Field Reference for Operate Pages

This section provides descriptions of the fields found in the pages under the **Operate** menu in Cisco Prime Infrastructure.

- Device Work Center, page 2-1
- Operational Tools, page 2-5

Device Work Center

The following topics contain descriptions of the fields found in Device Work Center:

- Configuration > Security > NAT, page 2-1
- Configuration > Security > Zone Based Firewall, page 2-4
- Service Container > Add, page 2-5

Configuration > Security > NAT

The following topics describe the fields in **Operate > Device Work Center > Configuration > Security > NAT > NAT44 Rules**.

- Add NAT Rule > Static Rule, page 2-1
- Add NAT Rule > Dynamic NAT Rule, page 2-2
- Add NAT Rule > Dynamic PAT Rule, page 2-3

Add NAT Rule > Static Rule

The following table describes the elements on **Operate > Device Work Center > Configuration > Security > NAT > NAT44 Rules > Add NAT Rule > Static Rule**.

Table 2-1 Add NAT Rule > Static Rule

Element	Description
Direction	Enter the directions. Cisco Prime Infrastructure Release 2.0 supports only the Inbound to Outbound direction.
VRF	Enter the virtual routing and forwarding (VRF) on which the NAT translation process occurs.

Table 2-1 Add NAT Rule > Static Rule (continued)

Element	Description
Source A	Enter a valid IPv4 address. A valid IPv4 address consists of four octets separated by a period (.). • If Source A is defined, Source B must also be defined. • If Source A is defined, Destination A will be **Any** by default.
Destination A	Enter a valid IPv4 address. A valid IPv4 address consists of four octets separated by a period (.). • If Destination A is defined, Destination B must also be defined. • If Destination A is defined, Source A will be **Any** by default.
Translation	Select the static translation type.
Source B	Enter a valid IPv4 address. A valid IPv4 address consists of four octets separated by a period (.). You can also select an interface from the list of interfaces. • If Source B is defined, Source A must also be defined. • If Source B is defined, Destination B will be **Any** by default.
Destination B	Enter a valid IPv4 address. A valid IPv4 address consists of four octets separated by a period (.). • If Destination B is defined, Destination A must also be defined. • If Destination B is defined, Source A and B will be **Any** by default.
Options	Enter the advance options for the Static type. Configure the following: • To ignore the embedded IP addresses (no-Payload), select the **Ignore Embedded IP Address** check box. • To enable port translation, select the **Enable Port Translation** check box, and then define the following: – TCP or UDP – Original Port – Translated Port

Add NAT Rule > Dynamic NAT Rule

The following table describes the elements in **Operate > Device Work Center > Configuration > Security > NAT > NAT44 Rules > Add NAT Rule > Dynamic NAT Rule**.

Table 2-2 Add NAT Rule > Dynamic NAT Page

Element	Description
Direction	Enter the directions. Cisco Prime Infrastructure Release 2.0 supports only the Inbound to Outbound direction.
VRF	Enter the VRF on which the NAT translation process occurs.
Source A	Select the ACL name from the list. • If Source A is defined, Source B must also be defined. • If Source A is defined, Destination A will be **Any** by default.

Table 2-2 Add NAT Rule > Dynamic NAT Page (continued)

Element	Description
Destination A	Select the ACL name from the list. • If Destination A is defined, Destination B must also be defined. • If Destination A is defined, Source A will be **Any** by default.
Translation	Select the Dynamic NAT translation type.
Source B	Choose the NAT pool from the drop-down list. You can also select an interface from the list of interfaces. • If Source B is defined, Source A must be defined. • If Source B is defined, Destination B will be **Any** by default.
Destination B	Choose the NAT pool from the drop-down list. • If Destination B is defined, Destination A must also be defined. • If Destination B is defined, Source A and B will be **Any** by default.
Options	Enter the advance options for the Dynamic type. • To ignore the embedded IP addresses (no-Payload), select the **Ignore Embedded IP Address** check box. • To enable port translation, select the **Enable Port Translation** check box, and then define the following: – TCP or UDP – Original Port – Translated Port **Note** This option is supported only on the Cisco Integrated Services Routers.

Add NAT Rule > Dynamic PAT Rule

The following table describes the elements in **Operate > Device Work Center > Configuration > Security > NAT > NAT44 Rules > Add NAT Rule > Dynamic PAT Rule**.

Table 2-3 Add NAT Rule > Dynamic PAT Page

Element	Description
Direction	Enter the directions. This release supports only the Inbound to Outbound direction.
VRF	Enter the VRF on which the NAT translation process occurs.
Source A	Select the ACL name from the list.
Destination A	Destination A cannot be defined.
Translation	Select the Dynamic PAT translation type.
Source B	Select the IP Pool Name from the list. You can also select an interface from the list of interfaces.
Destination B	Destination B cannot be defined.
Options	Enter the advance options for the Dynamic PAT. To ignore the embedded IP addresses (no-Payload), select the **Ignore Embedded IP Address** check box. **Note** This option is supported only on Cisco ISRs.

Configuration > Security > Zone Based Firewall

The following table describes the fields in **Operate > Device Work Center > Configuration > Security > Zone Based Firewall > Policy Rule**.

Table 2-4 Zone Based Firewall > Policy Rule Page

Element	Description
Name	(Optional) Enter a name for the policy rule.
Source Zone	Enter the name of the zone from which the traffic is originating.
Destination Zone	Enter the name of the zone to which the traffic is bound.
Source	Enter the source IP address of the inspected data. The valid parameters are: • Any • A combination of IPv4 addresses and subnets
Destination	Enter the destination IP address of the inspected data. The valid parameters are: • Any • A combination of IPv4 addresses and subnets
Service	Service of the inspected data. The valid parameters are: • Services • Port Based Applications • TCP • UDP • ICMP
Action	Choose the action to perform on the traffic when there is a match on a rule condition. A rule matches when: • The traffic source IP address matches the source rule condition. • The traffic destination IP address matches the destination rule condition, and the traffic-inspected service matches the service rule condition. Action options are: • Drop • Drop and Log • Inspect • Pass • Pass and Log
Advanced Options	Specify the configuration parameters to set the Firewall Rule Parameter-Map behavior when the Action option is set to Inspect.

For descriptions of the fields in the Security tab, refer to the "Security Templates Field Descriptions" section on page 1-71.

Service Container > Add

The following table describes the fields in **Operate > Device Work Center > Service Container> Add**.

Table 2-5 Operate > Device Work Center > Service Container > Add

Field	Description
Select an Operation	Choose either **Install** or **Install and Activate** depending on whether you want to activate the container later or during the current instance.
WAAS-XE IP Address/Mask	Enter the Cisco Wide Area Application Services (WAAS)-Cisco IOS XE container's IP address and mask.
Router Virtual Interface IP/Mask	Enter the IP and mask for the Router Virtual Interface on which you want to install the container.
OVA	From the list, choose the OVA image that is to be installed.
Resource Profile	From the list, choose a resource profile as per the memory requirement.
Service Container Name	Enter a name for the service container.
Enable WAN Optimization on	Select the check box to begin WAN optimization, and choose an interface role to initiate traffic redirection.

Operational Tools

The following topics contain field descriptions for Operational Tools:

- Packet Capture > Capture Sessions, page 2-5
- Wireless Operational Tools, page 2-6

Packet Capture > Capture Sessions

The following table describes the fields on **Operate > Operational Tools > Packet Capture > Capture Sessions**.

Table 2-6 Operate > Operational Tools > Packet Capture > Capture Sessions

Field	Description
Name	Enter a unique name for this capture session.
Packet Slice Size (bytes)	To capture the full packet, enter 0.
File Size (MB)	The total size of the capture file.
Rotate Files	If this option is enabled, the capture will be continuous until it is explicitly stopped. For NAM, the results are stored in round robin sequence by the "number of files" parameter. For example, if "rotate" is true and "number of files" is 2, two capture files will be used to store content. Packets will be saved in the first file until it is full, then the process is repeated in the next file. For ASR, the packet file is circular (the same file is used; the contents are overwritten).

Table 2-6 Operate > Operational Tools > Packet Capture > Capture Sessions (continued)

Field	Description
For ASR devices only:	• Packet-to-Sample: Which *n*th packet to capture. For example, "3" means every third packet. • Packet-Rate: Number of packets to be captured per second. (minimum: 1; valid entries: 0-9.). • Duration: How long to capture. • Packets: The total number of packets to capture.
Number of files	The number of files used to store content. For NAM devices only.

Wireless Operational Tools

The following sections contain field descriptions for pages found in **Operate > Operational Tools > Wireless**.

Guest User Controller Field Descriptions

The following topics describe the fields on the **Operate > Operational Tools > Wireless > Guest User > Add Guest User > New Controller Template** page.

- Guest User > Add Guest User > New Controller Template > General Tab, page 2-6
- Guest User > Add Guest User > New Controller Template > Advanced Tab, page 2-7

Guest User > Add Guest User > New Controller Template > General Tab

The following table describes the fields on **Operate > Operational Tools > Wireless > Guest User > Add Guest User > New Controller Template > General**.

Table 2-7 Guest User > Add Guest User > New Controller Template > General Tab Field Descriptions

Field	Description
User Name	Enter a guest username. The maximum size is 24 characters.
Generate Password	Select the check box to generate a username and password on every schedule of guest user account creation. If this is enabled, a different password is supplied for each day (up to the number of days chosen). If this is disabled (unselected), one password is supplied for a span of days. The generation of a new password on every schedule is optional.
Password	Enter a password. Password requirements include the following: • The password must have a minimum of eight characters. • The password must include at least three of the following elements: lowercase letters, uppercase letters, numbers, or special characters.
Confirm Password	Reenter the password that you entered in the Password field.
Description	Enter a description of the guest user template.
Disclaimer	The default disclaimer text.
Make this Disclaimer Default	Select the check box to set the disclaimer text as the default for this guest user template.

Guest User > Add Guest User > New Controller Template > Advanced Tab

The following table describes the fields on **Operate** > **Operational Tools** > **Wireless** > **Guest User** > **Add Guest User** > **New Controller Template** > **Advanced**.

Table 2-8 Guest User > Add Guest User > New Controller Template > Advanced Tab Field Descriptions

Field	Description
Import From File	Select the check box to import bulk guest user templates.
Profile	Select the profile to which the guest users would connect.
User Role	Choose a user role for the guest user from the drop-down list. User roles are predefined by the administrator and are associated with the access of the guest (such as contractor, customer, partner, vendor, visitor, and so on). User Role is used to manage the amount of bandwidth allocated to specific users within the network.
Life Time	Define how long the guest user account remains active by choosing one of the following options: • Limited—Choose the period of time that the guest user account is active using the hours and minutes drop-down lists. The default value for Limited is one day (8 hours). • Unlimited—There is no expiration date for the guest account. **Note** If you choose Unlimited when configuring the guest account for Cisco Catalyst 3850 Switches (Cisco IOS XE 3.2.1) and Cisco 5760 Wireless LAN Controllers, the maximum time period that the guest account will be active is one year.
Apply to	From the drop-down list, choose one of the following: • **Indoor Area**—Campus, Building, and Floor. • **Outdoor Area**—Campus, Outdoor Area. • **Controller List**—List of controller(s) on which the selected profile is created. • **Config Groups**—Config group names configured on Prime Infrastructure.

Voice Audit Field Descriptions

The following topics describe the fields on the **Operate** > **Operational Tools** > **Wireless** > **Voice Audit** page.

- Voice Audit > Controller Tab, page 2-8
- Voice Audit > Rules Tab, page 2-8
- Voice Audit > Report Tab, page 2-10

Voice Audit > Controller Tab

The following table describes the fields on **Operate** > **Operational Tools** > **Wireless** > **Voice Audit** > **Controller**.

Table 2-9 Voice Audit > Controller Tab Field Descriptions

Field	Description
Run audit on	Choose one of the following options: • All Controllers—No additional Controller information is necessary. • A Floor Area—From the drop-down lists, choose the applicable campus, building, floor, and controller. • A Single Controller—Choose the applicable controller from the drop-down list.

Voice Audit > Rules Tab

The following table describes the fields on **Operate** > **Operational Tools** > **Wireless** > **Voice Audit** > **Rules**.

Table 2-10 Voice Audit > Rules Tab Field Descriptions

Rule	Rule Details
VoWLAN SSID	Description—Checks whether or not the VoWLAN SSID exists. Rule validity—User-defined VoWLAN SSID.
CAC: 7920	Description—Checks whether or not 7920 AP CAC is enabled for VoWLAN. Rule validity—User-defined VoWLAN SSID.
CAC: 7920 Clients	Description—Checks whether or not the 7920 Client CAC is disabled for VoWLAN. Rule validity—User-defined VoWLAN SSID.
DHCP Assignment	Description—Checks whether or not DHCP assignment is disabled for VoWLAN. Rule validity—User-defined VoWLAN SSID.
MFP Client	Description—Checks whether or not MFP Client protection is not set to **Required** for VoWLAN. Rule validity—User-defined VoWLAN SSID.
Platinum QoS	Description—Checks whether or not QoS is set to Platinum (Voice) for VoWLAN. Rule validity—User-defined VoWLAN SSID.
Non Platinum QoS	Description—Checks that QoS is not set to Platinum for non-VoWLAN. Rule validity—User-defined VoWLAN SSID.
WMM	Description—Checks whether or not WMM is enabled for VoWLAN. Rule data—Choose **Allowed** or **Required** from the drop-down list. Rule validity—User-defined VoWLAN SSID.
CCKM	Description—Checks whether or not CCKM is enabled for VoWLAN. Rule validity—User-defined VoWLAN SSID.

Table 2-10 Voice Audit > Rules Tab Field Descriptions (continued)

Rule	Rule Details
CCKM With No AES- for 792x phones	Description—Check that AES encryption is not enabled with Cisco Centralized Key Management (CCKM) for VoWLAN. This rule is only for 792x phones. Rule validity—User-defined VoWLAN SSID.
TSM	Description—Check that Traffic Stream Metrics (TSM) is Enabled. Rule data—Select **802.11a/n TSM**, **802.11b/g/n TSM**, or both check boxes. Rule validity—At least one band must be selected.
DFS	Description—Checks whether the Channel Announcement and Channel Quite Mode are Enabled for Dynamic Frequency Selection (DFS).
ACM	Description—Checks whether or not Admission Control is enabled. Rule data—Select **802.11a/n ACM**, **802.11b/g/n ACM**, or both check boxes. Rule validity—At least one band must be selected.
DTPC	Description—Checks whether or not Dynamic Transmit Power Control is enabled. Rule data—Select **802.11a/n DTPC**, **802.11b/g/n DTPC**, or both check boxes. Rule validity—At least one band must be selected.
Expedited Bandwidth	Description—Checks whether or not Expedited Bandwidth is enabled. Rule data—Select **802.11a/n Expedited Bandwidth**, **802.11b/g/n Expedited Bandwidth**, or both check boxes. Rule validity—At least one band must be selected.
Load Based CAC	Description—Checks whether or not Load Based Admission Control (CAC) is enabled. Rule data—Select **802.11a/n Load Based CAC**, **802.11b/g/n Load Based CAC (LBCAC)**, or both check boxes. Rule validity—At least one band must be selected.
CAC: Max Bandwidth	Description—Checks whether or not Maximum RF Bandwidth for Call Admission Control is configured properly. Rule data—Enter percentages in the text boxes for Maximum Allowed Bandwidth for 802.11a/n and 802.11b/g/n. Rule validity—Data for at least one band must be provided. The valid range is 0 to 100%.
CAC: Reserved Roaming Bandwidth	Description—Checks whether or not Reserved Roaming Bandwidth for Call Admission Control is configured properly. Rule data—Enter percentages in the text boxes for Maximum Reserved Roaming Bandwidth for 802.11a/n and 802.11b/g/n. Rule validity—Data for at least one band must be provided. The valid range is 0 to 100%.
Pico Cell mode	Description—Checks whether or not Pico Cell mode is disabled. Rule data—Select **802.11a/n Pico Cell mode**, **802.11b/g/n Pico Cell mode**, or both check boxes. Rule validity—At least one band must be selected.

Table 2-10 Voice Audit > Rules Tab Field Descriptions (continued)

Rule	Rule Details
Beacon Period	Description—Checks whether or not Beacon Period is configured properly. Rule data—Enter the time (ms) in the text boxes for Beacon Period for 11a/n and 11b/g/n. Rule validity—Data for at least one band must be provided. The valid range is 20 to 1000. Enter 0 or keep it empty if a band should not be checked.
Short Preamble	Description—Checks whether or not Short Preamble is enabled for 11b/g.
Fragmentation Threshold	Description—Checks whether or not Fragmentation Threshold is configured properly. Rule data—Enter the threshold amount (bytes) in the text boxes for Fragmentation Threshold for 11a/n and 11b/g/n. Rule validity—Data for at least one band must be provided. The valid range is 256 to 2346. Enter 0 or keep it empty if a band should not be checked.
Data Rate	Description—Checks whether or not Data Rates are configured properly. Data Rate configuration for 11b/g—Select **Disabled**, **Supported**, or **Mandatory** for each Mbps category. Data Rate configuration for 11a—Select **Disabled**, **Supported**, or **Mandatory** for each Mbps category.
Aggressive Load Balancing	Description—Checks whether or not Aggressive Load Balancing is disable.
QoS Profile	Description—Checks that QoS Profiles are not altered from default values.
EAP Request Timeout	Description—Checks whether or not EAP Request Timeout is configured properly. Rule data—Enter the time limit (sec) for the EAP Request Timeout. Rule validity—Data cannot be left blank or as zero. The valid range is 1 to 120.
ARP Unicast	Description—Checks whether or not ARP Unicast is disabled.

Voice Audit > Report Tab

The following table describes the fields on **Operate > Operational Tools > Wireless > Voice Audit > Report**.

Table 2-11 Voice Audit > Report Tab Field Descriptions

Field	Description
Audit Status	Indicates whether or not the audit is complete.
Start Time and End Time	Indicates the time at which the voice audit starts and ends.
# Total Devices	Indicates the number of devices involved in the voice audit.
# Completed Devices	Indicates the number of devices the tool attempted to audit. **Note** If a controller is unreachable, the audit skips it. The Voice Audit does not complete any rule checks for that controller.
# Rules	Indicates the number of rules selected for the voice audit.
Report Results	

Table 2-11 Voice Audit > Report Tab Field Descriptions (continued)

Field	Description
IP Address	Indicates the IP address for the controller involved in the voice audit.
Rule	Indicates the rule that was applied for this controller.
Result	Indicates the result (Skipped, Violation, Unreachable) of the applied rule. **Note** If there is no mismatch between the current configuration and a rule value, no results are displayed for that rule.
Details	Defines an explanation for the rule results. **Note** If the applied rule results in a Violation, the Details link provides additional information including Name, the Device Value, and the Rule Value. Hover your mouse cursor over the link to view the additional details.
Time	Provides a timestamp for the voice audit.

Voice Diagnostic Field Descriptions

The following topics describe the fields on the **Operate > Operational Tools > Wireless > Voice Diagnostic** page.

- Voice Diagnostic Test List Page, page 2-11
- Voice Diagnostic Test Report Page, page 2-12

Voice Diagnostic Test List Page

The following table describes the fields on **Operate > Operational Tools > Wireless > Voice Diagnostic**.

Table 2-12 Voice Diagnostic Test List Page Field Descriptions

Field	Description
Test Name	Name of the test.
Duration of Test (Minutes)	The duration for which the test is performed. The duration can be either 10, 20, 30, 40, 50, or 60 minutes. The default selection is 10 minutes.
First Client	Displays the First Client details such as the Client MAC address and all the controllers provisioned for the client and if the controllers are not reachable then the failed provisioned controllers are also listed.
Second Client	Displays the Second Client details (if any) such as the Client MAC address and all the controllers provisioned for the client and if the controllers are not reachable then the failed provisioned controllers are also listed.
Start Time	The time when the test was started.
Remaining Time	The time remaining for the test.
State	The state of the test. It can be one of the four states, Running, Completed, Stopped or Aborted.
Problem	The status of the test. Red indicates a problem was discovered in the test. Green indicates the voice diagnostic test that no problems were discovered during the call.

Voice Diagnostic Test Report Page

The following table describes the tabs on **Operate > Operational Tools > Wireless > Voice Diagnostic Test Report**.

Table 2-13 Voice Diagnostic Test Report Page Tab Descriptions

Tab	Description
Summary	
This tab is divided into three areas where top area displays the test and client details, the middle area displays the problems, and the bottom area displays the corresponding log messages.	
Test and Client Details	The test status displays the test details like the Test Name, First Client MAC address, Second Client MAC address, device type, test status, start time, remaining time and the duration of the test. Restart if the test was stopped or completed the test. A stop button is provided to Stop the running test. The Refresh Status Tab and Refresh Client Tab buttons is used to refresh the status and client details. The client details such as the client user name, IP address, MAC address, Vendor, CCX Version, 802.11 state, protocol, SSID, profile-name, and AP details are displayed. You can click the Client MAC address for more client details.
Problems	The Problems pane appears below the test and client status details pane, This pane displays all the problems regarding the current diagnosis. This pane is updated every 5 seconds independently. There is no need to refresh the whole page. You can sort the information in this pane by clicking on any of the pane columns. A pop-up dialog box appears with the Problem detailed description and Suggested action when you click any row of the Problems pane. **Note** In some cases of inter controller roaming failure, the MAC address in the From AP information is incorrect and may appear as “00:00:00:00:00:00”.
Logs	The Logs pane appears below the Problems pane. This pane displays all the messages exchanged between the controller and the WCS during this diagnosis. You can sort the information in this pane by clicking on any of the pane columns. This pane is updated every 5 sec independently without refreshing the whole page.
Charts	
This tab displays the charts for each client's uplink and downlink traffic. The charts are updated every 10 secs.	
Client Uplink and DownLink TSM Chart with Roaming	The Client Uplink Traffic Stream Metric (TSM) chart shows the clients which support CCX V4 and above. The TSM data is plotted for every 10 sec. The TSM Chart displays the metrics for a set of series, that can be enabled or disabled using the Select Series button in the chart.
Client Uplink and DownLink QoS Chart	For each interval, QoS will be calculated and shown on the chart. represents the Client Uplink QoS chart. This pie chart provides the total Qos Chart counts and its distribution in three categories. These categories generally indicate the quality of a voice call.
Average Uplink and Downlink AC Queue	The AC Queue displays the type of packets and the number of packets for a series. You can enable or disable the series using the Select Series button.

Table 2-13 Voice Diagnostic Test Report Page Tab Descriptions (continued)

Tab	Description
Roam History	This tab shows the roaming history information in the Roaming Table. This Roaming table displays both the successful and the failed roaming history. The roaming table provides the following information: • Time at which the roaming of the client happened • The name of the AP from which the client moved • The type of Radio from which the client moved • The IP address of the controller from which the client moved • The name of the AP to which the client moved • The IP address of the controller to which the client moved • The type of radio to which the client moved • The roaming result, whether it was successful or a failure • If it was a failure it also provides the reason to the failure
Events	The Event tab shows the event history related to client and AP during a voice call in a list. It will show last 10 events. There is two Event tables available, Client Events and AP Events. Client Specific events during the voice call is shown in the Client Events table and AP Specific events in shown in the AP Event table.