Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive

€

CHAPTER

CHAPTER

Step 4 Browse to the location of the license file, then click **OK**Of . Cisco Prime Infrastructure 3.0 Administrator Guide for deleting licenses, troubleshooting licensing issues, and verifyin

To edit device parameters, follow these steps:

Step 1 Choose **Inventory > Device Management > Network Devices**.

Step 2 Select a single device or multiple devices and Click **Edit**.

Step 3

CHAPTER

CHAPTER

CHAPTER 6

Changing User Settings

Prime Infrastructure provides user preference settings that allows you to modify how information is displayed.

Changing Your User Preferences

CHAPTER

Related Topic

Managing and Editing Dashboards

Network Summary Dashboards

Choose one of the following dashboards under **Dashboard > Network Summary** to view a summary of important data points in your network. Table 7-4 describes the default information shown in each of the

€

The Current Tx Power Level setting controls the maximum conducted transmit power. The maximum available transmit power varies according to the configured channel, individual country regulation, and

Monitoring Rogue AP Alarms

- Failure Source
- Owner
- Time
- Message
- Category
- Condition
- Acknowledged

Step 2 Select the check box next to the alarm and modify the required fields in the **Alarm Browser** toolbar.

Monitoring Air Quality Alarms

To monitor air quality alarms on your network:

Step 1 Perform an advanced search for **Performance** alarms.

The **Search Results** page contains the following information for air quality alarms.

- Severity
- Failure Source
- Owner
- Time
- Message
- Category
- Condition
- Acknowledged

Step 2 Select the check box next to the alarm and modify the required fields in the **Alarm Browser** toolbar.

Monitoring CleanAir Security Alarms mwu: alarms.

- Acknowledged

Step 2

- SSID—Service Set Identifier being broadcast by the rogue access point radio. (Blank if SSID is not broadcast.)
- Containment Level—An access point which is being contained is either unable to provide service at all, or provides exceedingly slow service. There is a level associated with the containment activity

CHAPTER

Polled Data in Dashlets and Reports

When viewing polled data from devices, consider the following scenario:

- Device 1 data is polled from the last 6 hours.
- Device 2 data is polled from the last 2 days.

When you filter dashlets or reports to show data from the past 2 days, only the data from Device 2 is displayed.

Display Options

The following sections explain the various ways you can modify how alarms, events, and syslogs are displayed:

- Viewing Options for Alarms, Events, and Syslogs
- Displaying Alarm Icons
- Changing Alarm Display Behavior

Viewing Options for Alarms, Events, and Syslogs

When you choose

Where to Find Syslogs

Prime Infrastructure logs all syslogs from severity

CHAPTER

Launching the Client Troubleshooting Tool

You can launch the Client Troubleshooting tool fo

Figure 12-2 Client Troubleshooting page for Unsuccessful Wireless Client

Related Topics

- Launching the Client Troubleshooting Tool
- How the Client Troubleshooting Tool Gives Advice
- Searching for Clients

How the Client Troubleshooting Tool Gives Advice

Prime Infrastructure determines the number of connection areas and the type of troubleshooting advice to present on the Client Troubleshooting page based on the stages the client passes through when establishing connection and connectivit

- Purged Expired Entries—You can set the duration to keep tracked clients in Prime Infrastructure database. Clients can be purged as follows:
  - after 1 week
  - after 2 weeks
  - after 1 month
  - after 2 months
  - after 6 months
  - kept indefinitely
- Notification Frequency—You can specify when Prime Infrastructure sends a notification of a tracked client:
  - on first detection
  - on every detection
- Notification Method—You can specify that the tracked client event generates an alarm or sends an email message.

Step 5 Enter the email address.

Step 6 Click **Save**.

Related Topics

- Tracking Clients
- Identifying Unknown Users

When to Assign a Username

Not all users or devices are authenticated via 802.1x (for example, printers). In such a case, a network administer can assign a username to a device.

If a client device is authenticated to the network through web auth, Prime Infrastructure might not have username information for the client (applicable only for wired clients).

CecTw(}Tjp1e

Identifying Unknown Users

Viewing Client V5 Statistics

To access the Statistics request page, follow these steps:

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

Step 2 Select a client.

Step 3 From the **Test** drop-down list, choose **V5 Statistics**.

This menu is shown only for CCX v5 and later clients.

Step 4 Click **Go**.

Step 5 Select the desired type of stats (Dot11 Measurement or Security Measurement).

Step 6 Click **Initiate** to initiate the measurements.

- Maximum Packet loss% over time

A particular service provider may not have TCA, but may have RC events occurring when a route changes from the other service provider to the selected service provider. The Metrics panel may not show any graphs for the particular service provider whereas the PfR events table shows the RC events of the service provider.

Related Topics

- PfR Monitoring Landing Page
- Site to Site PfR Events Table
- Site to Site PfR Events Table
- Time Slider

Time Slider

A time slider present at the bottom of the page, represents the time range selected using the filter. You can drag the slider and set a particular time range. The Metrics Panels and the Site to Site PfR events table change corresponding to the set time range.

Related Topics

- PfR Monitoring Landing Page
- PfR Site To Site Details Page
- Metrics Crossing Thresholds Vs Service Provider(s)

Step 4

Step 5

CHAPTER

successfully joins a wireless controller, it cannot be managed by Prime Infrastructure, and it does not

CHAPTER 18

Viewing the Operations Center Dashboards

The Operations Center provides additional, Operations Center-specific dashboards that you can use to quickly determine the status of your network and identify any issues that require further attention. The Operations Center dashlets display aggregated data. The following types of dashboards are available:

-

€

CHAPTER

In this example, there are four custom dynamic groups, one for each region based on the cities in every region: North Region, South Region, East Region, and West Region. You must update the enable password for all of the devices in the north and south region. After this is complete, you plan to set another job to occur for the West and East region devices to occur three months later.

Step 3 From the Security Zone page, click **Add Object**.

Step 4 Specify a name and description for the security zone that is being created.

Step 5 Specify a set of rules that defines the interfaces that must be attached to the zone.

Step 6 To specify Device Level Override, choose **Device Level Override > Add Device**.

Step 7 Select the device you wish to add, and click **OK**.

Step 8 Click **OK**

The template appears in the Template List page. In the Template List page, you can apply this template

- TACACS+ Server Templates
- Local EAP General Templates
- Local EAP Profile Templates
- EAP-FAST Templates
- Creating Network User Priority Templates
- Local Network Users Templates
- Guest User Templates
- User Login Policies Templates
- Creating a MAC Filter Template
- Access Point or MSE Authorization Templates
- Creating a Manually Disabled Client Template
- Access Point Authentication and MFP Templates
- Web Authentication Templates
-

Related Topics

- Web Authentication Templates
- Customized Web Auth

Viewing Deployed Rogue AP Rules

You can view and edit the Rogue AP Rules that you previously deployed.

Step 1 Choose

- SIPs are available only on the Cisco 5500 Series

Step 4 In the MCS (Data Rate) Settings column, choose which level of data rate you want supported.

– **Default Values**—The roaming parameters ar

– Select the **Report Interferers** check box to enable CleanAir system to report and detect sources

Step 3 Click **Save as New Template**.

Step 9 Click **Save as New Template**

Step 2 Hover the mouse on

If the template is applied successfully and the Update Telnet Credentials option is enabled, the applied management user credentials are used in Prime Infrastructure for Telnet/SSH credentials to that applied

Step 11 Configure the Hyperlocation Config parameters:

-

Step 5 When you are finished, click **Save as Template**.

Related Topics

-

Step 2 Select **View Current Status** from the Select a command drop-down list in the Autonomous AP Migration Templates page to view the status of Cisco IOS access point migration.

The following information is displayed:

- IP Address—IP address of the access point.
-

Related Topics

-

  - Download Customized Web Auth
  - Download Vendor Device Certificate
  - Download Vendor CA Certificate
  - Bulk Update Controllers

- Configure
  - Save Config to Flash
  -

Step 3

-

Step 4 From the Upload/Download Commands drop-down list, choose **Upload File from Controller**, then click **Go**.

By default, configuration file encryption is disabled

Related Topics

Related Topics

- Configuring Controller

Viewing

Interface

-

Related Topics

- Configuring Controller Multicast Mode
-

Configuring a Global Access Point Password

The AP Username Password page enables you to set a global password that all access points inherit as they join a controller. When you are adding an access point, you can also choose to accept this global username and password or override it on a per-access point basis.

- Holdtime (seconds)—Enter the time in seconds before the CDP neighbor entry expires. The default is 180.
-

IGMP Snooping and timeout can be set only if Ethern

FlexConnect Authentication Process

Related Topics

- FlexConnect Groups and Backup RADIUS Servers
- FlexConnect Groups and CCKM
- FlexConnect Groups and Local Authentication
- Auditing FlexConnect Groups

FlexConnect Groups and Backup RADIUS Servers

You can configure the controller to allow a FlexConnect AP in standalone mode to perform full 802.1x authentication to a backup RADIUS server. You can either configure a primary RADIUS server or both a primary and secondary RADIUS server.

Related Topics

- FlexConnect Groups and CCKM
- FlexConnect Groups and Local Authentication
- Auditing FlexConnect Groups

FlexConnect Groups and CCKM

FlexConnect groups are required for CCKM fast roaming. When you configure your WLAN for CCKM fast secure roaming, EAP-enabled clients securely

Step 1 Choose **Configuration > Network > Network Devices**

Step 5

Step 3 From the left sidebar menu, choose

-

- Action—What the controller is directed to do when the signature detects an attack. For example:
  - None—No action is taken.
  - Report—Report the detection.
- State—Enabled or Disabled.
- Description—A more detailed description of the type of attack the signature is trying to detect.

Step 4 Click a signature Name to view individual parameters and to enable or disable the signature.

Related Topics

- Configuring IDS Signatures
- Downloading Signature Files
- Uploading Signature Files
- Global Settings for Standard and Custom Signatures
- Configuring IDS Signatures
- Viewing Controller Standard Signature Pa

- Media Stream Name
- Multicast Destination Start IP—Start IP address of the media stream to be multicast
- Multicast Destination End IP—End IP address of the media stream to be multicast
-

- Configuring 802.11a/n RRM Intervals
- Configuring 802.11a/n RRM Transmit Power Control
-

- Configuring 802.11a/n RRM Radio Grouping
- Configuring 802.11a/n Media Parameters
- Configuring 802.11a/n EDCA Parameters
-

- CleanAir—Select the check box to enable CleanAir functionality on the 802.11b/g/n network, or unselect to prevent the controller from detecting spectrum interference. The default value is selected.
- Reporting Configuration—Use the parameters in this section to configure the interferer devices you want to include for your reports.
  - Report—Select the **report interferers** check box to enable CleanAir system to report and detect sources of interference, or unselect it to prevent the controller from reporting interferers. The default value is selected.
  - Make sure that any sources of interference that need to be detected and reported by the CleanAir

-

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose

- Maximum Bindings Allowed—Maximum number of binding updates that the controller can send to the MAG. The valid range is between 0 to 40000.
- Binding Lifetime—Lifetime of the binding entries in the controller. The valid range is between 10 to 65535 seconds. The default value is 65535. The binding lifetime should be a multiple of 4 seconds.
- Binding Refresh Time—Refresh time of the binding entries in the controller. The valid range is between 4 to 65535 seconds. The default value is 300 seconds. The binding refresh time should be a multiple of 4 seconds.
- Binding Initial Retry Timeout—Initial timeout between the proxy binding updates (PBUs) when the controller does not receive the proxy binding acknowledgments (PBAs). The valid range is between 100 to 65535 seconds. The default value is 1000 second.
-

Step 5 Click **Save**.

Modifying Telnet/SSH Parameters

Prerequisites for using the Sniffer Feature

Before using the sniffer feature, you must complete the following:

-

Deleting SSID Groups

-

CHAPTER

Related Topics

- Adding Controller Configuration Groups

For more details on configuration options, see the *AeroScout Context-Aware Engine for Tags, for Cisco Mobility Services Engine User Guide* at the following URL: http://support.aeroscout.com.

To add a TDOA receiver to the Prime Infrastructure

Step 2 From the left sidebar menu, choose **Download Software**.

Step 3 Click the Controller to open the Download Software Task details page, then click **Select Controller** to view the controller list.

Step 4 Complete the required information in the **Rule Information, Platform Selection, Rule Inputs** and **Conditions and Actions** areas. See Table 25-1

Rule Inputs

New Rule Input	Click **New** to add inputs for the new rule. The input you create in this pane reflects in the Policy Profile page. You must provide rule inputs for the rule you have selected. For example, you can create an input to be IP Address. Any user who wants to run this rule can enter an IP address specific to the rule and add it to a specific profile. Enter the required details: For Identifier, h(.7(t yu).558 TCt)4.3(o)284.7wh n heniif2ier,forc(lick h)-1th58 TCek

Condition Scope Details

- Condition Scope—Select the scope of the conditions from one of the below:
  - Configuration—Checks the complete running configuration.
  - Device Command Outputs—Checks the output of show commands.
  -

Value	The value must be a regular expression. Rule inpu

NTP Server Redundancy

This compliance policy checks if the command **ntp server**

Global Configuration	• ACLs • CDP • Clock • •C

Running Compliance Profiles Against Devices

Fixing Compliance Violations on Devices

Viewing Field Notices for Devices

Step 2 From the Plug and Play Profiles page, select a profile from the list.

Step 3 Click **Device Details for Profile**.

Step 4 Click **Export Bootstrap > TFTP**.

Step 5

The following configurations are set by the Plug and Play profile, but you can modify them using the Getting Help Setting Up Access Switches workflow:

- SNMPv2 and SSH Credentials—The SNMP, Telnet, and SSH credentials you specify will be configured on *all* devices that use the Plug and Play profile. You c3(y]TJ-21.5396 Tc.2048 TD.0condentials

```
quit
exit
ip host pi-hateast-151 10.104.119.151
cns trusted-server all-agents pi-hateast-151
cns trusted-server all-agents 10.104.119.151
cns id hardware-serial
cns id hardware-serial event
cns id hardware-serial image
cns event pi-hateast-151 encrypt keepalive 120 2 reconnect-time 60
cns exec encrypt 443
cns image server https://pi-hateast-151/cns/HttpMsgDispatcher status
https://pi-hateast-151/cns/HttpMsgDispatcher
cns config partial pi-hateast-151 encrypt 443
cns config initial pi-hateast-151 encrypt 443
```

CI C

€

CHAPTER

CHAPTER

CHAPTER

CHAPTE

Creating Device Groups

You can create the following device groups:

- Static—Create and name a new device group to which you can add devices from **Inventory > Device**

€

CHAPTER 33

Using Network Topology Maps

Cisco Prime Infrastructure provides a visual map of your network's physical topology, including the

Topology Map Icons

In topology maps, device icons reflect the device alarm state and correspond to

Isolating Specific Sections of a Large Topology Map

In cases where a topology map is displaying thousands of devices, you may want to focus on specific devices or sets of devices. The Overview pane show

Getting More Information About Links

The representation of links in the topology map provides some information about the link:

•

Saving the Topology Map as an Image File

Selecting this setting prevents distortion when Prime Infrastructure resizes the imported map image.

Step 8 Enter the campus site's horizontal and vertical dimensions, in feet or meters.

Step 9

- Adding Image Files to Campus Maps

Adding Buildings to Campus Maps

-

- Display—Choose the tag identifier (MAC address, asset name, asset group, or asset category) to display on the map.
-

- Managing Location Presence Information

Adding Wi-Fi TDOA Receivers to Prime Infrastructure

To add Wi-Fi TDOA receivers to the Prime

- Channel

Configuring Google Earth Settings for Access Points

You can configure access point settings for the Google Earth Maps feature:

Step 1 Choose **Maps > Google Earth**.

Step 2 Configure the following parameters:

- Refresh Settings—Select the **Refresh from Netwlect the**

- Yellow—Marginal
- Red—No

The accuracy of the Green/Yellow/Red regions depends on the RF environment and whether or not the floor is calibrated. If the floor is calibrated, the accuracy of the regions is enhanced.

You can confirm that the synchroniz

Monitoring Mesh Networks Using Maps

Prime Infrastructure allows you to access and view details for the following elements from a mesh network map:

- Mesh Link Statisticsp:

€

Table 36-5 Layer 2 and Layer 3 Prerequisites for Guest Anchor Controller

Related Topics

- Prerequisites for Converged Access Deployment
- Prerequisites for Server Configuration

Related Topics

Configuring the Device using WSMA

NBAR Protocol Packs

Configuring Cellular WAN Interfaces

The Cisco ISRs provide a third-generation (3G) wireless interface that can be used over GSM and Code Division Multiple Access (CDMA) networks. Its primary application is WAN connectivity as a backup data link for critical data applications. However, the 3G wireless interface can3.3(t)3nect(o)4.5n (as th)4.5(e)]T

Step 9 Choose the **Migration** tab, and select the **Enable Passive SA**

Editing a Security Zone

To edit a security zone, follow these steps:

Step 1 Choose **Inventory > Device Management > Network Devices**, then select a device.

Step 2 In the Feature Configuration pane, expand the **Security** subfolder.

Step 3 In the Security subfolder, expand the **Zone Based Firewall > Common Building Blocks**, and then click **Zones**.

Step 4 In the Zones page, choose one of the following options:

- **a.** Click the Zone parameters row, and edit the parameters. or
- **b.** Select the zone, and click **Edit**. The selected Zone entity opens for editing.

Step 5

Monitoring Policy Rules

Figure 38-2 Sample Baseline Values

To enable baselining, follow these steps:

Step 1 Choose **Dashboard** > **Performance** > **Application**.

CHAPTER

CHAPTER

Viewing Microsoft Lync Data

CHAPTER

- Flag—The device on which the Mediatrace or Traceroute was initiated.
- Filmstrip—The device is Medianet-capable.
-

CHAPTER

Related Topics

- Adding MSEs to Prime Infrastructure
- Adding a Location Server
-

```
Time..................................... Fri Sep 7 08:00:26 2007
Timezone delta........................... -8:0
```

The time zone delta parameter in the **show time** command shows the difference in time between the local time zone and GMT (8 hours). Before configuration, the parameter setting is 0.0.

Related Topics

- Viewing MSEs
-

- IP address
- Port No.
- Community
- Destination type
- SNMP Version

Step 7 Click **OK**

Step 10 Click

- Tracked Tags Limit

Clients

Mobile Concierge Service Parameters

Viewing Configured Service Advertisements

To view the configured service

If you choose SOAP, specify whether to send notifications over HTTPS by selecting its corresponding check box. If you do not, HTTP is used. Also, enter the destination port number in the Port Number text box.

– **Mail**—Use this option to send notifications through e-mail.

If you choose Mail, you need to choose the protocol for sending the e-mail from the Mail Type

Step 1 Choose

Step 11

CHAPTER

CHAPTER

CHAPTER

Converting MAs to MCs (and vice versa) is limited to 3850 devices. For a changed role to take

Step 2

- **Profile Name**—Indicates the user-defined name for the current profile. Click the profile name to view or edit profile details.

  Hover your mouse cursor over the profile name to view the Profile ID and version.
- **MSE(s) Applied To**—Indicates the number of mobility services engines (MSEs) to which this profile is applied. Click the MSE number to view profile assignment details.
- **Controller(s) Applied To**—Indicates the number of controllers to which this profile is applied.

Click the report title to view the details for this report.

- Report Type—Identifies the specific report type.
- Scheduled—Indicates whether this report is enabled or disabled.
- Virtual Domain—Identifies the name of the virtual domain under which this report is scheduled.
- Run Now—Click the run icon to immediately run the current report.

APPENDIX A

Searching Controller Licenses

You can configure the following parameters when performing an advanced search