CHAPTER 31

Field Reference

This section provides reference information on Prime Infrastructure fields.

Configuration Templates Field Descriptions

The following sections contain field descriptions for configuration templates:

Controller Templates Field Descriptions

The following sections contain field descriptions for pages found in **Design > Configuration Templates > Features and Technologies > Controller**.

- Controller > Security > Wireless Protection Policies > Rogue Policies Template
- Controller > Security > IP Groups Template
- Controller > Security > Protocol Groups
- Controller > Security > 802.11 > Band Select
- Controller > Security > 802.11 > Media Stream
- Controller > Security > 802.11 > RF Profiles
- Controller > 80211a or n > Parameters
- Controller > 80211a or n > CleanAir
- Controller > 80211a or n > Media Parameters
- Controller > 80211a or n > Roaming Parameters
- Controller > 80211a or n > dot11a-RRM > Thresholds
- Controller > 80211a or n > dot11a-RRM > DCA
- Controller > 802.11b or g or n > Parameters
- Controller > 802.11b or g or n > Media Parameters
- Controller > 802.11b or g or n > Roaming Parameters
- Controller > 802.11b or g or n > CleanAir
- Controller > dot11b-RRM > Thresholds
- Controller > dot11b-RRM > TPC
- Controller > dot11b-RRM > DCA
- Controller > Management > Trap Control
- Controller > Management > Telnet SSH
- Controller > Location > Location Configuration
- Controller > PMIP > Global Config

Controller > System > General Template

Table 31-1 describes the fields on the **Design > Configuration Templates> Features and Technologies > Controller > System > General** page.

Table 31-1 Controller > System > General Template

Field	Description
802.3x Flow Control Mode	Enable or disable flow control mode.
802.3 Bridging	Enable or disable 802.3 bridging. This 802.3 bridging option is not available for Cisco 5500 and Cisco 2106 series controllers.
Web Radius Authentication	choose the desired Web RADIUS authentication. You can choose to use PAP, CHAP, or MD5-CHAP for authentication between the controller and the client during the user credential exchange.
AP Primary Discovery Timeout	Specify the number of seconds for the AP Primary Discovery Timeout. The default is 120 seconds, and the valid range is 30 to 3600.

Table 31-1 Controller > System > General Template (continued)

Field	Description
Back-up Primary Controller IP Address	Specify the Back-up primary and secondary controller details.
Back-up Primary Controller Name	
Back-up Secondary Controller IP Address	
Back-up Secondary Controller Name	
CAPWAP Transport Mode	Specify Layer 2 or Layer 3 transport mode. When set to Layer 3, the lightweight access point uses IP addresses to communicate with the access points; these IP addresses are collected from a mandatory DHCP server. When set to Layer 2, the lightweight access point uses proprietary code to communicate with the access points. Controllers through Version 5.2 use LWAPP and the new controller version uses CAPWAP.
Broadcast Forwarding	Choose to enable or disable broadcast forwarding. The default is disabled.
LAG Mode	Choose **Enable** or **Disable** from the LAG Mode drop-down list. Link aggregation allows you to reduce the number of IP addresses needed to configure the ports on your controller by grouping all the physical ports and creating a link aggregation group (LAG). If LAG is enabled on a controller, any dynamic interfaces that you have created are deleted to prevent configuration inconsistencies in the interface database. When you make changes to the LAG configuration, the controller has to be rebooted for the changes to take effect. Interfaces cannot be created with the Dynamic AP Manager flag set. Also, you cannot create more than one LAG on a controller.
Peer to Peer Blocking MOde	Choose to enable or disable peer-to-peer blocking mode. If you choose Disable, any same-subnet clients communicate through the controller. If you choose Enable, any same-subnet clients communicate through a higher-level router.
Over-the-Air Provisioning AP Mode	From the Over Air AP Provision Mode drop-down list, choose **enable** or **disable**.
AP Fallback	From the AP Fallback drop-down list, choose **enable** or **disable**. Enabling fallback causes an access point that lost a primary controller connection to automatically return to service when the primary controller returns. When a controller fails, the backup controller configured for the access point suddenly receives a number of discovery and join requests. This might cause the controller to reach a saturation point and reject some of the access points. By assigning priority to an access point, you have some control over which access points are rejected. In a failover situation when the backup controller is saturated, the higher priority access points can join the backup controller if the lower priority access points are disjoined. Choose **enable** from the AP Failover Priority drop-down list if you want to allow this capability.
AP Failover Priority	
Apple Talk Bridging	Choose to enable or disable AppleTalk bridging. This AppleTalk bridging option is not available on Cisco 5500 series controllers.

Table 31-1 Controller > System > General Template (continued)

Field	Description
Fast SSID Change	Choose to enable or disable the Fast SSID Change option. If the option is enabled, the client connects instantly to the controller between SSIDs without having much loss of connectivity. Normally, each client is connected to a particular WLAN identified by the SSID. If the client moves out of reach of the connected access point, the client has to reconnect to the controller using a different access point. This normal process consumes some time as the DHCP (Dynamic Host Configuration Protocol) server has to assign an IP address to the client. Because the master controller is normally not used in a deployed network, the master controller setting is automatically disabled upon reboot or operating system code upgrade. You might want to enable the controller as the master controller from the Master Controller Mode drop-down list.
Master Controller Mode	Choose to enable or disable access to the controller management interface from wireless clients. Because of IPsec operation, management via wireless is only available to operators logging in across WPA or Static WEP.
Wireless Management	Wireless management is not available to clients attempting to log in via an IPsec WLAN.
Symmetric Tunneling Mode	Choose to enable or disable symmetric tunneling mode. With symmetric mobility tunneling, the controller provides inter-subnet mobility for clients roaming from one access point to another within a wireless LAN. The client traffic on the wired network is directly routed by the foreign controller. If a router has Reverse Path Forwarding (RPF) enabled (which provides additional checks on incoming packets), the communication is blocked. Symmetric mobility tunneling allows the client traffic to reach the controller designated as the anchor, even with RPF enabled. All controllers in a mobility group must have the same symmetric tunneling mode. For symmetric tunneling to take effect, you must reboot.
ACL Counters	Use the ACL Counters drop-down list to enable or disable ACL counters. The values per ACL rule can be viewed for each controller.
Default Mobility Domain Name	Enter the operator-defined RF mobility group name in the Default Mobility Domain Name text box.
Mobility Anchor Group Keep Alive Interval	At the Mobility Anchor Group Keep Alive Interval, determine the delay between tries for clients attempting to join another access point. With this guest tunneling N+1 redundancy feature, the time it takes for a client to join another access point following a controller failure is decreased because a failure is quickly identified, the clients are moved away from the problem controller, and the clients are anchored to another controller. When you hover your mouse cursor over the field, the valid range of values appear.
Mobility ANchor Group Keep Alive Retries	At the Mobility Anchor Group Keep Alive Retries, specify the number of queries to anchor before the client declares it unreachable.
RF Network Name	Enter the RF network group name between 8 and 19 characters. Radio Resource Management (RRM) neighbor packets are distributed among access points within an RF network group. The Cisco access points only accept RRM neighbor packets sent with this RF network name. The RRM neighbor packets sent with different RF network names are dropped.

Table 31-1 Controller > System > General Template (continued)

Field	Description
User Idle Timeout	Specify the time out for idle clients. The factory default is 300 seconds. When the timeout expires, the client loses authentication, briefly disassociates from the access point, reassociates, and re-authenticates. Specify the timeout in seconds for the address resolution protocol. The factory default is 300 seconds.
ARP Timeout	Specify the timeout in seconds.
Global TCP Adjust MSS	Select the **Global TCP Adjust MMS** check box to start checking the TCP packets originating from the client, for the TCP SYN/ TCP ACK packets and MSS value and reset it to the configured value on the upstream and downstream side.
Disable local access	When this check box is selected, the AP will not broadcast local SSIDs or allow access to any of the Ethernet Ports.
Out of Box	Select this check box to create out-of-box RF profiles for both the radios along with out-of-box AP Group.
Web Auth Proxy Redirect Mode	Choose **enable** or **disable** Web Auth Proxy Redirect Mode if a manual proxy configuration is configured on the browser of the client; all web traffic going out from the client is destined for the PROXY IP and PORT configured on the browser.
Web Auth Proxy Redirect Port	Enter the Web Auth Proxy Redirect Port. The default ports are 8080 and 3128. The range is 0 to 65535.
AP Retransmit Count	Enter the AP Retransmit Count and Intervals. The AP Retransmit Count default value is 5 and the range is from 3 to 8. The AP Retransmit Interval default value is 3. The range is 2 to 5.
AP Retransmit Interval	

Controller > System > Global CDP Configuration Template

Table 31-2 describes the fields on the **Design > Configuration Templates> Features and Technologies > Controller > System > Global CDP Configuration** page.

Table 31-2 Controller > System > Global CDP Configuration Template

Field	Description
CDP on controller	Choose enable or disable CDP on the controller. This configuration cannot be applied on WiSM2 controllers.
Global CDP on APs	Choose to enable or disable CDP on the access points.
Refresh Interval	Enter the time in seconds at which CDP messages are generated. The default is 60.
Hold Time	Enter the time in seconds before the CDP neighbor entry expires. The default is 180.
CDP Advertisement Version	Enter which version of the CDP protocol to use. The default is v1.
Ethernet Interface Slot	Select the slots of Ethernet interfaces for which you want to enable CDP. CDP for Ethernet Interfaces fields are supported for Controller Version 7.0.110.2 and later.
Radio Interface Slot	Select the slots of Radio interfaces for which you want to enable CDP. CDP for Radio Interfaces fields are supported for Controller Version 7.0.110.2 and later.

Controller > System > Dynamic Interface Template

Table 31-3 describes the fields on the **Design > Configuration Templates> Features and Technologies > Controller > System > Dynamic Interface** page.

Table 31-3 Controller > System > Dynamic Interface

Field	Description
Guest LAN	Select to mark the interface as wired.
Quarantine	Enable/disable to quarantine a VLAN. Select the check box to enable.
Netmask	Enter the net mask address of the interface.
LAG Mode	Select this check box to enable or disable LAG Mod. If LAG mode is selected with this interface, then the settings can be applied only to the LAG-enabled controllers.
Primary Port Number	Enter the port currently used by the interface.
Secondary Port Number	Enter a secondary port to be used by the interface when the primary port is down. When the primary port is reactivated, the Cisco 4400 Series Wireless LAN controller transfers the interfaces back to the primary port. Primary and secondary port numbers are present only in the Cisco 4400 Series Wireless LAN controllers.
AP Management	Select this check box to enable access point management.
Primary DHCP Server	Enter the IP addresses of the primary DHCP servers.
Secondary DHCP Server	Enter the IP addresses of the secondary DHCP servers.
ACL Name	Choose a name from the list of defined names. From the Add Format Type drop-down list in the Add Interface Format Type group box, choose either **Device Info** or **File**. If you choose device info, you must configure the device-specific fields for each controller. If you choose File, you must configure CSV device-specific fields (Interface Name, VLAN Identifier, Quarantine VLAN Identifier, IP Address, and Gateway) for all the managed controllers specified in the CSV file (see Table 31-4). If you choose Device Info, continue to Step 12.

The sample CSV files are as follows.

Table 31-4 Sample CSV Files

ip_address	interface_name	vlan_id	quarantine_ vlan_id	interface_ ip_address	gateway
209.165.200.224	dyn-1	1	2	209.165.200.228	209.165.200.229
209.165.200.225	interface-1	4	2	209.165.200.230	209.165.200.231
209.165.200.226	interface-2	5	3	209.165.200.232	209.165.200.233
209.165.200.227	dyna-2	2	3	209.165.200.234	209.165.200.235

The first row of the CSV file is used to describe the columns included. The CSV files can contain the following fields:

- ip_address
- interface_name

- vlan_id
- quarantine_vlan_id
- interface_ip_address
- gateway

If you choose Apply to Controllers, you advance to the Apply To page where you can configure device-specific fields for each controller.

Use the **Add** and **Remove** options to configure device specific fields for each controllers. If you click **Edit**, a dialog box appears with the current parameter input.

Make the necessary changes in the dialog box, then click **OK**.

Note If you change the interface fields, the WLANs are temporarily disabled, therefore you might lose connectivity for some clients. Any changes to the interface fields are saved only after you successfully apply them to the controller(s).

Note If you remove an interface here, it is removed only from this template and not from the controllers.

Controller > WLANs > WLAN Configuration Template

The following tables describe the fields on the **Design > Configuration Templates> Features and Technologies > Controller > WLANs > WLAN Configuration** page:

- Table 31-5—General tab
- Table 31-6—Security tab
- Table 31-7—QoS tab
- Table 31-8—Advanced tab
- Table 31-9—Hot Spot tab

Controller > WLANs > WLAN Configuration > General

Table 31-5 describes the fields on the **Design > Configuration Templates> Features and Technologies > Controller > WLANs > WLAN Configuration > General** tab.

Table 31-5 Controller > WLANs > WLAN Configuration > General

Field	Description
Wired Lan	Check the box to indicate whether or not this WLAN is a wired LAN. **Note** Specify if you want guest users to have wired guest access from an Ethernet connection designated and configured for guest access. Wired guest access ports might be available in a guest office or specific ports in a conference room and accounts are added to the network using the Lobby Ambassador portal. (The Egress or Ingress interface configurations are applicable for Wired LAN only. Use the **Type** drop-down list to select the type of the wired LAN. • Guest LAN—Indicates that this wired LAN is a Guest LAN. If you select the Guest LAN option, you need to select an Ingress interface which has not already been assigned to any Guest LAN. • Remote LAN—Indicates that this wired LAN is a Remote LAN.
Profile Name	Enter a name in the Profile Name text box that identifies the WLAN or the guest LAN. Do not use any spaces in the name entered.
SSID	Enter the name of the WLAN SSID. An SSID is not required for a guest LAN. WLANs with the same SSID must have unique Layer 2 security policies so that clients can make a WLAN selection based on information advertised in the beacons and probes.
Status	Select the **Enable** check box for the Status field.
Security Policies	Modifications you make in the Security tab appear after you save the template.
Radio Policy	Set the WLAN policy to apply to All (802.11a/b/g/n), 802.11a only, 802.11g only, 802.11b/g only, or 802.11a/g only.
Interface/Interface Group	Choose the available names of interfaces created by the Controller > Interfaces module.
Multicast VLAN	Select the **Enable** check box to enable the multicast VLAN feature. From the Multicast VLAN Interface drop-down list, choose the appropriate interface name. This list is automatically populated when you enable the multicast VLAN feature
Broadcast SSID	Click to activate SSID broadcasts for this WLAN.

Related Topics

- Table 31-6—Security tab
- Table 31-7—QoS tab
- Table 31-8—Advanced tab
- Table 31-9—Hot Spot tab

Controller > WLANs > WLAN Configuration > Security

Table 31-6 describes the fields on the **Design > Configuration Templates> Features and Technologies > Controller > WLANs > WLAN Configuration > Security** tab.

Table 31-6 Controller > WLANs > WLAN Configuration > Security

Field	Description
Layer 2	
None	No Layer 2 security selected. • FT Enable—Select the check box to enable Fast Transition (FT) between access points. **Note** Fast transition is not supported with FlexConnect mode. Over the DS—Select the check box to enable or disable the fast transition over a distributed system. Reassociation Timeout—Time in seconds after which fast transition reassociation times out. The default is 20 seconds, and the valid range is 1 to 100. To enable Over the DS or Reassociation Timeout, you should enable fast transition.
802.1X	WEP 802.1X data encryption type: • 40/64 bit key • 104 bit key • 152 bit key
Static WEP	Static WEP encryption fields: • Key sizes: Not set, 40/64, 104, and 152 bit key sizes. • Key Index: 1 to 4 (Note 2). • Encryption Key: Encryption key required. • Key Format: ASCII or HEX. • Allowed Shared Key Authentication—Select the check box to enable shared key authentication. Regardless of the format you choose, for security reasons, only ASCII is visible on the WLC (and the Prime Infrastructure). For this reason, you cannot use a template to replicate the configuration on a second controller during auto provisioning. You should set the key format again in the template in case a discovered template is applied to another device.
Static WEP-802.1X	Use this setting to enable both Static WEP and 802.1X policies. If this option is selected, static WEP and 802.1X fields are displayed at the bottom of the page. Static WEP encryption fields: • Key sizes: Not set, 40/64, 104, and 152 bit key sizes. • Key index: 1 to 4 (Note 2). • Encryption Key: Enter encryption key. • Key Format: ASCII or HEX. • Allowed Shared Key Authentication—Select the check box to enable. • 802.1 Data Encryption: 40/64 bit key, 104 bit key, 152 bit key.

Table 31-6 Controller > WLANs > WLAN Configuration > Security (continued)

Field	Description
CKIP	Cisco Key Integrity Protocol (CKIP). A Cisco access point advertises support for CKIP in beacon and probe response packets. CKIP can be configured only when Aironet IE is enabled on the WLAN. **Note** CKIP is not supported on 10xx APs. When selected, these CKIP fields are displayed. • Key size: Not set, 40, or 104. • Key Index: 1 to 4 • Encryption Key: Specify encryption key. • Key Format: ASCII or HEX. **Note** Regardless of the format you choose, for security reasons, only ASCII is visible on the WLC (and Prime Infrastructure). For this reason, you cannot use a template to replicate the configuration on a second controller during auto provisioning. You should set the key format again in the template in case a discovered template is applied to another device. MMH Mode—Select the check box to enable. Key Permutation—Select the check box to enable
MAC Filtering	Check to filter clients by MAC address. **Note** The ability to join a controller without specification within a MAC filter list is only supported on mesh access points. **Note** For releases prior to 4.1.82.0, mesh access points do not join the controller unless they are defined in the MAC filter list. You might want to disable the MAC filter list to allow newly added access points to join the controller. Before enabling the MAC filter list again, you should enter the MAC addresses of the new access points.
Authentication Key Management	Choose the desired type of authentication key management. The choices are 802.1X, CCKM, or PSK. **Note** If you choose PSK, you must enter the shared key and type (ASCII or hexadecimal). **Note** Regardless of the format you choose, for security reasons, only ASCII is visible on the WLC (and Prime Infrastructure). For this reason, you cannot use a template to replicate the configuration on a second controller during auto provisioning. You should set the key format again in the template in case a discovered template is applied to another device.
Layer 3	
Layer 3 Security	Choose between None and VPN Pass Through. **Note** The VPN passthrough option is not available for the 2106 or 5500 series controllers.

Table 31-6 Controller > WLANs > WLAN Configuration > Security (continued)

Field	Description
Web Policy	You can modify the default static WEP (web authentication) or assign specific web authentication (login, logout, login failure) pages and the server source. 1. To change the static WEP to passthrough, select the **Web Policy** check box and choose the Passthrough option from the drop-down list. This option allows users to access the network without entering a username or password. An Email Input check box appears. Select this check box if you want users to be prompted for their e-mail address when attempting to connect to the network. 2. Choose the **WebAuth on MAC Filter Failure** option so that when clients fail on MAC filter, they are automatically switched to webAuth. **Note** The WebAuth on Mac Filter Failure option works only when the Layer 2 Mac Filtering option is enabled. 3. To specify custom web authentication pages, unselect the **Global WebAuth Configuration Enable** check box. When the Web Auth Type drop-down list appears, choose one of the following options to define the web login page for the wireless guest users: **Default Internal**—Displays the default web login page for the controller. This is the default value. **Customized Web Auth**—Displays custom web login, login failure, and logout pages. When the customized option is selected, three separate drop-down lists for login, login failure, and logout page selection appear. You do not need to define a customized page for all three of the options. Choose **None** from the appropriate drop-down list if you do not want to display a customized page for that option. These optional login, login failure, and logout pages are downloaded to the controller as webauth.tar files. **External**—Redirects users to an external server for authentication. If you choose this option, you must also enter the URL of the external server in the URL text box. **Note** External web auth is not supported for 2106 and 5500 series controllers. You can select specific RADIUS or LDAP servers to provide external authentication in the Security > AAA page. To do so, continue with Step 4. **Note** The RADIUS and LDAP servers must be already configured to have selectable options in the Security > AAA page. You can configure these servers in the RADIUS Authentication Servers page and TACACS+ Authentication Servers page. If you selected External as the Web Authentication Type in Step 2, choose **Security > AAA**, and choose up to three RADIUS and LDAP servers using the drop-down lists. Repeat this process if a second (anchor) controller is being used in the network.

Table 31-6 Controller > WLANs > WLAN Configuration > Security (continued)

Field	Description
AAA Server	
Radius Server Overwrite	Check to send the client authentication request through the dynamic interface which is set on the WLAN. When you enable the Radius Server Overwrite Interface option, the WLC sources all radius traffic for a WLAN using the dynamic interface configured on that WLAN. **Note** You cannot enable Radius Server Overwrite Interface when Diagnostic Channel is enabled. **Note** The Radius Server Overwrite Interface option is supported in controller Version 7.0.x and later. Select the **Enable** check boxes, then use the drop-down lists in the RADIUS and LDAP servers section to choose authentication and accounting servers. This selects the default RADIUS server for the specified WLAN and overrides the RADIUS server that is configured for the network. If all three RADIUS servers are configured for a particular WLAN, server 1 has the highest priority, and so on. If no LDAP servers are chosen here, Prime Infrastructure uses the default LDAP server order from the database.
Interim Update	Select t to enable interim update for RADIUS Server Accounting. If you have selected this check box, specify the Interim Interval value. The range is 180 to 3600 seconds, and the default value is 0. **Note** The Interim Interval can be entered only when Interim Update is enabled.
Local EAP Authentication	Select the **Local EAP Authentication** check box if you have an EAP profile already configured that you want to enable. Local EAP is an authentication method that allows users and wireless clients to locally authenticate. It is designed for use in remote offices that want to maintain connectivity to wireless clients when the backend system becomes disrupted or the external authentication server goes down.
Allow AAA Override	When you enable AAA Override, and a client has conflicting AAA and controller WLAN authentication fields, client authentication is performed by the AAA server. As part of this authentication, the operating system moves clients from the default Cisco WLAN Solution to a VLAN returned by the AAA server and predefined in the controller interface configuration (only when configured for MAC filtering, 802.1X, and/or WPA operation). In all cases, the operating system also uses QoS and ACL provided by the AAA server, as long as they are predefined in the controller interface configuration. (This VLAN switching by AAA override is also referred to as identity networking.) For instance, if the corporate WLAN primarily uses a management interface assigned to VLAN 2, and if AAA override returns a redirect to VLAN 100, the operating system redirects all client transmissions to VLAN 100, regardless of the physical port to which VLAN 100 is assigned. When AAA override is disabled, all client authentication defaults to the controller authentication parameter settings, and authentication is only performed by the AAA server if the controller WLANs do not contain any client-specific authentication parameters. The AAA override values might come from a RADIUS server, for example.

Related Topics

- Table 31-5—General tab
- Table 31-7—QoS tab
- Table 31-8—Advanced tab
- Table 31-9—Hot Spot tab

Controller > WLANs > WLAN Configuration > QoS

Table 31-7 describes the fields on the **Design > Configuration Templates> Features and Technologies > Controller > WLANs > WLAN Configuration > QoS** tab.

Table 31-7 Controller > WLANs > WLAN Configuration > QoS

Field	Description
Quality of Service (QoS)	Choose **Platinum** (voice), **Gold** (video), **Silver** (best effort), or **Bronze** (background). Services such as VoIP should be set to gold while non-discriminating services such as text messaging can be set to bronze.
Override Per-User Rate Limits	**Data rates on a per-user basis**
Average Data Rate	Define the average data rate for TCP traffic per user or per SSID by entering the rate in Kbps in the Average Data Rate text boxes. A value of 0 imposes no bandwidth restriction on the profile.
Burst Data Rate	Define the peak data rate for TCP traffic per user or per SSID by entering the rate in Kbps in the Burst Data Rate text boxes. A value of 0 imposes no bandwidth restriction on the profile. The Burst Data Rate should be greater than or equal to the Average Data Rate. Otherwise, the QoS policy may block traffic to and from the wireless client.
Average Real-Time Rate	Define the average real-time rate for UDP traffic per user or per SSID by entering the rate in Kbps in the Average Real-Time Rate text boxes. A value of 0 imposes no bandwidth restriction on the profile.
Burst Real-Time Rate	Define the peak real-time rate for UDP traffic per user or per SSID by entering the rate in Kbps in the Burst Real-Time Rate text boxes. A value of 0 imposes no bandwidth restriction on the profile. The Burst Real-Time Rate should be greater than or equal to the Average Real-Time Rate. Otherwise, the QoS policy may block traffic to and from the wireless client.
Override Per-SSID Rate Limits	**Data rates on a per SSID basis**
Average Data Rate	Define the average data rate TCP traffic per user or per SSID by entering the rate in Kbps in the Average Data Rate text boxes. A value of 0 imposes no bandwidth restriction on the profile.
Burst Data Rate	Define the peak data rate for TCP traffic per user or per SSID by entering the rate in Kbps in the Burst Data Rate text boxes. A value of 0 imposes no bandwidth restriction on the profile. The Burst Data Rate should be greater than or equal to the Average Data Rate. Otherwise, the QoS policy may block traffic in the WLANs.
Average Real-Time Rate	Define the average real-time rate for UDP traffic per user or per SSID by entering the rate in Kbps in the Average Real-Time Rate text boxes. A value of 0 imposes no bandwidth restriction on the profile.
Burst Real-Time Rate	Define the peak real-time rate for UDP traffic per user or per SSID by entering the rate in Kbps in the Burst Real-Time Rate text boxes. A value of 0 imposes no bandwidth restriction on the profile. The Burst Real-Time Rate should be greater than or equal to the Average Real-Time Rate. Otherwise, the QoS policy may block traffic in the WLANs.
WMM Policy	Choose **Disabled**, **Allowed** (so clients can communicate with the WLAN), or **Required** to make it mandatory for clients to have WMM enabled for communication.
7920 AP CAC	Select to enable support on Cisco 7920 phones. If you want WLAN to support older versions of the software on 7920 phones, select the **7920 Client CAC** check box to enable it. The CAC limit is set on the access point for newer versions of software.

Related Topics

- Table 31-5—General tab
- Table 31-6—Security tab
- Table 31-8—Advanced tab
- Table 31-9—Hot Spot tab

Controller > WLANs > WLAN Configuration > Advanced

Table 31-5 describes the fields on the **Design > Configuration Templates> Features and Technologies > Controller > WLANs > WLAN Configuration > Advanced** tab.

Table 31-8 Controller > WLANs > WLAN Configuration > Advanced

Field	Description
FlexConnect Local Switching	Click to enable FlexConnect local switching. If you enable FlexConnect local switching, the FlexConnect access point handles client authentication and switches client data packets locally. FlexConnect local switching is only applicable to the Cisco 1130/1240/1250 series access points. It is not supported with L2TP or PPTP authentications, and it is not applicable to WLAN IDs 9-16.
FlexConnect Local Auth	Select to enable FlexConnect local authentication. Local authentication is useful where you cannot maintain the criteria a remote office setup of minimum bandwidth of 128 kbps with the roundtrip latency no greater than 100 ms and the maximum transmission unit (MTU) no smaller than 500 bytes. In local switching, the authentication capabilities are present in the access point itself. Thus local authentication reduces the latency requirements of the branch office. **Note** Local authentication can only be enabled on the WLAN of a FlexConnect AP that is in local switching mode. Local authentication is not supported in the following scenarios: • Guest Authentication cannot be performed on a FlexConnect local authentication enabled WLAN. • RRM information is not available at the controller for the FlexConnect local authentication enabled WLAN. • Local radius is not supported. • Once the client has been authenticated, roaming is supported after the WLC and the other FlexConnects in the group are updated with the client information.
Learn Client IP Address	When you enable hybrid-REAP local switching, the Learn Client IP Address check box is enabled by default. However, if the client is configured with Fortress Layer 2 encryption, the controller cannot learn the client IP address, and the controller periodically drops the client. Disable this option so that the controller maintains the client connection without waiting to learn the client IP address. The ability to disable this option is supported only with hybrid-REAP local switching; it is not supported with hybrid-REAP central switching.
Diagnostic Channel	Choose to enable the diagnostic channel feature or leave it disabled. The diagnostic channel feature allows you to troubleshoot problems regarding client communication with a WLAN. When initiated by a client having difficulties, the diagnostic channel provides the most robust communication methods with the fewest obstacles to communication.

Table 31-8 Controller > WLANs > WLAN Configuration > Advanced (continued)

Field	Description
Aironet IE	Select to enable support for Aironet information elements (IEs) for this WLAN. If Aironet IE support is enabled, the access point sends an Aironet IE 0x85 (which contains the access point name, load, number of associated clients, and so on) in the beacon and probe responses of this WLAN, and the controller sends Aironet IEs 0x85 and 0x95 (which contains the management IP address of the controller and the IP address of the access point) in the reassociation response if it receives Aironet IE 0x85 in the reassociation request.
IPv6	Select the IPv6 check box. You can configure IPv6 bridging and IPv4 web auth on the same WLAN.
Session Timeout	Check to set the maximum time a client session can continue before requiring reauthorization.
Coverage Hole Detection	Choose to enable or disable coverage hold detection (CHD) on this WLAN. By default, CHD is enabled on all WLANs on the controller. If you disable CHD on a WLAN, a coverage hole alert is still sent to the controller, but no other processing is done to mitigate the coverage hole. This feature is useful for guest WLANs where highly mobile guests are connected to your network for short periods of time.
Override Interface ACL	The Override Interface drop-down lists provides a list of defined access control lists (ACLs). Upon choosing an ACL from the list, the WLAN associates the ACL to the WLAN. Selecting an ACL is optional, and the default for this field is None
Peer to Peer Blocking	You can configure peer-to-peer blocking per WLAN rather than applying the status to all WLANs. From the Peer to Peer Blocking drop-down list, choose one of the following: • Disable—Peer-to-peer blocking is disabled, and traffic is bridged locally whenever possible. • Drop—The packet is discarded. • Forward Up Stream—The packet is forwarded on the upstream VLAN, and the decision is made about what to do with the packet. **Note** For locally switched clients, the Forward Up Stream is same as Drop from 7.2.x version of controllers. If FlexConnect local switching is enabled for the WLAN, which prevents traffic from passing through the controller, this drop-down list is dimmed. **Note** Peer-to-peer blocking does not apply to multicast traffic.
Wi-Fi Direct Clients Policy	Choose one of the following options: • **Disabled**—Disables the Wi-Fi Direct Clients Policy for the WLAN and deauthenticates all Wi-Fi Direct capable clients. The default is Disabled. • **Allow**—Allows the Wi-Fi Direct clients to associate with an infrastructure WLAN. • **Not-Allow**—Disallows the Wi-Fi Direct clients from associating with an infrastructure WLAN. **Note** Wi-Fi Direct Client Policy is applicable to WLANs that have APs in local mode only. **Note** The Wi-Fi Direct Clients Policy is applicable for controller Version 7.2.x. and later.
Client Exclusion	Select the check box if you want to enable automatic client exclusion. If you enable client exclusion, you must also set the Timeout Value in seconds for disabled client machines. Client machines are excluded by MAC address, and their status can be observed. A timeout setting of 0 indicates that administrative control is required to reenable the client. **Note** When session timeout is not set, it implies that an excluded client remains and does not timeout from the excluded state. It does not imply that the exclusion feature is disabled.

Table 31-8 Controller > WLANs > WLAN Configuration > Advanced (continued)

Field	Description
Passive Client	Enter the maximum number of clients to be associated in a WLAN in the Maximum Clients text box. The valid range is from 0 to 7000. The default value is 0. **Note** A value of 0 allows unlimited number of clients to be associated with a WLAN.
Static IP Tunneling	Enable dynamic anchoring of static IP clients by selecting the Static IP Tunneling check box.
Media Session Snooping	This feature enables access points to detect the establishment, termination, and failure of voice calls and then report them to the controller and Prime Infrastructure. It can be enabled or disabled per WLAN. When media session snooping is enabled, the access point radios that advertise this WLAN snoop for Session Initiation Protocol (SIP) voice packets. Any packets destined to or originating from port number 5060 are considered for further inspection. The access point tracks whether Wi-Fi Multimedia (WMM) and non-WMM clients are establishing a call, already on an active call, or in the process of ending a call and then notify the controller of any major call events.
KTS based CAC	Select the KTS based CAC check box to enable KTS based CAC support per WLAN. WLC supports TSPEC based CAC and SIP based CAC. But there are certain phones that work with different protocols for CAC, which are based on the KTS (Key Telephone System). For supporting CAC with KTS-based SIP clients, WLC should understand and process the bandwidth request message from those clients to allocate the required bandwidth on the AP radio, in addition to handling and sending certain other messages, as part of this protocol. **Note** The KTS CAC configuration is only supported by Cisco 5508, 7500, WISM2, and 2500 controllers that run controller software Release 7.2.x. This feature is not supported by Cisco 4400 series controllers.
NAC State	Choose **SNMP NAC** or **Radius NAC**. SIP errors that are discovered generate traps that appear on the client troubleshooting and alarms screens. The controller can integrate with the NAC appliance in out-of-band mode, where the NAC appliance remains in the data path only until clients have been analyzed and cleaned. Out-of-band mode reduces the traffic load on the NAC appliance and enables centralized NAC processing.
Scan Defer Priority	Off-Channel Scanning Defer is essential to the operation of RRM, which gathers information about alternate channel choices such as noise and interference. Additionally, Off-Channel Scanning Defer is responsible for rogue detection. Devices that need to defer Off-Channel Scanning Defer should use the same WLAN as often as possible. If there are many of these devices (and the possibility exists that Off-Channel Defer scanning could be completely disabled by the use of this feature), you should implement an alternative to local AP Off-Channel Scanning Defer, such as monitor access points, or other access points in the same location that do not have this WLAN assigned. Assignment of a QoS policy (bronze, silver, gold, and platinum) to a WLAN affects how packets are marked on the downlink connection from the access point regardless of how they were received on the uplink from the client. UP=1,2 is the lowest priority, and UP=0,3 is the next higher priority. The marking results of each QoS policy are as follows: • Bronze marks all downlink traffic to UP= 1. • Silver marks all downlink traffic to UP= 0. • Gold marks all downlink traffic to UP=4. • Platinum marks all downlink traffic to UP=6. Set the Scan Defer Priority by clicking the priority argument and Set the time in milliseconds in the Scan Defer Interval text box. Valid values are 0 through 60000. The default value is 100 milliseconds.

Table 31-8 Controller > WLANs > WLAN Configuration > Advanced (continued)

Field	Description
DTIM Period	In 802.11a/n and 802.11b/g/n networks, lightweight access points broadcast a beacon at regular intervals, which coincides with the Delivery Traffic Indication Map (DTIM). After the access point broadcasts the beacon, it transmits any buffered broadcast and multicast frames based on the value set for the DTIM period. This feature allows power-saving clients to wake up at the appropriate time if they are expecting broadcast or multicast data. Normally, the DTIM value is set to 1 (transmit broadcast and multicast frames after every beacon) or 2 (transmit after every other beacon). For instance, if the beacon period of the 802.11a/n or 802.11b/g/n network is 100 ms and the DTIM value is set to 1, the access point transmits buffered broadcast and multicast frames 10 times per second. If the beacon period is 100 ms and the DTIM value is set to 2, the access point transmits buffered broadcast and multicast frames 5 times per second. Either of these settings might be suitable for applications, including VoIP, that expect frequent broadcast and multicast frames. However, the DTIM value can be set as high as 255 (transmit broadcast and multicast frames after every 255th beacon) if all 802.11a/n or 802.11b/g/n clients have power save enabled. Because the clients have to listen only when the DTIM period is reached, they can be set to listen for broadcasts and multicasts less frequently, resulting in longer battery life. For instance, if the beacon period is 100 ms and the DTIM value is set to 100, the access point transmits buffered broadcast and multicast frames once every 10 seconds, allowing the power-saving clients to sleep longer before they have to wake up and listen for broadcasts and multicasts, resulting in longer battery life. Many applications cannot tolerate a long time between broadcast and multicast messages, resulting in poor protocol and application performance. We recommend a low DTIM value for 802.11a/n and 802.11b/g/n networks that support such clients. Under DTIM Period, enter a value between 1 and 255 (inclusive) in the 802.11a/n and 802.11b/g/n fields. The default value is 1 (transmit broadcast and multicast frames after every beacon).
DHCP Server	Select the check box to override DHCP server,. Another field appears where you can enter the IP address of your DHCP server. For some WLAN configurations, this is required. Three valid configurations are as follows: • DHCP Required and a valid DHCP server IP address - All WLAN clients obtain an IP address from the DHCP server. • DHCP is not required and a valid DHCP server IP address - All WLAN clients obtain an IP address from the DHCP server or use a static IP address. • DHCP not required and DHCP server IP address 0.0.0.0 - All WLAN clients are forced to use a static IP address. All DHCP requests are dropped. You cannot choose to require a DHCP address assignment and then enter a DHCP server IP address.
MFP Signature Generation	Select to enable signature generation for the 802.11 management frames transmitted by an access point associated with this WLAN. Signature generation makes sure that changes to the transmitted management frames by an intruder are detected and reported.
MFP Client Protection	Choose **Enabled**, **Disabled**, or **Required** for configuration of individual WLANs of a controller. If infrastructure MFP is not enabled, this drop-down list is unavailable. **Note** The Enabled parameter is the same as the Optional parameter that you choose from the MFP Client Protection drop-down list in the WLC graphical user interface. **Note** Client-side MFP is only available for those WLANs configured to support Cisco Compatible Extensions (version 5 or later) clients, and WPA2 must first be configured.

Table 31-8 Controller > WLANs > WLAN Configuration > Advanced (continued)

Field	Description
DTIM Period	Enter a value between 1 and 255 beacon intervals in the 802.11a/n DTIM Period group box of the page. The controller sends a DTIM packet on the 802.11a/n radio for this WLAN based on what is entered as an interval. **Note** The DTIM configuration is not appropriate for guest LANs.
Client Profiling	Select to enable or disable profiling of all the clients that are associated with the WLAN. **Note** Client Profiling is not supported with FlexConnect local authentication. **Note** Client Profiling is configurable only when you select the DHCP Address Assignment check box.
PMIP Mobility	Choose the mobility type from the following options: • None—Configures the WLAN with Simple IP. • Mixed—Configures the WLAN with Simple IP and PMIPv6. • PMIPv6—Configures the WLAN with only PMIPv6.

Related Topics

- Table 31-5—General tab
- Table 31-6—Security tab
- Table 31-7—QoS tab
- Table 31-9—Hot Spot tab

Controller > WLANs > WLAN Configuration > Hot Spot

Table 31-5 describes the fields on the **Design > Configuration Templates> Features and Technologies > Controller > WLANs > WLAN Configuration > Hot Spot** tab.

Table 31-9 Controller > WLANs > WLAN Configuration > Hot Spot

Field	Description
General	
802.11u Status	Select to enable 802.11u on the WLAN. • From the drop-down list, In the HESSID field, enter the Homogenous Extended Service Set Identifier value. The HESSID is a 6-octet MAC address that identifies the homogeneous ESS.
Internet Access	Select to enable this WLAN to provide Internet services.

Table 31-9 Controller > WLANs > WLAN Configuration > Hot Spot (continued)

Field	Description
Network Type	Choose one of the following network types that best describes the 802.11u you want to configure on this WLAN: • Private Network • Private Network with Guest Access • Chargeable Public Network • Free Public Network • Emergency Services Only Network • Personal Device Network • Test or Experimental • Wildcard
Network Auth Type	Choose the authentication type that you want to configure for the 802.11u parameters on this network: • Not configured • Acceptance of Terms and Conditions • Online Enrollment • HTTP/HTTPS Redirection
OUI List	Enter the following details: • OUI name • Is Beacon • OUI Index Click Add to add the OUI (Organizationally Unique Identifier) entry to this WLAN. • In the group box,
Domain List	Enter the following details: • Domain Name—The domain name operating in the 802.11 access network. • Domain Index—Select the domain index from the drop-down list. Click Add to add the domain entry to this WLAN.
OUI List	Enter the following details: • Realm Name—The realm name. • Realm Index—The realm index. Click Add to add the domain entry to this WLAN.
MSAP	Click to enable service advertisements.

Table 31-9 Controller > WLANs > WLAN Configuration > Hot Spot (continued)

Field	Description
Server Index	If you enabled MSAP, you must provide a server index. Enter the server index for this WLAN. The server index field uniquely identifies an MSAP server instance serving a venue that is reachable through the BSSID. **Note** MSAP (Mobility Services Advertisement Protocol) is designed to be used primarily by mobile devices that are configured with a set of policies for establishing network services. These services are available for devices that offer higher-layer services, or network services that are enabled through service providers. Service advertisements use MSAP to provide services to mobile devices prior to association to a Wi-Fi access network. This information is conveyed in a service advertisement. A single-mode or dual-mode mobile device queries the network for service advertisements before association. The device's network discovery and the selection function may use the service advertisements in its decision to join the network.
HotSpot2 Enable	Choose to enable HotSpot2.
WAN Link Status	Select the link status.
WAN SIM Link Status	The symmetric link status. For example, you can configure the uplink and downlink to have different speeds or same speeds.
Down Link Speed	The downlink speed. The maximum value is 4,194,304 kbps.
Up Link Speed	The uplink speed. The maximum value is 4,194,304 kbps.
Operator Name List	Specify the following: • Operator Name—Specify the name of the 802.11 operator. • Operator Index—Select an operator index. The range is from 1 to 32. • Language Code—An ISO-14962-1997 encoded string defining the language. This string is a three character language code. Click Add to add the operator details.
Port Config List	Specify the following: • IP Protocol—The IP protocol that you want to enable. The following options are ESP, FTP, ICMP, and IKEV2. • Port No—The port number that is enabled on this WLAN. • Status—The status of the port.

Related Topics

- Table 31-5—General tab
- Table 31-6—Security tab
- Table 31-7—QoS tab
- Table 31-8—Advanced tab

Controller > FlexConnect > FlexConnect AP Groups Template

Table 31-1 describes the fields on the **Design > Configuration Templates> Features and Technologies > Controller > FlexConnect > FlexConnect AP Groups** page.

Table 31-10 Controller > FlexConnect > FlexConnect AP Groups

Field	Description
General	
Primary RADIUS	Choose the primary RADIUS authentication servers for each group. If a RADIUS authentication server is not present on the controller, Prime Infrastructure configured RADIUS server does not apply. A value of 10 indicates that the primary RADIUS server is not configured for this group.
Secondary RADIUS	**Note** Choose the secondary RADIUS authentication servers for each group. If a RADIUS authentication server is not present on the controller, Prime Infrastructure configured RADIUS server does not apply. A value of 0 indicates that the primary RADIUS server is not configured for this group.
FlexConnect AP	An access point Ethernet MAC address cannot exist in more than one FlexConnect group on the same controller. If more than one group is applied to the same controller, select the **Ethernet MAC** check box to unselect an access point from one of the groups. You should save this change or apply it to controllers. Click **Add AP**. The FlexConnect AP Group page appears.
FlexConnect Configuration	Click the FlexConnect Configuration tab to enable local authentication for a FlexConnect group. **Note** Make sure that the Primary RADIUS Server and Secondary RADIUS Server fields are set to **None** on the General tab.
FlexConnect Local Authentication	Click to enable local authentication for this FlexConnect group. The default value is unselected. **Note** When you attempt to use this feature, a warning message indicates that it is a licensed feature. **Note** You can click the **Users configured in the group** link that appears at the bottom of the page to view the list of FlexConnect users. You can create FlexConnect users only after you save the FlexConnect AP Group.
EAP Type	To allow a FlexConnect access point to authenticate clients using LEAP, select the LEAP check box. Otherwise, to allow a FlexConnect access point to authenticate clients using EAP-FAST, select the EAP-FAST check box. To use manual PAC provisioning, enter the key used to encrypt and decrypt PACs in the EAP-FAST Key and Confirm EAP-FAST Key text boxes.
Auto Key Generation	To allow PACs to be sent automatically to clients that do not have one during PAC provisioning, select the Auto Key Generation check box
EAP-FAST Key	Enter the authority identifier of the EAP-FAST server. The identifier must be 32 hexadecimal characters.
EAP-FAST Authority ID	Enter the authority identifier of the EAP-FAST server in text format. You can enter up to 32 hexadecimal characters.
EAP-FAST Authority Info	Enter the authority information of the EAP-FAST server.
EAP-FAST Pac Timeout	Specify a PAC timeout value by entering the number of seconds for the PAC to remain viable in the edit box. The valid range is 2 to 4095 seconds.
Image Upgrade	
FlexConnect AP Upgrade	Check to upgrade the FlexConnect access points.

Table 31-10 Controller > FlexConnect > FlexConnect AP Groups

Field	Description
Slave Maximum Retry Count	Enter the maximum retries for the slave to undertake to start the download from the master in the FlexConnect group. This option is available only if you select the FlexConnect AP Upgrade check box. **Note** You are allowed to add an access point as a master access point only if **FlexConnect AP Upgrade** check box is enabled on the General tab.
VLAN-ACL Mapping	Use the edit table on this tab to add VLAN-ACL mappings.
VLAN ID	Enter a VLAN ID. The valid VLAN ID range is 1—4094.
Ingress ACL	Choose an Ingress ACL.
Egress ACL	Choose an Engress ACL.
WLAN-ACL Mapping	Use the edit table on this tab to add WLAN-ACL mappings.
WLAN ID	WLAN ID.
WLAN Profile Name	Choose a WLAN profile.
Web-Auth ACL	Choose a WebAuth ACL.
Web Policies	Use the edit table on this tab to add or select Web Policy ACLs.
Web-Policy ACL	Choose a WebPolicy ACL. You can add up to a maximum of 16 Web-Policy ACLs.
Local Split	Use the edit table on this tab to add or select Local-Split ACLs
WLAN Profile Name	Choose a WLAN Profile Name from the list.
Local-Split ACL	Choose a Local-Split ACL.
Central DHCP	Use the edit table on this tab to add or select Central DHCP for each WLAN Profile.
WLAN Profile Name	Choose a WLAN Profile Name from the list.
Central DHCP	Choose Enable to enable central DHCP for this profile.
Override DNS	Choose Enable to enable DNS override for this profile.
NAT-PAT	Choose Enable to enable network address and port address translation for this profile.

Controller > Security > AAA > RADIUS Auth Servers Template

Table 31-11 describes the fields on the **Design > Configuration Templates> Features and Technologies > Controller > Security > AAA > RADIUS Auth Servers** page.

Table 31-11 Controller > Security > AAA > RADIUS Auth Servers

Field	Description
Server Address	Enter the server address.
Port Number	Enter the port address.
Shared Secret Format	Choose either **ASCII** or **hex**. **Note** Regardless of the format you choose, for security reasons, only ASCII is visible on the WLC (and Prime Infrastructure). For this reason, you cannot use a template to replicate the configuration on a second controller during auto provisioning. You should set the key format again in the template in case a discovered template is applied to another device.
Shared Secret	Enter the RADIUS shared secret used by your specified server.

Table 31-11 Controller > Security > AAA > RADIUS Auth Servers (continued)

Field	Description
Confirm Shared Secret	Reenter the RADIUS shared secret used by your specified server.
Key WRAP	Select the check box if you want to enable key wrap. If this check box is enabled, the authentication request is sent to RADIUS servers that have following key encryption key (KEK) and message authenticator code keys (MACK) configured. When enabled, the following fields appear: • Shared Secret Format: Enter ASCII or hexadecimal. **Note** Regardless of the format you choose, for security reasons, only ASCII is visible on the WLC (and Prime Infrastructure). For this reason, you cannot use a template to replicate the configuration on a second controller during auto provisioning. You should set the key format again in the template in the event a discovered template is applied to another device. • KEK Shared Secret: Enter the KEK shared secret. • MACK Shared Secret: Enter the MACK shared secret. **Note** Each time the controller is notified with the shared secret, the existing shared secret is overwritten with the new shared secret.
Admin Status	Click if you want to enable administration privileges.
Support for RFC 3576	Click if you want to enable support for RFC 3576. RFC 3576 is an extension to the Remote Authentication Dial In User Service (RADIUS) protocol. It allows dynamic changes to a user session and includes support for disconnecting users and changing authorizations applicable to a user session. With these authorizations, support is provided for Disconnect and Change-of-Authorization (CoA) messages. Disconnect messages immediately terminate a user session, whereas CoA messages modify session authorization attributes such as data filters.
Network User	Click if you want to enable network user authentication. If this option is enabled, this entry is considered as the RADIUS authenticating server for the network user.
Management User	Click if you want to enable management authentication. If this option is enabled, this entry is considered as the RADIUS authenticating server for the management user.
Retransmit Timeout	Specify the time in seconds after which the RADIUS authentication request times out and a retransmission is attempted by the controller. You can specify a value between 2 and 30 seconds.
IPSec	If you click to enable the IP security mechanism, additional IP security fields are added to the page, and Steps 13 to 19 are required. If you enable IPSec, complete the following fields.
IPsec Authentication	Choose which IP security authentication protocol to use. The options are **HMAC-SHA1**, **HMAC-MD5**, and **None**. Message Authentication Codes (MAC) are used between two parties that share a secret key to validate information transmitted between them. HMAC (Hash MAC) is a mechanism based on cryptographic hash functions and can be used in combination with any iterated cryptographic hash function. HMAC-MD5 and HMAC-SHA1 are two constructs of the HMAC using the MD5 hash function and the SHA1 hash function. HMAC also uses a secret key for calculation and verification of the message authentication values

Table 31-11 Controller > Security > AAA > RADIUS Auth Servers (continued)

Field	Description
IPsec Encryption	Select the IP security encryption mechanism to use: • DES—Data Encryption Standard is a method of data encryption using a private (secret) key. DES applies a 56-bit key to each 64-bit block of data. • Triple DES—Data Encryption Standard that applies three keys in succession. • AES 128 CBC—Advanced Encryption Standard uses keys with a length of 128, 192, or 256 bits to encrypt blocks with a length of 128, 192, or 256 bits. AES 128 CBC uses a 128-bit data path in Cipher Clock Chaining (CBC) mode. • None—No IP security encryption mechanism.
IKE Authentication	The Internet Key Exchange (IKE) authentication is not an editable text box. Internet Key Exchange protocol (IKE) is used as a method of distributing the session keys (encryption and authentication), as well as providing a way for the VPN endpoints to agree on how data should be protected. IKE keeps track of connections by assigning a bundle of security associations (SAs) to each connection
IKE Phase 1	Choose either aggressive or main. This sets the IKE protocol. IKE phase 1 is used to negotiate how IKE is protected. Aggressive mode passes more information in fewer packets, with the benefit of a slightly faster connection, at the cost of transmitting the identities of the security gateways in the clear
Lifetime	Set the timeout interval (in seconds) when the session expires
IKE Diffie Hellman Group	Set the IKE Diffie Hellman group. The options are group 1 (768 bits), group 2 (1024 bits), or group 5 (1536 bits). Diffie-Hellman techniques are used by two devices to generate a symmetric key where you can publicly exchange values and generate the same symmetric key. Although all three groups provide security from conventional attacks, Group 5 is considered more secure because of its larger key size. However, computations involving Group 1 and Group 2 based keys might occur slightly faster because of their smaller prime number size

Controller > Security > AAA > LDAP Servers Template

Table 31-12 describes the fields on the **Design > Configuration Templates> Features and Technologies > Controller > Security > AAA > LDAP Servers** page.

Table 31-12 Controller > Security > AAA > LDAP Servers

Field	Description
Server Address	Enter the IP address of the server.
Port Number	Port number of the controller to which the access point is connected.
Bind Type	Choose **Authenticated** or **Anonymous**. If you choose Authenticated, you must enter a bind username and password as well. A bind is a socket opening that performs a lookup. Anonymous bind requests are rejected.
Server User Base DN	Enter the distinguished name of the subtree in the LDAP server that contains a list of all the users.
Server User Attribute	Enter the attribute that contains the username in the LDAP server.
Server User Type	Enter the ObjectType attribute that identifies the user.

Table 31-12 Controller > Security > AAA > LDAP Servers (continued)

Field	Description
Retransmit Timeout	Enter the number of seconds between retransmissions. The valid range is 2 to 30 seconds, and the default value is 2 seconds.
Admin Status	Check if you want the LDAP server to have administrative privileges.

Controller > Security > AAA > TACACS+ Servers Template

Table 31-13 describes the fields on the **Design > Configuration Templates> Features and Technologies > Controller > Security > AAA > TACACS+ Servers** page.

Table 31-13 Controller > Security > AAA > TACACS+ Servers

Field	Description
Server Type	Select one or more server types by selecting their respective check boxes. The following server types are available: • authentication—Server for user authentication/authorization. • authorization—Server for user authorization only. • accounting—Server for RADIUS user accounting.
Server Address	Enter the IP address of the server.
Port Number	Enter the port number of the server. The default is 49.
Shared Secret Format	Choose either **ASCII** or **hex**. Regardless of which format you choose, for security reasons, only ASCII is visible on the WLC (and Prime Infrastructure). For this reason, you cannot use a template to replicate the configuration on a second controller during auto provisioning. Set the key format again in the template in the event a discovered template is applied to another device.
Shared Secret	Enter the TACACS+ shared secret used by your specified server.
Confirmed Shared Secret	Reenter the TACACS+ shared secret used by your specified server.
Admin Status	Check if you want the LDAP server to have administrative privileges.
Retransmit Timeout	Enter the time, in seconds, after which the TACACS+ authentication request times out and a retransmission is attempted by the controller.

Controller > Security > Local EAP > General - Local EAP Template

Table 31-14 describes the fields on the **Design > Configuration Templates> Features and Technologies > Controller > Security > Local EAP > General - Local EAP** page.

Table 31-14 Controller > Security > Local EAP > General - Local EAP

Field	Description
Local Auth Active Timeout	Enter the amount of time (in seconds) that the controller attempts to authenticate wireless clients using local EAP after any pair of configured RADIUS servers fail. The valid range is 1 to 3600 seconds, and the default setting is 1000 seconds
Note Enter the values specified below if you are using EAP-FAST, manual password entry, one-time password, or 7920/7921 phones. You must increase the 802.1x timeout values on the controller (default=2 seconds) for the client to obtain the PAC using automatic provisioning. The recommended and default timeout on the Cisco ACS server is 20 seconds. Roaming fails if these values are not set the same across multiple controllers.	
Local EAP Identity Request Timeout	1
Local EAP Identity Request Maximum Retries	20
Local EAP Dynamic WEP Key Index	0
Local EAP Request Timeout	20
Local EAP Request Maximum Retries	2
EAPOL-Key Timeout	1000 (in milli-seconds)
EAPOL-Key Max Retries	2
Max Login Ignore Identity Response	Choose Enable to limit the number of devices that can be connected to the controller with the same username.

Controller > Security > Local EAP > Local EAP Profiles Template

Table 31-15 describes the fields on the **Design > Configuration Templates> Features and Technologies > Controller > Security > Local EAP > Local EAP Profiles** page.

Table 31-15 Controller > Security > Local EAP > Local EAP Profiles

Field	Description
EAP Profile Name	User-defined identification.
Select Profile Methods	Choose the desired authentication type: • LEAP—This authentication type leverages Cisco Key Integrity Protocol (CKIP) and MMH message integrity check (MIC) for data protection. A username and password are used to perform mutual authentication with the RADIUS server through the access point. • EAP-FAST—This authentication type (Flexible Authentication via Secure Tunneling) uses a three-phased tunnel authentication process to provide advanced 802.1X EAP mutual authentication. A username, password, and PAC (protected access credential) are used to perform mutual authentication with the RADIUS server through the access point. • TLS—This authentication type uses a dynamic session-based WEP key derived from the client adapter and RADIUS server to encrypt data. It requires a client certificate for authentication. • PEAP—This authentication type is based on EAP-TLS authentication but uses a password instead of a client certificate for authentication. PEAP uses a dynamic session-based WEP key derived from the client adapter and RADIUS server to encrypt data.
Certificate Issuer	Determine whether Cisco or another vendor issued the certificate for authentication. Only EAP-FAST and TLS require a certificate.
Check Against CA Certificates	Check if you want the incoming certificate from the client to be validated against the certificate authority (CA) certificates on the controller.
Verify Certificate CN Identity	Check if you want the (CN) in the incoming certificate to be validated against the common name of the CA certificate.
Check Against Date Validity	Check if you want the controller to verify that the incoming device certificate is still valid and has not expired.
Local Certificate Required	Check if a local certificate is required.
Client Certificate Required	Check if a client certificate is required.

Controller > Security > Local EAP > EAP-FAST Parameters Template

Table 31-16 describes the fields on the **Design > Configuration Templates> Features and Technologies > Controller > Security > Local EAP > EAP-FAST Parameters** page.

Table 31-16 Controller > Security > Local EAP > EAP_FAST Parameters

Field	Description
Time to Live for the PAC	Enter the number of days for the PAC to remain viable. The valid range is 1 to 1000 days, and the default setting is 10 days.
Authority ID	Enter the authority identifier of the local EAP-FAST server in hexadecimal characters. You can enter up to 32 hexadecimal characters, but you must enter an even number of characters.
Authority Info	Enter the authority identifier of the local EAP-FAST server in text format.

Table 31-16 Controller > Security > Local EAP > EAP_FAST Parameters (continued)

Field	Description
Server Key and Confirm Server Key	Enter the key (in hexadecimal characters) used to encrypt and decrypt PACs
Anonymous Provision	Check to enable anonymous provisioning. This feature allows PACs to be sent automatically to clients that do not have one during PAC provisioning. If you disable this feature, PACs must be manually provisioned

Controller > Security > Wireless Protection Policies > Rogue Policies Template

Table 31-17 describes the fields on the **Design > Configuration Templates> Features and Technologies > Controller > Security > Wireless Protection Policies > Rogue Policies** page.

Table 31-17 Controller > Security > Wireless Protection Policies > Rogue Policies

Field	Description
Rogue Location Discovery Protocol	Determine whether or not the Rogue Location Discovery Protocol (RLDP) is connected to the enterprise wired network. Choose one of the following: • **Disable**—Disables RLDP on all access points. • **All APs**—Enables RLDP on all access points. • **Monitor Mode APs**—Enables RLDP only on access points in monitor mode. **Note** With RLDP, the controller instructs a managed access point to associate with the rogue access point and sends a special packet to the controller. If the controller receives the packet, the rogue access point is connected to the enterprise network. This method works for rogue access points that do not have encryption enabled.
Expiration TImeout for Rogue AP and Rogue Client Entries	Enter the expiration timeout (in seconds) for rogue access point entries.
Rogue Detection Report Interval	Enter the time interval in seconds at which the APs should send the rogue detection report to the controller. A valid range is 10 seconds to 300 seconds, and the default value is 10 seconds. This feature is applicable to APs that are in monitor mode only.
Rogue Detection Minimum RSSI	Enter the minimum RSSI value that a rogue should have for the APs to detect and for the rogue entry to be created in the controller. A valid range is -70 dBm to -128 dBm, and the default value is -128 dBm. This feature is applicable to all the AP modes. There can be many rogues with very weak RSSI values that do not provide any valuable information in the rogue analysis. Therefore, you can use this option to filter the rogues by specifying the minimum RSSI value at which the APs should detect rogues.
Rogue Detection Transient Interval (Enter 0 to Disable)	Enter the time interval at which a rogue has to be consistently scanned for by the AP after the first time the rogue is scanned. By entering the transient interval, you can control the time interval at which the AP should scan for rogues. The APs can filter the rogues based on their transient interval values. Valid range is between 120 seconds to 1800 seconds, and the default value is 0. This feature is applicable to APs that are in monitor mode only
Validate Rogue Clients against AAA	Check to enable the AAA validation of rogue clients.
Detect and Report Adhoc Networks	Check to enable detection and reporting of rogue clients participating in ad hoc networking.

Table 31-17 Controller > Security > Wireless Protection Policies > Rogue Policies (continued)

Field	Description
Rogue on Wire	Automatically contains rogues that are detected on the wired network.
Using our SSID	Automatically contains rogues that are advertising your network's SSID. If you leave this parameter unselected, the controller only generates an alarm when such a rogue is detected.
Valid Client on Rogue AP	Automatically contains a rogue access point to which trusted clients are associated. If you leave this parameter unselected, the controller only generates an alarm when such a rogue is detected.

Controller > Security > IP Groups Template

Table 31-18 describes the fields on the following page: **Design > Configuration Templates > Features and Technologies > Controller > Security > IP Groups**

Table 31-18 Controller > Security > IP Groups

Field	Description
Name	Name of the template.
Description	Description of the template.
Validation Criteria	Choose a device type from the drop-down list and enter the OS version.
IP Group Name	Lists all the IP address including IPv4 and IPv6 groups. One IP address group can have a maximum of 128 IP address and netmask combinations. For the IP address of any, an **any** group is predefined. For the IPv6 address of any, an **any** group is predefined with an IP address type of IPv6.
IP Address	For an IP Group, enter an IPv4 address format. For IPv6 groups, enter an IPv6 address format.
Netmask	Allows the user to set the subnet mask in dotted-decimal notation rather than the CIDR notation for the IP address property. A range of IP addresses defined so that only machines with IP addresses within the range are allowed to access an Internet service. This field does not apply for IPv6 groups.
CIDR	Classless InterDomain Routing. This field does not apply for IPv6 groups. A protocol which allows the assignment of Class C IP addresses in multiple contiguous blocks. CIDR notation allows the user to add a large number of clients that exist in a subnet range by configuring a single client object.
Prefix Length	Prefix for IPv6 addresses, ranging from 0 to 128.

Controller > Security > Protocol Groups

Table 31-19 describes the fields on the following page: **Design > Configuration Templates > Features and Technologies > Controller > Security > Protocol Groups.**

Table 31-19 Controller > Security > Protocol Groups

Field	Description
Name	Name of the template.
Description	Description of the template.
Rule Name	The rule name is provided for the existing rules, or you can now enter a name for a new rule. ACLs are not required to have rules defined. When a packet matches all the fields of a rule, the action for this rule is exercised.

Table 31-19 Controller > Security > Protocol Groups (continued)

Field	Description
Protocol	Choose a protocol from the drop-down list: • Any—All protocols • TCP—Transmission Control Protocol • UDP—User Datagram Protocol • ICMP—Internet Control Message Protocol • ESP—IP Encapsulating Security Payload • AH—Authentication Header • GRE—Generic Routing Encapsulation • IP—Internet Protocol • Eth Over IP—Ethernet over Internet Protocol • Other Port OSPF—Open Shortest Path First • Other—Any other IANA protocol (http://www.iana.org/)
Source Port	Enter the source port. Can be Any, HTTP, HTTPS, Telnet, RADIUS, DHCP Server, DHCP Client, DNS, L2TP, PPTP control, FTP control, SMTP, SNMP, LDAP, Kerberos, NetBIOS NS, NetBIOS DS, NetBIOS SS, MS Dir Server, Other and Port Range.
Dest Port	Enter the destination port. If TCP or UDP is selected, can be Any, HTTP, HTTPS, Telnet, RADIUS, DHCP Server, DHCP Client, DNS, L2TP, PPTP control, FTP control, SMTP, SNMP, LDAP, Kerberos, NetBIOS NS, NetBIOS DS, NetBIOS SS, MS Dir Server, Other and Port Range.
DSCP (Differentiated Services Code Point)	Choose Any or Specific from the drop-down list. If Specific is selected, enter the DSCP (range of 0 through 255). DSCP is a packet header code that can be used to define the quality of service across the Internet.

Controller > Security > 802.11 > Band Select

Table 31-20 describes the fields on the following page: **Design > Configuration Templates > Features and Technologies > Controller > Security > 802.11 > Band Select**.

Table 31-20 Controller > Security > 802.11 > Band Select

Field	Description
Probe Cycle Count	Enter a value between 1 and 10 for the probe cycle count. The cycle count sets the number of suppression cycles for a new client. The default cycle count is 2.
Scan Cycle Period Threshold	Enter a value between 1 and 1000 milliseconds for the scan cycle period threshold. This setting determines the time threshold during which new probe requests from a client come from a new scanning cycle. The default cycle threshold is 200 milliseconds.
Age Out Suppression	Enter a value between 10 and 200 seconds for the age out suppression field. Age-out suppression sets the expiration time for pruning previously known 802.11b/g clients. The default value is 20 seconds. After this time elapses, clients become new and are subject to probe response suppression.

Table 31-20 Controller > Security > 802.11 > Band Select (continued)

Field	Description
Age Out Dual Band	Enter a value between 10 and 300 seconds for the age out dual band field. The age-out period sets the expiration time for pruning previously known dual-band clients. The default value is 60 seconds. After this time elapses, clients become new and are subject to probe response suppression.
Acceptable Client RSSI	Enter a value between –20 and –90 dBm for the acceptable client RSSI field. This field sets the minimum RSSI for a client to respond to a probe. The default value is –80 dBm.

Controller > Security > 802.11 > Media Stream

Table 31-21 describes the fields on the following page: **Design > Configuration Templates > Features and Technologies > Controller > Security > 802.11 > Media Stream.**

Table 31-21 Controller > Security > 802.11 > Media Stream

Field	Description
Media Stream Name	The name of the media stream.
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. Start IP and End IP can be IPv4 or IPv6 multicast address, starting from controller Version 7.2.x.
Maximum Expected Bandwidth	Maximum bandwidth that a media stream can use.
Average Packet Size	Average packet size that a media stream can use.
RRC Periodical Update	Resource Reservation Control calculations that are updated periodically; if disabled, RRC calculations are done only once when a client joins a media stream.
RRC Priority	Priority of RRC with the highest at 1 and the lowest at 8.
Traffic Profile Violation	Appears if the stream is dropped or put in the best effort queue if the stream violates the QoS video profile.
Policy	Appears if the media stream is admitted or denied.

Controller > Security > 802.11 > RF Profiles

Table 31-22 describes the fields on the following page: **Design > Configuration Templates > Features and Technologies > Controller > Security > 802.11 > RF Profiles.**

Table 31-22 Controller > Security > 802.11 > RF Profiles

Field	Description
Template Name	User-defined name for the template.
Profile Name	User-defined name for the current profile.
Description	Description of the template.
Radio Type	The radio type of the access point. This is a drop-down list from which you can choose an RF profile for APs with 802.11a or 802.11b radios.

Table 31-22 Controller > Security > 802.11 > RF Profiles (continued)

Field	Description
Minimum Power Level Assignment (-10 to 30 dBm)	Indicates the minimum power assigned. Range: -10 to 30 dBm Default: -10 dBm.
Maximum Power Level Assignment (-10 to 30 dBm)	Indicates the maximum power assigned. Range: -10 to 30 dBm Default: 30 dBm.
Power Threshold v1(-80 to -50 dBm)	Indicates the transmitted power threshold.
Power Threshold v2(-80 to -50 dBm)	Indicates the transmitted power threshold.
Data Rates	Use the Data Rates drop-down lists to specify the rates at which data can be transmitted between the access point and the client. These data rates are available: • 802.11a—6, 9, 12, 18, 24, 36, 48, and 54 Mbps. • 802.11b/g—1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, or 54 Mbps For each data rate, you must also choose one of these options: • Mandatory—Clients must support this data rate to associate to an access point on the controller. • Supported—Any associated clients that support this data rate might communicate with the access point using that rate. However, the clients are not required to be able to use this rate to associate. • Disabled—The clients specify the data rates used for communication.

Controller > 80211a or n > Parameters

Table 31-23 describes the fields on the following page: **Design > Configuration Templates > Features and Technologies > Controller > 80211a or n > Parameters**.

Table 31-23 Controller > 80211a or n > Parameters

Field	Description
802.11a Network Status	Select the check box to enable 802.11a/n network status.
Client Link	Use this drop-down list to enable Clientlink on all access point 802.11a/n radios that support ClientLink. Otherwise, choose Disable.
Beacon Period	Enter the amount of time between beacons in kilomicroseconds. The valid range is from 20 to 1000 milliseconds.
DTIM Period	Enter the number of beacon intervals that might elapse between transmission of beacon frames containing a traffic indicator message (TIM) element whose delivery count text box is 0. This value is transmitted in the DTIM period field of beacon frames. When client devices receive a beacon that contains a DTIM, they normally wake up to check for pending packets. Longer intervals between DTIMS let clients sleep longer and preserve power. Conversely, shorter DTIM periods reduce the delay in receiving packets but use more battery power because clients wake up more often.
Fragmentation Threshold	Determine the size at which packets are fragmented (sent as several pieces instead of as one block). Use a low setting in areas where communication is poor or where there is a great deal of radio interference.
802.11e Max Bandwidth	Enter the percentage for 802.11e maximum bandwidth.

Table 31-23 Controller > 80211a or n > Parameters (continued)

Field	Description
Mode	Click the checkbox to enable Cisco Compatible Extension (CCX) Location Measurement. When enabled, this enhances the location accuracy of clients.
Interval	Enter the interval at which CCX Location Measurement signals are broadcast, in seconds. The CCX location measurement interval of the Cisco Compatible Extension can only be changed when measurement mode is enabled.
Data Rate Dropdowns	Select the negotiation type for each data rate. The client and controller negotiate data rates between them. If the data rate is set to Mandatory, the client must support it to use the network. If a data rate is set as Supported by the controller, any associated client that also supports that same rate might communicate with the access point using that rate. However, it is not required that a client uses all the rates marked supported to associate. For each rate, a drop-down list of Mandatory or Supported is available. Each data rate can also be set to Disable to match client settings.
Channel List	From this drop-down list in the Noise/Interference/Rogue Monitoring Channels section, choose between all channels, country channels, or DCA channels based on the level of monitoring you want. Dynamic Channel Allocation (DCA) automatically selects a reasonably good channel allocation amongst a set of managed devices connected to the controller.

Controller > 80211a or n > CleanAir

Table 31-24 describes the fields on the following page: **Design > Configuration Templates > Features and Technologies > Controller > 80211a or n > CleanAir.**

Table 31-24 Controller > 80211a or n > CleanAir

Field	Description
Report Interferers	Select the report interferers check box to enable the CleanAir system to report and detect sources of interference, or unselect it to prevent the controller from reporting interferers. The default value is unselected.
Interferers Ignored/Selected for Reporting	Make sure that any sources of interference that need to be detected and reported by the CleanAir system appear in the Interferences to Detect box and any that do not need to be detected appear in the Interferers to Ignore box. Use the > and < buttons to move interference sources between these two boxes. By default, all interference sources are ignored.
Persistent Device Propagation	Select the Persistent Device Propagation check box to enable propagation of information about persistent devices that can be detected by CleanAir. Persistent device propagation enables designating information about interference types and propagating this information to the neighboring access points. Persistent interferers are present at the a location and interfere with the WLAN operations even if they are not detectable at all times.
Air Quality Alarm	Select the Air Quality Alarm check box to enable the triggering of air quality alarms, or unselect the box to disable this feature.
Air Quality Alarm Threshold	If you selected the Air Quality Alarm check box, enter a value between 1 and 100 (inclusive) in the Air Quality Alarm Threshold field to specify the threshold at which you want the air quality alarm to be triggered. When the air quality falls below the threshold level, the alarm is triggered. A value of 1 represents the worst air quality, and 100 represents the best. The default value is 1.

Table 31-24 Controller > 80211a or n > CleanAir (continued)

Field	Description
Air Quality Unclassified Category Alarm	Category AlarmSelect the Air Quality Unclassified category Alarm check box to enable the alarms to be generated for unclassified interference category. CleanAir can detect and monitor unclassified interferences. Unclassified interference are interference that are detected but do not correspond to any of the known interference types.
Air Quality Unclassified Category Severity Threshold	If you selected the Air Quality Unclassified category Alarm check box, enter a value between 1 and 99 (inclusive) in the Air Quality Unclassified Severity Threshold text box to specify the threshold at which you want the unclassified category alarm to be triggered. The default is 20.
Interferers For Security Alarm	Select the Interferers For Security Alarm check box to trigger interferer alarms when the controller detects specified device types, or unselect it to disable this feature. The default value is unselected.
Interferers Ignored/Selected for Security Alarms	Make sure that any sources of interference that need to trigger interferer alarms appear in the Interferers Selected for Security Alarms box and any that do not need to trigger interferer alarms appear in the Interferers Ignored for Security Alarms box. Use the > and < buttons to move interference sources between these two boxes. By default, all interferer sources for security alarms are ignored.

Controller > 80211a or n > Media Parameters

The following tables describe the fields on the **Design > Configuration Templates > Features and Technologies > Controller > 802.11a or n > Media Parameters** page:

- Table 31-25—Voice tab
- Table 31-26—Video tab
- Table 31-27—General tab

Controller > 80211a or n > Media Parameters > Voice

Table 31-25 describes the fields on the **Design > Configuration Templates> Features and Technologies > Controller > 80211a or n > Media Parameters > Voice** tab.

Table 31-25 Controller > 80211a or n > Media Parameters > Voice

Field	Description
Admission Control (ACM)	Select the check box to enable admission control. For end users to experience acceptable audio quality during a VoIP phone call, packets must be delivered from one endpoint to another with low latency and low packet loss. To maintain QoS under differing network loads, call admission control (CAC) is required. CAC on an access point allows it to maintain controlled QoS when the network is experiencing congestion and keep the maximum allowed number of calls to an acceptable quantity.
CAC Method	If Admission Control (ACM) is enabled, specify the CAC method as either load-based or static. Load-based CAC incorporates a measurement scheme that takes into account the bandwidth consumed by all traffic types from itself, from co-channel access points, and by co-located channel interference. Load-based CAC also covers the additional bandwidth consumption resulting from PHY and channel impairment.
Maximum Bandwidth Allowed	Specify the percentage of maximum bandwidth allowed. This option is only available when CAC is enabled.

Table 31-25 Controller > 80211a or n > Media Parameters > Voice (continued)

Field	Description
Reserved Roaming Bandwidth	Specify the percentage of reserved roaming bandwidth. This option is only available when CAC is enabled.
Expedited Bandwidth	Select the check box to enable expedited bandwidth as an extension of CAC for emergency calls. You must have an expedited bandwidth IE that is CCXv5 compliant so that a TSPEC request is given higher priority.
SIP CAC	Select the check box to enable SIP CAC. SIP CAC should be used only for phones that support status code 17 and do not support TSPEC-based admission control.
SIP Codec	Specify the codec name you want to use on this radio. The available options are G.711, G.729, and User Defined.
SIP Call Bandwidth	Specify the bandwidth in kilobits per second that you want to assign per SIP call on the network. This field can be configured only when the SIP Codec selected is User Defined.
SIP Sample Interval	Specify the sample interval in milliseconds that the codec must operate in.
Metric Collection	Select the check box to enable metric collection. Traffic stream metrics are a series of statistics about VoIP over your wireless LAN which inform you of the QoS of the wireless LAN. For the access point to collect measurement values, traffic stream metrics must be enabled. When this is enabled, the controller begins collecting statistical data every 90 seconds for the 802.11b/g interfaces from all associated access points. If you are using VoIP or video, this feature should be enabled.

Related Topics

- Table 31-26—Video tab
- Table 31-27—General tab

Controller > 80211a or n > Media Parameters > Video

Table 31-26 describes the fields on the **Design > Configuration Templates> Features and Technologies > Controller > 80211a or n > Media Parameters > Video** tab.

Table 31-26 Controller > 80211a or n > Media Parameters > Video

Field	Description
Admission Control (ACM)	Select the check box to enable admission control.
Maximum Bandwidth	Specify the percentage of maximum bandwidth allowed. This option is only available when CAC is enabled.
Reserved Roaming Bandwidth	Specify the percentage of reserved roaming bandwidth. This option is only available when CAC is enabled.
CAC Method	If Admission Control (ACM) is enabled, specify the CAC method as either load-based or static. Load-based CAC incorporates a measurement scheme that takes into account the bandwidth consumed by all traffic types from itself, from co-channel access points, and by co-located channel interference. Load-based CAC also covers the additional bandwidth consumption resulting from PHY and channel impairment.
Unicast Video Redirect	Select the Unicast Video Redirect check box to enable all non-media stream packets in video queue are redirected to the best effort queue. If disabled, all packets with video marking are kept in video queue.

Table 31-26 Controller > 80211a or n > Media Parameters > Video (continued)

Field	Description
Client Minimum Phy Rate	Specify the physical data rate required for the client to join a media stream from the Client Minimum Phy Rate drop-down list.
Multicast Direct Enable	Select the Multicast Direct Enable check box to set the Media Direct for any WLAN with Media Direct enabled on a WLAN on this radio.
Maximum Number of Streams per Radio	Specify the maximum number of streams per Radio to be allowed.
Maximum Number of Streams per Client	Specify the maximum number of streams per Client to be allowed.
Best Effort QOS Admission	Select the Best Effort QOS Admission check box to redirect new client requests to the best effort queue. This happens only if all the video bandwidth has been used. If this is disabled and maximum video bandwidth has been used, then any new client request is rejected.

Related Topics

- Table 31-25—Voice tab
- Table 31-27—General tab

Controller > 80211a or n > Media Parameters > General

Table 31-27 describes the fields on the **Design > Configuration Templates> Features and Technologies > Controller > 80211a or n > Media Parameters > General** tab.

Table 31-27 Controller > 80211a or n > Media Parameters > General

Field	Description
Maximum Media Bandwidth (0 to 85%)	Specify the percentage of maximum of bandwidth allowed. This option is only available when CAC is enabled.

Related Topics

- Table 31-25—Voice tab
- Table 31-26—Video tab

Controller > 80211a or n > Roaming Parameters

Table 31-28 describes the fields on the following page: **Design > Configuration Templates > Features and Technologies > Controller > 80211a or n > Roaming Parameters**.

Table 31-28 Controller > 80211a or n > Roaming Parameters

Field	Description
Mode	Use the Mode drop-down list to choose one of the configurable modes: default values or custom values. If you select Default, the roaming parameters are unavailable for editing, and have the default values displayed in the text boxes. Select Custom to edit the roaming parameters.
Minimum RSSI	Enter a value for the minimum Received Signal Strength Indicator (RSSI) required for the client to associate to an access point. If the average received signal power of the client dips below this threshold, reliable communication is usually impossible. Therefore, clients must already have found and roamed to another access point with a stronger signal before the minimum RSSI value is reached. Range: -80 to -90 dBm. Default: -85 dBm
Roaming Hysteresis	Enter a value to indicate how strong the signal strength of a neighboring access point must be for the client to roam to it. This field is intended to reduce the amount of ping ponging between access points if the client is physically located on or near the border between two access points. Range: 2 to 4 dB. Default: 2 dB.
Adaptive Scan Threshold	Enter the RSSI value from the associated access point of the client, below which the client must be able to roam to a neighboring access point within the specified transition time. This field also provides a power-save method to minimize the time that the client spends in active or passive scanning. For example, the client can scan slowly when the RSSI is above the threshold and scan more rapidly when below the threshold. Range: -70 to -77 dB. Default: -72 dB.
Transition Time	Enter the maximum time allowed for the client to detect a suitable neighboring access point to roam to and to complete the roam, whenever the RSSI from the associated access point of the client is below the scan threshold. Range: 1 to 10 seconds. Default: 5 seconds.

Controller > 80211a or n > dot11a-RRM > Thresholds

Table 31-29 describes the fields on the following page: **Design > Configuration Templates > Features and Technologies > Controller > 80211a or n > dot11a-RRM > Thresholds.**

Table 31-29 Controller > 80211a or n > dot11a-RRM > Thresholds

Field	Description
Min Failed Clients	Enter the minimum number of failed clients currently associated with the controller.
Coverage Level	Enter the target range of coverage threshold.
Data RSSI	Enter the Data RSSI (–60 to –90 dBm). This number indicates the value for the minimum Received Signal Strength Indicator (RSSI) for data required for the client to associate to an access point.
Voice RSSI	Enter the Voice RSSI (–60 to –90 dBM). This number indicates the value for the minimum Received Signal Strength Indicator (RSSI) required for voice for the client to associate to an access point.
Max Clients	Enter the maximum number of failed clients that are currently associated with the controller.
RF Utilization	Enter the percentage of threshold for 802.11a/n.
Interference Threshold	Enter an interference threshold percentage.
Noise Threshold	Enter a noise threshold between -127 and 0 dBm. When the controller is outside of this threshold, it sends an alarm to Prime Infrastructure.
Coverage Exception Level Per AP	Enter the coverage exception level percentage. When the coverage drops by this percentage from the configured coverage for the minimum number of clients, a coverage hole is generated.

Controller > 80211a or n > dot11a-RRM > DCA

Table 31-30 describes the fields on the following page: **Design > Configuration Templates > Features and Technologies > Controller > 80211a or n > dot11a-RRM > DCA.**

Table 31-30 Controller > 80211a or n > dot11a-RRM > DCA

Field	Description
Assignment Mode	From the, choose one of three modes: • Automatic—The transmit power is periodically updated for all access points that permit this operation. • On Demand—Transmit power is updated when you click Assign Now. • Disabled—No dynamic transmit power assignments occur, and values are set to their global default.
Avoid Foreign AP Interference	Select the check box to have RRM consider interference from foreign Cisco access points (those non-Cisco access points outside RF/mobility domain) when assigning channels. This foreign 802.11 interference. Unselect this check box to have RRM ignore this interference.In certain circumstances with significant interference energy (dB) and load (utilization) from foreign access points, RRM might adjust the channel assignment to avoid these channels (and sometimes adjacent channels) in access points close to the foreign access points. This increases capacity and reduces variability for the Cisco WLAN Solution.
Avoid Cisco AP Load	Select the check box to have controllers consider the traffic bandwidth used by each access point when assigning channels to access points. Unselect this check box to have RRM ignore this value. In certain circumstances and with denser deployments, there might not be enough channels to properly create perfect channel reuse. In these circumstances, RRM can assign better reuse patterns to those access points that carry more traffic load.
Avoid non 802.11 Noise	Select the check box to have access points avoid channels that have interference from non-access point sources, such as microwave ovens or Bluetooth devices. Unselect this check box to have RRM ignore this interference. In certain circumstances with significant interference energy (dB) from non-802.11 noise sources, RRM might adjust the channel assignment to avoid these channels (and sometimes adjacent channels) in access points close to the noise sources. This increases capacity and reduces variability for the Cisco WLAN Solution.
Signal Strength Contribution	Always enabled (not configurable). This constantly monitors the relative location of all access points within the RF/mobility domain to ensure near-optimal channel reuse. The net effect is an increase in Cisco WLAN Solution capacity and a reduction in co-channel and adjacent channel interference.
Event Driven RRM	Select the check box to disable spectrum event-driven RRM. By default, Event Driven RRM is enabled. Event Driven RRM is used when a CleanAir-enabled access point detects a significant level of interference
Sensitivity Threshold	If Event Driven RRM is enabled, this field displays the threshold level at which event-driven RRM is triggered. It can have a value of either Low, Medium, or High. When the interference for the access point rises above the threshold level, RRM initiates a local Dynamic Channel Assignment (DCA) run and changes the channel of the affected access point radio if possible to improve network performance. Low represents a decreased sensitivity to changes in the environment while High represents an increased sensitivity.

Controller > 802.11b or g or n > Parameters

Table 31-31 describes the fields on the following page: **Design > Configuration Templates > Features and Technologies > Controller > 802.11b or g or n > Parameters**.

Table 31-31 Controller > 802.11b or g or n > Parameters

Field	Description
Policy Name	Security policy in force.
Beam Forming	Choose Enable or Disable from the drop-down list. Beam forming refers to a general signal processing technique used to control the directionality of the reception or transmission of a signal.
Transmitted Power Threshold	The valid range is from -50 to -80.
Beacon Period	The rate at which the SSID is broadcast by the access point (the amount of time between beacons). The valid range is from 100 to 600 milliseconds.
DTIM Period	The number of beacon intervals that might elapse between transmission of beacon frames containing a traffic indicator message (TIM) element whose delivery count field is 0. This value is transmitted in the DTIM period field of beacon frames. When client devices receive a beacon that contains a DTIM, they normally "wake up" to check for pending packets. Longer intervals between DTIMs let clients sleep longer and preserve power. Conversely, shorter DTIM periods reduce the delay in receiving packets but use more battery power because clients wake up more often. DTIM period is not applicable in controller Version 5.0.0.0 and later.
Fragmentation Threshold	Determine the size at which packets are fragmented (sent as several pieces instead of as one block). Use a low setting in areas where communication is poor or where there is a great deal of radio interference. The default value is 2346.
802.11e Max Bandwidth	Percentage for 802.11e max bandwidth. The default value is 100.
Dynamic Assignment	From the Dynamic Assignment drop-down list, choose any one of the following dynamic transmit power assignment modes.: • Automatic—The transmit power is periodically updated for all access points that permit this operation. • On Demand—Transmit power is updated when you click Assign Now. • Disabled—No dynamic transmit power assignments occur and values are set to their global default. The default is Automatic. The power levels and available channels are defined by the country code setting and are regulated on a country by country basis.
Dynamic Tx Power Control	Select this check box to enable DTPC support. If this option is enabled, the transmit power level of the radio is advertised in the beacons and the probe responses.

Table 31-31 Controller > 802.11b or g or n > Parameters (continued)

Field	Description
Assignment Mode	From the Assignment Mode drop-down list, choose any one of the following dynamic channel assignment modes: • Automatic—The channel assignment is periodically updated for all access points that permit this operation. • On Demand—Channel assignments are updated when desired. • Disabled—No dynamic channel assignments occur and values are set to their global default. The default is Automatic.
Avoid Foreign AP Interference	Enable this Radio Resource Management (RRM) foreign 802.11 interference-monitoring parameter to have Radio Resource Management consider interference from foreign (non-Cisco access points outside the RF/mobility domain) access points when assigning channels to Cisco access points. Disable this field to have Radio Resource Management ignore this interference. In certain circumstances with significant interference energy (dB) and load (utilization) from Foreign access points, Radio Resource Management might adjust the channel assignment to avoid these channels (and sometimes adjacent channels) in Cisco access points close to the Foreign access points to increase capacity and reduce variability for the Cisco WLAN Solution.
Avoid Cisco AP Load	Enable this Radio Resource Management (RRM) bandwidth-sensing parameter to have controllers consider the traffic bandwidth used by each access point when assigning channels to access points. Disable this field to have Radio Resource Management ignore this value. In certain circumstances and with denser deployments, there might not be enough channels to properly create perfect channel re-use. In these circumstances, Radio Resource Management can assign better re-use patterns to those APs that carry more traffic load.
Avoid non 802.11 Noise	Enable this Radio Resource Management (RRM) noise-monitoring field to have access points avoid channels that have interference from non-Access Point sources, such as microwave ovens or Bluetooth devices. Disable this field to have Radio Resource Management ignore this interference. In certain circumstances with significant interference energy (dB) from non-802.11 noise sources, Radio Resource Management might adjust the channel assignment to avoid these channels (and sometimes adjacent channels) in access points close to the noise sources to increase capacity and reduce variability for the Cisco WLAN Solution.
Signal Strength Contribution	This check box is always enabled (not configurable). Radio Resource Management (RRM) constantly monitors the relative location of all access points within the RF/mobility domain to ensure near-optimal channel reuse. The net effect is an increase in Cisco WLAN Solution capacity and a reduction in co-channel and adjacent channel interference.
Data Rates	The data rates set are negotiated between the client and the controller. If the data rate is set to Mandatory, the client must support it to use the network. If a data rate is set as Supported by the controller, any associated client that also supports that same rate might communicate with the access point using that rate. But it is not required that a client be able to use all the rates marked Supported to associate 6, 9, 12, 18, 24, 36, 48, 54 Mbps. For each rate, a drop-down list selection of Mandatory or Supported is available. Each data rate can also be set to Disabled to match Client settings.

Table 31-31 Controller > 802.11b or g or n > Parameters (continued)

Field	Description
Channel List	Choose between all channels, country channels, or DCA channels based on the level of monitoring you want. Dynamic Channel Allocation (DCA) automatically selects a reasonably good channel allocation among a set of managed devices connected to the controller.
Mode	Enable or disable the broadcast radio measurement request. When enabled, this enhances the location accuracy of clients.
Interval	Interval in seconds between measurement requests. Cisco Compatible Extension location measurement interval can be changed only when measurement mode is enabled.

Controller > 802.11b or g or n > Media Parameters

The following tables describe the fields on the **Design > Configuration Templates > Features and Technologies > Controller > 802.11b or g or n > Media Parameters** page:

- Table 31-32—Voice tab
- Table 31-33—Video tab
- Table 31-34—General tab

Controller > 802.11b or g or n > Media Parameters > Voice

Table 31-32 describes the fields on the **Design > Configuration Templates> Features and Technologies > Controller > 802.11b or g or n > Media Parameters > Voice** tab.

Table 31-32 Controller > 802.11b or g or n > Media Parameters > Voice

Field	Description
Admission Control (ACM)	Select the check box to enable admission control. For end users to experience acceptable audio quality during a VoIP phone call, packets must be delivered from one endpoint to another with low latency and low packet loss. To maintain QoS under differing network loads, Call Admission Control (CAC) is required. CAC on an access point allows it to maintain controlled QoS when the network is experiencing congestion and keep the maximum allowed number of calls to an acceptable quantity.
CAC Method	If Admission Control (ACM) is enabled, specify the CAC method as either load-based or static. Load-based CAC incorporates a measurement scheme that takes into account the bandwidth consumed by all traffic types from itself, from co-channel access points, and by co-located channel interference. Load-based CAC also covers the additional bandwidth consumption resulting from PHY and channel impairment.
Maximum Bandwidth Allowed	Enter the percentage of maximum bandwidth allowed. This option is only available when CAC is enabled.
Reserved Roaming Bandwidth	Enter the percentage of reserved roaming bandwidth. This option is only available when CAC is enabled.
Expedited Bandwidth	Select the check box to enable expedited bandwidth as an extension of CAC for emergency calls. You must have an expedited bandwidth IE that is CCXv5 compliant so that a TSPEC request is given higher priority.

Table 31-32 Controller > 802.11b or g or n > Media Parameters > Voice (continued)

Field	Description
SIP CAC	Select the check box to enable SIP CAC. SIP CAC should be used only for phones that support status code 17 and do not support TSPEC-based admission control.
SIP Codec	Choose the codec name you want to use on this radio from the SIP Codec drop-don list. The available options are G.711, G.729, and User Defined.
SIP Call Bandwidth	Enter the bandwidth in kilobits per second that you want to assign per SIP call on the network. This field can be configured only when the SIP Codec selected is User Defined.
SIP Sample Interval	Enter the sample interval in milliseconds that the codec must operate in.
Max Number of Calls per Radio	Enter the maximum number of calls per radio.
Metric Collection	Select the check box to enable metric collection. Traffic stream metrics are a series of statistics about VoIP over your wireless LAN which inform you of the QoS of the wireless LAN. For the access point to collect measurement values, traffic stream metrics must be enabled. When this is enabled, the controller begins collecting statistical data every 90 seconds for the 802.11b/g interfaces from all associated access points. If you are using VoIP or video, this feature should be enabled.

Related Topics

- Table 31-33—Video tab
- Table 31-34—General tab

Controller > 802.11b or g or n > Media Parameters > Video

Table 31-32 describes the fields on the **Design > Configuration Templates> Features and Technologies > Controller > 802.11b or g or n > Media Parameters > Video** tab.

Table 31-33 Controller > 802.11b or g or n > Media Parameters > Video

Field	Description
Admission Control (ACM)	Select the check box to enable admission control.
Maximum Bandwidth	Specify the percentage of maximum bandwidth allowed. This option is only available when CAC is enabled.
Reserved Roaming Bandwidth	Specify the percentage of reserved roaming bandwidth. This option is only available when CAC is enabled.
Unicast Video Redirect	Select the Unicast Video Redirect check box to enable all non-media stream packets in video queue are redirected to the best effort queue. If disabled, all packets with video marking are kept in video queue.
Client Minimum Phy Rate	Choose the physical data rate required for the client to join a media stream from the Client Minimum Phy Rate drop-down list.
Multicast Direct Enable	Select the Multicast Direct Enable check box to set the Media Direct for any WLAN with Media Direct enabled on a WLAN on this radio.
Maximum Number of Streams per Radio	Specify the maximum number of streams per Radio to be allowed.

Table 31-33 Controller > 802.11b or g or n > Media Parameters > Video (continued)

Field	Description
Maximum Number of Streams per Client	Specify the maximum number of streams per Client to be allowed.
Best Effort QOS Admission	Select the Best Effort QOS Admission check box to redirect new client requests to the best effort queue. This happens only if all the video bandwidth has been used. If disabled and maximum video bandwidth has been used, then any new client request is rejected.

Related Topics

- Table 31-32—Voice tab
- Table 31-34—General tab

Controller > 802.11b or g or n > Media Parameters > General

Table 31-34 describes the fields on the **Design > Configuration Templates> Features and Technologies > Controller > 802.11b or g or n > Media Parameters > General** tab.

Table 31-34 Controller > 80211b or g or n > Media Parameters > General

Field	Description
Maximum Media Bandwidth (0 to 85%)	Specify the percentage of maximum of bandwidth allowed. This option is only available when CAC is enabled.

Related Topics

- Table 31-32—Voice tab
- Table 31-33—Video tab

Controller > 802.11b or g or n > Roaming Parameters

Table 31-35 describes the fields on the following page: **Design > Configuration Templates > Features and Technologies > Controller > 802.11b or g or n > Roaming Parameters.**

Table 31-35 Controller > 802.11b or g or n > Roaming Parameters

Field	Description
Mode	Choose Default Values or Custom Values from the drop-down list. If you select Default Values, the roaming parameters are unavailable and the default values are displayed.
Minimum RSSI	Enter a value for the minimum Received Signal Strength Indicator (RSSI) required for the client to associate to an access point. If the client average received signal power dips below this threshold, reliable communication is usually impossible. Therefore, clients must already have found and roamed to another access point with a stronger signal before the minimum RSSI value is reached. Range: -80 to -90 dBm. Default: -85 dBm.
Roaming Hysteresis	Enter a value to indicate how strong the signal strength of a neighboring access point must be in order for the client to roam to it. This field is intended to reduce the amount of “ping ponging” between access points if the client is physically located on or near the border between two access points. Range: 2 to 4 dB. Default: 2 dB.

Table 31-35 Controller > 802.11b or g or n > Roaming Parameters (continued)

Field	Description
Adaptive Scan Threshold	Enter the RSSI value, from a client associated access point, below which the client must be able to roam to a neighboring access point within the specified transition time. This field also provides a power-save method to minimize the time that the client spends in active or passive scanning. For example, the client can scan slowly when the RSSI is above the threshold and scan more rapidly when below the threshold. Range: -70 to -77 dB. Default: -72 dB
Transition Time	Enter the maximum time allowed for the client to detect a suitable neighboring access point to roam to and to complete the roam, whenever the RSSI from the client associated access point is below the scan threshold. Range: 1 to 10 seconds. Default: 5 seconds.

Controller > 802.11b or g or n > CleanAir

Table 31-36 describes the fields on the following page: **Design > Configuration Templates > Features and Technologies > Controller > 802.11b or g or n > CleanAir**

Table 31-36 Controller > 802.11b or g or n > CleanAir

Field	Description
CleanAir	Select the check box to enable CleanAir functionality on the 802.11 b/g/n network, or unselect to prevent the controller from detecting spectrum interference. The default value is selected. If CleanAir is enabled, the Reporting Configuration and Alarm Configuration group boxes appear.
Report Interferers	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 system appear in the Interferences to Detect box and any that do not need to be detected appear in the Interferers to Ignore box. Use the > and < buttons to move interference sources between these two boxes. By default, all interference sources are ignored.
Air Quality Alarm	Select the Air Quality Alarm check box to enable the triggering of air quality alarms, or unselect the box to disable this feature.
Air Quality Alarm Threshold	If you selected the Air Quality Alarm check box, enter a value between 1 and 100 (inclusive) in the Air Quality Alarm Threshold text box to specify the threshold at which you want the air quality alarm to be triggered. When the air quality falls below the threshold level, the alarm is triggered. A value of 1 represents the worst air quality, and 100 represents the best. The default value is 1.
Interferers For Security Alarm	Select the Interferers For Security Alarm check box to trigger interferer alarms when the controller detects specified device types, or unselected it to disable this feature. The default value is unselected. Make sure that any sources of interference that need to trigger interferer alarms appear in the Interferers Selected for Security Alarms box and any that do not need to trigger interferer alarms appear in the Interferers Ignored for Security Alarms box. Use the > and < buttons to move interference sources between these two boxes. By default, all interferer sources for security alarms are ignored.

Controller > dot11b-RRM > Thresholds

Table 31-37 describes the fields on the following page: **Design > Configuration Templates > Features and Technologies > Controller > dot11b-RRM > Thresholds.**

Table 31-37 Controller > dot11b-RRM > Thresholds

Field	Description
Min. Failed Clients (#)	Enter the minimum number of failed clients currently associated with the controller.
Coverage Level	Enter the target range of coverage threshold (dB).
Signal Strength	When the Coverage Level field is adjusted, the value of the Signal Strength (dBm) automatically reflects this change. The Signal Strength field provides information regarding what the signal strength is when adjusting the coverage level.
Data RSSI	Enter the Data RSSI (-60 to -90 dBm). This number indicates the value for the minimum Received Signal Strength Indicator (RSSI) for data required for the client to associate to an access point.
Voice RSSI	Enter the Voice RSSI (-60 to -90 dBm). This number indicates the value for the minimum Received Signal Strength Indicator (RSSI) required for voice for the client to associate to an access point.
Max. Clients	Enter the maximum number of clients able to be associated with the controller.
RF Utilization	Enter the percentage of threshold for this radio type.
Interference Threshold	Enter an interference threshold between 0 and 100 percent.
Noise Threshold	Enter a noise threshold between -127 and 0 dBm. When outside of this threshold, the controller sends an alarm to Prime Infrastructure.
Coverage Exception Level	Enter the coverage exception level percentage. When the coverage drops by this percentage from the configured coverage for the minimum number of clients, a coverage hole is generated.

Controller > dot11b-RRM > TPC

Table 31-38 describes the fields on the following page: **Design > Configuration Templates > Features and Technologies > Controller > dot11b-RRM > TPC**

Table 31-38 Controller > dot11b-RRM > TPC

Field	Description
TPC Version	Choose TPCv1 or TPCv2 from the drop-down list. The TPCv2 option is applicable only for controller Version 7.2.x or later.
Dynamic Assignment	From the Dynamic Assignment drop-down list, choose one of three modes: Automatic—The transmit power is periodically updated for all access points that permit this operation. On Demand—Transmit power is updated when you click Assign Now. Disabled—No dynamic transmit power assignments occur, and values are set to their global default.
Maximum Power Assignment	Indicates the maximum power assigned. Range: -10 to 30 dB. Default: 30 dB.
Minimum Power Assignment	Indicates the minimum power assigned. Range: -10 to 30 dB. Default: 30 dB.
Dynamic Tx Power Control	Click the check box if you want to enable Dynamic Transmission Power Control.
Transmitted Power Threshold	Enter a transmitted power threshold between -50 and -80.
Control Interval	Shows the transmitted power control interval in seconds (read-only).

Controller > dot11b-RRM > DCA

Table 31-39 describes the fields on the following page: **Design > Configuration Templates > Features and Technologies > Controller > dot11b-RRM > DCA**.

Table 31-39 Controller > dot11b-RRM > DCA

Field	Description
Assignment Mode	From the Dynamic Assignment drop-down list, choose one of three modes: Automatic—The transmit power is periodically updated for all access points that permit this operation.On Demand—Transmit power is updated when you click Assign Now.Disabled—No dynamic transmit power assignments occur, and values are set to their global default.
Avoid Foreign AP Interference	Enable this field to have RRM consider interference from foreign Cisco access points (those non-Cisco access points outside RF/mobility domain) when assigning channels. This foreign 802.11 interference. Unselect this check box to have RRM ignore this interference. In certain circumstances with significant interference energy (dB) and load (utilization) from foreign access points, RRM might adjust the channel assignment to avoid these channels (and sometimes adjacent channels) in access points close to the foreign access points. This increases capacity and reduces variability for the Cisco WLAN Solution.
Avoid Cisco AP Load	Enable this bandwidth-sensing field to have controllers consider the traffic bandwidth used by each access point when assigning channels to access points. Unselect this check box to have RRM ignore this value. In certain circumstances and with denser deployments, there might not be enough channels to properly create perfect channel reuse. In these circumstances, RRM can assign better re-use patterns to those access points that carry more traffic load.
Avoid non 802.11 Noise	Enable this noise-monitoring field to have access points avoid channels that have interference from non-access point sources, such as microwave ovens or Bluetooth devices. Unselect this check box to have RRM ignore this interference. In certain circumstances with significant interference energy (dB) from non-802.11 noise sources, RRM might adjust the channel assignment to avoid these channels (and sometimes adjacent channels) in access points close to the noise sources. This increases capacity and reduces variability for the Cisco WLAN Solution.
Signal Strength Contribution	The Signal Strength Contribution check box is always enabled (not configurable). constantly monitors the relative location of all access points within the RF/mobility domain to ensure near-optimal channel re-use. The net effect is an increase in Cisco WLAN Solution capacity and a reduction in co-channel and adjacent channel interference.
Event Driven RRM	Select the checkbox to disable spectrum event-driven RRM. By default, Event Driven RRM is enabled. Event Driven RRM is used when a CleanAir-enabled access point detects a significant level of interference
Sensitivity Threshold	If Event Driven RRM is enabled, this field displays the threshold level at which event-driven RRM is triggered. It can have a value of either Low, Medium, or High. When the interference for the access point rises above the threshold level, RRM initiates a local Dynamic Channel Assignment (DCA) run and changes the channel of the affected access point radio if possible to improve network performance. Low represents a decreased sensitivity to changes in the environment while High represents an increased sensitivity.

Controller > Management > Trap Control

Table 31-40 describes the fields on the following page: **Design > Configuration Templates > Features and Technologies > Controller > Management > Trap Control**.

Table 31-40 Controller > Management > Trap Control

Field	Description
Select All Traps	Select this check box to enable all of the traps on this page.
SNMP Authentication	The SNMPv2 entity has received a protocol message that is not properly authenticated. When a user who is configured in SNMP V3 mode tries to access the controller with an incorrect password, the authentication fails and a failure message is displayed. However, no trap logs are generated for the authentication failure.
Link (Port) Up/Down	Link changes states from up or down.
Multiple Users	Two users log in with the same login ID.
Spanning Tree	Spanning Tree traps. See the STP specification for descriptions of individual parameters.
Rogue AP	Whenever a rogue access point is detected or when a rogue access point was detected earlier and no longer exists, this trap is sent with its MAC address.
Controller Config Save	Notification sent when the configuration is modified.
802.11 Association	A trap is sent when a client is associated to a WLAN. This trap does not guarantee that the client is authenticated.
802.11 Disassociation	The disassociate notification is sent when the client sends a disassociation frame.
802.11 Deauthentication	The deauthenticate notification is sent when the client sends a deauthentication frame.
802.11 Failed Authentication	The authenticate failure notification is sent when the client sends an authentication frame with a status code other than successful.
802.11 Failed Association	The associate failure notification is sent when the client sends an association frame with a status code other than successful.
Excluded	The associate failure notification is sent when a client is excluded.
AP Register	Notification sent when an access point associates or disassociates with the controller.
AP Interface Up/Down	Notification sent when access point interface (802.11a/n or 802.11b/g/n) status goes up or down.
Load Profile	Notification sent when Load Profile state changes between PASS and FAIL.
Noise Profile	Notification sent when Noise Profile state changes between PASS and FAIL.
Interference Profile	Notification sent when Interference Profile state changes between PASS and FAIL.
Coverage Profile	Notification sent when Coverage Profile state changes between PASS and FAIL.
Channel Update	Notification sent when the dynamic channel algorithm of an access point is updated.
Tx Power Update	Notification sent when the dynamic transmit power algorithm of an access point is updated.
User Auth Failure	This trap is to inform you that a client RADIUS authentication failure has occurred.
RADIUS Server No Response	This trap is to indicate that no RADIUS server(s) are responding to authentication requests sent by the RADIUS client.
ESP Authentication Failure	IPsec packets with invalid hashes were found in an inbound ESP SA.
ESP Replay Failure	IPsec packets with invalid sequence numbers were found in an inbound ESP SA.

Table 31-40 Controller > Management > Trap Control (continued)

Field	Description
Invalid SPI	A packet with an unknown SPI was detected from the specified peer with the specified SPI using the specified protocol.
IKE Negotiation Failure	An attempt to negotiate a phase 1 IKE SA failed. The notification counts are also sent as part of the trap, along with the current value of the total negotiation error counters.
IKE Suite Failure	An attempt to negotiate a phase 2 SA suite for the specified selector failed. The current total failure counts are passed as well as the notification type counts for the notify involved in the failure.
Invalid Cookie	ISAKMP packets with invalid cookies were detected from the specified source, intended for the specified destination. The initiator and responder cookies are also sent with the trap.
WEP Decrypt Error	Notification sent when the controller detects a WEP decrypting error.
Signature Attack	Select the check box to enable the 802.11 security trap.

Controller > Management > Telnet SSH

Table 31-41 describes the fields on the following page: **Design > Configuration Templates > Features and Technologies > Controller > Management > Telnet SSH**.

Table 31-41 Controller > Management > Telnet SSH

Field	Description
Session Timeout	Enter the number of minutes a Telnet session is allowed to remain inactive before being logged off. A zero means there is no timeout. The valid range is 0 to 160, and the default is 5.
Maximum Sessions	Enter the number of simultaneous Telnet sessions allowed. The valid range is 0 to 5, and the default is 5. New Telnet sessions can be allowed or disallowed on the DS (network) port. New Telnet sessions are always allowed on the service port.
Allow New Telnet Session	Select Yes to allow new Telnet sessions on the DS port, No to disallow them. New Telnet sessions can be allowed or disallowed on the DS (network) port. New Telnet sessions are always allowed on the service port. The default is Yes.
Allow New SSH Session	Select Yes to allow Secure Shell Telnet sessions, No to disallow them. The default is Yes.

Controller > Location > Location Configuration

The following tables describe the fields on the **Design > Configuration Templates > Features and Technologies > Controller > 802.11b or g or n > Media Parameters** page:

- Table 31-32—General tab
- Table 31-33—Advanced tab

Controller > Location > Location Configuration > General

Table 31-42 describes the fields on the following page: **Design > Configuration Templates > Features and Technologies > Controller > Location > Location Configuration > General**.

Table 31-42 Controller > Location > Location Configuration > General

Field	Description
RFID Tag Data Collection	Select the check box to enable tag collection. Before the mobility services engine can collect asset tag data from controllers, you must enable the detection of active RFID tags using the CLI command config rfid status enable on the controllers.
Calibrating Client	Select the check box to enable calibration for the client. Controllers send regular S36 or S60 requests (depending on the client capability) by way of the access point to calibrating clients. Packets are transmitted on all channels. All access points irrespective of channel (and without a channel change) gather RSSI data from the client at each location. These additional transmissions and channel changes might degrade contemporaneous voice or video traffic. To use all radios (802.11a/b/g/n) available, you must enable multiband in the Advanced tab.
Normal Client	Select the check box to have a non-calibrating client. No S36 requests are transmitted to the client. S36 and S60 are client drivers compatible with specific Cisco Compatible Extensions. S36 is compatible with CCXv2 or later. S60 is compatible with CCXv4 or later. For details, see the Cisco Context Aware and Location FAQ.
Tags, Clients and Rogue APs/Clients	Specify how many seconds should elapse before notification of the found tag, client, rogue AP, or rogue client.
For Clients	Enter the number of seconds after which RSSI measurements for clients should be discarded.
For Calibrating Clients	Enter the number of seconds after which RSSI measurements for calibrating clients should be discarded.
For Tags	Enter the number of seconds after which RSSI measurements for tags should be discarded.
For Rogue APs	Enter the number of seconds after which RSSI measurement for rogue access points should be discarded.

Related Topics

- Table 31-33—Advanced tab

Controller > Location > Location Configuration > Advanced

Table 31-43 describes the fields on the following page: **Design > Configuration Templates > Features and Technologies > Controller > Location > Location Configuration > Advanced**.

Table 31-43 Controller > Location > Location Configuration > Advanced

Field	Description
RFID Tag Data Timeout	Enter a value in seconds to set the RFID tag data timeout.
Calibrating Client Multiband	Select the check box to send S36 and S60 packets (where applicable) on all channels. Calibrating clients must be enabled on the General tab

Related Topics

- Table 31-32—General tab

Controller > PMIP > Global Config

Table 31-44 describes the fields on the following page: **Design > Configuration Templates > Features and Technologies > Controller > PMIP > Global Config**.

Table 31-44 Controller > PMIP > Global Config

Field	Description
Domain Name	The name of the domain.
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 seconds.
Binding Maximum Retry Timeout	Maximum 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 32000 seconds.
Replay Protection Timestamp	Maximum amount of time difference between the timestamp in the received proxy binding acknowledgment and the current time of the day. The valid range is between 1 to 255 milliseconds. The default value is 7 milliseconds.
Minimum BRI Retransmit Timeout	Minimum amount of time that the controller waits before retransmitting the BRI message. The valid range is between 500 to 65535 seconds.
Maximum BRI Retransmit Timeout	Maximum amount of time that the controller waits before retransmitting the Binding Revocation Indication (BRI) message. The valid range is between 500 to 65535 seconds. The default value is 2000 seconds.
BRI Retries	Maximum number of times that the controller retransmits the BRI message before receiving the Binding Revocation Acknowledgment (BRA) message. The valid range is between 1 to 10. The default value is 1.

Security Templates Field Descriptions

The following sections contain field descriptions for pages found in **Design > Configuration Templates > Features and Technologies > Security**.

- Security > DMVPN
- Security > GETVPN-GroupMember
- Security > GETVPN-KeyServer
- Security > ScanSafe

Security > DMVPN

Table 31-45 describes the fields on the following page: **Design > Configuration Templates> Features and Technologies > Security > DMVPN**.

Table 31-45 Security > DMVPN

Field	Description
Element	**Field Description**
Template Basic tab	
Name	Enter a name for the DMVPN template.
Description	(Optional) Enter a description for the DMVPN template.
Validation Criteria tab	
Device Type	Choose the device type from the drop-down list.
OS Version	Enter the OS version for the device.
IPsec Information	
Authentication Type	Click the Preshared Keys or Digital Certificates radio button. • Preshared Keys—Allow for a secret key to be shared between two peers and to be used by IKE during the authentication phase. • Digital Certificates—Authentication method in which RSA key pairs are used to sign and encrypt IKE key management messages. Certificates provide nonrepudiation of communication between two peers, meaning that it can be proven that the communication actually took place.
Priority	The priority value of the IKE proposal. The priority value determines the order of the IKE proposals compared by the two negotiating peers when attempting to find a common security association (SA). If the remote IPsec peer does not support the parameters selected in your first priority policy, the device tries to use the parameters defined in the policy with the next lowest priority number. Valid values range from 1 to 10000. The lower the number, the higher the priority. If you leave this field blank, Security Manager assigns the lowest unassigned value starting with 1, followed by 5, and continuing in increments of 5.
Authenticate	Choose the authentication type from the drop-down list.
Diffie-Hellman Group	The Diffie-Hellman group to use for deriving a shared secret between the two IPsec peers without transmitting it to each other. A larger modulus provides higher security but requires more processing time. The two peers must have a matching modulus group. Options are: 1—Diffie-Hellman Group 1 (768-bit modulus). 2—Diffie-Hellman Group 2 (1024-bit modulus). 5—Diffie-Hellman Group 5 (1536-bit modulus, considered good protection for 128-bit keys, but group 14 is better). If you are using AES encryption, use this group (or higher). The ASA supports this group as the highest group.

Table 31-45 Security > DMVPN (continued)

Field	Description
Encryption policy	Choose the encryption policy from the drop-down list. Choose the encryption algorithm from the drop-down list. The encryption algorithm used to establish the Phase 1 SA for protecting phase 2 negotiations: AES-128—Encrypts according to the Advanced Encryption Standard using 128-bit keys. AES-192—Encrypts according to the Advanced Encryption Standard using 192-bit keys. AES-256—Encrypts according to the Advanced Encryption Standard using 256-bit keys. DES—Encrypts according to the Data Encryption Standard using 56-bit keys. 3DES—Encrypts three times using 56-bit keys. 3DES is more secure than DES, but requires more processing for encryption and decryption. It is less secure than AES. A 3DES license is required to use this option.
Hash	The hash algorithm used in the IKE proposal. The hash algorithm creates a message digest, which is used to ensure message integrity. Options are: • SHA (Secure Hash Algorithm)—Produces a 160-bit digest. SHA is more resistant to brute-force attacks than MD5. • MD5 (Message Digest 5)—Produces a 128-bit digest. MD5 uses less processing time than SHA.
Lifetime	The lifetime of the SA, in seconds. When the lifetime is exceeded, the SA expires and must be renegotiated between the two peers. As a general rule, the shorter the lifetime (up to a point), the more secure your IKE negotiations will be. However, with longer lifetimes, future IPsec security associations can be set up more quickly than with shorter lifetimes. You can specify a value from 60 to 2147483647 seconds. The default is 86400.
Transform Set	
Name	Enter the transform set name. The transform set encrypts the traffic on the tunnel.
ESP Encryption Algorithm	The algorithm used to encrypt the payload. Choose the encryption algorithm from the drop-down list. The options are: • ESP with the 128-bit Advanced Encryption Standard (AES) encryption algorithm. • ESP with the 192-bit AES encryption algorithm. • ESP with the 256-bit AES encryption algorithm. • ESP with the 168-bit DES encryption algorithm (3DES or Triple DES). • Null encryption algorithm.
ESP Integrity Algorithm	The algorithm used to check the integrity of the payload. Choose the integrity algorithm from the drop-down list. The options are: • ESP with the MD5 (HMAC variant) authentication algorithm. • ESP with the SHA (HMAC variant) authentication algorithm.
AH Integrity	Choose the AH integrity from the drop-down list. The options are: • AH with the MD5 (Message Digest 5) (a Hash-based Message Authentication Code [HMAC] variant) authentication algorithm. • AH with the SHA (Secure Hash Algorithm) (an HMAC variant) authentication algorithm.

Table 31-45 Security > DMVPN (continued)

Field	Description
Compression	Enable the IP compression to compress payload. IP compression with the Lempel-Ziv-Stac (LZS) algorithm.
Mode	Choose the mode to transport the traffic.
Device Role and Topology	
Spoke radio button	Check the Spoke radio button to configure the router as a Spoke in the topology.
Hub radio button	Check the Hub radio button to configure the router as a Hub in the topology.
Dynamic Connection between Spokes	Check the Create Dynamic Connection between spokes check box to configure the dynamic connection between spokes.
EIGRP	Choose the routing information.
RIPV2	Choose the routing information.
Other	Check the **Other** check box to select other routing protocol.
NHRP and Tunnel Parameters	
Network ID	Enter the NHRP Network ID.The network ID is a globally unique, 32-bit network identifier from a nonbroadcast multiaccess (NBMA) network. The range is from 1 to 4294967295.
Hold Time	Enter the number of seconds that the Next Hop Resolution Protocol (NHRP) NBMA addresses should be advertised as valid. The default value is 7200 seconds.
Tunnel Key	Enter the tunnel key. The tunnel key is used to enable a key ID for a particular tunnel interface. The range is from 0 to 4294967295.
NHRP Authentication String	Enter the Authentication String.
IP MTU	Enter the MTU size of IP packets that are sent on a particular interface. The default value for Ethernet and the serial interface is 1500. The default value varies depending upon the media type.
TCP Maximum Segment Size	Enter the TCP maximum segment size. The range is from 500 to 1460.
Physical Interface	Enter the physical interface.
NHS Fallback Time	(Optional) Enter the NHS fallback time in seconds. The range is from 0 to 60.
NHS Server	
Cluster ID	Enter the cluster value to form a group having one or more hubs. The range is from 0 to 10.
Max Connections	Enter the maximum number of connections that can be active in a particular group/cluster.
Priority	The priority of the particular hub in a cluster. Depends on the priority of the spoke router that will form a tunnel with the hub devices.
Next Hop server	Enter the IP address of the next-hop server.
Hub's Physical IP Address	Enter the IP address of the hub's physical interface.

Security > GETVPN-GroupMember

Table 31-46 describes the fields on the following page: **Design > Configuration Templates> Features and Technologies > Security > GETVPN-GroupMember**.

Table 31-46 Security > GETVPN-GroupMember

Field	Description
Group ID	Enter the Group ID. The Group ID is a unique identity for the GETVPN group member. This can be a number or an IP address.
Group Name	Enter the Group Name for the GETVPN group member.
IKE Authentication Policy	Use this anchored field and its associated popup to specify authentication type and policies for this GETVPN group member.
Pre-Shared Key	Select this radio button o select Pre-Shared Key as the IKE authentication type. If you select this, you must provide the key in the Pre-Shared Key field immediately below the button.
Confirm Secret Key	Enter the pre-shared key again to confirm it. This field is displayed only when you select Pre-Shared Key as the authentication type.
Digital Certificate	Select this radio button o select Digital Certificate as the IKE authentication type. If you choose this authentication type, the router must have a digital certificate issued by a Certificate Authority to authenticate itself.
IKE Policies	Use this edit table to create a set of IKE policies for this GETVPN group member.
Priority	Set the authentication policy's negotiation priority by entering a value from 1 to 10000, with 1 as the highest priority. The priority value determines the order of the IKE proposals compared by the two negotiating peers when attempting to find a common security association (SA). If the remote IPsec peer does not support the parameters selected in your first priority policy, the device tries to use the parameters defined in the policy with the next lowest priority number.
Authentication	Select the authentication policy's authentication type from the list.
D-H Group	Select the authentication policy's Diffie-Hellman group from the list.
Encryption	Select the authentication policy's encryption type from the list.
Hash	Select the authentication policy's hash type from the list
IKE Lifetime	Enter the security association (SA) lifetime in seconds. When the lifetime is exceeded, the SA expires and must be renegotiated between the two peers. As a general rule, the shorter the lifetime (up to a point), the more secure your IKE negotiations will be.
WAN Interface	Enter the registration WAN Interface for the GETVPN group member.
Local Exception Policy ACL	Enter the Local Exception Policy ACL specifying the traffic that the GETVPN group member must send in clear text.
Fail Close ACL	Enter the Fail Close ACL specifying the traffic that must be allowed when GETVPN encryption fails. If the Fail Close ACL feature is configured, all the traffic passing through the group member will be dropped until the group member is registered successfully. Once the group member registers successfully and SAs are downloaded, this feature turns off by itself.
Primary Key Server	Enter the IP address or host name of the primary encryption key server. The primary key server is responsible for creating and distributing group policies to all group members and periodically synchronizing with the secondary key servers.
Secondary Key Servers	Use this edit table to specify the set of secondary key servers. Enter them in order of priority, with the highest priority at the top of the edit table. During periods when the primary key server is down or inaccessible, the accessible secondary key server with the highest priority is elected to serve as the primary key server.
Enable Passive SA	Check the Enable Passive SA check box to enable Passive SA mode on this group member

Security > GETVPN-KeyServer

Table 31-47 describes the fields on the following page: **Design > Configuration Templates> Features and Technologies > Security > GETVPN-KeyServer**.

Table 31-47 Security > GETVPN-KeyServer

Field	Description
Template Detail	
Group Name	Enter the group name for the GETVPN group member template.
Group ID	Enter a unique identity for the GETVPN group member. This can be a number or an IP address. The range is from 0 to 2147483647.
IKE Authentication Policy	
Authorization Type	Click the Preshared Keys or Digital Certificates radio button: • Preshared Keys—Preshared keys allow for a secret key to be shared between two peers and to be used by IKE during the authentication phase. • Digital Certificates—An authentication method in which RSA key pairs are used to sign and encrypt IKE key management messages. Certificates provide nonrepudiation of communication between two peers, meaning that it can be proven that the communication actually took place.
Priority	The priority value of the IKE proposal. The priority value determines the order of the IKE proposals compared by the two negotiating peers when attempting to find a common SA. If the remote IPsec peer does not support the parameters selected in your first priority policy, the device tries to use the parameters defined in the policy with the next lowest priority number. Valid values range from 1 to 10000. The lower the number, the higher the priority.
Encryption	Choose the encryption algorithm from the drop-down box.The encryption algorithm is used to establish the Phase 1 SA for protecting Phase 2 negotiations: • AES-128—Encrypts according to the Advanced Encryption Standard using 128-bit keys. • AES-192—Encrypts according to the Advanced Encryption Standard using 192-bit keys. • AES-256—Encrypts according to the Advanced Encryption Standard using 256-bit keys. • DES—Encrypts according to the Data Encryption Standard using 56-bit keys. • 3DES—Encrypts three times using 56-bit keys. 3DES is more secure than DES, but requires more processing for encryption and decryption. It is less secure than AES. A 3DES license is required to use this option.
Hash	The hash algorithm used in the IKE proposal. The hash algorithm creates a message digest, which is used to ensure message integrity. Options are: • SHA (Secure Hash Algorithm)—Produces a 160-bit digest. SHA is more resistant to brute-force attacks than MD5. • MD5 (Message Digest 5)—Produces a 128-bit digest. MD5 uses less processing time than SHA.

Table 31-47 Security > GETVPN-KeyServer (continued)

Field	Description
Diffie-Hellman Group	The Diffie-Hellman group to use for deriving a shared secret between the two IPsec peers without transmitting it to each other. A larger modulus provides higher security but requires more processing time. The two peers must have a matching modulus group. Options are: • 1—Diffie-Hellman Group 1 (768-bit modulus). • 2—Diffie-Hellman Group 2 (1024-bit modulus). • 5—Diffie-Hellman Group 5 (1536-bit modulus, considered good protection for 128-bit keys, but group 14 is better). If you are using AES encryption, use this group (or higher). The ASA supports this group as the highest group.
Lifetime	The lifetime of the SA, in seconds. When the lifetime is exceeded, the SA expires and must be renegotiated between the two peers. As a general rule, the shorter the lifetime (up to a point), the more secure your IKE negotiations will be. However, with longer lifetimes, future IPsec security associations can be set up more quickly than with shorter lifetimes. You can specify a value from 60 to 2147483647 seconds. The default is 86400.
Registration Interface	Enter the interface to which the crypto map needs to be associated.
Traffic Details	
Local Exception ACL	Choose an ACL for the traffic that must be excluded from the encryption.
Fail Close ACL	Choose an ACL for the traffic that must be sent in clear text until the group member registers with the key server. If the Fail Close feature is configured, all the traffic passing through the group member will be dropped until the group member is registered successfully. Once the group member registers successfully and SAs are downloaded, this feature turns off by itself.
Key Server Information	
Primary Key Server	Specify the primary key server IP address to which the client connects. The primary key server is responsible for creating and distributing group policies to all group members and periodically synchronizing with the secondary key servers. The server with the highest priority is elected as a primary key server.
Secondary Key Server	Specify the secondary key server IP address to which the group member falls back when the primary key server registration fails. A group member can be configured to register to any available key server from a list of all secondary key servers. Group member configuration determines the registration order. The key server defined first is contacted first, followed by the second defined key server, and so on. You can have a maximum of eight key servers for a group member.
Migration	
Enable Passive SA	The Passive SA mode overrides the receive-only SA option on the key server and encrypts all outbound traffic. Use this option to turn on the Passive SA mode on the group member.
Group Name	Enter the group name for the GETVPN group member template.

Security > ScanSafe

Table 31-48 describes the fields on the following page: **Design > Configuration Templates > Features and Technologies > Security > ScanSafe**.

Table 31-48 Security > ScanSafe

Field	Description
Primary Server	Enter the IPv4 address or host name of the primary ScanSafe server.
HTTP Port	Specify the HTTP port to redirect the HTTP requests to the primary server. By default, the ScanSafe uses port 80 for the HTTP traffic. However, you can choose to use different ports for each request type.
HTTPS Port	Specify the HTTPs port to redirect the HTTPS requests to the primary server. By default, the ScanSafe uses the port 443 for HTTPs traffic. However, you can choose to use different ports for each request type.
Secondary Server	Enter the IPv4 address or host name of the secondary ScanSafe server.
HTTP Port (secondary)	Specify the HTTP port to which to redirect the HTTP requests to the secondary server. By default, ScanSafe uses port 80 for HTTP traffic.
HTTPS Port	Specify the HTTPs port to which to redirect the HTTPS requests to the secondary server. By default, ScanSafe uses port 443 for HTTPs traffic.
ScanSafe License	Specify the license key that the ISR sends to the ScanSafe proxy servers to indicate the organization from which the request originated. The license is a 16-byte hexadecimal key.
Server Timeout	Specify the primary ScanSafe server timeout in seconds. The ISR waits for the specified timeout period before polling the ScanSafe proxy server to check its availability.
Session Timeout	Specify the primary ScanSafe session idle timeout in seconds. If the primary server fails, the ISR will use the secondary server as the active ScanSafe proxy server. The ISR automatically falls back to the primary server as long as it is active for three consecutive timeout periods.
Source Interface	Specify the source IPv4 address or interface name on which ScanSafe Web Security is enabled.
Router behavior when ScanSafe server fail to respond	Specify how the ISR router should handle the incoming traffic when it cannot reach the configured ScanSafe proxy servers: Drop all traffic or Allow all traffic. Drop all traffic is the default.
Global User	Enter a Global User when the web authentication (webauth) is not configured under the router's Ingress Interface.
Global User Group	Enter a Global User Group when the web authentication (webauth) is not configured on the router's Egress Interfaces.
User Group Inclusion & Exclusion Info	Use the two edit tables to specify the user group information to be included or excluded during exchanges with the ScanSafe tower. This is used only when web authentication (webauth) is configured on the router's Ingress and Egress interfaces
Notify Whitelist Info to ScanSafe Tower	Select this option to sending the Whitelist information to the ScanSafe Tower and specify the Safe URL, Safe User Agent, and Safe ACL information to be sent.

Wireless Configuration Templates Field Descriptions

The following sections contain field descriptions for pages found in **Design > Wireless Configuration**.

- Lightweight AP Configuration Templates
- Autonomous AP Migration Templates

Lightweight AP Configuration Templates

The following tables describe the fields on the **Design > Wireless Configuration > Lightweight AP Configuration Templates** page:

- Table 31-49—AP Parameters Tab
- Table 31-50—Mesh Tab
- Table 31-51—802.11a/n Tab
- Table 31-52—802.11a SubBand Tab
- Table 31-53—802.11b/g/n Tab
- Table 31-54—CDP Tab
- Table 31-55—FlexConnect Tab
- Table 31-56—Select APs Tab
- Table 31-57—Apply/Schedule
- Table 31-58—Report Tab

Lightweight AP Configuration Templates> AP Parameters

Table 31-49 describes the fields on the following page: **Design > Wireless Configuration > Lightweight AP Configuration Templates > AP Parameters**.

Table 31-49 Lightweight AP Configuration Templates> AP Parameters

Field	Description
Admin Status	Select the **Admin and Enabled** check box to enable administrative status. To conserve energy, access points can be turned off at specified times during non-working hours. Select the **Enabled** check box to allow access points to be turned on or off.

Table 31-49 Lightweight AP Configuration Templates> AP Parameters (continued)

Field	Description
AP Mode	From the drop-down list, choose one of the following: • **Local**—Default • **Monitor**—Monitor mode only. Choose **Monitor** to enable this access point template for Cisco Adaptive wIPS. Once Monitor is selected, select the **Enhanced WIPS Engine** check box and the Enabled check box. Then select the **AP Monitor Mode Optimization** check box and choose WIPS from the AP Monitor Mode Optimization drop-down list. • FlexConnect—Cisco 1030 remote edge lightweight access point (REAP) used for Cisco 1030 IEEE 802.11a/b/g/n remote edge lightweight access points. FlexConnect must be selected to configure an OfficeExtend access point. When the AP mode is FlexConnect, FlexConnect configuration options display including the option to enable OfficeExtend AP and to enable Least Latency Controller Join. • Rogue Detector—Monitors the rogue access points but does not transmit or contain rogue access points. • Bridge • Sniffer—The access point "sniffs" the air on a given channel. It captures and forwards all the packets from the client on that channel to a remote machine that runs airopeek (a packet analyzer for IEEE 802.11 wireless LANs). It includes information on timestamp, signal strength, packet size, and so on. If you choose Sniffer as an operation mode, you are required to enter a channel and server IP address on the AP/Radio Templates 802.11b/g/n or 802.11a/n parameters tab. The sniffer feature can be enabled only if you are running AiroPeek, which is a third-party network analyzer software that supports decoding of data packets. For more information on AiroPeek, see http://www.wildpackets.com. • SE-Connect—This mode allows a CleanAir-enabled access point to be used extensively for interference detection on all monitored channels. All other functions such as IDS scanning and Wi-Fi are suspended. This option is displayed only if the access point is CleanAir-capable. Changing the AP mode reboots the access point.
Enhanced wIPS Engine	Select the **Enhanced wIPS engine** and the **Enabled** check box to enable.
AP Sub Mode	Choose an option from the drop-down list.
Country Code	Select the appropriate country code from the drop-down list. **Note** Changing the country code might cause the access point to reboot.
AP Failover Priority	Choose **Low**, **Medium**, **High**, or **Critical** from the drop-down list to indicate the access point failover priority. The default priority is low.
Power Injector State	When enabled, this allows you to manipulate power injector settings through NCS without having to go directly to the controllers. If the Enable Power Injector State is selected, power injector options appear.
Primary, Secondary, and Tertiary Controller IP	The Primary/Secondary/Tertiary Controller IP is the Management IP of the controller.

Table 31-49 Lightweight AP Configuration Templates> AP Parameters (continued)

Field	Description
Domain Name Server IP Address	Domain Name Server IP and Domain Name can be configured only on access points which have static IPs.
Encryption	Enabling or disabling encryption functionality causes the access point to reboot which then causes a loss of connectivity for clients. DTLS data encryption is enabled automatically for OfficeExtend access points to maintain security. Encryption is only available if the access point is connected to a 5500 series controller with a Plus license. Encryption is not available for all access point models. Enabling encryption might impair performance.
Rogue Detection	Rogue detection is disabled automatically for OfficeExtend access points because these access points, which are deployed in a home environment, are likely to detect a large number of rogue devices. For more information regarding OfficeExtend access points, see *Cisco Wireless LAN Controller Configuration Guide*.
Telnet Access	An OfficeExtend access point might be connected directly to the WAN which could allow external access if the default password is used by the access point. Because of this, Telnet and SSH access are disabled automatically for OfficeExtend access points.
Link Latency	You can configure link latency on the controller to measure the link between an access point and the controller. This feature can be used with all access points joined to the controller but is especially useful for FlexConnect access points, for which the link could be a slow or unreliable WAN connection. **Note** Link latency is supported for use only with FlexConnect access points in connected mode. FlexConnect access points in standalone mode are not supported.
Reboot AP	Select the check box to enable a reboot of the access point after making any other updates.
AP Failover Priority	Choose **Low**, **Medium**, **High**, or **Critical** from the drop-down list to indicate the access point failover priority. The default priority is low.
Controllers	Select the **Controllers** check box to enable the drop-down lists for the primary, secondary, and tertiary controller names.
Override Global Username Password	Select the check box to enable an override for the global username/password. Enter and confirm the new access point username and password in the appropriate text boxes.
Override Supplicant Credentials	Select the Override Supplicant Credentials check box to prevent this access point from inheriting the authentication username and password from the controller. The default value is unselected. The Override Supplicant Credentials option is supported in controller Version 6.0 and later. • In the Username, Password, and Confirm Password text boxes, enter the unique username and password that you want to assign to this access point. **Note** The information that you enter is retained across controller and access point reboots and whenever the access point joins a new controller.

Lightweight AP Configuration Templates> Mesh

Table 31-50 describes the fields on the **Design > Wireless Configuration > Lightweight AP Configuration Templates > Mesh** page.

Table 31-50 Lightweight AP Configuration Templates > Mesh

Field	Description
Bridge Group Name	Enter a bridge group name (up to 10 characters) in the text box. Bridge groups are used to logically group the mesh access points to avoid two networks on the same channel from communicating with each other. For mesh access points to communicate, they must have the same bridge group name. For configurations with multiple RAPs, make sure that all RAPs have the same bridge group name to allow failover from one RAP to another.
Data Rate (Mbps)	Choose the data rate for the backhaul interface from the drop-down list. Data rates available are dictated by the backhaul interface. The default rate is 18 Mbps. This data rate is shared between the mesh access points and is fixed for the whole mesh network. Do not change the data rate for a deployed mesh networking solution.
Ethernet Bridging	Select the **Enable** check box. From the Ethernet Bridging drop-down list, enable Ethernet bridging for the mesh access point.
Role	Choose the role of the mesh access point from the drop-down list (**MAP** or **RAP**). The default setting is MAP

Related Topics

- Lightweight AP Configuration Templates> AP Parameters
- Lightweight AP Configuration Templates> 802.11a/n
- Lightweight AP Configuration Templates > 802.11a SubBand
- Lightweight AP Configuration Templates > 802.11b/g/n
- Lightweight AP Configuration Templates > CDP
- Lightweight AP Configuration Templates >FlexConnect
- Lightweight AP Configuration Templates > Select APs
- Lightweight AP Configuration Templates > Report

Lightweight AP Configuration Templates> 802.11a/n

Table 31-51 describes the fields on the **Design > Wireless Configuration > Lightweight AP Configuration Templates > 802.11a/n** page.

Table 31-51 Lightweight AP Configuration Templates> 802.11a/n

Field	Descriptions
Channel Assignment	Choose a Global assignment method or choose Custom to specify a channel.
Admin Status	Select if you want to enable administration privileges.
Antenna Mode	Choose an antenna mode.
Antenna Diversity	Choose enabled or disabled. Antenna diversity refers to the access point sampling the radio signal from two integrated antenna ports to choose the preferred antenna.
Antenna Type	Indicate an external or internal antenna.
Antenna Name	Select the Antenna Type check box, then choose the applicable antenna name from the drop-down list.

Table 31-51 Lightweight AP Configuration Templates> 802.11a/n (continued)

Field	Descriptions
Power Assignment	Choose a Global assignment method or choose Custom to specify a power assignment.
WLAN Override	Choose Disable or Enable from the drop-down list. The access point must be reset for the WLAN override change to take effect.
Antenna Selection	Select the Antenna Selection check box, then select the appropriate antennas from the list.
CleanAir	Select to enable.

Related Topics

- Lightweight AP Configuration Templates> AP Parameters
- Lightweight AP Configuration Templates> Mesh
- Lightweight AP Configuration Templates > 802.11a SubBand
- Lightweight AP Configuration Templates > 802.11b/g/n
- Lightweight AP Configuration Templates > CDP
- Lightweight AP Configuration Templates >FlexConnect
- Lightweight AP Configuration Templates > Select APs
- Lightweight AP Configuration Templates > Report

Lightweight AP Configuration Templates > 802.11a SubBand

Table 31-52 describes the fields on the **Design > Wireless Configuration > Lightweight AP Configuration Templates > 802.11a SubBand** page.

Table 31-52 Lightweight AP Configuration Templates > 802.11a SubBand

Field	Description
Admin Status	Click if you want to enable administration privileges.
Channel Assignment	Select the check box and then choose the appropriate channel from the drop-down list. **Note** The channel number is validated against the radio list of supported channels.
Power Assignment	Select the check box and then choose the appropriate power level from the drop-down list. **Note** The power level is validated against the radio list of supported power levels.
WLAN Override	Select the check box and then choose **Disable** or **Enable** from the drop-down list. **Note** The access point must be reset for the WLAN override change to take effect.
Antenna Type	Indicate an external or internal antenna.
Antenna Name	Select the Antenna Type check box, then choose the applicable antenna name from the drop-down list.

Related Topics

- Lightweight AP Configuration Templates> AP Parameters
- Lightweight AP Configuration Templates> Mesh
- Lightweight AP Configuration Templates> 802.11a/n

- Lightweight AP Configuration Templates > 802.11b/g/n
- Lightweight AP Configuration Templates > CDP
- Lightweight AP Configuration Templates >FlexConnect
- Lightweight AP Configuration Templates > Select APs
- Lightweight AP Configuration Templates > Report

Lightweight AP Configuration Templates > 802.11b/g/n

Table 31-53 describes the fields on the **Design > Wireless Configuration > Lightweight AP Configuration Templates > 802.11b/g/n** page.

Table 31-53 Lightweight AP Configuration Templates> 802.11b/g/n

Field	Descriptions
Channel Assignment	Choose a Global assignment method or choose Custom to specify a channel.
Admin Status	Select if you want to enable administration privileges.
Antenna Mode	Choose an antenna mode.
Antenna Diversity	Choose enabled or disabled. Antenna diversity refers to the access point sampling the radio signal from two integrated antenna ports to choose the preferred antenna.
Antenna Type	Indicate an external or internal antenna.
Antenna Name	Select the Antenna Type check box, then choose the applicable antenna name from the drop-down list.
Power Assignment	Choose a Global assignment method or choose Custom to specify a power assignment.
WLAN Override	Choose Disable or Enable from the drop-down list. The access point must be reset for the WLAN override change to take effect.
Tracking Optimized Monitor Mode	Select to enable.
Antenna Selection	Select the Antenna Selection check box, then select the appropriate antennas from the list.
CleanAir	Select to enable.

Related Topics

- Lightweight AP Configuration Templates> AP Parameters
- Lightweight AP Configuration Templates> Mesh
- Lightweight AP Configuration Templates> 802.11a/n
- Lightweight AP Configuration Templates > 802.11a SubBand
- Lightweight AP Configuration Templates > CDP
- Lightweight AP Configuration Templates >FlexConnect
- Lightweight AP Configuration Templates > Select APs
- Lightweight AP Configuration Templates > Report

Lightweight AP Configuration Templates > CDP

Table 31-54 describes the fields on the **Design > Wireless Configuration > Lightweight AP Configuration Templates > 802.11b/g/n** page.

Table 31-54 Lightweight AP Configuration Templates > CDP

Field	Description
Cisco Discovery Protocol on Ethernet Interfaces	Select the check boxes for the ethernet interface slots for which you want to enable CDP.
Cisco Discovery Protocol on Radio Interfaces	Select the checkbox for the radio interfaces slots for which you want to enable CDP.

Related Topics

- Lightweight AP Configuration Templates> AP Parameters
- Lightweight AP Configuration Templates> Mesh
- Lightweight AP Configuration Templates> 802.11a/n
- Lightweight AP Configuration Templates > 802.11a SubBand
- Lightweight AP Configuration Templates > 802.11b/g/n
- Lightweight AP Configuration Templates >FlexConnect
- Lightweight AP Configuration Templates > Select APs
- Lightweight AP Configuration Templates > Report

Lightweight AP Configuration Templates >FlexConnect

Table 31-55 describes the fields on the **Lightweight AP Template Details > FlexConnect** page.

Table 31-55 Lightweight AP Configuration Templates > FlexConnect

Field	Description
FlexConnect Configuration	Select the check box to enable FlexConnect configuration (including VLAN support, native VLAN ID, and profile name VLAN mappings). **Note** These options are only available for access points in FlexConnect mode.
OfficeExtend	The default is Enabled. Unselecting the check box simply disables OfficeExtend mode for this access point. It does not undo all of the configuration settings on the access point. If you want to clear the access point configuration and return it to factory default settings, click **Clear Config** at the bottom of the access point details page. If you want to clear only the access point personal SSID, click Reset Personal SSID at the bottom of the access point details page. When you select Enable for the OfficeExtend AP, several configuration changes automatically occur including: encryption and link latency are enabled; rogue detection, SSH access, and Telnet access are disabled. When you enable the OfficeExtend access point, you must configure at least one primary, secondary, and tertiary controller (including name and IP address).
Least Latency Controller Join	When enabled, the access point switches from a priority order search (primary, secondary, and then tertiary controller) to a search for the controller with the best latency measurement (least latency). The controller with the least latency provides the best performance. The access point only performs this search once when it initially joins the controller. It does not recalculate the latency measurements of primary, secondary, and tertiary controllers once joined to see if the measurements have changed.

Table 31-55 Lightweight AP Configuration Templates > FlexConnect (continued)

Field	Description
Native VLAN ID	The valid native VLAN ID range is 1 to 4094. If you are changing the mode to REAP and if the access point is not already in REAP mode, then all other REAP parameters are not applied on the access point.
VLAN ID ACL Mapping	Enter a VLAN ID and choose the Ingress and Egress ACLs from the drop-down list boxes to map to the VLAN ID specified.
WebAuth ACL Mapping	Enter a WLAN ID and choose the WLAN Profile and WebAuth ACLs from the drop-down list boxes to map to the WLAN ID specified.
WebPolicy ACL Mapping	Choose a WebPolicy ACL from the drop-down list boxes.
Local Split ACL Mapping	Choose a WLAN Profile and Local Split ACL from the drop-down list boxes to map to.

Related Topics

- Lightweight AP Configuration Templates> AP Parameters
- Lightweight AP Configuration Templates> Mesh
- Lightweight AP Configuration Templates> 802.11a/n
- Lightweight AP Configuration Templates > 802.11a SubBand
- Lightweight AP Configuration Templates > 802.11b/g/n
- Lightweight AP Configuration Templates > CDP
- Lightweight AP Configuration Templates > Select APs
- Lightweight AP Configuration Templates > Report

Lightweight AP Configuration Templates > Select APs

Table 31-56 describes the fields on the **Lightweight AP Template Details > Select APs** page.

Table 31-56 Lightweight AP Configuration Templates > Select APs

Field	Description
Search	Use the Search APs drop-down list to search for and select the APs to which to apply the configuration template: • Last Applied AP(s) • Scheduled AP(s) • All • All Mesh MAP AP(s) • All Mesh RAP AP(s) You can also search by the following indices, and will be prompted for additional information as described in the fields below: • By Controller • By Controller Name • By Floor Area • By Outdoor Area • By Model • By AP MAC Address • By AP Name, • By AP IP Address Range
Controller	Choose the controller from the drop-down list.
Controller Name	Choose the controller name from the drop-down list
Campus	Choose the campus from the drop-down list.
Building	Choose the building from the drop-down list.
FLoor Area	Choose the floor area from the drop-down list.
Outdoor Area	Choose the outdoor area from the drop-down list.
Models	Choose the model from the drop-down list.
AP MAC Address	Enter the access point MAC address.
AP Name	Enter the complete AP name or the starting characters of the name.
IP Address Range	Enter the range of AP IPv4 addresses. The input text for IP address search can be of two formats X.X.X.* or X.X.X.[0-255]. For example, 10.10.10.* or 10.10.10.[20-50] searches the APs in 10.10.10.10 to 10.10.10.50 IP address range.

Lightweight AP Configuration Templates > Apply/Schedule

Table 31-57 describes the fields on the **Lightweight AP Template Details > Apply/Schedule** page.

Table 31-57 Lightweight AP Configuration Templates > Select APs

Field	Description
Schedule	Select the check box to enable scheduling

Table 31-57 Lightweight AP Configuration Templates > Select APs (continued)

Field	Description
Start Date	Enter the start date for the scheduled template application, or select the start date by clicking on the calendar icon.
Start Time	Select the starting hour and minute
Recurrence	Select the range of recurrence for this schedule: Daily, Weekly, Hourly, or No Recurrence.

Related Topics

- Lightweight AP Configuration Templates> AP Parameters
- Lightweight AP Configuration Templates> Mesh
- Lightweight AP Configuration Templates> 802.11a/n
- Lightweight AP Configuration Templates > 802.11a SubBand
- Lightweight AP Configuration Templates > 802.11b/g/n
- Lightweight AP Configuration Templates > CDP
- Lightweight AP Configuration Templates >FlexConnect
- Lightweight AP Configuration Templates > Report

Lightweight AP Configuration Templates > Report

Table 31-58 describes the fields on the **Lightweight AP Template Details > Report** page.

Table 31-58 Lightweight AP Configuration Templates > Report

Field	Description
AP Name	The name of the applicable access point.
Status	Indicates whether the report run was a success, partial failure, failure, or not initiated. For failed or partially failed provisioning, click **Details** to view the failure details (including what failed and why it failed).
Ethernet MAC	Indicates the Ethernet MAC address for the applicable access point.
Controller	Indicates the controller IP address for the applicable access point.
Map	Identifies a map location for the access point.

Related Topics

- Lightweight AP Configuration Templates> AP Parameters
- Lightweight AP Configuration Templates> Mesh
- Lightweight AP Configuration Templates> 802.11a/n
- Lightweight AP Configuration Templates > 802.11a SubBand
- Lightweight AP Configuration Templates > 802.11b/g/n
- Lightweight AP Configuration Templates > CDP
- Lightweight AP Configuration Templates >FlexConnect
- Lightweight AP Configuration Templates > Select APs

Autonomous AP Migration Templates

Table 31-59 describes the fields on the following page: **Design > Wireless Configuration > Autonomous AP Migration Templates**.

Table 31-59 Autonomous AP Migration Templates

Field	Description
Name	Template name.
Description	Enter a description of the template.
DHCP Support	Ensures that after the conversion every access point gets an IP from the DHCP server.
Retain AP HostName	Allows you to retain the same hostname for this access point. The hostname is retained in the CAPWAP, only when you are migrating the AP to CAPWAP for the first time. It might not be retained if you are upgrading an AP for several times. The CAPWAP access points hostname is set to default if autonomous access points hostname has more than 32 characters. If you upgrade the access points to LWAPP from 12.3(11)JA, 12.3(11)JA1, 12.3(11)JA2, 12.3(11)JA3 autonomous images, the converted access points might not retain their Static IP Address, Netmask, Hostname and Default Gateway.
Migrate over WANLink	Increases the default timeouts for the CLI commands executed on the access point. If you enable this option, the *env_vars* file stores the remote TFTP server location. This information is copied to the access point. If this option is not selected, then the Prime Infrastructure internal TFTP server is used to copy the *env_vars* file to the access point.
DNS Address	Enter the DNS address.
Domain Name	Enter the domain name.
Controller IP	Enter controller IP address.
AP Manager IP	Specify the controller the access point should join by entering the access point manager IP address. For SSC-enabled access points, this IP address must be the same as the controller IP field. For MIC-enabled access points, the IP addresses need not match.
User Name	Enter user name.
Password	Enter password for the user name.
TFTP Server IP	Enter the IP address of the Prime Infrastructure server. Prime Infrastructure provides its own TFTP and FTP server during the installation and setup
File Path	Enter the TFTP directory which was defined during Prime Infrastructure setup.
File Name	Enter the CAPWAP conversion file defined in the TFTP directory during Prime Infrastructure setup (for example, c1240-rcvk9w8-tar.123-11JX1.tar).
Apply Template	Choose an option by which you want to apply the template for migration.
Notification	Enter the email address of recipient to send notifications.

Designing Mobility Services Engine Field Description

The following section contains field descriptions for designing mobility services engine:

Mobility Services Engine Page Field Description

The following section contains field description for pages found in **Design** > **Mobility Services** > **Mobility Services Engine** page.

Mobility Services Engine > Select a command > Add Location Server

Table 31-60 describes the fields on the **Design** > **Mobility Services** > **Mobility Services Engine** > **Select a command** > **Add Location Server** page.

Table 31-60 Add Location Server

Field	Description
Device Name	Device Name of the mobility services engine
IP Address	IP address of the mobility services engine.
Contact Name	The mobility service engine administrator.
User Name	The default username is admin. This is Prime Infrastructure communication username configured for MSE.
Password	The default password is admin.This is Prime Infrastructure communication password configured for MSE.
Port	Port number of the mobility services engines device.
HTTPS	When enabled, HTTPS is used for communication between Prime Infrastructure and location server.

Mobility Services Engine > Select a command > Add Mobility Services Engine

Table 31-61 describes the fields on the **Design** > **Mobility Services** > **Mobility Services Engine** > **Select a command** > **Add a Mobility Services Engine** page.

Table 31-61 Add a Mobility Services Engine

Field	Description
Device Name	User-assigned name for the mobility services engine.
IP Address	The IP address of the mobility service engine.
Contact Name	The mobility services engine administrator.

Field	Description
Username	The default username is admin. This is Prime Infrastructure communication username configured for MSE.
Password	The default password is admin.This is Prime Infrastructure communication password configured for MSE.
HTTP	When enabled, HTTP is used for communication between Prime Infrastructure and mobility services engine. By default, Prime Infrastructure uses HTTPS to communicate with MSE.

Mobility Services Engine Database Synchronization

Table 31-61 describes the fields on the **Administration > Background Task > Mobility Service Synchronization** link **> Task > Mobility Service Synchronization > Select a command > Add a Mobility Services Engine** page.

Table 31-62 Add a Mobility Services Engine

Field	Description
Device Name	User-assigned name for the mobility services engine.
IP Address	The IP address of the mobility service engine.
Contact Name	The mobility services engine administrator.
Username	The default username is admin. This is Prime Infrastructure communication username configured for MSE.
Password	The default password is admin.This is Prime Infrastructure communication password configured for MSE.
HTTP	When enabled, HTTP is used for communication between Prime Infrastructure and mobility services engine. By default, Prime Infrastructure uses HTTPS to communicate with MSE.

High Availability Field Description

Table 31-63 describes the fields on the **Design > Mobility Services > High Availability** page.

Table 31-63 Configuring High Availability

Field	Description
Device Name	Secondary device name with which you want to pair the primary MSE.
IP Address	Secondary IP address which is the health monitor IP address of the secondary MSE.
Contact Name	The mobility services engine administrator.
Failover Type	Specify the failover type. You can choose either Manual or Automatic. After 10 seconds, the system fails over. The secondary server waits for a maximum of 10 seconds for the next heartbeat from the primary server. If it does not get the heartbeat in 10 seconds, it declares a failure.

Field	Description
Failback Type	Specify the failback type. It can be either Manual or Automatic.
Long Failover Wait	Specify the long failover wait in seconds. After 10 seconds, the system fails over. The maximum failover wait is 2 seconds.

Adding Trap Destinations for a mobility services engine

Table 31-64 describes the fields on the **Design** > **Mobility Services** > Device Name > System > Trap Destinations > Add Trap Destinations page.

Table 31-64 Add Trap Destinations

Field	Description
IP Address	IP address of the trap destination
Port No.	Port number for the trap destination. The default port number is 162.
Destination Type	This field is not editable and has a value of **Other**.
SNMP Version	Select either v2c or v3.
The following set of fields appear only if you select v3 as the SNMP version.	
User Name	Username for the SNMP Version 3.
Security Name	Security name for the SNMP Version 3.
Authentication Type	Select one of the following: HMAC-MD5 HMAC-SHA
Authentication Password	Authentication password for the SNMP Version 3.
Privacy Type	Select one of the following: CBC-DES CFB-AES-128 CFB-AES-192 CFB-AES-256
Privacy Password	Privacy password for the SNMP Version 3.

Adding User to a mobility services engine

Table 31-65 describes the fields on the **Design** > **Mobility Services** > **Mobility Services Engine** > **Device Name** > **Systems Account** > **Users** > **Select a command** > **Add User** page.

Table 31-65 Add User

Field	Description
Username	Enter the username
Password	Enter the password
Confirm Password	Re-enter the password
Group Name	Group name to which the user belongs
Permission Level	Choose a permission level. There are three permission levels to choose from: Read Access, Write Access, and Full Access (required for Prime Infrastructure to access a mobility services engine).

Adding User Groups

Table 31-61 describes the fields on the **Design** > **Mobility Services** > **Mobility Services Engine** > **Device** > **Systems** > **Accounts** > **Users** > **Select a Command** > **Add Group** page.

Table 31-66 Design > Mobility Services > Mobility Services Engine > Device Name > Systems > Accounts > Users > Select a command > Add Group

Field	Description
Group Name	Enter the name of the group.
Permission Level	Choose a permission level. There are three permission levels to choose from: Read Access, Write Access, and Full Access (required for Prime Infrastructure to access a mobility services engine).

Provisioning MSAP service advertisement

Table 31-67 describes the fields on the **Design** > **Mobility Services** > **MSAP** > **Select a command** > **Add Service Advertisement** page.

Table 31-67 Design > Mobility Services > MSAP > Select a command > Add Service Advertisement

Field	Description
General	
Provider Name	Enter the service provider name. It is the name of the provider who wants to provide advertisements to the client.
Icon	Select an icon that is associated with the service provider by clicking the **Choose File**. This is the icon that is displayed on the client handset.
Venue Name	Enter the venue name at which you want the advertisements to be broadcasted on.
Area Type	Choose the area type where you want to display the service advertisements.
Campus	Choose the campus type where you want to display the service advertisements.
Building	Choose the building name where you want the advertisements to appear.
Floor	Choose the floor type.

Field	Description
Coverage Area	Choose the coverage area.
Selected Map	Shows the selected map position.
SSID	Choose SSIDs on which you want to broadcast the service advertisements.
Display Rule	You can select either the **Display everywhere** or **Display near selected APs** radio button. By default, Display everywhere radio button is selected.
Advertisement	
Friendly Name	Enter the service description.
Advertisement Type	Choose the type of advertisement you want to display.

Wireless Operational Tools Field Descriptions

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

- Guest User Controller Templates Field Descriptions, page 31-73
- Voice Audit Field Descriptions, page 31-74
- Voice Diagnostic Field Descriptions, page 31-78

Guest User Controller Templates Field Descriptions

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

- Table 31-68—General Tab
- Table 31-69—Advanced Tab

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

Table 31-68 describes the fields on the **Operate > Operational Tools > Wireless > Guest User > Add Guest User > New Controller Template > General** page.

Table 31-68 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.

Table 31-68 Guest User > Add Guest User > New Controller Template > General Tab Field Descriptions (continued)

Field	Description
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 make the disclaimer text as default for this guest user template.

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

Table 31-69 describes the fields on the **Operate > Operational Tools > Wireless > Guest User > Add Guest User > New Controller Template > Advanced** page.

Table 31-69 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.
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 tables describe the fields on the **Operate > Operational Tools > Wireless > Voice Audit** page:

- Table 31-70—Controllers Tab
- Table 31-71—Rules Tab
- Table 31-72—Report Tab

Voice Audit > Controller Tab

Table 31-70 describes the fields on the **Operate > Operational Tools > Wireless > Voice Audit > Controller** page.

Table 31-70 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

Table 31-71 describes the fields on the **Operate > Operational Tools > Wireless > Voice Audit > Rules** page.

Table 31-71 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.

Table 31-71 Voice Audit > Rules Tab Field Descriptions (continued)

Rule	Rule Details
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.
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—Choose **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—Choose **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—100%.

Table 31-71 Voice Audit > Rules Tab Field Descriptions (continued)

Rule	Rule Details
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—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.
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—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—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—120.
ARP Unicast	Description—Checks whether or not ARP Unicast is disabled.

Voice Audit > Report Tab

Table 31-72 describes the fields on the **Operate > Operational Tools > Wireless > Voice Audit > Report** page.

Table 31-72 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	
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 tables describe the fields on the **Operate > Operational Tools > Wireless > Voice Diagnostic** page:

- Table 31-73—Voice Diagnostic Test List Page
- Table 31-74—Voice Diagnostic Test Report Page

Voice Diagnostic Test List Page

Table 31-73 describes the fields on the **Operate > Operational Tools > Wireless > Voice Diagnostic** page.

Table 31-73 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.

Table 31-73 Voice Diagnostic Test List Page Field Descriptions (continued)

Field	Description
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

Table 31-74 describes the tabs on the **Operate > Operational Tools > Wireless > Voice Diagnostic Test Report** page.

Table 31-74 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 will be updated every 10 secs.	

Table 31-74 Voice Diagnostic Test Report Page Tab Descriptions (continued)

Tab	Description
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.
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.	

Switch Location Configuration Templates

Table 31-75 describes the fields on the **Design > Wireless Configuration > Switch Location Configuration** page.

Table 31-75 Switch Location Configuration Template Page Field Descriptions

Field	Description
General	
Template Name	
Map Location	
Campus	Choose a campus for the map location for a switch/switch port.
Building	Choose a building for the map location for a switch/switch port.

Table 31-75 Switch Location Configuration Template Page Field Descriptions (continued)

Field	Description
Floor	Choose a floor for the map location for a switch/switch port.
Import	Imports the civic information for the campus, building, and floor selected.
ELIN and Civic Location	
ELIN	The Emergency Location Identification Number.
Civic Address tab	The available civic address information for the switch/switch port.
Advanced tab	Detailed information about the switch/switch port location.
NMSP	Select or unselect this check box to enable or disable NMSP for the switch.