Prime Infrastructure User Interface Reference

Cisco Prime Infrastructure is a web-based application.

If any of your installed Cisco Prime products are not yet enabled through licensing, the menu items or options for those features are not displayed in the web interface.

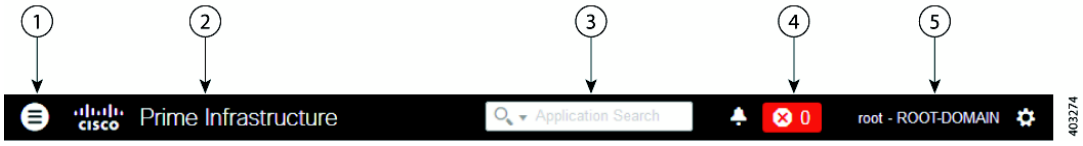
Understanding the Prime Infrastructure User Interface

When you first log in to Prime Infrastructure, an overlay window shows you the major components of the graphical interface. To view this overlay window again, click your login name at the top-right of the screen, then choose **Help > Getting Started**.

Toolbar

The toolbar shown in Figure A-1is at the top of every page:

Figure A-1 Prime Infrastructure Toolbar



1	Click to open the menu.
2	Click to go to the Prime Infrastructure product page on cisco.com.
3	Type to search for data within Prime Infrastructure. You can enter any text string such as a partial or complete IP address or a username.

1	Click to open the menu.
4	Displays the number of alarms, and the color corresponds to the highest severity level alarm in your network. Click to display the alarm summary window, displaying all alarms and the number of critical, major, and minor alarms.
5	Displays login name and the virtual domain to which you are assigned. Click to change your user preferences, change your password, log out, access help, and submit product feedback.

Related Topics

- Search Methods

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
- Advanced Filter—See Performing an Advanced Filter
- Dashboard Filter—See Using Dashboard Filters

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).

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

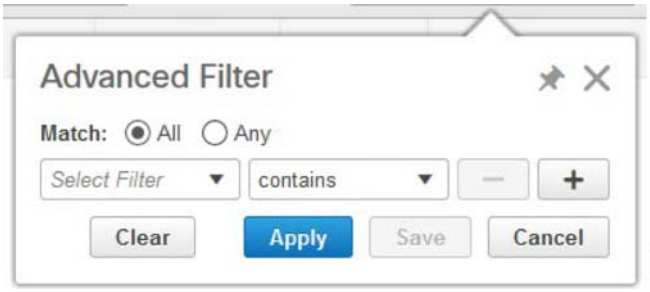
To clear the Quick Filter, click **Filter**.

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-2 Advanced Filter



To save the filter criteria used in the Advanced filter, follow these steps:

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**.

Using Dashboard Filters

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-3 Dashboard Filters Toolbar

To filter the data for all dashlets in a dashboard, follow these steps:

Step 1 Open a dashboard (for example, choose **Dashboard > Overview > General**).

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:

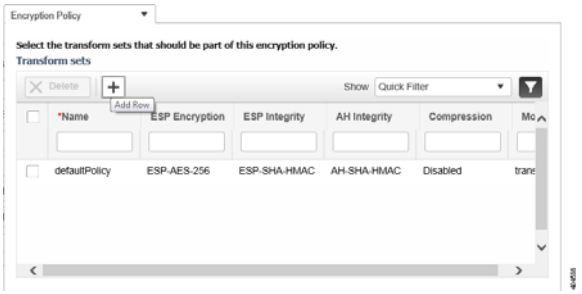
- Edit Tables
- Data Popups

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). Edit tables are often displayed in data popups that are triggered by check boxes.

Figure A-4 Edit Table



To use edit tables:

- To add a new row in the edit table:

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

  Select 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, or other data-entry feature. It is displayed automatically when you select a feature, so that 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.

To use a data popup:

1. Select the feature that triggers the data popup, such as an anchored field or a check box.
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.

Related Topics

- Edit Tables

Interactive Graphs

Prime Infrastructure provides interactive line, area, pie, and stacked bar graphs of both time-based and non time-based data. Interactive graph features include the following:

- Support for automatic refresh—The graphs refresh automatically within a predetermined time interval.
- Two graph views:
  - Graph (Chart) view (this is the default)
  - Table (Grid) view

- Graph enlargement

Related Topics

- Using Interactive Graphs
- Time-based Graphs

Using Interactive Graphs

The following table summarizes how to use interactive graphs.

Table A-1 Using Interactive Graphs

To do this:	Do this:
Get help with the graph buttons	Hover your mouse cursor over the button. Prime Infrastructure displays a popup tooltip describing the button.
View the data as a graph or chart.	Click **View in Chart**.
View the data in grid or table form	Click **View in Grid**.
Enlarge the graph	Click the button located at the bottom right side of the graph. Prime Infrastructure displays an enlarged version of the graph in a separate page. The **View in Chart** and **View in Grid** toggle buttons are available in the new page, so you can change the type of enlarged graph displayed.

Related Topics

- Interactive Graphs
- Time-based Graphs

Time-based Graphs

Some graphs display time-based data. For these time-based graphs, Prime Infrastructure provides a link bar at the top of the graph. The link bar contains a set of links representing standard time-frames (such as the last six hours, one day, and so on) appropriate for the type of data in the chart. When you select one of these time-frame links, the data for that time frame is retrieved and the graph is refreshed to show only the data for that time-frame.

The time-frame links displayed in time-based graphs include the following:

- 6h—Denotes the last six hours of data from the current time. The data is gathered from the current database table.
- 1d—Denotes the last day (24 hours) of data from the current time. The data is gathered from the current database table.
- 1w—Denotes the last week (seven days) of data from the current time. The data is gathered from the hourly aggregated table.
- 2w—Denotes the last two weeks of data from the current time. The data is gathered from the hourly aggregated table.
- 4w—Denotes the last four weeks of data from the current time. The data is gathered from the hourly aggregated table.

- 3m—Denotes the last three months of data from the current time. The data is gathered from the daily aggregated table.
- 6m—Denotes the last six months of data from the current time. The data is gathered from the weekly aggregated table.
- 1y—Denotes the past year (12 months) of data from the current time. The data is gathered from the weekly aggregated table.
- Custom—User-selected time period. You can set the day and time for the start and end dates. The use of a current or hourly, daily, or weekly aggregated source for data depends upon the selected start date.

The default, maximum and minimum retention periods for the aggregated data displayed in time-based graphs are controlled by Prime Infrastructure administrators. For details, see "About Historical Data Retention" in Related Topics.

Related Topics

- Interactive Graphs
- Using Interactive Graphs
- About Historical Data Retention

Common UI Tasks

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

- Changing Your Password
- Changing Your Active Domain
- Setting Your Home Page
- Changing User Preferences
- Getting Device Details from Device 360° View
- Getting User Details from the User 360° View
- Getting Help

Changing Your Password

Step 1 Click your login name at the top-right of the screen 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 Click your login name at the top-right of the screen and choose **Virtual Domain**.

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

Setting Your Home Page

Step 1 Navigate to the page that you want to set as your home page.

Step 2 Click your login name at the top-right of the screen and choose **Set Current Page as Home**.

Changing User Preferences

You can modify how many items are displayed on list pages, map settings, idle timeout settings, and alarm display options.

Step 1 Click your login name at the top-right of the screen and choose **My Preferences**.

Step 2 Modify any of the settings, then click **Save**.

Getting Device Details from 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, click the info icon next to the device IP address.

Figure A-5 shows a sample of the Device 360° View.

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

Figure A-5 Sample Device 360° View

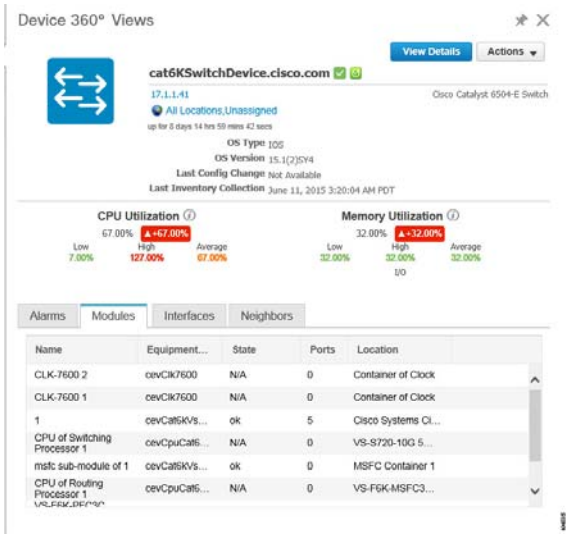


Table A-2 Device 360° View Features

Device 360° View Feature	Description
Device status	Indicates whether the device is reachable, is being managed, and is synchronized with the Prime Infrastructure database.
Action drop-down list	Choose one of the following options from the **Action** drop-down list at the top right of the device 360° view. • Alarm Browser—Launches the Alarm Browser. See Monitoring Alarms for more information. • Device Details—Displays device details. • Support Community—Launches the Cisco Support Community. See Launching the Cisco Support Community. • Support Request—Allows you to open a support case. See Opening a Support Case for more information. • Ping—Allows you to ping the device. • Traceroute—Allows you to perform a traceroute on the device. • Connect to Device—Allows you to connect to the device using Telnet, SSH, HTTP, and HTTPS protocols. **Note** There are some prerequisites for 360° view Telnet and SSH to work in client browser. • Firefox: Use external applications such as Putty for Telnet, and FireSSH add-on for SSH. • Internet Explorer (IE) and Google Chrome: Add Regedit entries for Telnet and SSH. (See Related Topics.)
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.

Table A-2 Device 360° View Features

Device 360° View Feature	Description
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.

Related Topics

- Connecting Device using Telnet and SSH in Internet Explorer and Google Chrome

Connecting Device using Telnet and SSH in Internet Explorer and Google Chrome

Before You Begin

Ensure that you have the Telnet and SSH browser plug-ins installed in Internet Explorer and Chrome.

Enabling Telnet client functionality in Internet Explorer

To enable Telnet client functionality in 64 bit Windows operating System with 32 bit Internet Explorer, follow these steps:

Step 1 Open the Telnet client in control panel.

- Go to Control Panel.
- Click **Programs And Features**.
- Click **Turn Windows features on or off** in the left pane.
- Check the Telnet Client check box.
- Click **OK**.

Step 2 Copy the 64 bit version of telnet.exe from System32 in Windows directory to SysWOW64 in the same directory.

Step 3 Add the following registry key for the 32 bit version of Internet Explorer.

- Open regedit.exe and navigate to the following registry key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet
Explorer\MAIN\FeatureControl\FEATURE_DISABLE_TELNET_PROTOCOL
```

- For backing up the key, right- click FEATURE_DISABLE_TELNET_PROTOCOL and select export. Save the key to a location where you can easily locate it when it needs to be restored.

Note If this key does not exist, please add the key as named above.

- Right-click FEATURE_DISABLE_TELNET_PROTOCOL again and select New and select DWORD (32-bit) Value from the drop-down list.
- In the right pane, rename the New Value as iexplore.exe.
- Verify that the value for iexplore.exe is 0x00000000 and close regedit.exe.

Step 4 Copy the file System32\en-US\telnet.exe.mui to the folder SysWOW64\en-US.

Enabling SSH

Follow these steps to start SSH session in Internet Explorer.

Step 1 Create a file called ssh.reg with the following content:

```
REGEDIT4
[HKEY_CLASSES_ROOT\ssh]
@="URL:ssh Protocol"
"URL Protocol"=""
[HKEY_CLASSES_ROOT\ssh\shell]
[HKEY_CLASSES_ROOT\ssh\shell\open]
[HKEY_CLASSES_ROOT\ssh\shell\open\command]
@="\"C:\\Program Files\\putty\\putty.exe\" \"%1\""
```

Step 2 Run this file to add the information to the Windows Registry.

Note If you perform Enabling Telnet client functionality in Internet Explorer and Enabling SSH, the changes will also be reflected in your Google chrome.

Related Topics

- Getting Device Details from Device 360° View

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, follow these steps:

Step 1 Choose **Monitor > Monitoring Tools > Clients and Users**.

Step 2 Click the expand icon next to a user name under the **User Name** column. You can view the User 360° View.

Figure A-6 shows a sample of the User 360° View.

Figure A-6 Sample User 360° View

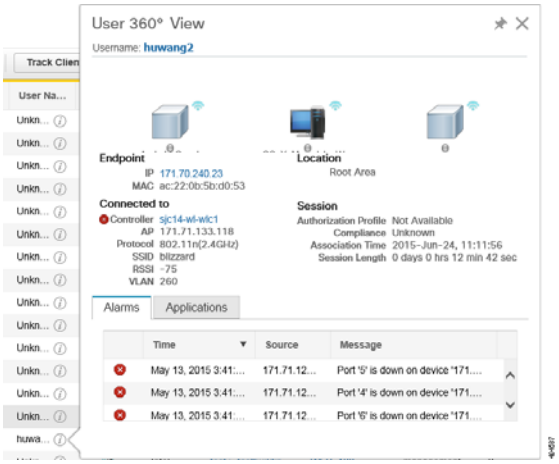


Table A-3 User 360° View Features

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.
Connected To	Displays 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 wheel next to your domain name (at the top-right of the screen) and choose **Contextual Help**.

Search Methods

Prime Infrastructure provides the following search methods:

- Application Search—See Performing an Application Search.
- Advanced Search—See Performing an Advanced Search.
- Saved Search—See Performing a Saved Search.

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

Performing an Application Search

To quickly search for data within Prime Infrastructure, you can enter any text string such as a partial or complete IP address or a username if you are searching for a client.

Step 1 Click the Search icon at the top-right of the screen.

Step 2 In the Search text box, enter a search string and click **Search Prime Infrastructure**.

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, follow these steps:

Step 1 Click the Search icon at the top-right of the screen.

Step 2 From the Search pulldown menu, select **Advanced Search**.

Step 3 In the Advanced Search dialog box, choose a category from the Search Category drop-down list.

Step 4 Choose all applicable filters or parameters for your search.

Note Search parameters change depending on the category that you selected.

Step 5 To save this search, select 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 for more information.

The Search categories include the following:

- Access Points—See Searching Access Points
- Alarms—See Searching Alarms
- Clients—See Searching Clients
- Chokepoints—See Searching Chokepoints

- Configuration Versions—See Searching Configuration Versions
- Controller Licenses—See Searching Controller Licenses
- Controllers—See Searching Controllers
- Device Type—See Searching Device Types
- Events—See Searching Events
- Interferers—See Searching Interferers
- Jobs—See Searching Jobs
- Maps—See Searching Maps
- Rogue Client—See Searching Rogue Clients
- Shunned Client—See Searching Shunned Clients
- Switches—See Searching Switches
- Tags—See Searching Tags
- Wi-Fi TDOA Receivers—See Searching Wi-Fi TDOA Receivers

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.

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 Office Extend 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.
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 configuration 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.
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.
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.

Table A-10 Search Clients Fields (continued)

Field	Options
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-10).

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 Types

You can configure the following parameters when performing an advanced search for device type (see Table A-19).

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-20).

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, follow these steps:

Step 1 Click the icon in the Application Search box, then 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**.