm Summary or Alarm Browser to get information on the latest active alarms.

Getting Device Details from the Device 360° View

The Device 360° View provides detailed device information including device status, interface status, and associated device information. You can see the device 360° view from nearly all pages in which device IP addresses are displayed.

To launch the 360° view of any device, hover your mouse cursor on a device IP address, then click the icon that appears.

Note The features that appear in the Device 360° View differ depending on the device type.

Figure A-10 Sample Device 360° View

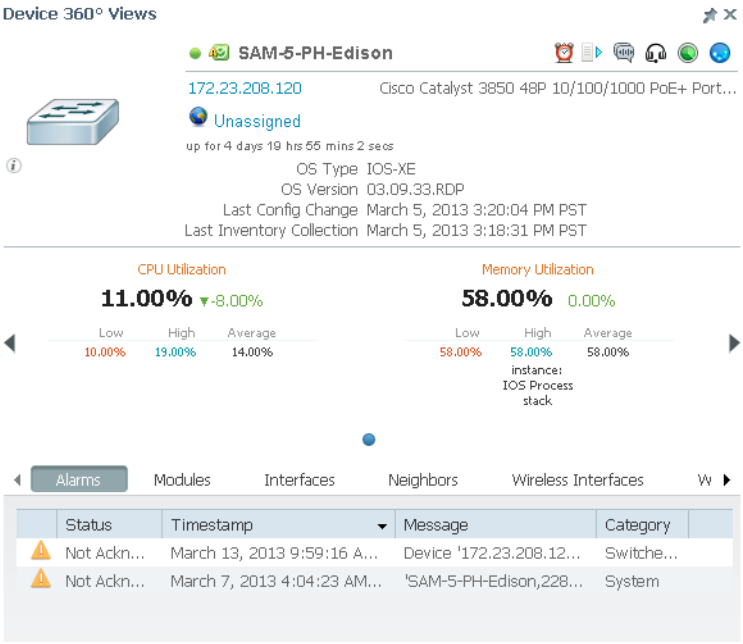


Table A-2 Device 360° View Features

Device 360° View Feature	Description
Device status	Indicates whether the device is reachable, is being managed, and is synchronized with the Prime Infrastructure database.
Tool icons	Click one of the following icons at the top right of the device 360° view: • Alarm Browser—Launches the Alarm Browser. See Monitoring Alarms, page 11-1 for more information. • Device Details—Displays device details. • Support Community—Launches the Cisco Support Community. See Launching the Cisco Support Community, page 21-1. • Support Request—Allows you to open a support case. See Opening a Support Case, page 21-2 for more information. • Ping—Allows you to ping the device. • Traceroute—Allows you to perform a traceroute on the device.
Alarms	Lists alarms on the device, including the alarm status, time stamp, and category.
Modules	Lists the device modules and their name, type, state, and ports.
Interfaces	Lists the device interfaces and the top three applications for each interface.
Neighbors	Lists the device neighbors, including their index, port, duplex status, and sysname.
Wireless Interfaces	Lists the interface names, associated WLANs, VLAN IDs and IP addresses.
WLAN	Lists the WLAN names, SSIDs, security policies, and number of clients.

Getting User Details from the User 360° View

The User 360° View provides detailed information about an end user, including:

- End user network connection and association
- Authentication and authorization
- Possible problems with the network devices associated with the user's network attachment
- Application-related issues
- Other issues in the broader network

To access the 360° view for a user:

Step 1 Enter the user name in the Search field (see Search Methods, page A-15).

Figure A-11 Sample User Search Entry

Step 2 Multiple matches are displayed in the Search Results dialog. Click **View List** to display the matches.

Step 3 To launch the User 360° View, hover your mouse over the name in the User Name field, then click the icon that appears as shown in Figure A-12.

Figure A-12 Launching User 360° View

Step 4 Figure A-13 shows a sample of the User 360° View.

Figure A-13 Sample User 360° View

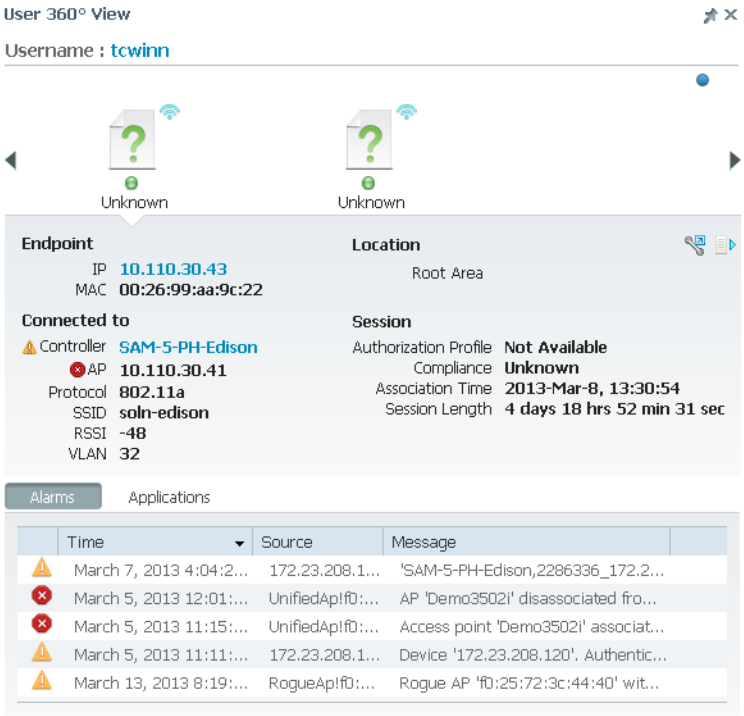


Table A-3 User 360° View Features

User 360° View Feature	Description
User information	Displays key information about the end user.
Endpoint	Displays endpoint information. This feature requires integration with an ISE server.

Table A-3 User 360° View Features

User 360° View Feature	Description
Connected To	Network attachment information: • Network device (access switch or AP + Controller): Visible indication of existence and severity of any active alarms associated with the device • Attachment port: Visible indication of existence and severity of any active alarms associated with the port
Location Session	Displays network session information: • The location is the Prime Infrastructure hierarchy location. • Access Policy (ISE Authorization Profile). Visible indication of the existence of any errors associated with authentication. This feature requires integration with an ISE server. • Endpoint compliance status. This feature requires integration with an ISE server. • Session start time and end time.
Alarms	Click the **Alarms** tab to view a list of alarms and statistics associated with the network session.
Applications	Click the **Applications** tab to view a list of applications and statistics associated with the network session. Session information (Netflow/NAM data, Assurance licenses) must be available.

Getting Help

You can access online help by clicking the question mark icon at the top right of any Prime Infrastructure page.

Search Methods

Prime Infrastructure provides the following search methods:

- Quick Search—See Performing a Quick Search, page A-15
- Advanced Search—See Performing an Advanced Search, page A-16
- Saved Search—See Performing a Saved Search, page A-26

You can access the search options from any page within Prime Infrastructure.

Performing a Quick Search

For a quick search, you can enter a partial or complete IP address or name. You can also enter a username if you are searching for a client.

To quickly search for a device:

Step 1 In the Search text box, enter a search string and.

Step 2 Click **Search** to display all matches for the Quick Search parameter.

Step 3 Click **View List** to view the matching devices from the Monitor or Configuration page.

Performing an Advanced Search

To perform a more specific search in Prime Infrastructure:

Step 1 Choose **Advanced Search** from the search menu.

Step 2 In the New Search dialog box, choose a category from the Search Category drop-down list.

Step 3 Choose all applicable filters or parameters for your search.

Note Search parameters change depending on the category you selected.

Step 4 To save this search, check the **Save Search** check box, enter a unique name for the search in the text box, and click **Go**.

Note You can decide what information appears on the search results page. See the "Configuring the Search Results Display (Edit View)" section on page A-26 for more information.

The Search categories include the following:

- Alarms—See Searching Alarms, page A-17
- Jobs—See Searching Jobs, page A-17
- Access Points—See Searching Access Points, page A-18
- Controller Licenses—See Searching Controller Licenses, page A-19
- Controllers—See Searching Controllers, page A-19
- Switches—See Searching Switches, page A-20
- Clients—See Searching Clients, page A-20
- Chokepoints—See Searching Chokepoints, page A-22
- Events—See Searching Events, page A-22
- Interferers—See Searching Interferers, page A-23
- Wi-Fi TDOA Receivers—See Searching Wi-Fi TDOA Receivers, page A-24
- Maps—See Searching Maps, page A-24
- Rogue Client—See Searching Rogue Clients, page A-24
- Shunned Client—See Searching Shunned Clients, page A-25
- Tags—See Searching Tags, page A-25
- Device Type—See Searching Device Type, page A-26
- Configuration Versions—See Searching Configuration Versions, page A-26

Searching Alarms

You can configure the following parameters when performing an advanced search for alarms (see Table A-4).

Table A-4 Search Alarms Fields

Field	Options
Severity	Choose **All Severities**, **Critical**, **Major**, **Minor**, **Warning**, or **Clear**.
Alarm Category	Choose **All Types**, **System**, **Access Points**, **Controllers**, **Coverage Hole**, **Config Audit**, **Mobility Service**, **Context Aware Notifications**, **SE Detected Interferers**, **Mesh Links**, **Rogue AP**, **Adhoc Rogue**, **Security**, **Performance**, **Application Performance, Routers, Switches and Hubs,** or **Cisco Interfaces and Modules**.
Condition	Use the drop-down list to choose a condition. Also, you can enter a condition by typing it in this drop-down list. **Note** If you have selected an alarm category, this drop-down list would contain the conditions available in that category.
Time Period	Choose a time increment from Any Time to Last 7 days. The default is Any Time.
Acknowledged State	Select this check box to search for alarms with an Acknowledged or Unacknowledged state. If this check box is not selected, the acknowledged state is not taken into search criteria consideration.
Assigned State	Select this check box to search for alarms with an Assigned or Unassigned state or by Owner Name. If this check box is not selected, the assigned state is not part of the search criteria. **Note** If you choose Assigned State > Owner Name, type the owner name in the available text box.

Searching Jobs

You can configure the following parameters when performing an advanced search for jobs (see Table A-5).

Table A-5 Search Jobs Fields

Field	Options
Job Name	Type the name of the job that you want to search.
Job Type	Type the job type that you want to search.
Job Status	Choose **All Status**, **Completed**, **or Scheduled**.

For more information, see the "Monitoring Jobs" section on page 10-6.

Note You can use wildcards such as *, ? in the Job Name and Job Type text box to narrow or broaden your search.

Searching Access Points

You can configure the following parameters when performing an advanced search for access points (see Table A-6).

Table A-6 Search Access Points Fields

Field	Options
Search By	Choose **All APs**, **Base Radio MAC**, **Ethernet MAC**, **AP Name**, **AP Model, AP Location**, **IP Address**, **Device Name**, **Controller IP**, **All Unassociated APs**, **Floor Area**, **Outdoor Area**, **Unassigned APs**, or **Alarms**. **Note** Search parameters might change depending on the selected category. When applicable, enter the additional parameter or filter information to help identify the Search By category. For example, when you select Floor Area, you also must identify its campus and building. Or, if you select Alarms, you can search for access points based on the severity of the alarm.
AP Type	Choose **All Types**, **LWAPP**, or **Autonomous**.
AP Mode	Choose **All Modes**, **Local, Monitor**, **FlexConnect**, **Rogue Detector**, **Sniffer**, **Bridge**, or **SE-Connect**.
Radio Type	Choose **All Radios**, **802.11a**, or **802.11b/g**.
802.11n Support	Select this check box to search for access points with 802.11n support.
OfficeExtend AP Enabled	Select this check box to search for OfficeExtend access points.
CleanAir Support	Select this check box to search for access points which support CleanAir.
CleanAir Enabled	Select this check box to search for access points which support CleanAir and which are enabled.
Items per page	Configure the number of records to be displayed in the search results page.

Searching Controller Licenses

You can configure the following parameters when performing an advanced search for controller licenses (see Table A-7).

Table A-7 Search Controller Licenses Fields

Field	Options
Controller Name	Type the controller name associated with the license search.
Feature Name	Choose **All**, **Plus**, or **Base** depending on the license tier.
Type	Choose **All**, **Demo**, **Extension**, **Grace Period**, or **Permanent**.
% Used or Greater	Choose the percentage of the license use from this drop-down list. The percentages range from 0 to 100.
Items per page	Configure the number of records to be displayed in the search results page.

Searching Controllers

You can configure the following parameters when performing an advanced search for controllers (see Table A-8).

Table A-8 Search Controllers Fields

Field	Options
Search for controller by	Choose **All Controllers**, **IP Address**, or **Controller Name**. **Note** Search parameters might change depending on the selected category. When applicable, enter the additional parameter or filter information to help identify the Search By category.
Enter Controller IP Address	This text box appears only if you choose IP Address from the Search for controller by drop-down list.
Enter Controller Name	This text box appears only if you choose Controller Name from the Search for controller by drop-down list.

Table A-8 Search Controllers Fields (continued)

Field	Options
Audit Status	Choose one of the following from the drop-down list: • **All Status** • **Mismatch**—Config differences were found between Prime Infrastructure and controller during the last audit. • **Identical**—No config differences were found during the last audit. • **Not Available**—Audit status is unavailable.
Items per page	Configure the number of records to be displayed in the search results page.

Searching Switches

You can configure the following parameters when performing an advanced search for switches (see Table A-9).

Table A-9 Search Switches Fields

Field	Options
Search for Switches by	Choose **All Switches**, **IP Address**, or **Switch Name**. You can use wildcards (*). For example, if you select IP Address and enter **172***, Prime Infrastructure returns all switches that begin with IP address 172.
Items per page	Configure the number of records to be displayed in the search results page.

Searching Clients

You can configure the following parameters when performing an advanced search for clients (see Table A-10).

Table A-10 Search Clients Fields

Field	Options
Media Type	Choose **All**, **Wireless Clients**, or **Wired Clients**.
Wireless Type	Choose **All**, **Lightweight** or **Autonomous Clients** if you chose Wireless Clients from the Media Type list.

Table A-10 Search Clients Fields (continued)

Field	Options
Search By	Choose **All Clients**, **All Excluded Clients**, **All Wired Clients**, **All Logged in Guests**, **IP Address**, **User Name**, **MAC Address**, **Asset Name**, **Asset Category**, **Asset Group**, **AP Name**, **Controller Name**, **Controller IP**, **MSE IP**, **Floor Area**, **Outdoor Area**, **Switch Name**, or **Switch Type**. **Note** Search parameters might change depending on the selected category. When applicable, enter the additional parameter or filter information to help identify the Search By category. For example, when you select IP address, you must enter the specific IP address for this search.
Clients Detected By	Choose **Prime Infrastructure** or **MSEs**. Clients detected by Prime Infrastructure—Clients stored in Prime Infrastructure databases. Clients detected by MSE—Clients located by Context Aware service in the MSE directly communicating with the controllers.
Client States	Choose **All States**, **Idle**, **Authenticated**, **Associated**, **Probing**, or **Excluded**.
Posture Status	Choose **All**, **Unknown**, **Passed**, **Failed** if you want to know if the devices are clean or not.
Restrict By Radio Band	Select the check box to indicate a specific radio band. Choose **5 GHz** or **2.4 GHz** from the drop-down list.
Restrict By Protocol	Select the check box to indicate a specific protocol. Choose **802.11a**, **802.11b**, **802.11g**, **802.11n**, or **Mobile** from the drop-down list.
SSID	Select the check box and choose the applicable SSID from the drop-down list.
Profile	Select the check box to list all of the clients associated to the selected profile. **Note** Once the check box is selected, choose the applicable profile from the drop-down list.
CCX Compatible	Select the check box to search for clients that are compatible with Cisco Client Extensions. **Note** Once the check box is selected, choose the applicable version, **All Versions**, or **Not Supported** from the drop-down list.

Table A-10 Search Clients Fields (continued)

Field	Options
E2E Compatible	Select the check box to search for clients that are end–to–end compatible. **Note** Once the check box is selected, choose the applicable version, **All Versions**, or **Not Supported** from the drop-down list.
NAC State	Select the check box to search for clients identified by a certain Network Admission Control (NAC) state. **Note** Once the check box is selected, choose the applicable state from the drop-down list: **Quarantine**, **Access**, **Invalid**, and **Not Applicable**.
Include Disassociated	Select this check box to include clients that are no longer on the network but for which Prime Infrastructure has historical records.
Items per page	Configure the number of records to be displayed in the search results page.

Searching Chokepoints

You can configure the following parameters when performing an advanced search for chokepoints (see Table A-11).

Table A-11 Search Chokepoint Fields

Field	Options
Search By	Choose **MAC Address** or **Chokepoint Name**. **Note** Search parameters might change depending on the selected category. When applicable, enter the additional parameter or filter information to help identify the Search By category. For example, when you select MAC address, you must enter the specific MAC address for this search.

Searching Events

You can configure the following parameters when performing an advanced search for events (see Table A-12).

Table A-12 Search Events Fields

Field	Options
Severity	Choose **All Severities**, **Critical**, **Major**, **Minor**, **Warning**, **Clear**, or **Info. Color coded**.
Event Category	Choose **All Types**, **Access Points**, **Controller**, **Security**, **Coverage Hole, Rogue AP**, **Adhoc Rogue**, **Interference**, **Mesh Links**, **Client**, **Mobility Service**, **Location Notifications**, **Pre Coverage Hole**, or **Prime Infrastructure**.
Condition	Use the drop-down list to choose a condition. Also, you can enter a condition by typing it in this drop-down list. **Note** If you selected an event category, this drop-down list contains the conditions available in that category.
Search All Events	Configure the number of records to be displayed in the search results page.

Searching Interferers

You can configure the following parameters when performing an advanced search for interferers detected by access points (see Table A-13).

Table A-13 Search SE-Detected Interferers Fields

Field	Options
Search By	Choose **All Interferers**, **Interferer ID**, **Interferer Category**, **Interferer Type**, **Affected Channel**, **Affected AP**, **Severity**, **Power**, or **Duty Cycle**. **Note** Search parameters might change depending on the selected category. When applicable, enter the additional parameter or filter information to help identify the Search By category.
Detected By	Choose **All Spectrum Experts** or a specific spectrum expert from the drop-down list.
Detected within the last	Choose the time range for the interferer detections. The times range from 5 minutes to 24 hours to All History.
Interferer Status	From this drop-down list, choose **All**, **Active**, or **Inactive**.
Restrict by Radio Bands/Channels	Configure the search by radio bands or channels.
Items per page	Configure the number of records to be displayed in the search results page.

Searching Wi-Fi TDOA Receivers

You can configure the following parameters when performing an advanced search for Wi-Fi TDOA receivers (see Table A-14).

Table A-14 Search Wi-Fi TDOA Receivers Fields

Field	Options
Search By	Choose **MAC Address** or **Wi-Fi TDOA Receivers Name**. **Note** Search parameters might change depending on the selected category. When applicable, enter the additional parameter or filter information to help identify the Search By category.

Searching Maps

You can configure the following parameters when performing an advanced search for maps (see Table A-15).

Table A-15 Search Map Fields

Field	Options
Search for	Choose **All Maps**, **Campuses**, **Buildings**, **Floor Areas**, or **Outdoor Areas**.
Map Name	Search by Map Name. Enter the map name in the text box.
Items per page	Configure the number of records to be displayed in the search results page.

Searching Rogue Clients

You can configure the following parameters when performing an advanced search for rogue clients (see Table A-16).

Table A-16 Search Rogue Client Fields

Field	Options
Search for clients by	Choose **All Rogue Clients**, **MAC Address**, **Controller**, **MSE**, **Floor Area**, or **Outdoor Area**.
Search In	Choose **MSEs** or **Prime Infrastructure Controllers**.
Status	Select the check box and choose **Alert**, **Contained**, or **Threat** from the drop-down list to include status in the search criteria.

Searching Shunned Clients

Note When a Cisco IPS sensor on the wired network detects a suspicious or threatening client, it alerts the controller to shun this client.

You can configure the following parameters when performing an advanced search for shunned clients (see Table A-17).

Table A-17 Search Shunned Client Fields

Field	Options
Search By	Choose **All Shunned Clients**, **Controller**, or **IP Address**. **Note** Search parameters might change depending on the selected category. When applicable, enter the additional parameter or filter information to help identify the Search By category.

Searching Tags

You can configure the following parameters when performing an advanced search for tags (see Table A-18).

Table A-18 Search Tags Fields

Field	Options
Search for tags by	Choose **All Tags**, **Asset Name**, **Asset Category**, **Asset Group**, **MAC Address**, **Controller**, **MSE**, **Floor Area**, or **Outdoor Area**. **Note** Search parameters might change depending on the selected category. When applicable, enter the additional parameter or filter information to help identify the Search By category.
Search In	Choose **MSEs** or **Prime Infrastructure Controllers**.
Last detected within	Choose a time increment from 5 minutes to 24 hours. The default is 15 minutes.
Tag Vendor	Select the check box and choose Aeroscout, G2, PanGo, or WhereNet.
Telemetry Tags only	Select the **Telemetry Tags only** check box to search tags accordingly.
Items per page	Configure the number of records to be displayed in the search results page.

Searching Device Type

You can configure the following parameters when performing an advanced search for device type (see Table A-18).

Table A-19 Search Device Type Fields

Field	Options
Select Device Type	Choose **All**, **Switches and Hubs**, **Wireless Controller**, **Unified AP**, **Autonomous AP**, **Unmanaged AP**, and **Routers**.
Enter Device IP	Enter the IP address of the device selected in the Select Device Type field.

Searching Configuration Versions

You can configure the following parameter when performing an advanced search for configuration versions (see Table A-18).

Table A-20 Search Configuration Versions Fields

Field	Options
Enter Tag	Enter the tag name.

Performing a Saved Search

Note Saved searches apply only to the current partition.

To access and run a previously saved search:

Step 1 Click **Saved Search**.

Step 2 Choose a category from the Search Category drop-down list, then choose a saved search from the Saved Search List drop-down list.

Step 3 If necessary, change the current parameters for the saved search, then click **Go**.

Configuring the Search Results Display (Edit View)

The Edit View pageenables you to choose which columns appear in the Search Results page.

Note The Edit View page is available only from the Classic View.

Column names appear in one of the following lists:

- Hide Information—Lists columns that do not appear in the table. The Hide button points to this list.

- View Information—Lists columns that do appear in the table. The Show button points to this list.

To display a column in a table, click it in the Hide Information list, then click **Show**. To remove a column from a table, click it in the View Information list, then click **Hide**. You can select more than one column by holding down the shift or control key.

To change the position of a column in the View Information list, click it, then click **Up** or **Down**. The higher a column is in the list, the farther left it appears in the table.