



## Field Reference for Design Pages

This chapter provides descriptions of the fields found in the pages under **Design tab of Cisco Prime Infrastructure Release 2.0**. This chapter contains the following topics:

- [Features and Technologies Field Descriptions, page 1-1](#)
- [CLI Templates Field Descriptions, page 1-94](#)
- [Wireless Configuration Field Descriptions, page 1-117](#)
- [Plug and Play Profile Field Descriptions, page 1-129](#)
- [Mobility Services Field Descriptions, page 1-132](#)

## Features and Technologies Field Descriptions

The following topics contain descriptions of the fields found in the Features and Technologies templates:

- [Application Visibility Field Descriptions, page 1-1](#)
- [Controller Templates Field Descriptions, page 1-3](#)
- [Interfaces Templates Field Descriptions, page 1-69](#)
- [Security Templates Field Descriptions, page 1-71](#)
- [Security Templates Field Descriptions, page 1-71](#)

## Application Visibility Field Descriptions

The Application Visibility feature allows you to monitor the traffic sent toward the Internet. Also, you can monitor the traffic flow and generate reports based on the traffic flow.

The following table describes the fields in **Design > Configuration > Feature Design > Features and Technologies > Application Visibility > AVC Configuration**.

**Table 1-1**      *Application Visibility > AVC Configuration*

Field	Description
<b>Template Detail</b>	
Apply to Interface Role	Choose an interface role from the drop-down list. For information about creating the interface role, see the “Creating an Interface Role” section in the <a href="#">Cisco Prime Infrastructure 2.0 User Guide</a> .

Table 1-1 Application Visibility &gt; AVC Configuration (continued)

Field	Description
<b>Traffic Statistics</b>	
On/Off	Click <b>Off</b> if you do not want to collect the statistics pertaining to data packets. We recommend that you: <ul style="list-style-type: none"> <li>• Configure the required minimal set of filters.</li> <li>• Collect only traffic statistics for sites that run only IPv4 traffic.</li> </ul>
IPs, Subnets	Select an option to generate the report on IPv4, IPv6, or both IPv4 and IPv6 traffic.
Advanced Options	Select <b>Sampling Rate</b> and <b>Direction</b> . You can monitor ingress traffic only, egress traffic only, or both ingress and egress traffic. To reduce the performance impact on the device, select only the relevant traffic to be monitored.
<b>HTTP URL Visibility</b>	
On/Off	Click <b>Off</b> if you do not want to collect the statistics on HTTP URL visibility.
IPs, Subnets	Select a specific set of IPv4 addresses or subnets to be monitored and decide whether to generate the report for IPv6 traffic.
Applications	Select a specific set of applications that should be monitored (there could be up to 32 monitored applications). By default, all the enterprise related HTTP-based applications are included in the list.
Advanced Options	Select the Sampling Rate and Direction from the drop-down list. To reduce the performance impact on the device, select only the relevant traffic to be monitored.
<b>Application Response Time</b>	
On/Off	Click <b>Off</b> if you do not want to collect the Application Response Time metrics.
IPs, Subnets	Select a specific set of IPv4 addresses or subnets to be monitored and decide whether to generate the report for IPv6 traffic.
Applications	Select a specific set of applications that should be monitored (there could be up to 32 monitored applications). By default, all the enterprise related HTTP-based applications are included in the list.
Advanced Options	Select the Sampling Rate and Direction from the drop-down list. To reduce the performance impact on the device, select only the relevant traffic to be monitored.
<b>Voice/Video Metrics</b>	
On/Off	Click <b>Off</b> if you do not want to collect the metrics on voice/video traffic.
IPs, Subnets	Select a specific set of IPv4 addresses or subnets to be monitored and decide whether to generate the report for IPv6 traffic.
Applications	Select a specific set of applications that should be monitored (there could be up to 32 monitored applications). By default, all the enterprise related RTP enterprise-related applications are monitored.

## Controller Templates Field Descriptions

Altering configurations across a large number of controllers can be tedious and time-consuming, and templates save you time by applying the necessary configurations and by ensuring consistency across controllers. When you are implementing new services or a new site, use these controller templates to define controller parameters and settings, which you can later deploy to a specified number of wireless LAN controllers.

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

- [Controller > 802.11, page 1-3](#)
- [Controller > 802.11a or n, page 1-6](#)
- [Controller > 802.11b or g or n, page 1-15](#)
- [Controller > CLI > General, page 1-22](#)
- [Controller > FlexConnect > FlexConnect AP Groups, page 1-23](#)
- [Controller > IPv6, page 1-25](#)
- [Controller > Location, page 1-26](#)
- [Controller > Management, page 1-27](#)
- [Controller > Mesh > Mesh Settings, page 1-31](#)
- [Controller > PMIP, page 1-31](#)
- [Controller > Security, page 1-33](#)
- [Controller > System, page 1-46](#)
- [Controller > WLANs > WLAN Configuration, page 1-55](#)
- [Controller > mDNS, page 1-68](#)

### Controller > 802.11

The following topics contain field descriptions for pages found in **Design > Configuration > Feature Design > Features and Technologies > Controller > 802.11**.

- [Controller > 802.11 > Band Select, page 1-3](#)
- [Controller > 802.11 > Load Balancing, page 1-4](#)
- [Controller > 802.11 > Media Stream, page 1-4](#)
- [Controller > 802.11 > Preferred Call, page 1-5](#)
- [Controller > 802.11 > RF Profiles, page 1-5](#)

#### Controller > 802.11 > Band Select

The following table describes the Template Detail fields found in **Design > Configuration > Feature Design > Features and Technologies > Controller > 802.11 > Band Select**.

**Table 1-2**      **Controller > 802.11 > Band Select**

Field	Description
Probe Cycle Count	Enter a value from 1 to 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 from 1 to 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 from 10 to 200 seconds for the age-out suppression. 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.
Age Out Dual Band	Enter a value from 10 to 300 seconds for the age-out dual band. 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 Received Signal Strength Indicator (RSSI). This field sets the minimum RSSI for a client to respond to a probe. The default value is –80 dBm.

**Controller > 802.11 > Load Balancing**

The following table describes the Template Detail fields on **Design > Configuration > Feature Design > Features and Technologies > Controller > 802.11 > Load Balancing**.

**Table 1-3**      **Controller > 802.11 > Load Balancing**

Field	Description
Client Window Size	Enter a value from 1 to 20. The page size becomes part of the algorithm that determines whether an access point is too heavily loaded to accept more client associations:  $\text{load-balancing page} + \text{client associations on AP with lightest load} = \text{load-balancing threshold}$
Max Denial Count	Enter a value from 0 to 10. The denial count sets the maximum number of association denials during load balancing.

**Controller > 802.11 > Media Stream**

The following table describes the Template Detail fields on **Design > Configuration > Feature Design > Features and Technologies > Controller > 802.11 > Media Stream**.

**Table 1-4**      **Controller > 802.11 > Media Stream**

Field	Description
Media Stream Name	Enter the name of the media stream.
Multicast Destination Start IP	Enter the start IP address of the media stream to be multicast.
Multicast Destination End IP	Enter the 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.

**Table 1-4**      **Controller > 802.11 > Media Stream (continued)**

Field	Description
Maximum Expected Bandwidth	Enter the maximum bandwidth that a media stream can use.
Average Packet Size	Enter the average packet size that a media stream can use.
RRC Periodical Update	Enter the Resource Reservation Control (RRC) calculations that are updated periodically; if disabled, RRC calculations are done only once when a client joins a media stream.
RRC Priority	Enter the priority of RRC with the highest at 1 and the lowest at 8.
Traffic Profile Violation	Choose the Traffic Profile Violation from the drop-down list. The drop-down list appears if the stream is dropped or put in the best effort queue if the stream violates the QoS video profile.
Policy	Choose the Policy from the drop-down list. The drop-down list appears if the media stream is admitted or denied.

**Controller > 802.11 > Preferred Call**

The following table describes the Template Detail fields on **Design > Configuration > Feature Design > Features and Technologies > Controller > 802.11 > Preferred Call**.

**Table 1-5**      **Controller > 802.11 > Preferred Call**

Field	Description
Number Id	Enter a value to identify the preferred number. You can have a maximum of six preferred call numbers. The valid range is from 1 to 6. The default value is 1.
Preferred Number	Enter the preferred call number.

**Controller > 802.11 > RF Profiles**

The following table describes the Template Detail fields on **Design > Configuration > Feature Design > Features and Technologies > Controller > 802.11 > RF Profiles**.

**Table 1-6**      **Controller > 802.11 > RF Profiles**

Field	Description
Template Name	Enter the name of the template.
Profile Name	Enter the name of the current profile.
Description	Enter the Description of the template.
Radio Type	Choose the radio type of the access point from the drop-down list.
Minimum Power Level Assignment (-10 to 30 dBm)	Enter a value from -10 to 30dBm for the minimum power level assignment. The default value is -10 dBm.
Maximum Power Level Assignment (-10 to 30 dBm)	Enter a value from -10 to 30dBm for the maximum power level assignment. The default value is 30 dBm.
Power Threshold v1(-80 to -50 dBm)	Enter a value from -80 to -50dBm for the power threshold v1. The default value is -70 dBm.

**Table 1-6**      **Controller > 802.11 > RF Profiles (continued)**

Field	Description
Power Threshold v2(-80 to -50 dBm)	Enter a value from -80 to -50dBm for the power threshold v2.The default value is -67 dBm.
Data Rates	<p>Select the data rates from the 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:</p> <ul style="list-style-type: none"> <li>802.11a—6, 9, 12, 18, 24, 36, 48, and 54 Mbps.</li> <li>802.11b/g—1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, or 54 Mbps.</li> </ul> <p>For each data rate, you must also choose one of these options:</p> <ul style="list-style-type: none"> <li>Mandatory—Clients must support this data rate to associate to an access point on the controller.</li> <li>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.</li> <li>Disabled—The clients specify the data rates used for communication.</li> </ul>

## Controller > 80211a or n

The following topics contain field descriptions for pages found in **Design > Configuration > Feature Design > Features and Technologies > Controller > 80211a or n**.

- [Controller > 80211a or n > dot11a-RRM > DCA, page 1-6](#)
- [Controller > 80211a or n > dot11a-RRM > Intervals, page 1-8](#)
- [Controller > 80211a or n > dot11a-RRM > Thresholds, page 1-8](#)
- [Controller > 80211a or n > dot11b-RRM > TPC, page 1-9](#)
- [Controller > 80211a or n > 802.11h, page 1-9](#)
- [Controller > 80211a or n > CleanAir, page 1-10](#)
- [Controller > 80211a or n > EDCA Parameters, page 1-11](#)
- [Controller > 80211a or n > High Throughput \(802.11n\), page 1-11](#)
- [Controller > 80211a or n > Media Parameters > General, page 1-12](#)
- [Controller > 80211a or n > Media Parameters > Video, page 1-12](#)
- [Controller > 80211a or n > Media Parameters > Voice, page 1-13](#)
- [Controller > 80211a or n > Parameters, page 1-14](#)
- [Controller > 80211a or n > Roaming Parameters, page 1-15](#)

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

The Radio Resource Management (RRM) Dynamic Channel Assignment (DCA) page allows you to choose the DCA channels as well as the channel width for this controller.

RRM DCA supports 802.11n 40-MHz channel width in the 5-GHz band. The higher bandwidth allows radios to achieve higher instantaneous data rates.

**Note**

Choosing a larger bandwidth reduces the nonoverlapping channels that could potentially reduce the overall network throughput for certain deployments.

The following table describes the Template Detail fields on **Design > Configuration > Feature Design > Features and Technologies > Controller > 80211a or n > dot11a-RRM > DCA**.

**Table 1-7**      **Controller > 80211a or n > dot11a-RRM > DCA**

Field	Description
Assignment Mode	<p>From the drop-down list, choose one of three modes:</p> <ul style="list-style-type: none"> <li>Automatic—The transmit power is periodically updated for all access points that permit this operation.</li> <li>On Demand—Transmit power is updated when you click Assign Now.</li> <li>Disabled—No dynamic transmit power assignments occur, and values are set to their global default.</li> </ul>
Avoid Foreign AP Interference	Select the enable check box to have RRM consider interference from foreign Cisco access points (those non-Cisco access points outside RF/mobility domain) when assigning channels. 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 adjustment increases capacity and reduces variability for the Cisco WLAN Solution.
Avoid Cisco AP Load	Select the enable 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 enable check box to have access points avoid channels that have interference from nonaccess 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 adjustment increases capacity and reduces variability for the Cisco WLAN Solution.
Signal Strength Contribution	Always enabled (not configurable). Signal Strength Contribution 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 enable 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 > 80211a or n > dot11a-RRM > Intervals**

The following table describes the Template Detail fields on **Design > Configuration > Feature Design > Features and Technologies > Controller > 80211a or n > dot11a-RRM > Intervals**.

**Table 1-8** *Controller > 80211a or n > dot11a-RRM > Intervals*

Field	Description
Neighbor Packet Frequency	Enter the interval at which you want strength measurements taken for each access point. The default is 300 seconds.
Channel Scan Duration	Enter the interval at which you want noise and interference measurements taken for each access point. The default is 300 seconds.
Load Measurement Interval	Enter the interval at which you want load measurements taken for each access point. The default is 300 seconds. <b>Note</b> This parameter cannot be applied to Cisco WLC Release 4.3 or later.
Coverage Measurement Interval	Enter the interval at which you want coverage measurements taken for each access point. The default is 300 seconds. <b>Note</b> This parameter cannot be applied to Cisco WLC Release 4.3 or later.

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

Use this option to create or modify a template for setting various RRM thresholds such as load, interference, noise, and coverage.

The following table describes the Template Detail fields on **Design > Configuration > Feature Design > Features and Technologies > Controller > 80211a or n > dot11a-RRM > Thresholds**.



**Note** You must disable the 802.11a/n network before applying these RRM threshold values.

**Table 1-9** *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 (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 from 0 to 100 percent.



**Table 1-9**      **Controller > 80211a or n > dot11a-RRM > Thresholds (continued)**

Field	Description
Noise Threshold	Enter a noise threshold from -127 to 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 > dot11b-RRM > TPC**

The controller dynamically controls access point transmit power based on real-time wireless LAN conditions. Normally, power can be kept low to gain extra capacity and reduce interference. The controller attempts to balance the transmit power of the access points according to how the access points are seen by their third strongest neighbor.

The transmit power control (TPC) algorithm both increases and decreases the power of an access point in response to changes in the RF environment. In most instances, TPC seeks to lower the power of an access point to reduce interference, but in the case of a sudden change in the RF coverage—for example, if an access point fails or becomes disabled—TPC can also increase power on surrounding access points. This feature is different from Coverage Hole Detection. Coverage Hole Detection is primarily concerned with clients, while TPC is tasked with providing enough RF power to achieve desired coverage levels while avoiding channel interference between access points.

The following table describes the Template Detail fields on **Design > Configuration > Feature Design > Features and Technologies > Controller > 80211a or n > dot11b-RRM > TPC**.

**Table 1-10**      **Controller > 80211a or n > dot11b-RRM > TPC**

Field	Description
TPC Version	Choose TPCv1 or TPCv2 from the drop-down list. <b>Note</b> 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: <ul style="list-style-type: none"> <li>Automatic—The transmit power is periodically updated for all access points that permit this operation.</li> <li>On Demand—Transmit power is updated when you click Assign Now.</li> <li>Disabled—No dynamic transmit power assignments occur, and values are set to their global default.</li> </ul>
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 from -50 to -80.
Control Interval	Shows the transmitted power control interval in seconds (read-only).

**Controller > 80211a or n > 802.11h**

802.11h informs client devices about channel changes and can limit the transmit power of the client device. Create or modify a template for configuration 802.11h parameters (such as power constraint and channel controller announcement) and applying these settings to multiple controllers.

The following table describes the Template Detail fields on **Design > Configuration > Feature Design > Features and Technologies > Controller > 80211a or n > 802.11h**.

**Table 1-11**      **Controller > 80211a or n > 802.11h**

Field	Description
Power Constraint	Select the <b>Power Constraint</b> check box if you want the access point to stop transmission on the current channel.
Channel Announcement	Select the <b>Channel Announcement</b> check box to enable channel announcement. Channel announcement is a method in which the access point announces when it is switching to a new channel and the new channel number.

### Controller > 80211a or n > CleanAir

Use this option to create or modify a template for configuring CleanAir parameters for the 802.11a/n radio. You can configure the template to enable or disable CleanAir. You can also configure the type of interfering devices to include for reporting and alarms.

The following table describes the Template Detail fields on **Design > Configuration > Feature Design > Features and Technologies > Controller > 80211a or n > CleanAir**.

**Table 1-12**      **Controller > 80211a or n > CleanAir**

Field	Description
Report Interferers	Select the <b>Report interferers</b> 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 <b>Persistent Device Propagation</b> 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 location and interfere with the WLAN operations even if they are not detectable at all times.
Air Quality Alarm	Select the <b>Air Quality Alarm</b> 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 <b>Air Quality Alarm</b> check box, enter a value from 1 to 100 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.
Air Quality Unclassified Category Alarm	Select the <b>Air Quality Unclassified Category Alarm</b> 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 <b>Air Quality Unclassified Category Alarm</b> check box, enter a value from 1 to 99 in the Air Quality Unclassified Category Severity Threshold text box to specify the threshold at which you want the unclassified category alarm to be triggered. The default is 20.

**Table 1-12**      **Controller > 80211a or n > CleanAir (continued)**

Field	Description
Interferers For Security Alarm	Select the <b>Interferers For Security Alarm</b> 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 under <b>Interferers Selected for Security Alarms</b> and any that do not need to trigger interferer alarms appear in the <b>Interferers Ignored for Security Alarms</b> . 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 > EDCA Parameters**

Enhanced distributed channel access (EDCA) parameters are designed to provide preferential wireless channel access for voice, video, and other quality of service (QoS) traffic.

The following table describes the Template Detail fields on **Design > Configuration > Feature Design > Features and Technologies > Controller > 80211a or n > EDCA Parameters**.

**Table 1-13**      **Controller > 80211a or n > EDCA Parameters**

Field	Description
EDCA Profile	<p>Choose one of the following options from the <b>EDCA Profile</b> drop-down list:</p> <ul style="list-style-type: none"> <li>• <b>WMM</b>—Enables the Wi-Fi Multimedia (WMM) default parameters. This is the default value. Choose this option when voice or video services are not deployed on your network.</li> <li>• <b>Spectralink Voice Priority</b>—Enables Spectralink voice priority parameters. Choose this option if Spectralink phones are deployed on your network to improve the quality of calls.</li> <li>• <b>Voice Optimized</b>—Enables EDCA voice-optimized profile parameters. Choose this option when voice services other than Spectralink are deployed on your network.</li> <li>• <b>Voice &amp; Video Optimized</b>—Enables EDCA voice- and video-optimized profile parameters. Choose this option when both voice and video services are deployed on your network.</li> </ul> <p><b>Note</b> Video services must be deployed with admission control (ACM). Video services without ACM are not supported.</p> <p><b>Note</b> You must shut down the radio interface before configuring EDCA parameters.</p>
Low Latency MAC	Enable low latency MAC only if all clients on the network are WMM compliant.

**Controller > 80211a or n > High Throughput (802.11n)**

The following table describes the Template Detail fields on **Design > Configuration > Feature Design > Features and Technologies > Controller > 80211a or n > High Throughput (802.11n)**.

**Table 1-14**      **Controller > 80211a or n > High Throughput (802.11n)**

Field	Description
802.11n Network Status Enabled	Select the <b>802.11n Network Status Enabled</b> check box to enable high throughput.
Selected MCS Indexes	Choose which level of data rate you want supported. Modulation coding schemes (MCS) are similar to 802.11a data rate. The defaults are 20 MHz and short guarded interval. When you select the <b>Supported</b> check box next to a numbered Data Rate, the chosen numbers appear in the Selected MCS Indexes field at the bottom of the column.

**Controller > 80211a or n > Media Parameters > General**

The following table describes the Template Detail fields on **Design > Feature Design > Features and Technologies > Controller > 80211a or n > Media Parameters > General**.

**Table 1-15**      **Controller > 80211a or n > Media Parameters > General**

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

**Controller > 80211a or n > Media Parameters > Video**

The following table describes the Template Detail fields on **Design > Configuration > Feature Design > Features and Technologies > Controller > 80211a or n > Media Parameters > Video**.

**Table 1-16**      **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 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 <b>Unicast Video Redirect</b> check box to enable all nonmedia 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	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 <b>Multicast Direct Enable</b> 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 1-16**      **Controller > 80211a 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 <b>Best Effort QOS Admission</b> 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.

**Controller > 80211a or n > Media Parameters > Voice**

The following table describes the Template Detail fields on **Design > Feature Design > Features and Technologies > Controller > 80211a or n > Media Parameters > Voice**.

**Table 1-17**      **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.
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 that 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.

**Controller > 80211a or n > Parameters**

The following table describes the Template Detail fields on **Design > Configuration > Feature Design > Features and Technologies > Controller > 80211a or n > Parameters**.

**Table 1-18**      **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 milliseconds. 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.
Mode	Select the check box 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 either 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 > Roaming Parameters

The following table describes the Template Detail fields on **Design > Configuration > Feature Design > Features and Technologies > Controller > 80211a or n > Roaming Parameters**.

**Table 1-19**      **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	<p>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.</p> <p><b>Note</b> The Scan Threshold and Transition Time parameters guarantee a minimum level of client roaming performance. Together with highest expected client speed and Roaming Hysteresis, these parameters make it possible to design a wireless LAN network that supports roaming simply by ensuring a certain minimum overlap distance between access points.</p>
Transition Time	<p>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.</p> <p><b>Note</b> The Scan Threshold and Transition Time parameters guarantee a minimum level of client roaming performance. Together with highest expected client speed and Roaming Hysteresis, these parameters make it possible to design a wireless LAN network that supports roaming simply by ensuring a certain minimum overlap distance between access points.</p>

## Controller > 80211b or g or n

The following topics contain field descriptions for pages found in **Design > Configuration > Feature Design > Features and Technologies > Controller > 80211b or g or n**.

- [Controller > 802.11b or g or n > dot11a-RRM > DCA, page 1-16](#)
- [Controller > 802.11b or g or n > dot11a-RRM > Intervals, page 1-16](#)
- [Controller > 802.11b or g or n > dot11a-RRM > Thresholds, page 1-16](#)
- [Controller > 802.11b or g or n > dot11b-RRM > TPC, page 1-16](#)
- [Controller > 802.11b or g or n > CleanAir, page 1-16](#)

- [Controller > 802.11b or g or n > EDCA Parameters](#), page 1-16
- [Controller > 802.11b or g or n > High Throughput \(802.11n\)](#), page 1-17
- [Controller > 802.11b or g or n > Media Parameters](#), page 1-17
- [Controller > 802.11b or g or n > Parameters](#), page 1-19
- [Controller > 802.11b or g or n > Roaming Parameters](#), page 1-22

### Controller > 802.11b or g or n > dot11a-RRM > DCA

For a description of the fields on **Design > Configuration > Feature Design > Features and Technologies > Controller > 802.11b or g or n > dot11a-RRM > DCA**, see [Controller > 802.11a or n > dot11a-RRM > DCA](#), page 1-6.

### Controller > 802.11b or g or n > dot11a-RRM > Intervals

For a description of the fields on **Design > Configuration > Feature Design > Features and Technologies > Controller > 802.11b or g or n > dot11a-RRM > Intervals**, see [Controller > 802.11a or n > dot11a-RRM > Intervals](#), page 1-8.

### Controller > 802.11b or g or n > dot11a-RRM > Thresholds

For a description of the fields on **Design > Configuration > Feature Design > Features and Technologies > Controller > 802.11b or g or n > dot11a-RRM > Thresholds**, see [Controller > 802.11a or n > dot11a-RRM > Thresholds](#), page 1-8.

### Controller > 802.11b or g or n > dot11b-RRM > TPC

For a description of the fields on **Design > Configuration > Feature Design > Features and Technologies > Controller > 802.11b or g or n > dot11b-RRM > TPC**, see [Controller > 802.11a or n > dot11b-RRM > TPC](#), page 1-9.

### Controller > 802.11b or g or n > CleanAir

For a description of the fields on **Design > Configuration > Feature Design > Features and Technologies > Controller > 802.11b or g or n > CleanAir**, see [Controller > 802.11a or n > CleanAir](#), page 1-10.

### Controller > 802.11b or g or n > EDCA Parameters

Use this option to create or modify a template for configuring 802.11b/g/n EDCA parameters. EDCA parameters designate preconfigured profiles at the MAC layer for voice and video.

The following table describes the Template Detail fields in **Design > Configuration > Feature Design > Features and Technologies > Controller > 802.11b or g or n > EDCA Parameters**.



**Table 1-20**      **Controller > 802.11b or g or n > EDCA Parameters**

Field	Description
EDCA Profile	<p>Profiles include Wi-Fi Multimedia (WMM), Spectralink Voice Priority (SVP), Voice Optimized, and Voice &amp; Video Optimized. WMM is the default EDCA profile.</p> <p><b>Note</b> You must shut down the radio interface before configuring EDCA Parameters.</p> <p><b>Note</b> Disabling WMM or changing the EDCA profile from WMM on the device will disable the 11n rates when the AP is rebooted.</p>
Low Latency MAC	Enable this option only if DSCP marking is correct for media (RTP) and signaling packets.

**Controller > 802.11b or g or n > High Throughput (802.11n)**

Use this option to create or modify a template for configuring high-throughput parameters such as MCS (data rate) settings and indexes and for applying these 802.11n settings to multiple controllers.

The following table describes the Template Detail fields in **Design > Configuration > Feature Design > Features and Technologies > Controller > 802.11b or g or n > High Throughput (802.11n)**.

**Table 1-21**      **Controller > 802.11b or g or n > High Throughput (802.11n)**

Field	Description
802.11n Network Status	Select the check box to enable high throughput.
MCS (Data Rate) Settings	Choose which level of data rate you want supported. MCS is modulation coding schemes that are similar to 802.11a data rate. The values 20 MHz and short guarded interval are used as defaults. When you select the <b>Supported</b> check box, the chosen numbers appear in the Selected MCS Indexes page.

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

Use this option to create or modify a template for configuring 802.11b/g/n voice parameters such as Call Admission Control and traffic stream metrics.

The following table describes the Template Detail fields on **Design > Feature Design > Features and Technologies > Controller > 802.11b or g or n > Media Parameters**.

**Table 1-22**      **Controller > 802.11b or g or n > Media Parameters**

Field	Description
<b>General</b>	
Maximum Media Bandwidth (0 to 85%)	Specify the percentage maximum of bandwidth allowed. This option is only available when CAC is enabled.
<b>Video</b>	
Admission Control (ACM)	Select the check box to enable admission control.

**Table 1-22**      **Controller > 80211b or g or n > Media Parameters (continued)**

Field	Description
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 <b>Unicast Video Redirect</b> check box to enable all nonmedia stream packets in the video queue to be 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 <b>Multicast Direct Enable</b> 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 <b>Best Effort QOS Admission</b> 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.
<b>Voice</b>	
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 maintains a 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.
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-down list. The available options are G.711, G.729, and User Defined.

**Table 1-22**      **Controller > 802.11b or g or n > Media Parameters (continued)**

Field	Description
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 that 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.

**Controller > 802.11b or g or n > Parameters**

Use this option to create or modify a template for configuring 802.11b/g/n parameters (such as power and channel status, data rates, channel list, and CCX location measurement) and/or applying these settings to controller(s).

The following table describes the Template Detail fields in **Design > Configuration > Feature Design > Features and Technologies > Controller > 802.11b or g or n > Parameters**.

**Table 1-23**      **Controller > 802.11b or g or n > Parameters**

Field	Description
Policy Name	Enter the name of the 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	Enter the 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.  The 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.

**Table 1-23**      **Controller > 802.11b or g or n > Parameters (continued)**

Field	Description
Dynamic Assignment	<p>From the Dynamic Assignment drop-down list, choose any one of the following dynamic transmit power assignment modes:</p> <ul style="list-style-type: none"> <li>Automatic—The transmit power is periodically updated for all access points that permit this operation.</li> <li>On Demand—Transmit power is updated when you click Assign Now.</li> <li>Disabled—No dynamic transmit power assignments occur and values are set to their global default.</li> </ul> <p>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.</p>
Dynamic Tx Power Control	<p>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.</p>
Assignment Mode	<p>From the Assignment Mode drop-down list, choose any one of the following dynamic channel assignment modes:</p> <ul style="list-style-type: none"> <li>Automatic—The channel assignment is periodically updated for all access points that permit this operation.</li> <li>On Demand—Channel assignments are updated when desired.</li> <li>Disabled—No dynamic channel assignments occur and values are set to their global default.</li> </ul> <p>The default is Automatic.</p>
Avoid Foreign AP Interference	<p>Enable this Radio Resource Management (RRM) foreign 802.11 interference-monitoring field 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.</p> <p>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.</p>
Avoid Cisco AP Load	<p>Enable this Radio Resource Management (RRM) bandwidth-sensing field 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.</p> <p>In certain circumstances and with denser deployments, there might not be enough channels to properly create perfect channel reuse. In these circumstances, Radio Resource Management can assign better reuse patterns to those APs that carry more traffic load.</p>

**Table 1-23**      **Controller > 802.11b or g or n > Parameters (continued)**

Field	Description
Avoid non 802.11 Noise	<p>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.</p> <p>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.</p>
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	<p>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, and 54 Mbps.</p> <p>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.</p>
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 parameter enhances the location accuracy of clients.
Interval	<p>Interval in seconds between measurement requests.</p> <p>The Cisco Compatible Extension location measurement interval can be changed only when measurement mode is enabled.</p>

**Controller > 802.11b or g or n > Roaming Parameters**

The following table describes the Template Detail fields in **Design > Configuration > Feature Design > Features and Technologies > Controller > 802.11b or g or n > Roaming Parameters**.

**Table 1-24**      **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.
Adaptive Scan Threshold	<p>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.</p> <p><b>Note</b> The Scan Threshold and Transition Time parameters guarantee a minimum level of client roaming performance. Together with the highest expected client speed and roaming hysteresis, these parameters make it possible to design a wireless LAN network that supports roaming simply by ensuring a certain minimum overlap distance between access points.</p>
Transition Time	<p>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.</p> <p><b>Note</b> The Scan Threshold and Transition Time parameters guarantee a minimum level of client roaming performance. Together with the highest expected client speed and roaming hysteresis, these parameters make it possible to design a wireless LAN network that supports roaming simply by ensuring a certain minimum overlap distance between access points.</p>

**Controller > CLI > General**

Use this option to create templates containing a set of CLI commands and apply them to one or more controllers from Prime Infrastructure. These templates are meant for provisioning features in multiple controllers for which there is no SNMP support or custom Prime Infrastructure user interface. The template contents are simply a command array of strings. No support for substitution variables, conditionals, and the like exist.

The CLI sessions to the device are established based on user preferences. The default protocol is SSH.

**Note**

If the Controller Telnet credentials check fails or the Controller CLI template fails with an invalid username and password even though the correct username and password are configured on the controller, check whether the controller has exceeded the number of CLI connections it can accept. If the connections have exceeded the maximum limit, then either increase the maximum allowed CLI sessions or terminate any preexisting CLI sessions on the controller, and then retry the operation.

The following table describes the Template Detail fields on **Design > Configuration > Feature Design > Features and Technologies > Controller > CLI > General**.

**Table 1-25**      **Controller > CLI > General**

Field	Description
Commands	Enter the series of CLI commands.
Refresh Config after Apply	Select the <b>Refresh Config after Apply</b> check box to perform a refresh config on the controller after the CLI template is applied successfully.
Save Config to Flash after apply	Select the <b>Save Config to Flash after apply</b> check box to save the configuration.
Reboot Controller after apply	Select the <b>Reboot Controller after apply</b> check box to reboot the controller.
Ignore errors on Apply Template to Controllers	Select the <b>Ignore errors on Apply Template to Controllers</b> to ignore all the errors while applying the template.

## Controller > FlexConnect > FlexConnect AP Groups

The following table describes the Template Detail fields in **Design > Configuration > Feature Design > Features and Technologies > Controller > FlexConnect > FlexConnect AP Groups**.

**Table 1-26**      **Controller > FlexConnect > FlexConnect AP Groups**

Field	Description
<b>General</b>	
Primary RADIUS	The primary RADIUS authentication servers for this AP group. If a RADIUS authentication server is not present on the controller, Prime Infrastructure configured RADIUS server does not apply.
Port Number	Enter the port number. of the primary RADIUS server.
Shared Secret	Enter the shared secret in the text box.
Confirm Shared Secret	Re-enter the shared secret.
Secondary RADIUS	The secondary RADIUS authentication servers for this AP group. If a RADIUS authentication server is not present on the controller, Prime Infrastructure configured RADIUS server does not apply.
Port Number	Enter the port number of the secondary RADIUS server.
Shared Secret	Enter the shared secret in the text box.
Confirm Shared Secret	Re-enter the shared secret.

Table 1-26 Controller &gt; FlexConnect &gt; FlexConnect AP Groups (continued)

Field	Description
<b>FlexConnect AP</b>	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 <b>Ethernet MAC</b> check box to unselect an access point from one of the groups. You can save this change or apply it to controllers.
<b>FlexConnect Configuration</b>	Enables local authentication for a FlexConnect group. <b>Note</b> Make sure that the Primary RADIUS Server and Secondary RADIUS Server fields are set to <b>None</b> on the General tab.
FlexConnect Local Authentication	Enables local authentication for this FlexConnect group. The default value is unselected. <b>Note</b> When you attempt to use this feature, a warning message indicates that it is a licensed feature. <b>Note</b> You can click the <b>Users configured in the group</b> 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	Allows a FlexConnect access point to authenticate clients using LEAP. To allow a FlexConnect access point to authenticate clients using EAP-FAST, select the <b>EAP-FAST</b> check box. To use manual PAC provisioning, enter the key used to encrypt and decrypt PACs in the <b>EAP-FAST Key</b> and <b>Confirm EAP-FAST Key</b> text boxes.
Auto Key Generation	Allows PACs to be sent automatically to clients that do not have one during PAC provisioning.
EAP-FAST Key	The authority identifier of the EAP-FAST server. The identifier must be 32 hexadecimal characters.
EAP-FAST Authority ID	The authority identifier of the EAP-FAST server in text format. You can enter up to 32 hexadecimal characters.
EAP-FAST Authority Info	The authority information of the EAP-FAST server.
EAP-FAST Pac Timeout	The number of seconds for the PAC to remain viable in the edit box. The valid range is 2 to 4095 seconds.
<b>Image Upgrade</b>	
FlexConnect AP Upgrade	Select to upgrade the FlexConnect access points.
Slave Maximum Retry Count	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 <b>FlexConnect AP Upgrade</b> check box. <b>Note</b> You can add an access point as a master access point only if the <b>FlexConnect AP Upgrade</b> check box is enabled on the General tab.
<b>VLAN-ACL Mapping</b>	Use the edit table on this tab to add VLAN-ACL mappings.
VLAN ID	The valid VLAN ID range is 1 to 4094.
Ingress ACL	Choose an Ingress ACL.
Egress ACL	Choose an Egress ACL.
<b>WLAN-ACL Mapping</b>	Use the edit table on this tab to add WLAN-ACL mappings.
WLAN ID	WLAN ID.
WLAN Profile Name	Choose a WLAN profile.



**Table 1-26**      **Controller > FlexConnect > FlexConnect AP Groups (continued)**

Field	Description
WebAuth ACL	Choose a WebAuth ACL.
<b>Web Policies</b>	Use the edit table on this tab to add or select Web Policy ACLs.
Web-Policy ACL	Choose a Web Policy ACL. You can add up to a maximum of 16 Web-Policy ACLs.
<b>Local Split</b>	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.
<b>Central DHCP</b>	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 > IPv6

The following topics contain field descriptions for pages found in **Design > Configuration > Feature Design > Features and Technologies > Controller > IPv6**.

- [Controller > IPv6 > Neighbor Binding Timers, page 1-25](#)
- [Controller > IPv6 > RA Guard, page 1-26](#)
- [Controller > IPv6 > RA Throttle Policy, page 1-26](#)

### Controller > IPv6 > Neighbor Binding Timers

The following table describes the Template Detail fields in **Design > Configuration > Feature Design > Features and Technologies > Controller > IPv6 > Neighbor Binding Timers**.

**Table 1-27**      **Controller > IPv6 > Neighbor Binding Timers**

Field	Description
Down Lifetime Interval	This field enables the down lifetime. If you have selected this check box, specify the value in the Down Lifetime Interval text box. This down lifetime interval indicates the maximum time, in seconds, an entry learned from a down interface is kept in the binding table before the entry is deleted or proof is received that the entry is reachable. The range is 0 to 86400 seconds, and the default value is 0.
Reachable Lifetime Interval	This field enables the reachable lifetime. If you have selected this check box, specify the value in the Reachable Lifetime Interval text box. The reachable lifetime interval indicates the maximum time, in seconds, an entry is considered reachable without getting a proof of reachability (direct reachability through tracking, or indirect reachability through Neighbor Discovery protocol [NDP] inspection). After that, the entry is moved to stale. The range is 0 to 86400 seconds, and the default value is 0.
Stale Lifetime Interval	This field enables the stale lifetime. If you have selected this check box, specify the value in the Stale Lifetime Interval text box. The stale lifetime interval indicates the maximum time, in seconds, a stale entry is kept in the binding table before the entry is deleted or proof is received that the entry is reachable. The range is 0 to 86400 seconds, and the default value is 0.

**Controller > IPv6 > RA Guard**

RA Guard is a Unified Wireless solution used to drop RA from wireless clients. It is configured globally, and by default it is enabled. You can create or modify a template for configuring IPv6 Router Advertisement parameters.

**Controller > IPv6 > RA Throttle Policy**

Use this option to limit the amount of multicast Router Advertisements (RA) circulating on the wireless network. You can create or modify a template for configuring IPv6 Router Advertisement parameters such as RA Throttle Policy, Throttle Period, and other options.

The following table describes the Template Detail fields in **Design > Configuration > Feature Design > Features and Technologies > Controller > Down Lifetime IntervalIPv6 > RA Throttle Policy**.

**Table 1-28**      **Controller > IPv6 > RA Throttle Policy**

Field	Description
RA Throttle Policy	Enables the RA throttle policy.
Throttle Period	Duration of the throttle period in seconds. The range is 10 to 86400 seconds.
Max Through	The number of RA that passes through over a period in seconds.
Interval Option	Indicates the behavior in case of RA with an interval option.
Allow At-least	Indicates the minimum number of RA <i>not</i> throttled per router.
Allow At-most	Indicates the maximum number of RA <i>not</i> throttled per router.

**Controller > Location**

The following topics contain field descriptions for pages found in **Design > Configuration > Feature Design > Features and Technologies > Controller > Location**.

- [Controller > Location > Location Configuration > General, page 1-26](#)
- [Controller > Location > Location Configuration > Advanced, page 1-27](#)

**Controller > Location > Location Configuration > General**

The following table describes the Template Detail fields on **Design > Configuration > Feature Design > Features and Technologies > Controller > Location > Location Configuration > General**.

**Table 1-29**      **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 <b>config rfid status enable</b> command 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.

**Table 1-29**      **Controller > Location > Location Configuration > General (continued)**

Field	Description
Normal Client	Select the check box to have a noncalibrating 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 <a href="#">Cisco Context Aware and Location FAQ</a> .
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.

**Controller > Location > Location Configuration > Advanced**

The following table describes the Template Detail fields on **Design > Configuration > Feature Design > Features and Technologies > Controller > Location > Location Configuration > Advanced**.

**Table 1-30**      **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.

**Controller > Management**

The following topics contain field descriptions for pages found in **Design > Configuration > Feature Design > Features and Technologies > Controller > Management**.

- [Controller > Management > Legacy Syslog, page 1-27](#)
- [Controller > Management > Local Management User, page 1-28](#)
- [Controller > Management > Telnet SSH, page 1-28](#)
- [Controller > Management > Trap Control, page 1-29](#)
- [Controller > Management > Trap Receiver, page 1-30](#)

**Controller > Management > Legacy Syslog****Note**

Legacy Syslog applies to controllers Version 5.0.6.0 and earlier.

For basic information about creating this template, see the Creating Feature-Level Configuration Templates section in the [Cisco Prime Infrastructure 2.0 User Guide](#).

**Controller > Management > Local Management User**

Use this option to configure local users, their privilege level, and password.

The following table describes the Template Detail fields on **Design > Configuration > Feature Design > Features and Technologies > Controller > Management > Local Management User**.

**Table 1-31**      **Controller > Management > Local Management User**

Field	Description
User Name	Enter a template username.
Password	Enter a password for this local management user template.
Confirm Password	Reenter the password.
Access Level	Use the Access Level drop-down list to choose either <b>Read Only</b> or <b>Read Write</b> .
Update Telnet Credentials	Select the <b>Update Telnet Credentials</b> check box to update the user credentials in Prime Infrastructure for Telnet/SSH access.  <b>Note</b> If the template is applied successfully and the Update Telnet Credentials option is enabled, the applied management user credentials are used in Prime Infrastructure for Telnet/SSH credentials to that applied controller.

**Controller > Management > Telnet SSH**

The following table describes the Template Detail fields on **Design > Configuration > Feature Design > Features and Technologies > Controller > Management > Telnet SSH**.

**Table 1-32**      **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 or select 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 or select No to disallow them. The default is Yes.

**Controller > Management > Trap Control**

The following table describes the Template Detail fields in **Design > Configuration > Feature Design > Features and Technologies > Controller > Management > Trap Control**.

**Table 1-33**      **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	Select the <b>Link (Port) Up/Down</b> check box to change the state to up or down.
Multiple Users	Select the <b>Multiple Users</b> check box to allow two users to log in with the same login ID.
Spanning Tree	Select the <b>Spanning Tree</b> check box to enable spanning tree traps. See the STP specification for descriptions of individual parameters.
Rogue AP	Select the <b>Rogue AP</b> check box to send a trap with the MAC address whenever a rogue access point is detected or when a rogue access point was detected earlier and no longer exists.
Controller Config Save	Select the <b>Controller Config Save</b> check box to send a notification when the configuration is modified.
802.11 Association	Select the <b>802.11 Association</b> check box to send a trap when a client is associated to a WLAN. This trap does not guarantee that the client is authenticated.
802.11 Disassociation	Select the <b>802.11 Disassociation</b> check box to send the disassociate notification when the client sends a disassociation frame.
802.11 Deauthentication	Select the <b>802.11 Deauthentication</b> check box to send the deauthenticate notification when the client sends a deauthentication frame.
802.11 Failed Authentication	Select the <b>802.11 Failed Authentication</b> check box to send the authenticate failure notification when the client sends an authentication frame with a status code other than successful.
802.11 Failed Association	Select the <b>802.11 Failed Association</b> check box to send the associate failure notification when the client sends an association frame with a status code other than successful.
Excluded	Select the <b>Excluded</b> check box to send the associate failure notification when a client is excluded.
AP Register	Select the <b>AP Register</b> check box to send a notification when a access point associates or disassociates with the controller.
AP Interface Up/Down	Select the <b>AP Interface Up/Down</b> check box to send a notification when a access point interface (802.11a/n or 802.11b/g/n) status goes up or down.
Load Profile	Select the <b>Load Profile</b> check box to send a notification when the load profile state changes between PASS and FAIL.
Noise Profile	Select the <b>Noise Profile</b> check box to send a notification when the noise profile state changes between PASS and FAIL.
Interference Profile	Select the <b>Interference Profile</b> check box to send a notification when the interference profile state changes between PASS and FAIL.

**Table 1-33**      **Controller > Management > Trap Control (continued)**

Field	Description
Coverage Profile	Select the <b>Coverage Profile</b> check box to send a notification when the coverage profile state changes between PASS and FAIL.
Channel Update	Select the <b>Channel Update</b> check box to send a notification when the dynamic channel algorithm of an access point is updated.
Tx Power Update	Select the <b>Tx Power Update</b> check box to send a notification when the dynamic transmit power algorithm of an access point is updated.
User Auth Failure	Select the <b>User Auth Failure</b> check box to send a trap to inform you that a client RADIUS authentication failure has occurred.
RADIUS Server No Response	Select the <b>RADIUS Server No Response</b> check box to send a trap to indicate that no RADIUS server(s) are responding to authentication requests sent by the RADIUS client.
ESP Authentication Failure	Select the check box to send a IPsec packets with invalid hashes were found in an inbound ESP SA.
ESP Replay Failure	Select the <b>ESP Authentication Failure</b> check box to send a notification when IPsec packets with invalid sequence numbers were found in an inbound ESP SA.
Invalid SPI	Select the <b>Invalid SPI</b> check box to send a notification when a packet with an unknown SPI is detected from the specified peer with the specified SPI using the specified protocol.
IKE Negotiation Failure	Select the check box <b>IKE Negotiation Failure</b> to send a notification when an attempt to negotiate a phase 1 IKE SA fails. 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	Select the <b>IKE Suite Failure</b> check box to send a notification when a attempt to negotiate a phase 2 SA suite for the specified selector fails. The current total failure counts are passed as well as the notification type counts for the notify involved in the failure.
Invalid Cookie	Select the <b>Invalid Cookie</b> check box to send a notification when ISAKMP packets with invalid cookies are detected from the specified source, intended for the specified destination. The initiator and responder cookies are also sent with the trap.
WEP Decrypt Error	Select the <b>WEP Decrypt Error</b> check box to send a notification when the controller detects a WEP decrypting error.
Signature Attack	Select the <b>Signature Attack</b> check box to enable the 802.11 security trap.

**Controller > Management > Trap Receiver**

If you have monitoring devices on your network that receive SNMP traps, you can use this page to add a trap receiver template.

The following table describes the Template Detail fields in **Design > Configuration > Feature Design > Features and Technologies > Controller > Management > Trap Receiver**.

**Table 1-34**      **Controller > Management > Trap Receiver**

Field	Description
IP Address	Enter the IP address of the server.
Admin Status	Select this check box to enable the administrator status if you want SNMP traps to be sent to the receiver.

## Controller > Mesh > Mesh Settings

Use this option to configure an access point to establish a connection with the controller.

The following table describes the Template Detail fields in **Design > Configuration > Feature Design > Features and Technologies > Controller > Mesh > Mesh Settings**.

**Table 1-35**      **Controller > Mesh > Mesh Settings**

Field	Description
RootAP to MeshAP Range	The Root AP to Mesh AP Range is 12000 feet by default. Enter the optimum distance (in feet) that should exist between the root access point and the mesh access point. This global field applies to all access points when they join the controller and all existing access points in the network.
Client Access on Backhaul Link	The <b>Client Access on Backhaul Link</b> check box is not selected by default. When this option is enabled, mesh access points can associate with 802.11a/n wireless clients over the 802.11a/n backhaul. This client association is in addition to the existing communication on the 802.11a/n backhaul between the root and mesh access points.  <b>Note</b> This feature applies only to access points with two radios.
Background Scanning	Select the <b>Background Scanning</b> check box to enable background scanning or unselect it to disable the feature. The default value is disabled. Background scanning allows Cisco Aironet 1510 Access Points to actively and continuously monitor neighboring channels for more optimal paths and parents.
Mesh DCA Channels	The <b>Mesh DCA Channels</b> check box is not selected by default. Select this option to enable backhaul channel deselection on the Controller using the DCA channel list configured in the Controller. Any change to the channels in the Controller DCA list is pushed to the associated access points. This feature applies only to the 1524SB mesh access points. For more information on this feature, see the <i>Controller Configuration Guide</i> .
Global Public Safety	Select the <b>Global Public Safety</b> check box to enable global public safety.
Security Mode	From the Security Mode drop-down list, choose <b>EAP</b> (Extensible Authentication Protocol) or <b>PSK</b> (pre-shared key).

## Controller > PMIP

Proxy Mobile IPv6 is a network-based mobility management protocol that supports a mobile node by acting as the proxy for the mobile node in any IP mobility-related signaling. The mobility entities in the network track the movements of the mobile node and initiate the mobility signaling and set up the required routing state.

The main functional entities are the Local Mobility Anchor (LMA) and Mobile Access Gateway (MAG). The LMA maintains the reachability state of the mobile node and is the topological anchor point for the IP address of the mobile node. The MAG performs the mobility management on behalf of a mobile node. The MAG resides on the access link where the mobile node is anchored. The controller implements the MAG functionality.

The following topics contain field descriptions for pages found in **Design > Configuration > Feature Design > Features and Technologies > Controller > PMIP**.

- [Controller > PMIP > Global Config, page 1-32](#)
- [Controller > PMIP > LMA Config, page 1-32](#)
- [Controller > PMIP > PMIP Profile, page 1-33](#)

**Controller > PMIP > Global Config**

The following table describes the Template Detail fields on **Design > Configuration > Feature Design > Features and Technologies > Controller > PMIP > Global Config**.

**Table 1-36**      **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 from 0 to 40000.
Binding Lifetime	Lifetime of the binding entries in the controller. The valid range is from 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 from 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 from 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 from 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 from 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 from 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 from 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 from 1 to 10. The default value is 1.

**Controller > PMIP > LMA Config**

The following table describes the Template Detail fields on **Design > Configuration > Feature Design > Features and Technologies > Controller > PMIP > LMA Config**.

**Table 1-37**      **Controller > PMIP > LMA Config**

Field	Description
LMA Name	Name of the LMA connected to the controller.
LMA IP Address	IP address of the LMA connected to the controller.



**Controller > PMIP > PMIP Profile**

The following table describes the Template Detail fields on **Design > Configuration > Feature Design > Features and Technologies > Controller > PMIP > PMIP Profile**.

**Table 1-38**      **Controller > PMIP > PMIP Profile**

Field	Description
PMIP Profile	Enter the profile name, then click <b>Add</b> .
Network Access Identifier	Name of the Network Access Identifier (NAI) associated with the profile.
LMA Name	Name of the LMA with which the profile is to be associated.
Access Point Node	Name of the access point node connected to the controller.

**Controller > Security**

The following topics contain field descriptions for pages found in **Design > Configuration > Feature Design > Features and Technologies > Controller > Security**.

- [Controller > Security > AAA > LDAP Servers, page 1-34](#)
- [Controller > Security > AAA > RADIUS Acct Servers, page 1-34](#)
- [Controller > Security > AAA > RADIUS Auth Servers, page 1-35](#)
- [Controller > Security > AAA > TACACS+ Servers, page 1-37](#)
- [Controller > Security > Local EAP > EAP-FAST Parameters, page 1-38](#)
- [Controller > Security > Local EAP > General - Local EAP, page 1-38](#)
- [Controller > Security > Local EAP > Local EAP Profiles, page 1-39](#)
- [Controller > Security > Wireless Protection Policies > Friendly Access Point, page 1-40](#)
- [Controller > Security > Wireless Protection Policies > Ignored Rogue AP, page 1-41](#)
- [Controller > Security > Wireless Protection Policies > Rogue AP Rules, page 1-42](#)
- [Controller > Security > Wireless Protection Policies > Rogue Policies, page 1-43](#)
- [Controller > Security > Access Control Lists, page 1-44](#)
- [Controller > Security > CPU Access Control List, page 1-44](#)
- [Controller > Security > File Encryption, page 1-44](#)
- [Controller > Security > IP Groups, page 1-44](#)
- [Controller > Security > IPv6 Groups, page 1-45](#)
- [Controller > Security > Protocol Groups, page 1-45](#)

**Controller > Security > AAA > LDAP Servers**

This section explains how to configure a Lightweight Directory Access Protocol (LDAP) server as a backend database, similar to a RADIUS or local user database. An LDAP backend database allows the controller to query an LDAP server for the credentials (username and password) of a particular user. These credentials are then used to authenticate the user. For example, local EAP might use an LDAP server as its backend database to retrieve user credentials.

The following table describes the Template Detail fields in **Design > Configuration > Feature Design > Features and Technologies > Controller > Security > AAA > LDAP Servers**.

**Table 1-39**      **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 <b>Authenticated</b> or <b>Anonymous</b> . 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.
Retransmit Timeout	Enter the number of seconds between retransmissions. The valid range is from 2 to 30 seconds, and the default value is 2 seconds.
Admin Status	Select the <b>Enable</b> check box if you want the LDAP server to have administrative privileges.

**Controller > Security > AAA > RADIUS Acct Servers**

This page allows you to add a RADIUS accounting template or make modifications to an existing RADIUS accounting template.

The following table describes the Template Detail fields in **Design > Configuration > Feature Design > Features and Technologies > Controller > Security > AAA > RADIUS Acct Servers**.

**Table 1-40**      **Controller > Security > AAA > RADIUS Acct Servers**

Field	Description
Server Address	Enter the server address.
Port Number	Enter the port address.
Shared Secret Format	Choose either <b>ASCII</b> or <b>Hex</b> .  <b>Note</b> Regardless of the format you choose, for security reasons, only ASCII is visible on the wireless lan controller (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 Confirm Shared Secret	Enter and confirm the RADIUS shared secret used by the server you specified.
Admin Status	Select the <b>Enable</b> check box if you want to establish administrative privileges for the server.

**Table 1-40**      **Controller > Security > AAA > RADIUS Acct Servers (continued)**

Field	Description
Network User	Select if you want to enable the network user authentication. If this option is enabled, this entry is considered as the RADIUS authenticating server for the network user.
Retransmit Timeout	Specify the time in seconds after which the RADIUS authentication request times out and a retransmission by the controller occurs. You can specify a value from 2 to 30 seconds.
IPsec Enable	Select the <b>Enable</b> check box to enable IP security.

**Controller > Security > AAA > RADIUS Auth Servers**

Use this option to add a RADIUS authentication template or make modifications to an existing template. After these server templates are configured, controller users who log in to the controller through the CLI or GUI are authenticated.

The following table describes the Template Detail fields in **Design > Configuration > Feature Design > Features and Technologies > Controller > Security > AAA > RADIUS Auth Servers**.

**Table 1-41**      **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 <b>ASCII</b> or <b>hex</b> .  <b>Note</b> 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.
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: <ul style="list-style-type: none"> <li>Shared Secret Format: Enter ASCII or hexadecimal.</li> </ul> <b>Note</b> 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. <ul style="list-style-type: none"> <li>KEK Shared Secret: Enter the KEK shared secret.</li> <li>MACK Shared Secret: Enter the MACK shared secret.</li> </ul> <b>Note</b> Each time the controller is notified with the shared secret, the existing shared secret is overwritten with the new shared secret.
Admin Status	Select if you want to enable administration privileges.

**Table 1-41**      **Controller > Security > AAA > RADIUS Auth Servers (continued)**

Field	Description
Support for RFC 3576	Select 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	Select 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	Select 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 from 2 to 30 seconds.
IPsec	If you click to enable the IP security mechanism, additional IP security fields are added to the page.
IPsec Authentication	<p>Choose which IP security authentication protocol to use. The options are <b>HMAC-SHA1</b>, <b>HMAC-MD5</b>, and <b>None</b>.</p> <p>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</p>
IPsec Encryption	<p>Select the IP security encryption mechanism to use:</p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• Triple DES—Data Encryption Standard that applies three keys in succession.</li> <li>• 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 Block Chaining (CBC) mode.</li> <li>• None—No IP security encryption mechanism.</li> </ul>
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.

**Table 1-41**      **Controller > Security > AAA > RADIUS Auth Servers (continued)**

Field	Description
Lifetime	Set the timeout interval (in seconds) when the session expires.
IKE Diffie Hellman Group	<p>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.</p> <p>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-based or Group 2-based keys might occur slightly faster because of their smaller prime number size.</p>

**Controller > Security > AAA > TACACS+ Servers**

Use this option to add a TACACS+ server or make modifications to an existing TACACS+ server template. After these server templates are configured, controller users who log in to the controller through the CLI or GUI are authenticated.

The following table describes the Template Detail fields in **Design > Configuration > Feature Design > Features and Technologies > Controller > Security > AAA > TACACS+ Servers**.

**Table 1-42**      **Controller > Security > AAA > TACACS+ Servers**

Field	Description
Server Type	<p>Select one or more server types by selecting their respective check boxes. The following server types are available:</p> <ul style="list-style-type: none"> <li>• authentication—Server for user authentication/authorization.</li> <li>• authorization—Server for user authorization only.</li> <li>• accounting—Server for RADIUS user accounting.</li> </ul>
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	<p>Choose either <b>ASCII</b> or <b>hex</b>.</p> <p>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.</p>
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	Select 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 > EAP-FAST Parameters**

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 are used to perform mutual authentication with the RADIUS server through the access point. This page allows you to add an EAP-FAST template or make modifications to an existing EAP-FAST template.

The following table describes the Template Detail fields in **Design > Configuration > Feature Design > Features and Technologies > Controller > Security > Local EAP > EAP-FAST Parameters**.

**Table 1-43**      **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.
Server Key and Confirm Server Key	Enter the key (in hexadecimal characters) used to encrypt and decrypt PACs.
Anonymous Provision	Select 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 > Local EAP > General - Local EAP**

This page allows you to specify a timeout value for local EAP. You can then add or make changes to an existing local EAP general template.

**Note**

If any RADIUS servers are configured on the controller, the controller tries to authenticate the wireless clients using the RADIUS servers first. Local EAP is attempted only if no RADIUS servers are found, either because the RADIUS servers timed out or no RADIUS servers were configured. If four RADIUS servers are configured, the controller attempts to authenticate the client with the first RADIUS server, then the second RADIUS server, and then local EAP. If the client attempts to then reauthenticate manually, the controller tries the third RADIUS server, then the fourth RADIUS server, and then local EAP.

The following table describes the Template Detail fields in **Design > Configuration > Feature Design > Features and Technologies > Controller > Security > Local EAP > General - Local EAP**.

**Table 1-44**      **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
<b>Note</b>	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 milliseconds)
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**

This page allows you to add a local EAP profile template or make modifications to an existing template. Local EAP is an authentication method that allows users and wireless clients to be authenticated locally. 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. When you enable local EAP, the controller serves as the authentication server and the local user database, thereby removing dependence on an external authentication server. Local EAP retrieves user credentials from the local user database or the LDAP backend database to authenticate users.



**Note** The LDAP backend database supports only these local EAP methods: EAP-TLS and EAP-FAST with certificates. LEAP and EAP-FAST with PACs are not supported for use with the LDAP backend database.

The following table describes the Template Detail fields in **Design > Configuration > Feature Design > Features and Technologies > Controller > Security > Local EAP > Local EAP Profiles**.

**Table 1-45**      **Controller > Security > Local EAP > Local EAP Profiles**

Field	Description
EAP Profile Name	User-defined identification.
Select Profile Methods	Choose the desired authentication type: <ul style="list-style-type: none"> <li>• LEAP—This authentication type leverages Cisco Key Integrity Protocol (CKIP) and Multi-Modal Hashing (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.</li> <li>• 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.</li> <li>• 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.</li> <li>• 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.</li> </ul>
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	Select 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	Select if you want the common name (CN) in the incoming certificate to be validated against the common name of the CA certificate.
Check Against Date Validity	Select if you want the controller to verify that the incoming device certificate is still valid and has not expired.
Local Certificate Required	Select if a local certificate is required.
Client Certificate Required	Select if a client certificate is required.

**Controller > Security > Wireless Protection Policies > Friendly Access Point**

This template allows you to import friendly internal access points. Importing these friendly access points prevents nonlightweight access points from being falsely identified as rogues.

**Note**

*Friendly Internal* access points were previously referred to as *Known APs*.

The Friendly AP page identifies the MAC address of an access point, status, any comments, and whether or not the alarm is suppressed for this access point.

Friendly access points can be added by either importing the access point or manually entering the access point information:

- To import an access point using the Import feature:
  - Select the **Import from File** check box.



- Enter the file path or click **Browse** to navigate to the correct file.

**Note**

Use a line break to separate MAC addresses in the file that you import. For example, enter the MAC addresses as follows:

```
00:00:11:22:33:44
00:00:11:22:33:45
00:00:11:22:33:46
```

- To manually add an access point:

- 
- Step 1** Unselect the **Import from File** check box.
- Step 2** Enter the MAC address for the access point.
- Step 3** Choose **Internal** access point from the Status drop-down list.
- Step 4** Enter a comment regarding this access point, if necessary.
- Step 5** Select the **Suppress Alarms** check box to suppress all alarms for this access point.
- 

## Controller > Security > Wireless Protection Policies > Ignored Rogue AP

The Ignored Rogue AP Template page allows you to create or modify a template for importing ignored access points. Access points in the Ignored AP list are not identified as rogues.

An Ignored Rogue AP template does not get applied to any controller. It suppresses the rogue AP/Adhoc alarm if Ignored Rogue AP Template has the rogue MAC address when the controller reports the Rogue AP to Prime Infrastructure and this MAC address is added to the Rogue AP Ignore-List on the controller.

Ignored rogue access points can be added by either importing the access point or manually entering the access point information:

- 
- Step 1** To import an ignored rogue access point using the Import feature:
- Step 2** Select the **Import from File** check box.
- Step 3** Enter the file path or use the **Browse** button to navigate to the correct file. The import file must be a CSV file with MAC address (one MAC Address per line).

**Note**

For example, enter the MAC addresses as follows:

```
00:00:11:22:33:44
00:00:11:22:33:45
00:00:11:22:33:46
```

---

To manually add an ignored rogue access point unselect the **Import from File** check box.

---

**Controller > Security > Wireless Protection Policies > Rogue AP Rules**

Rogue access point rules allow you to define rules to automatically classify rogue access points. Prime Infrastructure applies the rogue access point classification rules to the controllers. These rules can limit the appearance of a rogue on maps based on RSSI level (weaker rogue access points are ignored) and time limit (a rogue access point is not flagged unless it is seen for the indicated period of time).

The rogue access point rules also help reduce false alarms.

Rogue classes include the following types:

- **Malicious Rogue**—A detected access point that matches the user-defined malicious rules or has been manually moved from the Friendly AP category.
- **Friendly Rogue**—Known, acknowledged, or trusted access point or a detected access point that matches user-defined friendly rules.
- **Unclassified Rogue**—A detected access point that does not match the malicious or friendly rules.

The following table describes the Template Detail fields in **Design > Configuration > Feature Design > Features and Technologies > Controller > Security > Wireless Protection Policies > Rogue AP Rules**.

**Table 1-46**      **Controller > Security > Wireless Protection Policies > Rogue AP Rules**

Field	Description
Rule Type	Choose <b>Malicious</b> or <b>Friendly</b> from the drop-down list. A rogue is considered malicious if a detected access point matches the user-defined malicious rules or has been manually moved from the Friendly AP category. A rogue is considered friendly if it is a known, acknowledged, or trusted access point or a detected access point that matches the user-defined Friendly rules.
Match Type	Choose <b>Match All Conditions</b> or <b>Match Any Condition</b> .
Open Authentication	Select the check box to enable open authentication.
Match Managed AP SSID	Select the check box to enable the matching of a managed AP SSID.  <b>Note</b> Managed SSIDs are the SSIDs configured for the WLAN and known to the system.
Match User Configured SSID	Select the check box to enable the matching of user-configured SSIDs.  <b>Note</b> User-configured SSIDs are the SSIDs that are manually added. Enter the user-configured SSIDs (one per line) in the Match User Configured SSID text box.
Minimum RSSI	Select the check box to enable the Minimum RSSI threshold limit.  <b>Note</b> Enter the minimum RSSI threshold level (dB) in the text box. The detected access point is classified as malicious if it is detected above the indicated RSSI threshold.
Time Duration	Select the check box to enable the Time Duration limit.  <b>Note</b> Enter the time duration limit (in seconds) in the text box. The detected access point is classified as malicious if it is viewed for a longer period of time than the indicated time limit.
Minimum Number Rogue Clients	Select the check box to enable the Minimum Number Rogue Clients limit. Enter the minimum number of rogue clients allowed. The detected access point is classified as malicious if the number of clients associated to the detected access point is greater than or equal to the indicated value.

**Controller > Security > Wireless Protection Policies > Rogue Policies**

This page enables you to configure the rogue policy (for access points and clients) applied to the controller.

The following table describes the Template Detail fields in **Design > Configuration > Feature Design > Features and Technologies > Controller > Security > Wireless Protection Policies > Rogue Policies**.

**Table 1-47**      **Controller > Security > Wireless Protection Policies > Rogue Policies**

Field	Description
Rogue Location Discovery Protocol	<p>Determine whether or not the Rogue Location Discovery Protocol (RLDP) is connected to the enterprise wired network. Choose one of the following:</p> <ul style="list-style-type: none"> <li>• <b>Disable</b>—Disables RLDP on all access points.</li> <li>• <b>All APs</b>—Enables RLDP on all access points.</li> <li>• <b>Monitor Mode APs</b>—Enables RLDP only on access points in monitor mode.</li> </ul> <p><b>Note</b> 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.</p>
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 from 10 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	<p>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 from -70 to -128 dBm, and the default value is -128 dBm. This feature is applicable to all the AP modes.</p> <p>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.</p>
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. The valid range is from 120 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	Select to enable the AAA validation of rogue clients.
Detect and Report Adhoc Networks	Select to enable detection and reporting of rogue clients participating in ad hoc networking.
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 > Access Control Lists**

The following table describes the Template Detail fields in **Design > Configuration > Feature Design > Features and Technologies > Controller > Security > Access Control Lists**.

**Table 1-48**      **Controller > Security > Access Control Lists**

Field	Description
ACL Type	IPv6 is supported from controller Version 7.2.x.

**Related Topics**

- To create reusable grouped IP addresses, see [Controller > Security > IP Groups, page 1-44](#).
- To create a new protocol group, see [Controller > Security > Protocol Groups, page 1-45](#).

**Controller > Security > CPU Access Control List****Note**

CPU ACL configuration with IPv6 is not supported in this release because all IP addresses of controllers on interfaces use IPv4 except the virtual interface.

Use the existing ACLs established in the Creating a FlexConnect Access Control List Template (see the [Cisco Prime Infrastructure 2.0 User Guide](#)) to set traffic controls between the Central Processing Unit (CPU) and Network Processing Unit (NPU).

**Controller > Security > File Encryption**

This page enables you to add a file encryption template or make modifications to an existing file encryption template.

The following table describes the Template Detail fields in **Design > Configuration > Feature Design > Features and Technologies > Controller > Security > File Encryption**.

**Table 1-49**      **Controller > Security > File Encryption**

Field	Description
Encryption Key Confirm Encryption Key	Enter an encryption key text string of exactly 16 ASCII characters.

**Controller > Security > IP Groups**

The following table describes the Template Detail fields on **Design > Configuration > Feature Design > Features and Technologies > Controller > Security > IP Groups**.

**Related Topics**

To create IPv6 groups, see [Controller > Security > IPv6 Groups, page 1-45](#).

**Table 1-50**      **Controller > Security > IP Groups**

Field	Description
IP Address	Enter an IPv4 address format.
NetmaskNotation	Netmask allows you 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.
CIDR Notation	Classless InterDomain Routing (CIDR) notation is a protocol that allows the assignment of Class C IP addresses in multiple contiguous blocks. Use this protocol to add a large number of clients that exist in a subnet range by configuring a single client object.
List of IP Addresses/Netmasks	<p>All the IP address groups are listed. One IP address group can have a maximum of 128 IP address and netmask combinations. To define a new IP address group, choose <b>Add</b>. To view or modify an existing IP address group, click the URL of the IP address group. The IP address group page opens.</p> <p><b>Note</b> For the IP address of any, an <i>any</i> group is predefined.</p> <p>Use the Move Up and Move Down buttons to rearrange the order of the list items. Use the Delete button to delete any IP address or netmask.</p>

**Controller > Security > IPv6 Groups**

The following table describes the Template Detail fields on **Design > Configuration > Feature Design > Features and Technologies > Controller > Security > IPv6 Groups**.

**Related Topics**

To create IPv4 groups, see [Controller > Security > IP Groups, page 1-44](#).

**Table 1-51**      **Controller > Security > IPv6 Groups**

Field	Description
IP Address	Enter an IPv6 address format.
Prefix Length	Prefix for IPv6 addresses, ranging from 0 to 128.
List of IP Addresses/Netmasks	<p>All the IP address groups are listed. One IP address group can have a maximum of 128 IP address and netmask combinations. To define a new IP address group, choose <b>Add</b>. To view or modify an existing IP address group, click the URL of the IP address group. The IP address group page opens.</p> <p><b>Note</b> For the IP address of any, an <i>any</i> group is predefined.</p> <p>Use the Move Up and Move Down buttons to rearrange the order of the list items. Use the Delete button to delete any IP address or netmask.</p>

**Controller > Security > Protocol Groups**

The following table describes the Template Detail fields on **Design > Configuration > Feature Design > Features and Technologies > Controller > Security > Protocol Groups**.

**Table 1-52**      **Controller > Security > Protocol Groups**

Field	Description
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.
Protocol	<p>Choose a protocol from the drop-down list:</p> <ul style="list-style-type: none"> <li>Any—All protocols</li> <li>TCP—Transmission Control Protocol</li> <li>UDP—User Datagram Protocol</li> <li>ICMP—Internet Control Message Protocol</li> <li>ESP—IP Encapsulating Security Payload</li> <li>AH—Authentication Header</li> <li>GRE—Generic Routing Encapsulation</li> <li>IP—Internet Protocol</li> <li>Eth Over IP—Ethernet over Internet Protocol</li> <li>Other Port OSPF—Open Shortest Path First</li> <li>Other—Any other IANA protocol (<a href="http://www.iana.org/">http://www.iana.org/</a>)</li> </ul> <p>Some protocol choices (such as TCP or UDP) cause additional Source Port and Dest Port GUI elements to appear.</p>
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 <b>Any</b> or <b>Specific</b> from the drop-down list. If Specific is selected, enter the DSCP (0 through 255). DSCP is a packet header code that can be used to define the quality of service across the Internet.

## Controller > System

The following topics contain field descriptions for pages found in **Design > Configuration > Feature Design > Features and Technologies > Controller > System**.

- [Controller > System > AP 802.1X Supplicant Credentials, page 1-47](#)
- [Controller > System > AP Username Password, page 1-47](#)
- [Controller > System > DHCP, page 1-47](#)
- [Controller > System > General, page 1-49](#)
- [Controller > System > Global CDP Configuration, page 1-52](#)
- [Controller > System > QoS Profiles, page 1-53](#)
- [Controller > System > SNMP Community, page 1-53](#)

- [Controller > System > Traffic Stream Metrics QoS, page 1-53](#)
- [Controller > System > User Roles, page 1-54](#)
- [Controller > WLANs > WLAN Configuration, page 1-55](#)

### Controller > System > AP 802.1X Supplicant Credentials

Use this option to configure 802.1X authentication between lightweight access points and the switch. The access point acts as an 802.1X supplicant and is authenticated by the switch using EAP-FAST with anonymous PAC provisioning. You can set global authentication settings that all access points inherit as they join the controller. All access points that are currently joined to the controller and any that join in the future are included.

For basic information about creating this template, see the Creating Feature-Level Configuration Templates section in the *Cisco Prime Infrastructure 2.0 User Guide*.

### Controller > System > AP Username Password

Use this option to create or modify a template for setting an access point username and password. All access points inherit the password as they join the controller and these credentials are used to log in to the access point via the console or Telnet/SSH.

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

Also, in controller software Release 5.0, after an access point joins the controller, the access point enables console port security and you are prompted for your username and password whenever you log in to the access point console port. When you log in, you are in nonprivileged mode and you must enter the enable password to use the privileged mode.

For basic information about creating this template, see the Creating Feature-Level Configuration Templates section in the *Cisco Prime Infrastructure 2.0 User Guide*.

### Controller > System > DHCP

The following table describes the Template Detail fields in **Design > Configuration > Feature Design > Features and Technologies > Controller > System > DHCP**.

**Table 1-53**      **Controller > System > DHCP**

Field	Description
DHCP Option 82 Remote Id field format	This field provides additional security when DHCP is used to allocate network addresses. Specifically, it enables the controller to act as a DHCP relay agent to prevent DHCP client requests from untrusted sources. The controller can be configured to add option 82 information to DHCP requests from clients before forwarding the requests to the DHCP server.
DHCP Proxy	Select the <b>DHCP Proxy</b> check box to enable DHCP proxy on a global basis rather than on a WLAN basis.  When DHCP proxy is enabled on the controller, the controller unicasts DHCP requests from the client to the configured servers. At least one DHCP server must be configured on either the interface associated with the WLAN or on the WLAN itself.
DHCP Timeout	(For Controller Version 7.0.114.74 and later) Enter the DHCP timeout, in seconds.

**Controller > System > Dynamic Interface**

The following table describes the Template Detail fields in **Design > Configuration > Feature Design > Features and Technologies > Controller > System > Dynamic Interface**.

**Table 1-54** *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 netmask address of the interface.
LAG Mode	Select this check box to enable or disable LAG Mode. 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 <b>Device Info</b> or <b>File</b> . 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 the following table).

The sample CSV files are as follows.

**Table 1-55** *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 > System > General

The following table describes the Template Detail fields in **Design > Configuration > Feature Design > Features and Technologies > Controller > System > General**.

**Table 1-56**      **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 seconds.
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	

Table 1-56 Controller &gt; System &gt; General Template (continued)

Field	Description
CAPWAP Transport Mode	<p>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.</p> <p>Controllers through Version 5.2 use LWAPP and the new controller version uses CAPWAP.</p>
Broadcast Forwarding	Choose to enable or disable broadcast forwarding. The default is disabled.
LAG Mode	<p>Choose <b>Enable</b> or <b>Disable</b> 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).</p> <p>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.</p> <p>Interfaces cannot be created with the Dynamic AP Manager flag set. Also, you cannot create more than one LAG on a controller.</p>
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-the-Air AP Provision Mode drop-down list, choose <b>enable</b> or <b>disable</b> .
AP Fallback	<p>From the AP Fallback drop-down list, choose <b>enable</b> or <b>disable</b>. Enabling fallback causes an access point that lost a primary controller connection to automatically return to service when the primary controller returns.</p> <p>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 <b>enable</b> from the AP Failover Priority drop-down list if you want to allow this capability.</p>
AP Failover Priority	
Apple Talk Bridging	<p>Choose to enable or disable AppleTalk bridging.</p> <p>This AppleTalk bridging option is not available on Cisco 5500 series controllers.</p>

**Table 1-56**      **Controller > System > General Template (continued)**

Field	Description
Fast SSID Change	<p>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.</p> <p>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.</p>
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	<p>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.</p> <p>All controllers in a mobility group must have the same symmetric tunneling mode. For symmetric tunneling to take effect, you must reboot.</p>
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	<p>Specify 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.</p> <p>When you hover your mouse cursor over the field, the valid range of values appear.</p>
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 from 8 to 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 1-56**      **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 reauthenticates.  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 <b>Global TCP Adjust MSS</b> 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 <b>enable</b> or <b>disable</b> 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 from 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 from 2 to 5.
AP Retransmit Interval	

**Controller > System > Global CDP Configuration**

Cisco Discovery Protocol (CDP) is a device-discovery protocol that runs on all Cisco network equipment. Each device sends identifying messages to a multicast address, and each device monitors the messages sent by other devices. CDP is enabled on the Ethernet and radio ports of the bridge by default.

The following table describes the Template Detail fields in **Design > Configuration > Feature Design > Features and Technologies > Controller > System > Global CDP Configuration**.

**Table 1-57**      **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 > QoS Profiles**

The following table describes the Template Detail fields in **Design > Configuration > Feature Design > Features and Technologies > Controller > System > QoS Profiles**.

**Table 1-58**      **Controller > System > QoS Profiles Template**

Field	Description
<b>Per-User Bandwidth Contracts</b>	<b>Note</b> All have a default of 0 or Off.
Average Data Rate	The average data rate for non-UDP traffic.
Global CDP on APs	The peak data rate for non-UDP traffic.
Average Real-time Rate	The average data rate for UDP traffic.
Burst Real-time Rate	The peak data rate for UDP traffic.
<b>Over-the-Air QoS</b>	<b>Note</b> The Air QoS configurations are applicable for controller Version 7.0 and earlier.
Maximum QoS RF Usage per AP	The maximum air bandwidth available to clients. The default is 100%.
QoS Queue Depth	The depth of queue for a class of client. The packets with a greater value are dropped at the access point.
<b>Wired QoS Protocol</b>	
Wired QoS Protocol	Choose <b>802.1P</b> to activate 802.1P priority tags or <b>None</b> to deactivate 802.1P priority flags.
802.1P Tag	Choose <b>802.1P priority tag</b> for a wired connection from 0 to 7. This tag is used for traffic and CAPWAP packets.

**Controller > System > SNMP Community**

Use this option to create or modify a template for configuring SNMP communities on controllers. SNMP communities only apply to SNMPv1 and v2c. SNMPv3 uses usernames and passwords.

For basic information about creating this template, see the Creating Feature-Level Configuration Templates section in the *Cisco Prime Infrastructure 2.0 User Guide*.

**Note**

When you enter the SNMP Community information, if you set the Access Mode option to Read Only, then after applying this template, *Prime Infrastructure will only have read access to the controller*.

**Controller > System > Traffic Stream Metrics QoS**

Traffic stream metrics are a series of statistics about VoIP over your wireless LAN and informs you of the QoS of the wireless LAN. These statistics are different than the end-to-end statistics provided by VoIP systems. End-to-end statistics provide information on packet loss and latency covering all the links comprising the call path. However, traffic stream metrics are statistics for only the WLAN segment of the call. Because of this, system administrators can quickly determine whether audio problems are being caused by the WLAN or by other network elements participating in a call. By observing which access points have impaired QoS, system administrators can quickly determine the physical area where the problem is occurring. This is important when lack of radio coverage or excessive interference is the root problem.

Four QoS values (packet latency, packet jitter, packet loss, and roaming time), which can affect the audio quality of voice calls, are monitored. All the wireless LAN components participate in this process. Access points and clients measure the metrics, access points collect the measurements and then send them to the controller. The access points update the controller with traffic stream metric information

every 90 seconds, and 10 minutes of data is stored at one time. The Prime Infrastructure queries the controller for the metrics and displays them in the Traffic Stream Metrics QoS Status. These metrics are compared to threshold values to determine their status level and if any of the statistics are displaying a status level of fair (yellow) or degraded (red), the administrator investigates the QoS of the wireless LAN.

For the access points to collect measurement values, traffic stream metrics must be enabled on the controller.

The Traffic Stream Metrics QoS Controller Configuration page shows several QoS values. An administrator can monitor voice and video quality of the following:

- Upstream delay
- Upstream packet loss rate
- Roaming time
- Downstream packet loss rate
- Downstream delay

Packet Loss Rate (PLR) affects the intelligibility of voice. Packet delay can affect both the intelligibility and conversational quality of the connection. Excessive roaming time produces undesired gaps in audio.

There are three levels of measurement:

- Normal: Normal QoS (green)
- Fair: Fair QoS (yellow)
- Degraded: Degraded QoS (red)

System administrators should employ some judgment when setting the green, yellow, and red alarm levels. Some factors to consider are:

- Environmental factors including interference and radio coverage that can affect PLR.
- End-user expectations and system administrator requirements for audio quality on mobile devices (lower audio quality can permit greater PLR).
- Different codec types used by the phones have different tolerance for packet loss.
- Not all calls are mobile-to-mobile; therefore, some have less stringent PLR requirements for the wireless LAN.

## Controller > System > User Roles

Use this option to create or modify a template for configuring user roles. User roles determine how much bandwidth the network can use. Four QoS levels (Platinum, Bronze, Gold, and Silver) are available for the bandwidth distribution to Guest Users. Guest Users are associated with predefined roles (Contractor, Customer, Partner, Vendor, Visitor, Other) with respective bandwidth configured by the Admin. These roles can be applied when adding a new Guest User.

For basic information about creating this template, see the Creating Feature-Level Configuration Templates section in the [Cisco Prime Infrastructure 2.0 User Guide](#).

## Controller > WLANs > WLAN Configuration

WLAN templates allow you to define various WLAN profiles for application to different controllers.

**Note**

You can configure multiple WLANs with the same SSID. This feature enables you to assign different Layer 2 security policies within the same wireless LAN. When you deploy the WLAN Configuration templates, the controllers configured with Interface/Interface Group, selected RADIUS servers, LDAP servers, ACL name with rules, and Ingress interface appear in the Template Deployment - Prepare and Schedule page.

These restrictions apply when configuring multiple WLANs with the same SSID:

- 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. These are the available Layer 2 security policies:
  - None (open WLAN)
  - Static WEP or 802.1
  - CKIP
  - WPA/WPA2
- Broadcast SSID must be enabled on the WLANs that share an SSID so that the access points can generate probe responses for these WLANs.
- FlexConnect access points do not support multiple SSIDs.

The following topics describe the fields on **Design > Configuration > Feature Design > Features and Technologies > Controller > WLANs > WLAN Configuration**:

- [Controller > WLANs > WLAN Configuration > General](#), page 1-56
- [Controller > WLANs > WLAN Configuration > Security](#), page 1-57
- [Controller > WLANs > WLAN Configuration > QoS](#), page 1-61
- [Controller > WLANs > WLAN Configuration > Advanced](#), page 1-62
- [Controller > WLANs > WLAN Configuration > HotSpot](#), page 1-66

**Controller > WLANs > WLAN Configuration > General**

The following table describes the Template Detail fields in **Design > Configuration > Feature Design > Features and Technologies > Controller > WLANs > WLAN Configuration > General**.

**Table 1-59**      **Controller > WLANs > WLAN Configuration > General**

Field	Description
Wired LAN	<p>Select the check box to indicate whether or not this WLAN is a wired LAN.</p> <p><b>Note</b> 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.)</p> <p>Use the <b>Type</b> drop-down list to choose the type of the wired LAN.</p> <ul style="list-style-type: none"> <li>• Guest LAN—Indicates that this wired LAN is a guest LAN. If you select the Guest LAN option, you need to select an Egress interface that has not already been assigned to any guest LAN.</li> <li>• Remote LAN—Indicates that this wired LAN is a remote LAN.</li> </ul>
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	<p>Enter the name of the WLAN SSID. An SSID is not required for a guest LAN.</p> <p>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.</p>
Status	Select the <b>Enable</b> check box for the Status field.
Configure Wlan Id	<p>Select the check box to give the WLAN an identifier.</p> <p>Use the <b>Wlan Id</b> text box to enter the WLAN identifier (an integer).</p>
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	<p>Select the <b>Enable</b> check box to enable the multicast VLAN feature.</p> <p>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.</p>
Broadcast SSID	Select to activate SSID broadcasts for this WLAN.



**Controller > WLANs > WLAN Configuration > Security**

The following table describes the Template Detail fields in **Design > Configuration > Feature Design > Features and Technologies > Controller > WLANs > WLAN Configuration > Security**.

**Table 1-60**      **Controller > WLANs > WLAN Configuration > Security**

Field	Description
<b>Layer 2</b>	
None	<p>No Layer 2 security selected.</p> <ul style="list-style-type: none"> <li>FT Enable—Select the check box to enable fast transition (FT) between access points.</li> </ul> <p><b>Note</b> Fast transition is not supported with FlexConnect mode.</p> <p>Over the DS—Select the check box to enable or disable the fast transition over a distributed system (DS).</p> <p>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.</p> <p>To enable Over the DS or Reassociation Timeout, you should enable fast transition.</p>
802.1X	<p>WEP 802.1X data encryption type:</p> <ul style="list-style-type: none"> <li>40/64 bit key</li> <li>104 bit key</li> <li>152 bit key</li> </ul>
Static WEP	<p>Static WEP encryption fields:</p> <ul style="list-style-type: none"> <li>Key sizes: Not set, 40/64, 104, and 152 bit key sizes.</li> <li>Key Index: 1 to 4.</li> <li>Encryption Key: Encryption key required.</li> <li>Key Format: ASCII or HEX.</li> <li>Allowed Shared Key Authentication—Select the check box to enable shared key authentication.</li> </ul> <p>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.</p>
Static WEP-802.1X	<p>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.</p> <p>Static WEP encryption fields:</p> <ul style="list-style-type: none"> <li>Key sizes: Not set, 40/64, 104, and 152 bit key sizes.</li> <li>Key index: 1 to 4.</li> <li>Encryption Key: Enter encryption key.</li> <li>Key Format: ASCII or HEX.</li> <li>Allowed Shared Key Authentication—Select the check box to enable.</li> <li>802.1 Data Encryption: 40/64 bit key, 104 bit key, 152 bit key.</li> </ul>

Table 1-60 Controller &gt; WLANs &gt; WLAN Configuration &gt; Security (continued)

Field	Description
CKIP	<p>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.</p> <p><b>Note</b> CKIP is not supported on 10xx APs.</p> <p>When selected, these CKIP fields are displayed.</p> <ul style="list-style-type: none"> <li>Key size: Not set, 40, or 104.</li> <li>Key Index: 1 to 4</li> <li>Encryption Key: Specify encryption key.</li> <li>Key Format: ASCII or HEX.</li> </ul> <p><b>Note</b> 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.</p> <p>MMH Mode—Select the check box to enable.</p> <p>Key Permutation—Select the check box to enable.</p>
MAC Filtering	<p>Select to filter clients by MAC address.</p> <p><b>Note</b> The ability to join a controller without specification within a MAC filter list is only supported on mesh access points.</p> <p><b>Note</b> 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.</p> <p>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.</p>
Authentication Key Management	<p>Choose the desired type of authentication key management. The choices are 802.1X, CCKM, or PSK.</p> <p><b>Note</b> If you choose PSK, you must enter the shared key and type (ASCII or hexadecimal).</p> <p><b>Note</b> 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.</p>
<b>Layer 3</b>	
Layer 3 Security	<p>Choose between None and VPN Pass Through.</p> <p><b>Note</b> The VPN passthrough option is not available for the 2106 or 5500 series controllers.</p>

Table 1-60 Controller &gt; WLANs &gt; WLAN Configuration &gt; Security (continued)

Field	Description
Web Policy	<p>You can modify the default static WEP (web authentication) or assign specific web authentication (login, logout, login failure) pages and the server source.</p> <ol style="list-style-type: none"> <li>1. To change the static WEP to passthrough, select the <b>Web Policy</b> 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.</li> </ol> <p>An <b>Email Input</b> check box appears. Select this check box if you want users to be prompted for their email address when attempting to connect to the network.</p> <ol style="list-style-type: none"> <li>2. Select the <b>WebAuth on MAC Filter Failure</b> radio button so that when clients fail on MAC filter, they are automatically switched to WebAuth.</li> </ol> <p><b>Note</b> The WebAuth on Mac Filter Failure option works only when the Layer 2 Mac Filtering option is enabled.</p> <ol style="list-style-type: none"> <li>3. To specify custom web authentication pages, unselect the <b>Global WebAuth Configuration Enable</b> check box.</li> </ol> <p>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:</p> <p><b>Default Internal</b>—Displays the default web login page for the controller. This is the default value.</p> <p><b>Customized Web Auth</b>—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 <b>None</b> from the appropriate drop-down list if you do not want to display a customized page for that option.</p> <p>These optional login, login failure, and logout pages are downloaded to the controller as webauth.tar files.</p> <p><b>External</b>—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.</p> <p><b>Note</b> External web auth is not supported for 2106 and 5500 series controllers.</p> <p>You can select specific RADIUS or LDAP servers to provide external authentication in the Security &gt; AAA page.</p> <p><b>Note</b> The RADIUS and LDAP servers must be already configured to have selectable options in the Security &gt; AAA page. You can configure these servers in the RADIUS Authentication Servers page and TACACS+ Authentication Servers page.</p> <p>If you selected External as the Web Authentication Type, choose <b>Security &gt; AAA</b>, and choose up to three RADIUS and LDAP servers using the drop-down lists.</p> <p>Repeat this process if a second (anchor) controller is being used in the network.</p>

Table 1-60 Controller &gt; WLANs &gt; WLAN Configuration &gt; Security (continued)

Field	Description
<b>AAA Server</b>	
Radius Server Overwrite	<p>Select to send the client authentication request through the dynamic interface that 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.</p> <p><b>Note</b> You cannot enable Radius Server Overwrite Interface when Diagnostic Channel is enabled.</p> <p><b>Note</b> The Radius Server Overwrite Interface option is supported in controller Version 7.0.x and later.</p> <p>Select the <b>Enable</b> check box, 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.</p> <p>If no LDAP servers are chosen here, Prime Infrastructure uses the default LDAP server order from the database.</p>
Interim Update	<p>Select 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.</p> <p><b>Note</b> The Interim Interval can be entered only when Interim Update is enabled.</p>
Local EAP Authentication	<p>Select the <b>Local EAP Authentication</b> 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.</p>
Allow AAA Override	<p>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.)</p> <p>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.</p> <p>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.</p> <p>The AAA override values might come from a RADIUS server, for example.</p>

**Controller > WLANs > WLAN Configuration > QoS**

The following table describes the Template Detail fields in **Design > Configuration > Feature Design > Features and Technologies > Controller > WLANs > WLAN Configuration > QoS**.

**Table 1-61 Controller > WLANs > WLAN Configuration > QoS**

Field	Description
Quality of Service (QoS)	Choose <b>Platinum</b> (voice), <b>Gold</b> (video), <b>Silver</b> (best effort), or <b>Bronze</b> (background). Services such as VoIP should be set to gold while nondiscriminating services such as text messaging can be set to bronze.
<b>Override Per-User Rate Limits</b>	<b>Data rates on a per-user basis</b>
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 box. 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 box. 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 box. 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 box. 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.
<b>Override Per-SSID Rate Limits</b>	<b>Data rates on a per SSID basis</b>
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 box. 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 box. 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 box. 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 box. 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 <b>Disabled</b> , <b>Allowed</b> (so clients can communicate with the WLAN), or <b>Required</b> (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 <b>7920 Client CAC</b> check box to enable it. The Call Admission Control (CAC) limit is set on the access point for newer versions of software.

**Controller > WLANs > WLAN Configuration > Advanced**

The following table describes the Template Detail fields in **Design > Configuration > Feature Design > Features and Technologies > Controller > WLANs > WLAN Configuration > Advanced**.

**Table 1-62**      **Controller > WLANs > WLAN Configuration > Advanced**

Field	Description
FlexConnect Local Switching	<p>Select to enable FlexConnect local switching. If you enable FlexConnect local switching, the FlexConnect access point handles client authentication and switches client data packets locally.</p> <p>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 to 16.</p>
FlexConnect Local Auth	<p>Select to enable FlexConnect local authentication.</p> <p>Local authentication is useful where you are unable to maintain the criteria of 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.</p> <p><b>Note</b> Local authentication can only be enabled on the WLAN of a FlexConnect AP that is in local switching mode.</p> <p>Local authentication is not supported in the following scenarios:</p> <ul style="list-style-type: none"> <li>• Guest authentication cannot be performed on a FlexConnect local authentication enabled WLAN.</li> <li>• RRM information is not available at the controller for the FlexConnect local authentication enabled WLAN.</li> <li>• Local RADIUS is not supported.</li> <li>• 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.</li> </ul>
Learn Client IP Address	<p>When you enable hybrid-REAP local switching, the <b>Learn Client IP</b> 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.</p>
Diagnostic Channel	<p>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.</p>
Aironet IE	<p>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.</p>
IPv6	<p>Select the <b>IPv6</b> check box. You can configure IPv6 bridging and IPv4 web auth on the same WLAN.</p>
Session Timeout	<p>Select to set the maximum time a client session can continue before requiring reauthorization.</p>

**Table 1-62**      **Controller > WLANs > WLAN Configuration > Advanced (continued)**

Field	Description
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 ACL drop-down list 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	<p>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:</p> <ul style="list-style-type: none"> <li>• <b>Disable</b>—Peer-to-peer blocking is disabled, and traffic is bridged locally whenever possible.</li> <li>• <b>Drop</b>—The packet is discarded.</li> <li>• <b>Forward Up Stream</b>—The packet is forwarded on the upstream VLAN, and the decision is made about what to do with the packet.</li> </ul> <p><b>Note</b> For locally switched clients, the Forward Up Stream is same as Drop from 7.2.x version of controllers.</p> <p>If FlexConnect local switching is enabled for the WLAN, which prevents traffic from passing through the controller, this drop-down list is dimmed.</p> <p><b>Note</b> Peer-to-peer blocking does not apply to multicast traffic.</p>
Wi-Fi Direct Clients Policy	<p>Choose one of the following options:</p> <ul style="list-style-type: none"> <li>• <b>Disabled</b>—Disables the Wi-Fi Direct Clients Policy for the WLAN and deauthenticates all Wi-Fi Direct capable clients. The default is Disabled.</li> <li>• <b>Allow</b>—Allows the Wi-Fi Direct clients to associate with an infrastructure WLAN.</li> <li>• <b>Not-Allow</b>—Disallows the Wi-Fi Direct clients from associating with an infrastructure WLAN.</li> </ul> <p><b>Note</b> Wi-Fi Direct Client Policy is applicable to WLANs that have APs in local mode only.</p> <p><b>Note</b> The Wi-Fi Direct Clients Policy is applicable for controller Version 7.2.x. and later.</p>
Client Exclusion	<p>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.</p> <p><b>Note</b> 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.</p>
Passive Client	<p>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.</p> <p><b>Note</b> A value of 0 allows unlimited number of clients to be associated with a WLAN.</p>
Static IP Tunneling	Enable dynamic anchoring of static IP clients by selecting the <b>Static IP Tunneling</b> check box.

Table 1-62 Controller &gt; WLANs &gt; WLAN Configuration &gt; Advanced (continued)

Field	Description
Media Session Snooping	<p>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.</p> <p>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.</p>
KTS based CAC	<p>Select the <b>KTS based CAC</b> check box to enable KTS-based CAC support per WLAN.</p> <p>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.</p> <p><b>Note</b> 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.</p>
NAC State	<p>Choose <b>SNMP NAC</b> or <b>Radius NAC</b>. 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.</p>
Scan Defer Priority	<p>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.</p> <p>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:</p> <ul style="list-style-type: none"> <li>• Bronze marks all downlink traffic to UP=1.</li> <li>• Silver marks all downlink traffic to UP=0.</li> <li>• Gold marks all downlink traffic to UP=4.</li> <li>• Platinum marks all downlink traffic to UP=6.</li> </ul> <p>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 to 60000. The default value is 100 milliseconds.</p>



**Table 1-62**      **Controller > WLANs > WLAN Configuration > Advanced (continued)**

Field	Description
DTIM Period	<p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>Under DTIM Period, enter a value from 1 to 255 in the 802.11a/n and 802.11b/g/n fields. The default value is 1 (transmit broadcast and multicast frames after every beacon).</p>
DHCP Server	<p>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:</p> <ul style="list-style-type: none"> <li>• DHCP Required and a valid DHCP server IP address—All WLAN clients obtain an IP address from the DHCP server.</li> <li>• DHCP is not required and a valid DHCP server address—All WLAN clients obtain an IP address from the DHCP server or use a static IP address.</li> <li>• 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.</li> </ul> <p>You cannot choose to require a DHCP address assignment and then enter a DHCP server IP address.</p>
MFP Signature Generation	<p>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.</p>
MFP Client Protection	<p>Choose <b>Enabled</b>, <b>Disabled</b>, or <b>Required</b> for configuration of individual WLANs of a controller. If infrastructure MFP is not enabled, this drop-down list is unavailable.</p> <p><b>Note</b> 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.</p> <p><b>Note</b> 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.</p>

**Table 1-62**      **Controller > WLANs > WLAN Configuration > Advanced (continued)**

Field	Description
DTIM Period	Enter a value from 1 to 255 beacon intervals. The controller sends a DTIM packet for this WLAN based on what is entered as an interval. <b>Note</b> 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. <b>Note</b> Client profiling is not supported with FlexConnect local authentication. <b>Note</b> Client profiling is configurable only when you select the <b>DHCP Address Assignment</b> check box.
PMIP Mobility	Choose the mobility type from the following options: <ul style="list-style-type: none"> <li>None—Configures the WLAN with simple IP.</li> <li>Mixed—Configures the WLAN with simple IP and PMIPv6.</li> <li>PMIPv6—Configures the WLAN with only PMIPv6.</li> </ul>

**Controller > WLANs > WLAN Configuration > HotSpot**

Mobile Concierge is a solution that enables 802.1X capable clients to interwork with external networks. The Mobile Concierge feature provides service availability information to clients and can help them to associate available networks.

The services offered by the network can be broadly classified into two protocols:

- 802.11u MSAP
- 802.11u HotSpot 2.0

The following guidelines and limitations apply to Mobile Concierge:

- Mobile Concierge is not supported on FlexConnect Access Points.
- 802.11u configuration upload is not supported. If you perform a configuration upgrade and upload a configuration on the controller, the HotSpot configuration on the WLANs is lost.

To create Mobile Concierge (802.11u) Groups, choose **Design > Configuration > Feature Design > Features and Technologies > Controller > WLANs > WLAN Configuration > Hot Spot**.

The following table describes the Template Detail fields in **Design > Configuration > Feature Design > Features and Technologies > Controller > WLANs > WLAN Configuration > HotSpot**.

**Table 1-63**      **Controller > WLANs > WLAN Configuration > HotSpot**

Field	Description
<b>General</b>	
802.11u Status	Select to enable 802.11u on the WLAN. <ul style="list-style-type: none"> <li>• 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.</li> </ul>
Internet Access	Select to enable this WLAN to provide Internet services.

**Table 1-63**      **Controller > WLANs > WLAN Configuration > HotSpot (continued)**

Field	Description
Network Type	<p>Choose one of the following network types that best describes the 802.11u you want to configure on this WLAN:</p> <ul style="list-style-type: none"> <li>• Private Network</li> <li>• Private Network with Guest Access</li> <li>• Chargeable Public Network</li> <li>• Free Public Network</li> <li>• Emergency Services Only Network</li> <li>• Personal Device Network</li> <li>• Test or Experimental</li> <li>• Wildcard</li> </ul>
Network Auth Type	<p>Choose the authentication type that you want to configure for the 802.11u parameters on this network:</p> <ul style="list-style-type: none"> <li>• Not configured</li> <li>• Acceptance of Terms and Conditions</li> <li>• Online Enrollment</li> <li>• HTTP/HTTPS Redirection</li> </ul>
OUI List	<p>Enter the following details:</p> <ul style="list-style-type: none"> <li>• OUI name</li> <li>• Is Beacon</li> <li>• OUI Index</li> </ul> <p>Select Add to add the OUI (Organizationally Unique Identifier) entry to this WLAN.</p> <ul style="list-style-type: none"> <li>• In the group box,</li> </ul>
Domain List	<p>Enter the following details:</p> <ul style="list-style-type: none"> <li>• Domain Name—The domain name operating in the 802.11 access network.</li> <li>• Domain Index—Select the domain index from the drop-down list.</li> </ul> <p>Select Add to add the domain entry to this WLAN.</p>
OUI List	<p>Enter the following details:</p> <ul style="list-style-type: none"> <li>• Realm Name—The realm name.</li> <li>• Realm Index—The realm index.</li> </ul> <p>Select Add to add the domain entry to this WLAN.</p>
MSAP	Select to enable service advertisements.

**Table 1-63**      **Controller > WLANs > WLAN Configuration > HotSpot (continued)**

Field	Description
Server Index	<p>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.</p> <p><b>Note</b> 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.</p>
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	<p>Specify the following:</p> <ul style="list-style-type: none"> <li>Operator Name—Specify the name of the 802.11 operator.</li> <li>Operator Index—Select an operator index. The range is from 1 to 32.</li> <li>Language Code—An ISO-14962-1997 encoded string defining the language. This string is a three character language code.</li> </ul> <p>Select Add to add the operator details.</p>
Port Config List	<p>Specify the following:</p> <ul style="list-style-type: none"> <li>IP Protocol—The IP protocol that you want to enable. The following options are ESP, FTP, ICMP, and IKEV2.</li> <li>Port No—The port number that is enabled on this WLAN.</li> <li>Status—The status of the port.</li> </ul>

## Controller > mDNS

Multicast DNS (mDNS) service discovery provides a way to announce and discover services on the local network. mDNS performs DNS queries over IP multicast. mDNS supports zero configuration IP networking.

Follow these guidelines and limitations when creating mDNS templates:

- You cannot delete an mDNS service when it is mapped to one or more profiles.
- The length of the profile name and the services name can be a maximum 31 characters.
- The length of the service string can be a maximum 255 characters.
- You cannot delete the default profile (default-mdns-profile).
- You cannot delete profiles when they are mapped to interfaces, interface-groups, or WLANs.

- You cannot remove mDNS services from a profile when they are mapped to an interface, interface-groups, or WLANs. You can add new services.
- Whenever you create and apply any mDNS template, it overwrites existing configuration on controller.
- You cannot enable mDNS snooping for WLAN when FlexConnect local switching is enabled.
- You cannot attach mDNS profiles to interfaces when AP Management is enabled.

The following table describes the Template Detail fields on **Design > Configuration > Feature Design > Features and Technologies > Controller > mDNS > mDNS**.

**Table 1-64**      **Controller > mDNS > mDNS**

Field	Description
<b>Services Tab</b>	Use the fields in this tab to configure the global mDNS parameters and update the Master Services database.
MDNS Global Snooping	Select the check box to enable snooping of mDNS packets.  <b>Note</b> The controller does not support IPv6 mDNS packets even when you enable mDNS snooping.
Query Interval(10-120)	The mDNS query interval, in minutes, that you can set. This interval is used by WLC to send periodic mDNS query messages to services that do not send service advertisements automatically after they are started. The range is from 10 to 120 minutes. The default value is 15 minutes.
Master Services	A list of the supported services that can be queried.
Service Name	Name of the mDNS service.
Service String	Unique string associated to an mDNS service. For example, _airplay._tcp.local. is the service string associated to AppleTV.
Query Status	Select the check box to enable an mDNS query for a service.  <b>Note</b> Periodic mDNS query messages will be sent by WLC at configured Query Interval for services only when the query status is enabled; otherwise, service should automatically advertised for other services where the query status is disabled (for example AppleTV).
<b>Profiles Tab</b>	Use this tab to view the mDNS profiles configured on the controller and create new mDNS profiles. After creating a new profile, you must map the profile to an interface group, an interface, or a WLAN.  Clients receive service advertisements only for the services associated with the profile. The controller gives the highest priority to the profiles associated to interface groups, followed by the interface profiles, then the WLAN profiles. Each client is mapped to a profile based on the order of priority.  By default, the controller has an mDNS profile, default-mdns-profile. You cannot delete this default profile.
Profile Name	Name of the mDNS profile. You can create a maximum of 16 profiles.
Services	Select the services (using the check boxes) that you want to map to the mDNS profile.

## Interfaces Templates Field Descriptions

The following topics contain field descriptions for pages found in **Design > Configuration > Feature Design > Features and Technologies > Interfaces**:

- [Interfaces > Cellular Profile](#), page 1-70
- [Interfaces > GSM Profile](#), page 1-71

## Interfaces > Cellular Profile



### Note

To deploy the cellular profile template on any UMTS, GSM, HSPA, HSPA+R7 modem, you should have the GSM profile ([“Interfaces > GSM Profile” section on page 1-71](#)) on the router.

The following table describes the Template Detail fields on **Design > Feature Design > Features and Technologies > Interfaces > Cellular Profile**.

**Table 1-65** *Interfaces > Cellular Profile*

Field	Description
<b>Validation Criteria</b>	
Device Type	Choose the device type from the drop-down list.
<b>Interface Details</b>	
Cellular Interface	Enter the name of the cellular interface. For fixed platform routers(8xx), it is always Cellular 0, for modular platforms it is of the following form; Cellular slot/sub slot or port. For example, Cellular 0/1/0.
Define this cellular interface as	Choose one of the following options to configure the cellular interface: <ul style="list-style-type: none"> <li>• Primary WAN Interface</li> <li>• Backup WAN Interface</li> </ul>
Primary Interface	Enter the primary interface details. This field appears when <b>Define this cellular interface as</b> is set to Backup WAN Interface.
<b>Routemap Configuration</b>	
Route Map Tag	Enter a unique name to identify the route map.
Sequence Number	Enter a numeric value to define a route map condition.
Action	The field value is set to Permit by default.
Access List	Enter the details of the access list that is associated with the route map to inspect an interesting traffic. The ACL must be an extended ACL and can be named ACL also.
First Hop Interface	(Read only) The details are auto populated when a user enters the primary interface.
<b>IP SLA Configuration</b>	
Target Address	Enter the IP address of the server to which connectivity is checked. This server is decided as part of Service Level Agreement (SLA).
Timeout Value	Enter the timeout value in milliseconds for each ping request.
Time Interval	Enter the time interval at which the pings are generated.
<b>Dialer Configuration</b>	
Persistent Data Connection	Choose <b>Yes</b> to enable the persistent data connection.
Associate Dialer	Enter the associate dialer. This field appears when <b>Persistent Data Connection</b> is set to yes.
Dialer Idle Timeout	Enter the dialer idle timeout. This field appears when <b>Persistent Data Connection</b> is set to no.

**Table 1-65** *Interfaces > Cellular Profile (continued)*

Field	Description
<b>Chat-Script Configuration</b>	
Chat-Script Name	Enter the string value that causes the cellular modem to dial out and initiate the traffic.
Timeout Value	Enter the timeout value used by the Cisco IOS device to wait for a response from the modem. The call fails in case the Cisco IOS device does not get any expected response or no response from the cellular modem.

## Interfaces > GSM Profile

The following table describes the Template Detail fields on **Design > Feature Design > Features and Technologies > Interfaces > GSM Profile**.

**Table 1-66** *Interfaces > GSM Profile*

Field	Description
Device Type	Choose device type from the drop-down list.
<b>Template Detail</b>	
Cellular Interface	Enter the Cisco wireless WAN interface that support up to 16 profiles, but only one can be active at a time. Generally profile number 1 is selected by default.
Access Point Name (APN)	Enter the name that identifies the packet data network (PDN), that a mobile data user wants to communicate with. Generally the APN is shared by the service provider, when a user buys a particular cellular modem.
Profile Number	Select the profile number from the drop-down list.
PDP Type	Choose the Packet Data Protocol (PDP) type from the drop-down list. PDP offers a packet data connection over which the user equipment such as mobiles and the network can exchange IP packets.  The PDP types available are: <ul style="list-style-type: none"> <li>IPv4 (Default)</li> <li>PPP</li> </ul>
Authentication	Choose the type of authentication that is used by your service provider. CHAP authentication is more secure than PAP authentication.
Username Password	For CHAP or PAP authentication, enter the username given to you by your Internet service provider or network administrator.

## Security Templates Field Descriptions

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

- [Security > VPN Components, page 1-72](#)
- [Security > Zone Based Firewall, page 1-76](#)
- [Security > DMVPN, page 1-78](#)
- [Security > Easy VPN Remote, page 1-82](#)

- [Security > Easy VPN Server](#), page 1-85
- [Security > Easy VPN Server Proxy Setting](#), page 1-88
- [Security > GETVPN-GroupMember](#), page 1-88
- [Security > GETVPN-KeyServer](#), page 1-90
- [Security > ScanSafe](#), page 1-92

## Security > VPN Components

The following topics contain descriptions of the fields found in **Design > Configuration > Feature Design > Features and Technologies > Security > VPN Components**:

- [Security > VPN Components > IKE Policies](#), page 1-72
- [Security > VPN Components > IKE Settings](#), page 1-73
- [Security > VPN Components > IPSec Profile](#), page 1-74
- [Security > VPN Components > Pre-shared Keys](#), page 1-74
- [Security > VPN Components > RSA-Keys](#), page 1-75
- [Security > VPN Components > Transform Sets](#), page 1-75

### Security > VPN Components > IKE Policies


The following table describes the Template Detail fields on **Design > Feature Design > Features and Technologies > Security > VPN Components > IKE Policies**.

**Table 1-67**      *Security > VPN Components > IKE Policies*

Field	Description
<b>IKE Policies</b>	
Priority	<p>Enter 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.</p> <p>The range is from 1 to 10000. The lower the number, the higher the priority.</p>
Authentication	<p>Choose one of the following options from the Authentication drop-down list:</p> <ul style="list-style-type: none"> <li>• PRE_SHARE—Authentication will be performed using pre-shared keys.</li> <li>• RSA_SIG—Authentication will be performed using digital signatures.</li> </ul>
D-H Group	<p>Choose the Diffie-Hellman (D-H) group used for driving a shared secret between two IPsec peers without transmitting it to each other. A large modulus provides higher security but requires more processing time. The two peers must have a matching modulus group. Choose one of the following options from Diffie-Hellman Group drop-down list:</p> <ul style="list-style-type: none"> <li>• 1—Diffie-Hellman Group 1 (768-bit modulus).</li> <li>• 2—Diffie-Hellman Group 2 (1024-bit modulus).</li> <li>• 5—Diffie-Hellman Group 5 (1536-bit modulus; considered good protection for 128-bit keys).</li> </ul>



**Table 1-67**      **Security > VPN Components > IKE Policies (continued)**

Field	Description
Encryption	<p>Choose one of the encryption algorithms from the Encryption drop-down list:</p> <ul style="list-style-type: none"> <li>AES-128—Encrypts according to the Advanced Encryption Standard (AES) using 128-bit keys.</li> <li>AES-192—Encrypts according to the AES using 192-bit keys.</li> <li>AES-256—Encrypts according to the AES using 256-bit keys.</li> <li>DES—Encrypts according to the Data Encryption Standard (DES) using 56-bit keys.</li> <li>3DES—Encrypts three times using 56-bit keys. 3DES is more secure than DES but requires more processing for encryption and decryption. However, it is less secure than AES.</li> </ul> <p> <b>Note</b>      A 3DES license is required to use this option.</p>
Hash	<p>Choose the hash algorithm drop-down list. The hash algorithm creates a message digest that is used to ensure message integrity. The options are:</p> <ul style="list-style-type: none"> <li>SHA (Secure Hash Algorithm)—Produces a 160-bit digest. SHA is more resistant to brute-force attacks than MD5.</li> <li>MD5 (Message Digest 5)—Produces a 128-bit digest. MD5 uses less processing time than SHA.</li> </ul>
IKE lifetime	<p>Enter 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.</p> <p>The range is from 60 to 86400. The default value is 86400.</p>

**Security > VPN Components > IKE Settings**

The following table describes the Template Detail fields on **Design > Feature Design > Features and Technologies > Security > VPN Components > IKE Settings**.

**Table 1-68**      **Security > VPN Components > IKE Settings**

Field	Description
<b>IKE Settings</b>	
Enable IKE	<p>Select the <b>Enable IKE</b> check box to globally enable the IKE. (By default, the IKE is enabled.) You do not have to enable IKE for individual interfaces, but it can be enabled globally for all the interfaces in the router.</p> <p>If you do not want to use the IKE for your IP Security (IPsec) implementation, you can disable the IKE for all your IPsec peers. If you disable the IKE for one peer, you must disable it for all the IPsec peers.</p>
Enable Aggressive Mode	<p>Select the <b>Enable Aggressive Mode</b> check box to enable the Internet Security Association and Key Management Protocol (ISAKMP) aggressive mode. If you disable the aggressive mode, all the aggressive mode requests to the device and all the aggressive mode requests made by the device will be blocked.</p>

**Table 1-68**      **Security > VPN Components > IKE Settings (continued)**

Field	Description
IKE Identity	<p>Choose one option from the IKE identity drop-down list.</p> <p>An ISAKMP identity is set whenever you specify pre-shared keys or RSA signature authentication. As a general rule, you should set all the peers' identities in the same way, either by IP address or by hostname. The options are:</p> <ul style="list-style-type: none"> <li>• IP Address—Sets the ISAKMP identity to the IP address of the interface that is used to communicate to the remote peer during the IKE negotiations.</li> <li>• DISTINGUISHED NAME—Sets the ISAKMP identity to the distinguished name (DN) of the router certificate.</li> <li>• HOSTNAME—Sets the ISAKMP identity to the hostname concatenated with the domain name (for example, myhost.example.com).</li> </ul>
Enable Dead Peer Detection (DPD)	Enable the gateway to send the Dead Peer Detection (DPD) messages to the peer. DPD is a keepalive scheme that allows the router to query the liveliness of its IKE peer.
Keepalive	Specify the number of seconds between the DPD messages in the DPD Keepalive field. The range is from 10 to 3600.
Retry	Specify the number of seconds between retries if the DPD messages fail during DPD Retry. The range is from 2 to 60.

**Security > VPN Components > IPSec Profile**

The following table describes the Template Detail fields on **Design > Feature Design > Features and Technologies > Security > VPN Components > IPSec Profile**.

**Table 1-69**      **Security > VPN Components > IPSec Profile**

Field	Description
Name	Enter a name for this IPsec profile. When you edit a profile, you cannot edit the name of the IPsec profile.
Description	Add a description for the IPsec profile that you are adding or editing.
Transform Sets	Enter the transform set name. The transform set (see <a href="#">Security &gt; VPN Components &gt; Transform Sets, page 1-75</a> ) encrypts the traffic on the tunnel.
IPSec SA Lifetime (secs)	Enter the IPSec SA Lifetime to establish a new SA after the set period of time elapses. Enter the time in seconds. The range is from 120 to 86400.

**Security > VPN Components > Pre-shared Keys**

The following table describes the Template Detail fields on **Design > Feature Design > Features and Technologies > Security > VPN Components > Pre-shared Keys**.

**Table 1-70**      **Security > VPN Components > Pre-shared Keys**

Field	Description
IP Address/Host Name	Enter the IP address or the hostname of the remote peer.

**Table 1-70**      **Security > VPN Components > Pre-shared Keys (continued)**

Field	Description
Subnet Mask	Enter the subnet mask.
Pre-shared Key/ Confirm Pre-shared Key	Enter the pre-shared key, and reenter the key to confirm the pre-shared key.

**Security > VPN Components > RSA-Keys**

The following table describes the Template Detail fields on **Design > Feature Design > Features and Technologies > Security > VPN Components > RSA-Keys**.

**Table 1-71**      **Security > VPN Components > RSA-Keys**

Field	Description
Label	Enter the name for the key pair.
Modulus	Enter the key modulus value. If you want a modulus value from 512 to 1024, enter an integer value that is a multiple of 64. If you want a value higher than 1024, you can enter 1536 or 2048. If you enter a value greater than 512, key generation may take a minute or longer.  The modulus determines the size of the key. The larger the modulus, the more secure the key, but keys with large modulus take longer to generate, and encryption/decryption operations take longer with larger keys.
Type	Select the type of the RSA key to be generated. The options are: <ul style="list-style-type: none"> <li>• general-keys</li> <li>• usages-keys</li> <li>• encryption</li> <li>• signature</li> </ul>
Enable Exportable	Enable this field to generate RSA as an exportable key.

**Security > VPN Components > Transform Sets**

A transform set represents a certain combination of security protocols and algorithms. During the IPsec security association negotiation, the peers agree to use a particular transform set for protecting a particular data flow. A transform set describes a particular security protocol with its corresponding algorithms.

The following table describes the Template Detail fields on **Design > Feature Design > Features and Technologies > Security > VPN Components > Transform Sets**.

**Table 1-72**      **Security > VPN Components > Transform Sets**

Field	Description
Name	Enter a name for the transform set.
ESP Encryption	Choose the ESP encryption algorithm used to encrypt the payload.
ESP Integrity	Choose the ESP integrity algorithm used to check the integrity of the payload.

**Table 1-72**      **Security > VPN Components > Transform Sets**

Field	Description
AH Integrity	Choose the AH integrity from the drop-down list. The options are: <ul style="list-style-type: none"> <li>AH with the MD5 (Message Digest 5) (a Hash-based Message Authentication Code [HMAC] variant) authentication algorithm.</li> <li>AH with the SHA (Secure Hash Algorithm) (an HMAC variant) authentication algorithm.</li> </ul>
Compression	Enable or disable the IP compression with the Lempel-Ziv-Stac (LZS) algorithm.
Mode	Choose the mode from the drop-down list. The options are: <ul style="list-style-type: none"> <li>Transport—Encrypt data only. Transport mode is used when both endpoints support IPsec. Transport mode places the authentication header or encapsulated security payload after the original IP header; thus, only the IP payload is encrypted. This method allows users to apply network services such as quality-of-service (QoS) controls to encrypted packets.</li> <li>Tunnel—Encrypt data and IP header. Tunnel mode provides stronger protection than transport mode. Because the entire IP packet is encapsulated within AH or ESP, a new IP header is attached, and the entire datagram can be encrypted. Tunnel mode allows network devices such as a router to act as an IPsec proxy for multiple VPN users; tunnel mode should be used in those configurations.</li> </ul>

## Security > Zone Based Firewall

The following section contains descriptions of the fields in **Design > Configuration > Feature Design > Features and Technologies > Security > Zone Based Firewall**:

- [Security > Zone Based Firewall > Policy Rules, page 1-76](#)

### Security > Zone Based Firewall > Policy Rules

The following table describes the Template Detail fields on **Design > Configuration > Feature Design > Features and Technologies > Security > Zone Based FireWall > Policy Rules**.

**Table 1-73**      **Security > Zone Based FireWall > Policy Rules**

Element	Description
Name	(Optional) Enter a name for the policy rule.
Source Zone	Select the source zone from the list of interface roles. The source zone specifies the name of the interface from which the traffic is originating.
Destination Zone	Select the destination zone from the list of interface roles. The destination zone specifies the name of the interface to which the traffic is bound.
Source	Enter the source IP address of the inspected data. The valid parameters are: <ul style="list-style-type: none"> <li>Any</li> <li>Other—If you select the Other option, you can choose a combination of IP address, Subnets, and Network Objects.</li> </ul>

**Table 1-73**      **Security > Zone Based FireWall > Policy Rules (continued)**

Element	Description
Destination	<p>Enter the destination IP address of the inspected data. The valid parameters are:</p> <ul style="list-style-type: none"> <li>Any</li> <li>Other—If you select the Other option, you can choose a combination of IP address, Subnet, and Network Objects.</li> </ul>
Service	<p>Select the service of the inspected data from the object selector. The valid parameters are:</p> <ul style="list-style-type: none"> <li>L3/4 Applications</li> <li>ACL-Based Application: TCP, UDP, ICMP</li> </ul>
Action	<p>Choose an action to perform on the traffic when the rule matches the condition. The rule matches when:</p> <ul style="list-style-type: none"> <li>The traffic Source IP matches the Source Rule condition.</li> <li>The traffic Destination IP matches the Destination Rule condition and the traffic Inspected Service matches the Service Rule condition.</li> </ul> <p>The action options are:</p> <ul style="list-style-type: none"> <li>Drop—Traffic that is handled by the drop action is silently dropped. The system does not send a notification to the end host.</li> <li>Drop and Log—Traffic that is handled by the drop and log action is dropped and a syslog notification is sent to the end host.</li> <li>Inspect—The inspect action offers state-based traffic control, the router maintains the connection or session information for TCP and UDP traffic.</li> <li>Pass—This action allows the router to forward the traffic from one zone to another.</li> <li>Pass and Log—This action allows the router to forward traffic from one zone to another while creating a syslog notification of the forwarded traffic.</li> </ul>

## Security > DMVPN

The following table describes the Template Detail fields on **Design > Feature Design > Features and Technologies > Security > DMVPN**.

**Table 1-74**      **Security > DMVPN**

Field		Description
<b>IPsec Information</b>		
IKE Authentication	Authentication Type	<p>Select the <b>Preshared Keys</b> or <b>Digital Certificates</b> radio button.</p> <ul style="list-style-type: none"> <li>• <b>Preshared Keys</b>—This allows a secret key to be shared between two peers and be used by IKE during the authentication phase.</li> <li>• <b>Digital Certificates</b>—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.</li> </ul>
	Priority	<p>Enter 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.</p> <p>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.</p>
	Authentication	Choose the authentication type from the drop-down list.

Table 1-74 Security &gt; DMVPN (continued)

Field	Description
D-H Group	<p>Select the Diffie-Hellman (D-H) group. The D-H group is used for deriving a shared secret between 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. The options are:</p> <ul style="list-style-type: none"> <li>1—Diffie-Hellman Group 1 (768-bit modulus).</li> <li>2—Diffie-Hellman Group 2 (1024-bit modulus).</li> <li>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.</li> </ul>
Encryption	<p>Choose the encryption algorithm from the drop-down list. The encryption algorithm is used to establish the Phase 1 SA for protecting phase 2 negotiations:</p> <ul style="list-style-type: none"> <li>AES-128—Encrypts according to the AES using 128-bit keys.</li> <li>AES-192—Encrypts according to the AES using 192-bit keys.</li> <li>AES-256—Encrypts according to the AES using 256-bit keys.</li> <li>DES—Encrypts according to the DES using 56-bit keys.</li> <li>3DES—Encrypts three times using 56-bit keys. 3DES is more secure than DES but requires more processing for encryption and decryption. However, it is less secure than AES. A 3DES license is required to use this option.</li> </ul>
Hash	<p>Select the algorithm used in the IKE proposal. The hash algorithm creates a message digest that is used to ensure message integrity. The options are:</p> <ul style="list-style-type: none"> <li>• SHA (Secure Hash Algorithm)—Produces a 160-bit digest. SHA is more resistant to brute-force attacks than MD5.</li> <li>• MD5 (Message Digest 5)—Produces a 128-bit digest. MD5 uses less processing time than SHA.</li> </ul>

Table 1-74 Security &gt; DMVPN (continued)

Field		Description
	IKE Lifetime	Specify the IKE lifetime value from 60 to 86400. The default is 86400. 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.
Encryption Policy	Name	Enter the transform set name. The transform set encrypts the traffic on the tunnel.
	ESP Encryption	Choose the algorithm used to encrypt the payload from the drop-down list. The options are: <ul style="list-style-type: none"> <li>• ESP with the 128-bit AES encryption algorithm.</li> <li>• ESP with the 192-bit AES encryption algorithm.</li> <li>• ESP with the 256-bit AES encryption algorithm.</li> <li>• ESP with the 168-bit DES encryption algorithm (3DES or Triple DES).</li> <li>• Null encryption algorithm.</li> </ul>
	ESP Integrity	Choose the integrity algorithm used to check the integrity of the payload from the drop-down list. The options are: <ul style="list-style-type: none"> <li>• ESP with the MD5 (HMAC variant) authentication algorithm.</li> <li>• ESP with the SHA (HMAC variant) authentication algorithm.</li> </ul>
	AH Integrity	Choose <b>AH integrity</b> from the drop-down list. The options are: <ul style="list-style-type: none"> <li>• AH with the MD5 (Message Digest 5) (a Hash-based Message Authentication Code [HMAC] variant) authentication algorithm.</li> <li>• AH with the SHA (Secure Hash Algorithm) (an HMAC variant) authentication algorithm.</li> </ul>
	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.
Topology and Routing Information		
Spoke	—	Select the <b>Spoke</b> radio button to configure the router as a spoke in the topology.



**Table 1-74**      **Security > DMVPN (continued)**

Field		Description
Hub	—	Select the <b>Hub</b> radio button to configure the router as a Hub in the topology.  Select one of the following routing protocols: <ul style="list-style-type: none"> <li>EIGRP—Enter the AS number</li> <li>RIPV2</li> <li>Other</li> </ul>
Create dynamic connection between Spokes	—	Select the <b>Create Dynamic Connection between Spokes</b> check box to configure the dynamic connection between spokes.
<b>Multipoint GRE Interface Information (These fields appear only under Operate &gt; Device Work Center)</b>		
Select the Tunnel source that connects to internet	—	Choose the WAN interface that connects to the Internet from the drop-down list.
IP Address of this router's GRE Tunnel Interface	—	Enter the IP address of the tunnel interface.
Subnet Mask	—	Enter the subnet mask.
<b>NHRP and Tunnel Parameters</b>		
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	—	(Optional) Enter the number of seconds for which the Next Hop Resolution Protocol (NHRP) NBMA addresses should be advertised as valid. The default value is 7200.
NHRP Authentication String	—	Enter the authentication string.
Tunnel Key	—	Enter the tunnel key. This is used to enable a key ID for a particular tunnel interface. The range is from 0 to 4294967295.
Bandwidth	—	Enter the bandwidth. This is an optional field.
IP MTU	—	(Optional) 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.
Tunnel Source Interface	—	(Optional) Enter the physical interface.
<b>IPsec Information (These fields appear only under Operate &gt; Device Work Center)</b>		

**Table 1-74**      **Security > DMVPN (continued)**

Field		Description
Encryption Policy	Name	Enter the name of the transform set.
	ESP Encryption	Choose the encryption algorithm. The algorithm used to encrypt the payload.
	ESP Integrity	Choose the integrity algorithm. The algorithm used to check the integrity of the payload.
	AH Integrity	Choose the AH integrity from the drop-down list.
	Compression	Choose appropriate option to enable or disable payload compression.
	Mode	Choose the mode. Indicates the mode to transport the traffic.
<b>NHS Server</b>		
Cluster Support	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 or cluster.
	Priority	Select 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.
IP Address of Hub's physical interface	—	Enter the IP address of the hub's physical interface.

## Security > Easy VPN Remote

Cable modems, xDSL routers, and other forms of broadband access provide high-performance connections to the Internet, but many applications also require the security of VPN connections that perform a high level of authentication and encrypt the data between two endpoints. However, establishing a VPN connection between two routers can be complicated and typically requires tedious coordination between network administrators to configure the VPN parameters of the two routers.

The Cisco Easy VPN Remote feature eliminates much of this tedious work by implementing Cisco Unity Client Protocol, which allows most of the VPN parameters to be defined at a Cisco IOS Easy VPN server. This server can be a dedicated VPN device, such as a Cisco VPN 3000 series concentrator or a Cisco PIX Firewall or a Cisco IOS router that supports the Cisco Unity Client Protocol.

After the Cisco Easy VPN server is configured, VPN connection is created with minimal configuration on a Cisco device. When the Easy VPN remote initiates the VPN tunnel connection, the Cisco Easy VPN server pushes the IPsec policies to the Easy VPN remote and creates the corresponding VPN tunnel connection.

Before you create an Easy VPN Client template, create the necessary ACLs, such as the identical addressing ACL, the interesting traffic ACL, and the protected subnet ACL using the ACL template. For more information, refer to the [Cisco Prime Infrastructure 2.0 User Guide](#).

The following table describes the Template Detail fields on **Design > Feature Design > Features and Technologies > Security > Easy VPN Remote**.

**Table 1-75**      **Security > Easy VPN Remote**


Field	Description	
Easy VPN Remote Profile Name and Interface Configuration		
Profile Name	—	Enter a name for the profile.
Interface and Server Association	Inside Interfaces	These are the interfaces that are included in the Easy VPN connection. All hosts or subnets that are connected to these interfaces are a part of the VPN.
	Outside Interfaces	The WAN interface that connects to the Easy VPN server or concentrator.
	Virtual Template Number	This number provides a routable interface to selectively send traffic to different Easy VPN concentrators and to the Internet.
	Easy VPN Servers	Enter the Easy VPN server address. Up to ten IPv4 server addresses or server hostnames can be added.
	Idle Time	Enter the idle time for the server in seconds. The range is from 60 to 86400. The default value is 60.
Each VPN Remote Connection Settings		
Mode of Operation	Client	Choose the <b>Client</b> mode if you want the PCs and other devices on the router’s inside networks to form a private network with private IP addresses. Network Address Translation (NAT) and Port Address Translation (PAT) will be used for routing the traffic. Devices outside the LAN will not be able to ping the devices on the LAN or reach them directly.
	Network Extension	Choose the <b>Network Extension</b> mode if you want the devices that are connected to the inside interfaces to have IP addresses that are routable and reachable by the destination network. The devices at both ends of the connection will form one logical network. PAT is automatically disabled, allowing the PCs and hosts at both ends of the connection to have direct access to one another.
	Network Extension Plus	<div>Choose the <b>Network Extension Plus</b> mode to request an IP address via mode configuration and automatically assign it to an available loopback interface. The IPsec SAs for this IP address are automatically created by Easy VPN Remote. This IP address can be used for connecting to your router for remote management and troubleshooting (ping, Telnet, and Secure Shell).</div> <div><b>Note</b> If the router is not running a Cisco IOS image that supports Easy VPN Remote Phase 4 or later, you will not be able to set the Network Extension Plus mode.</div>
Protected Subnets ACL	—	Enter the ACL for the subnets that are not directly a part of the provided inside interface.

Table 1-75 Security &gt; Easy VPN Remote (continued)

Field		Description
Connection Method	Auto	Choose Auto if you want the VPN tunnel to be established automatically when the Easy VPN configuration is delivered to the router configuration file. However, you will not be able to control the tunnel manually.
	Manual	Choose Manual if you want to control when the VPN tunnel is established and terminated.
	Interesting Traffic	Choose Interesting Traffic when you want the tunnel to be established only when a specific traffic is sensed. This traffic is determined by the Interesting Traffic ACL.
<b>EasyVPN Remote Authentication Mechanisms</b>		
Primary Authentication	—	Choose the device authentication method. The options are Pre-shared Key and Digital Certificate.
Pre Shared Key Configuration	Group Name	Enter the IPsec group name. This group name must match the group name defined in the VPN concentrator or server. Obtain this information from your network administrator.
	Enable Encrypted Password	Select the <b>Enable Encrypted Password</b> check box to encrypt the password.
	Pre Shared Key	Selecting pre-shared keys allows for a secret key to be shared between two peers and be used by IKE during the authentication phase.
	Confirm Pre Shared Key	Reenter the pre-shared Key to confirm the key.
Digital Certificate	—	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 proved that the communication actually took place.
<b>Extended Authentication</b>		
Enable XAuth	—	Enable XAuth is enabled by default on Cisco IOS devices.
Use Web Authentication	—	Choose the <b>Use Web Authentication</b> radio button to use the web authentication method. Select the <b>Use HTTP Authorization for each client behind the Easy VPN Remote</b> check box to use the HTTP authorization.
Save Credentials	—	Select the <b>Save Credentials</b> radio button and provide the username and password. Reenter the password to confirm the password.
Prompt for Credential	—	Select the <b>Prompt for Credentials</b> radio button and provide the credentials when prompted.
<b>EasyVPN Remote Firewall Settings</b>		
Enable EasyVPN through Firewall	—	Select the <b>EasyVPN through Firewall</b> check box to enable the firewall settings.
cTCP Port Number	—	Enter the Cisco Tunneling Control Protocol (cTCP) port number. This number should match the cTCP port number on the EZVPN server. The range is from 1 to 65535. The default value is 10000.
NAT/Firewall Keepalive	—	Enter the Firewall Keepalive period, in seconds. The range is from 5 to 3600. The default value is 5.

## Security > Easy VPN Server

The Easy VPN Server feature introduces server support for the Cisco VPN Client Release 3.x and later and Cisco VPN hardware clients (such as the Cisco Integrated Services Routers and the Cisco Application-Specific Routers). By using IP Security (IPsec), the centrally managed IPsec policies are pushed to the client device by the server and helps end users minimize the configuration.

You can use the Dynamic Virtual Tunnel Interface or Dynamic Crypto Map method to configure an Easy VPN server.

The following table describes the Template Detail fields on **Design > Feature Design > Features and Technologies > Security > Easy VPN Server**.

**Table 1-76**      **Security > Easy VPN Server**

Field		Description
<b>Validation Criteria</b>		
Device Type	—	Choose <b>Routers</b> .
<b>Interface Configuration Methods</b>		
Outside Interface	—	Enter the interface name that connect to the WAN link.
Configure Dynamic Virtual Tunnel Interface	—	Enter the virtual template number and the IPsec profile name that you created in the IPsec Profile template (see <a href="#">“Security &gt; VPN Components &gt; IPsec Profile”</a> section on page 1-74). Alternatively, you can enter the name of an IPsec profile that already exists in the device. The IPsec profiles that already exist in the device are displayed in the device view.
Configure Dynamic Crypto Map	—	Enter the crypto map name and the transform set name that you created in the Transform Set template (see <a href="#">“Security &gt; VPN Components &gt; Transform Sets”</a> section on page 1-75). Alternatively you can enter the name of a transform set that already exists in the device. The transform sets that already exist in the device are shown in the device view.
<b>ISAKMP Settings</b>		
Client Configuration Address Type	—	Select the client configuration address type from the drop down list.
Enable Dead Peer Detection	—	Enable the device to send dead peer detection (DPD) messages to Easy VPN clients. If a client does not respond to the DPD messages, the connection is terminated.
Keep Alive Interval	—	Specify the number of seconds between DPD messages in the Keepalive Interval field. The range is from 10 to 3600.
Retry Interval	—	Specify the number of seconds between retries if the DPD messages fail. The range is from 2 to 60.
<b>AAA Group/User Policy</b>		
AAA Group Method List	—	Enter the same AAA Group Method List profile name that you created in the CLI template.
AAA User Method List	—	Enter the same AAA User Method List profile name that you created in the CLI template.

Table 1-76 Security &gt; Easy VPN Server (continued)

Field		Description
Enable PKI download	—	Select the <b>Enable PKI download</b> check box to obtain user attributes from the AAA server and push to the remote device through mode configuration. The username that is used to get the attributes is retrieved from the remote device certificate.
VPN groups	—	Provide those ISAKMP group names that are not present locally in the router but whose identity still needs to be matched with the ISAKMP profile.

**EasyVPN Group Configuration**

<b>General</b>		
General	Group Name	Enter an EasyVPN group name.
	Enable Encrypted Key	Select the <b>Enable Encrypted Key</b> check box to allow providing an encrypted pre-shared key.
	Pre-Shared Key	Pre-shared keys allow for a secret key to be shared between two peers and to be used by IKE during the authentication phase.
	Confirm Pre-Shared Key	Reenter the pre-shared Key to confirm the key.
Address Pool Configuration	Assign IP Address to Remote Clients	Select the <b>Assign IP Address to Remote Clients</b> check box to create new IP address pools for internal IP address allocation to clients.
	Starting IP Address	Enter the starting IP address of the range, for example, 1.1.1.1.
	Ending IP Address	Enter the ending IP address of the range, for example, from 1.1.1.1 to 1.1.254.1.
	Subnet Mask	Enter the subnet mask used by the connecting clients for local connectivity.
	Max Connections Allowed	Enter the maximum number of connections allowed in the configuration. The range is from 1 to 5000.
XAuth Options	Enable XAuth	Select the <b>Enable XAuth</b> check box to enable the extended authentication methods.
	XAuth Banner	Enter the banner that the server pushes to the Easy VPN Remote.
	Max Logins allowed per user	The maximum number of logins allowed per user. The range is from 1 to 10.
	Enable group lock for XAuth	Select the <b>Enable group lock for XAuth</b> check box to perform an extra authentication check during XAuth. The group name entered during XAuth is compared by the server with the group name sent for the pre-shared key device authentication. If they do not match, the server denies the connection.
	Save XAuth password on router	The client is allowed to store the password locally when prompted for its XAuth credentials after receiving the policy during IKE mode configuration on a subsequent connection to the server.
<b>DNS &amp; WINS</b>		
Domain Name	—	Enter the name of the DNS domain to which a group belongs.
Configure DNS Servers	—	Select the <b>Configure DNS Servers</b> check box to specify the primary and secondary DNS server for the group.

**Table 1-76**      **Security > Easy VPN Server (continued)**

Field		Description
Primary DNS Server	—	Enter the IP address of the primary DNS server.
Secondary DNS Server	—	Enter the IP address of the secondary DNS server.
Configure WINS Server	—	Select the <b>Configure WINS Server</b> check box to specify the primary and secondary WINS server for the group.
Primary WINS Server	—	Enter the IP address of the primary WINS server.
Secondary WINS Server	—	Enter the IP address of the secondary WINS server.
<b>Split Tunneling</b>		
Split Tunnel ACL	—	Enter the name of the ACL that represents the protected subnets for split tunneling purposes.
Split DNS Configuration	—	Enter the domain names that must be tunneled or resolved to the private network.
<b>Settings</b>		
Configuration Push	URL	Enter the URL that the remote device must use to get the configuration from the server. The URL must be a nonnull-terminated ASCII string that specifies the complete path of the configured file.
	Version	Enter the version of the configuration. The range is from 1 to 32767.
Backup Configuration	Backup Gateways	Assign backup gateways to push the list of backup gateways to the client device. These gateways are used if a previous gateway fails.
Access Settings	Include local LAN	Select the <b>Include local LAN</b> check box to allow a nonsplit tunneling connection to access the local subnetwork at the same time as the client.
	Enable perfect forward secrecy	Select the <b>Enable perfect forward secrecy</b> check box to notify the client about whether perfect forward secrecy is required for any IPsec SA.
Firewall and Proxy Settings	Enable Firewall Are-U-There	Select the <b>Enable Firewall Are-U-There</b> check box to enable the Are-U-There firewall.
	Browse Proxy Settings	Enter the browser proxy profile as configured by the Easy VPN Browser Proxy Template.
<b>Firewall Settings</b>		
Enable cTCP	—	Select the <b>Enable cTCP</b> check box to configure cTCP encapsulation for Easy VPN. A maximum of 10 port numbers can be configured.
cTCP Port Number(s)	—	Enter the cTCP port number.
cTCP Keep Alive	—	Enter the cTCP keep alive period, in seconds. The range is from 5 to 3600.

## Security > Easy VPN Server Proxy Setting

The Easy VPN Server Proxy Setting feature allows you to specify the browser proxy settings that will be pushed by the Easy VPN server to the EasyVPN remote and the Easy VPN clients. When you use the Easy VPN Server Proxy Setting feature, you do not have to manually modify the proxy settings of the web browser when you connect to the corporate network using the Cisco IOS VPN client or manually revert the proxy settings when you disconnect from the network.

The following table describes the Template Detail fields on **Design > Feature Design > Features and Technologies > Security > Easy VPN Server Proxy Setting**.

**Table 1-77**      **Security > Easy VPN Server Proxy Setting**

Field	Description
Browser Proxy Name	Enter a name for the browser proxy setting profile.
Proxy Server Settings Used by Client Browser	<ul style="list-style-type: none"> <li>Choose the <b>No Proxy Server</b> option if you do not want the clients in this group to use proxy server.</li> <li>Choose the <b>Automatically Detect Proxy Settings</b> option if you want the clients in this group to automatically detect a proxy server when they use the VPN tunnel.</li> <li>Choose the <b>Manual Configuration</b> option to manually configure a proxy server for the clients in this group.</li> </ul>
IP Address of Proxy Server	Enter the IP address of the proxy server.
Port	Enter the port number of the proxy server.
Do not Use Proxy Server for Accessing the Following Hosts	Enter the addresses of the hosts for whom the proxy server will not be used.
Bypass Proxy Serve for Local Addresses	Select the check box to prevent the clients from using the proxy server for local (LAN) addresses.

## Security > GETVPN-GroupMember

The following table describes the Template Detail fields on **Design > Feature Design > Features and Technologies > Security > GETVPN-GroupMember**.

**Table 1-78**      **Security > GETVPN-GroupMember**

Field	Description
<b>Group Information</b>	
Group ID	— Enter the group ID. This is a unique identity for a GETVPN group member. This can be a number or an IP address.
Group Name	— Enter the group Name for the GETVPN group member.



**Table 1-78**      **Security > GETVPN-GroupMember (continued)**

Field		Description
IKE Authentication Policy	—	Use this anchored field and its associated pop-up dialog box to specify the authentication type and policies for this GETVPN group member.
	Pre-Shared Key	Select this radio button to select pre-shared Key as the IKE authentication type. If you select this radio button, you must provide the key in the Pre-Shared Key field that is present immediately below the button.
	Confirm Pre-Shared Key	Enter the pre-shared key again to confirm. This field is displayed only when you select Pre-Shared Key as the authentication type.
	Digital Certificate	Select this radio button to 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.
	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 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 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, the more secure your IKE negotiations will be.
WAN Interface	—	Enter the WAN interface registration for the GETVPN group member.
<b>Traffic Details</b>		
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 via the group member will be dropped until the group member is registered successfully. After the group member is registered successfully and SAs are downloaded, this feature is disabled automatically.
<b>Key Servers</b>		

**Table 1-78**      **Security > GETVPN-GroupMember (continued)**

Field		Description
Primary Key Server	—	Enter the IP address or hostname 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	—	Select the <b>Enable Passive SA</b> check box to enable the Passive SA mode on the group member.

## Security > GETVPN-KeyServer

The following table describes the Template Detail fields on **Design > Configuration > Feature Design > Features and Technologies > Security > GETVPN-KeyServer**.

**Table 1-79**      **Security > GETVPN-KeyServer**

Field	Description
<b>Template Detail</b>	
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 number range is from 0 to 2147483647.
<b>IKE Authentication Policy</b>	
Authorization Type	<p>Click the <b>Preshared Keys</b> or <b>Digital Certificates</b> radio button:</p> <ul style="list-style-type: none"> <li>• <b>Preshared Keys</b>—This allows for a secret key to be shared between two peers and to be used by IKE during the authentication phase.</li> <li>• <b>Digital Certificates</b>—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.</li> </ul>
Priority	<p>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.</p> <p>Valid values range from 1 to 10000. The lower the number, the higher the priority.</p>

**Table 1-79**      **Security > GETVPN-KeyServer (continued)**

Field	Description
Encryption	<p>Choose the encryption algorithm from the drop-down list. The encryption algorithm is used to establish the Phase 1 SA for protecting Phase 2 negotiations:</p> <ul style="list-style-type: none"> <li>• AES-128—Encrypts according to the AES using 128-bit keys.</li> <li>• AES-192—Encrypts according to the AES using 192-bit keys.</li> <li>• AES-256—Encrypts according to the AES using 256-bit keys.</li> <li>• DES—Encrypts according to the DES using 56-bit keys.</li> <li>• 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.</li> </ul>
Hash	<p>The hash algorithm used in the IKE proposal. This algorithm creates a message digest that is used to ensure message integrity. The options are:</p> <ul style="list-style-type: none"> <li>• SHA (Secure Hash Algorithm)—Produces a 160-bit digest. SHA is more resistant to brute-force attacks than MD5.</li> <li>• MD5 (Message Digest 5)—Produces a 128-bit digest. MD5 uses less processing time than SHA.</li> </ul>
Diffie-Hellman Group	<p>The Diffie-Hellman group is used 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. The options are:</p> <ul style="list-style-type: none"> <li>• 1—Diffie-Hellman Group 1 (768-bit modulus).</li> <li>• 2—Diffie-Hellman Group 2 (1024-bit modulus).</li> <li>• 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.</li> </ul>
Lifetime	<p>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.</p> <p>You can specify a value from 60 to 2147483647. The default is 86400.</p>
Registration Interface	Enter the name of the interface to which the crypto map must be associated.
<b>Traffic Details</b>	
Local Exception ACL	Choose an ACL for the traffic that must be excluded from 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 via the group member will be dropped until the group member is registered successfully. After the group member is registered successfully and SAs are downloaded, this feature is disabled automatically.
<b>Key Server Information</b>	
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.

**Table 1-79**      **Security > GETVPN-KeyServer (continued)**

Field	Description
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 the 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.
<b>Migration</b>	
Enable Passive SA	Use this option to enable the Passive SA mode on the group member. The Passive SA mode overrides the receive-only SA option on the key server and encrypts all outbound traffic.
Group Name	Enter the group name for the GETVPN group member template.

## Security > ScanSafe

Cisco ISR Web Security with Cisco Scansafe is a cloud-based Security as a Service (SaaS) that allows you to scan the content of the HTTP and HTTPS traffic. When Cisco ISR Web Security with Cisco ScanSafe is integrated with a router, the selected HTTP and HTTPS traffic is redirected to the ScanSafe cloud for content scanning and malware detection.

When Cisco ISR Web Security with Cisco ScanSafe is enabled and the ISR is configured to redirect web traffic to Cisco ISR Web Security with Cisco ScanSafe, the ISR transparently redirects HTTP and HTTPS traffic to the ScanSafe proxy server based on the IP address and port. You can configure the ISR to relay web traffic directly to the originally requested web server without being scanned by Cisco ISR Web Security with Cisco ScanSafe.

### Whitelisting Traffic

You can configure the ISR so that approved web traffic is not redirected to Cisco ISR Web Security with Cisco ScanSafe for scanning. When you bypass this scanning, the ISR retrieves the content directly from the originally requested web server without contacting Cisco ISR Web Security with Cisco ScanSafe. When it receives the response from the web server, it sends the data to the client. This is called *whitelisting* traffic.

See

[http://www.cisco.com/en/US/docs/security/web\\_security/ISR\\_SS/ISR\\_ScanSafe\\_SolutionGuide.pdf](http://www.cisco.com/en/US/docs/security/web_security/ISR_SS/ISR_ScanSafe_SolutionGuide.pdf) for more information on ScanSafe.

The following table describes the Template Detail fields on **Design > Configuration > Feature Design > Features and Technologies > Security > ScanSafe**.

**Table 1-80**      **Security > ScanSafe**

Field	Description
<b>Server Information</b>	
Primary Server	Enter the IPv4 address or hostname of the primary ScanSafe server.
HTTP Port	Specify the HTTP port through which HTTP requests are to be redirected to the primary server. By default, ScanSafe uses port 80 for the HTTP traffic. However, you can choose to use different ports for each request type.

**Table 1-80**      **Security > ScanSafe (continued)**

Field	Description
HTTPS Port	Specify the HTTPS port to redirect the HTTPS requests to the primary server. By default, ScanSafe uses port 443 for HTTPS traffic. However, you can choose to use different ports for each request type.
Secondary Server	Enter the IPv4 address or hostname of the secondary ScanSafe server.
HTTP Port (secondary)	Specify the HTTP port through which HTTP requests are to be redirected to the secondary server. By default, ScanSafe uses port 80 for HTTP traffic.
HTTPS Port	Specify the HTTPS port through which HTTPS requests are to be redirected 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 server to indicate the organization from which the request originated. The license is a 16-byte hexadecimal key.
Encrypt License Info	Select the <b>Encrypt License Info</b> check box to encrypt the license information.
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 is enabled.
Router behavior when ScanSafe server fail to respond	Specify how the ISR should handle the incoming traffic when it cannot reach the configured ScanSafe proxy servers. The options are Drop all traffic or Allow all traffic. Drop all traffic is the default.
<b>User Information</b>	
Global User	Enter a Global User when web authentication (webauth) is not configured under the router's ingress interface.
Global User Group	Enter a Global User Group when 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. The user group information 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 send the whitelist information to the ScanSafe Tower and specify the Safe URL, Safe User Agent, and Safe ACL information that is to be sent.

# CLI Templates Field Descriptions

The following topics describe the fields used in the system CLI templates.

- [802.1X Change of Authorization-IOS, page 1-94](#)
- [Access Layer-IOS, page 1-95](#)
- [Authentication Proxy-IOS, page 1-97](#)
- [Banner Configuration-IOS, page 1-98](#)
- [Certificate Authority-IOS, page 1-99](#)
- [Core Layer-IOS, page 1-100](#)
- [Crypto Map Configuration-IOS, page 1-101](#)
- [DNS Configuration-IOS, page 1-102](#)
- [DNS Configuration-NAM, page 1-103](#)
- [DNS Configuration-Nexus, page 1-103](#)
- [Distribution Layer-IOS, page 1-104](#)
- [EEM Environmental Variables-IOS, page 1-106](#)
- [Embedded Event Manager Configuration-IOS, page 1-107](#)
- [Enable Password-IOS, page 1-108](#)
- [GOLD Boot Level and Monitoring Test for Cat6k Devices-IOS, page 1-109](#)
- [GOLD Monitoring Test for Non Stack Devices-IOS, page 1-110](#)
- [GOLD Monitoring Test for Stack Enabled Devices-IOS, page 1-111](#)
- [HTTP-HTTPS Server and WSMA Configuration-IOS, page 1-111](#)
- [MAC Trap Configuration, page 1-112](#)
- [Mediatrace-Responder-Configuration, page 1-113](#)
- [Medianet-PerfMon, page 1-113](#)
- [RADIUS Configuration-IOS, page 1-114](#)
- [Reload Configuration-IOS, page 1-116](#)
- [Reload Configuration-NAM, page 1-116](#)
- [Web User Configuration-NAM, page 1-116](#)
- [User Defined Protocol Configuration-NAM, page 1-117](#)

## 802.1X Change of Authorization-IOS

Use this option to support RADIUS client configuration for dynamic authorization for switches.

The following table describes the Template Detail fields in **CLI Templates > System Templates - CLI > 802.1X Change of Authorization-IOS**.

**Table 1-81** CLI Templates > System Templates - CLI > 802.1X Change of Authorization-IOS

Field	Description
<b>Form View</b>	
RADIUS client IP Address or Host Name	DNS host name or IP address of the RADIUS server host
Type of authorization the device uses for RADIUS clients	Specify the type of authorization ( <b>any</b> , <b>all</b> , <b>session key</b> ) the device must use for RADIUS clients. The client must match the configured attributes for authorization.
RADIUS Key shared between the device and RADIUS clients	Specify the authentication and encryption key to the RADIUS server.  The key is a text string that must match the encryption key used on the RADIUS server. The leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in the key, do not enclose the key in quotation marks unless the quotation marks themselves are part of the key
Port on which the device listens for RADIUS requests	Specify the port number on which the device listens for RADIUS requests.  The port number should be from 0 to 65535. The default value is 1700.

## Access Layer-IOS

Use this option to configure the platform, LAN Switch Universal Settings, Access Switch Global Settings, Client Connectivity, and connect the devices to Distribution or WAN Router.

The following table describes the Template Detail fields in **CLI Templates > System Templates - CLI > Access Layer-IOS**.

**Table 1-82** CLI Templates > System Templates - CLI > Access Layer-IOS

Field	Description
<b>Form View tab</b>	
Device Type	Deploys the template only on the selected device type.  <b>Note</b> To avoid deployment issues, do not edit this field.
Device OID	Deploys the template only on the selected device OID.  <b>Note</b> To avoid deployment issues, do not edit this field.
Switch Number	Enter the Switch number for Catalyst 2960-S and 3750-X Platform.
<b>LAN Switch Universal Configuration</b>	
Host name	Enter the hostname for the device to be configured.
IP Domain-name	Enter the default domain name that the Cisco IOS software uses to complete unqualified hostnames (names without a dotted-decimal domain name). Do not include the initial period that separates an unqualified name from the domain name.
SNMP-server community RO	Enter the SNMP-server community read-only access (RO) to set up the community access string to permit access to the Simple Network Management Protocol (SNMP).
SNMP-server community RW	Enter the SNMP-server community read-write access (RW) to set up the community access string to permit access to the Simple Network Management Protocol (SNMP).
Enable Secret Password	Enter the <b>Enable Secret Password</b> command to provide encryption automatically.
Username Admin Password	Enter the Username Admin Password.

**Table 1-82** CLI Templates > System Templates - CLI > Access Layer-IOS (continued)

Field	Description
IP Address of Tacacs Server	Enter the IP address of the TACACS server.
TACACS Key	Enter the TACACS secret key to authenticate the switch to the TACACS server.
NTP Server IP Address	Enter the IP address of the NTP Server in order to keep the clocks in sync for applications and other desktop processes.
Time Zone	Enter the time zone to comply with the new Daylight Saving Time (DST) changes.
Hours offset from UTC	Select the number of hours behind or ahead from Coordinated Universal Time (UTC).
Minutes offset from UTC	Enter the number of minutes behind or ahead from Coordinated Universal Time (UTC).
Summer Time zone	Enter the Daylight Saving Time.
<b>Access Switch Global Settings and Client Connectivity</b>	
Voice VLAN	Enter the voice VLAN to enable access ports to carry IP voice traffic from an IP phone.
Data VLAN	Enter the data VLAN to carry only user-generated traffic.
<b>Configure Access Switch Global Settings</b>	
Management VLAN	Enter the management VLAN for managing the switch from a remote location by using protocols such as telnet, SSH, SNMP, syslog, and so forth.
Management IP Address	Enter the management IP address for discovering, monitoring, auditing, and managing the IP address space used on a network.
Management Subnet Mask	Enter the management subnet mask.
Default Router IP Address	Enter the IP address of the default router.
<b>Other Settings</b>	
Interface Type to Configure Client Connectivity	Select the interface type from the drop-down list
Start Interface Number	Enter the starting interface number, for example, 0/1 for Gigabit Ethernet, 1 for PortChannel.
End Interface Number	Enter the ending interface number, for example, 2.
Connect to Distribution or WAN Router	Select the required option from the drop-down list.
Channel Group Number	Enter the Channel Group number to assign and configure an EtherChannel interface to an EtherChannel group.
Interface Type for Connect to Distribution or WAN Router	Select the Interface Type from the drop-down list.
Start Interface Number	Enter the starting interface number, for example, 0/1 for Gigabit Ethernet, 1 for PortChannel.
End Interface Number	Enter the ending interface number, for example, 2.
Unused VLAN for Hopping	Enter the unused VLAN as native VLAN.



## Authentication Proxy-IOS

Use this option to log in to the network or access the Internet using HTTP and helps you to deploy the Authentication Proxy system-defined configuration template on Cisco IOS devices that have been configured for VPN functionality.

The following table describes the Template Detail fields on **CLI Templates > System Templates - CLI > Authentication Proxy-IOS**.

**Table 1-83** CLI Templates > System Templates - CLI > Authentication Proxy-IOS

Field	Description
AAA Action	Select the required option to enable, disable. If you do not want to make any change, select <b>No Change</b> .
AAA Method1	Select either TACACS+ or RADIUS as your first method of authorization. Select <b>None</b> if you do not want to configure.
AAA Method2	Select either TACACS+ or RADIUS as your second method of authorization, based on your selection in the first method. Select <b>None</b> if you do not want to configure.
Cache Timeout in Minutes	Timeout value. The default timeout value can be in the range from 1 to 2147483647. The default value is 60.
Banner Action	Select <b>Enable</b> or <b>Disable</b> to set or reset Banner display in the login page. <ul style="list-style-type: none"> <li>If you select Enable, the router name is displayed in the login page.</li> <li>If you select Disable, then the router name is not displayed.</li> </ul> If you do not want to make any changes to the banner, select <b>No Change</b> .
Banner Text	Enter the text that you want displayed in the banner. If you enter the banner text, then this text is displayed instead of the router name in the login page.  This is an optional field.
Authentication Proxy Rule Action	Select <b>Enable</b> or <b>Disable</b> an authentication proxy rule. <ul style="list-style-type: none"> <li>If you select Enable, a named authentication proxy rule is created and associated with access list.</li> <li>If you select Disable, the associated proxy rule is removed.</li> </ul> Select <b>No Change</b> if you do not want to make changes to the Authentication Proxy Rule group of fields.
Authentication Proxy Rule Name	Enter a name for the authentication proxy rule.  The name can be up to 16 alphanumeric characters.
Authentication Proxy Rule Overriding Timeout	Enter a timeout value to override the default cache timeout.  This is an optional field. The overriding timeout value should be in the range of 1 and 2147483647.
Authentication Proxy Rule ACL Number/Name	Enter a Standard Access list name or number to be used with the Authentication proxy.  This is an optional field.
New Model [AAA] Action	Select the required option to enable or disable AAA.

## Banner Configuration-IOS

The following table describes the Template Detail fields on **CLI Templates > System Templates - CLI > Banner Configuration-IOS**.

**Table 1-84** CLI Templates > System Templates - CLI > Banner Configuration-IOS

Field	Description
<b>Form View tab</b>	
Motd Action	Select the appropriate option to add or remove a message of the day banner. Select <b>No Change</b> if you are not modifying an existing task, and you do not want to change the value in this field.
Motd Message	Enter message, if you select Add in Action field. When a user connects to the router, the message-of-the-day (Motd) banner appears before the login prompt.
Exec Action	Select the appropriate option to add or remove an Exec banner. Select <b>No Change</b> if you are not modifying an existing task, and you do not want to change the value in this field.
Exec Message	Enter message, if you select Add in Action field. After the user logs in to the router, the Exec banner or the incoming banner will be displayed.
Incoming Action	Select the appropriate option to add or remove an Incoming banner. Select <b>No Change</b> if you are not modifying an existing task, and you do not want to change the value in this field.
Incoming Message	Enter message, if you select Add in Action field. After the user successfully logs in to the router, the Exec banner or the incoming banner will be displayed.
Login Action	Select the appropriate option to add or remove a Login banner. Select <b>No Change</b> if you are not modifying an existing task, and you do not want to change the value in this field.
Login Message	Enter message, if you select Add in Action field. When a user connects to the router, the Motd banner (if configured) appears first, followed by the login banner and prompts.
Slip_PPP Action	Select the appropriate option to add or remove a Slip/PPP banner. Select <b>No Change</b> if you are not modifying an existing task, and you do not want to change the value in this field.
Slip_PPP Message	Enter custom SLIP or PPP connection message, if you select Add in Action field. This is useful when legacy client applications require a specialized connection string.

## Certificate Authority-IOS

This template provides manageability and scalability for IP security standards on VPN devices.

The following table describes the Template Detail fields on **CLI Templates > System Templates - CLI > Certificate Authority-IOS**.

**Table 1-85** *CLI Templates > System Templates - CLI > Certificate Authority-IOS*

Field	Description
<b>Form View tab</b>	
Certificate Authority Action	Select Enable or Disable to activate/deactivate Certificate Authority (CA). <ul style="list-style-type: none"> <li>If you select Enable you can create or modify CA.</li> <li>If you select Disable, you can delete the CA.</li> </ul>
Certificate Authority Name	Enter the CA name. This name is used to identify the Certificate Authority to be configured.  This name is the CA domain name.
Enrollment URL Action	<ul style="list-style-type: none"> <li>Select Enable to allow router to connect to the CA, using the URL specified in the Value field.</li> <li>Select Disable, if you do not want to connect to the CA.</li> <li>Select <b>No Change</b> to leave the Enrollment URL field unchanged.</li> </ul>
Enrollment URL Value	Enter the URL of the CA.  The URL should include any available nonstandard cgi-bin script location.
Enrollment Mode Action	<ul style="list-style-type: none"> <li>Select Enable if the CA provides a Registration Authority (RA).</li> <li>Select Disable to disable the specified LDAP Server.</li> <li>Select <b>No Change</b> to leave the Enrollment Mode field unchanged.</li> </ul>
Enrollment Mode LDAP Server	Enter the LDAP server of the CA, if your CA system provides an RA.  LDAP server contains the location of CRLs (certification revocation lists) and certificates.
Enrollment Retry Period in Minutes	Enter the wait period between certification request retries.  The wait period is from 1 to 60 minutes.  Select this option to set the default wait period to 1 minute.
Enrollment Retry Count Number	Enter the certification request retry number.  The retry number must be from 1 to 100.  Select this option to set the default retry period to 1 minute.
CRL Optional Action	Select Enable to check the Certificate Revocation List.  If you select Disable, Certificate Revocation list is unchecked.  If you do not want to make any change, select <b>No Change</b> .
Certificate Query Action	Select an option to enable, disable or make no change to certificate query. <ul style="list-style-type: none"> <li>If you select Enable, certificate query will be added to all trust points on the router.</li> <li>If you select Disable, the certificate will not be queried.</li> </ul>

**Table 1-85** *CLI Templates > System Templates - CLI > Certificate Authority-IOS (continued)*

Field	Description
RSA Key pairs Action	Select an option to generate, delete or make no change to the RSA key pairs. This feature allows you to configure a Cisco IOS router to have multiple key pairs.  Thus, the Cisco IOS software can maintain a different key pair for each identity certificate.
RSA Key pairs Key Type	Specify the key type: <ul style="list-style-type: none"> <li>General Purpose—To generate a general purpose key pair that is used for both encryption and signature.</li> <li>Usage—To generate separate usage key pairs for encrypting and signing documents.</li> </ul>
Enter number of modulus bits	Choose the size of the key modulus in the range of 360 to 4096 for Signature Keys. Choosing a key modulus greater than 512 may take a few minutes.

## Core Layer-IOS

Use this option to configure the Platform, LAN Switch Universal Settings, Core Switch Global Settings, IP Multicast Routing, and connect the devices to Distribution Layer.

The following table describes the Template Detail fields on **CLI Templates > System Templates - CLI > Core Layer-IOS**.

**Table 1-86** *CLI Templates > System Templates - CLI > Core Layer-IOS*

Field	Description
<b>Form View tab</b>	
<b>Configure LAN Switch Universal Setting</b>	
Host name	Enter the hostname of the LAN Switch Universal Configuration.
IP Domain-name	Enter the default domain name that the Cisco IOS software uses to complete unqualified hostnames (names without a dotted-decimal domain name). Do not include the initial period that separates an unqualified name from the domain name.
SNMP-server community RO	Enter the SNMP-server community read-only access (RO) to set up the community access string to permit access to the Simple Network Management Protocol (SNMP).
SNMP-server community RW	Enter the SNMP-server community read-write access (RW) to set up the community access string to permit access to the Simple Network Management Protocol (SNMP).
Enable Secret Password	Enter the <b>enable secret password</b> command to provide encryption automatically
Username Admin Password	Enter the Username Admin Password.
IP Address of Tacacs Server	Enter the IP Address of the TACACS server.
TACACS Key	Enter the TACACS secret key to authenticate the switch to the TACACS server.
NTP Server IP Address	Enter the IP address of the NTP Server in order to keep the clocks in sync for applications and other desktop processes.
Time Zone	Enter the time zone to comply with the new Daylight Saving Time (DST) changes.

**Table 1-86** *CLI Templates > System Templates - CLI > Core Layer-IOS (continued)*

Field	Description
Hours offset from UTC	Select the number of hours behind or ahead from Coordinated Universal Time (UTC).
Minutes offset from UTC	Enter the number of minutes behind or ahead from Coordinated Universal Time (UTC).
Summer Time zone	Enter the Daylight Saving Time.
<b>Configure the Core Switch Global Settings</b>	
Loopback-1 IP Address	Enter the Loopback-1 IP address.
Loopback-2 IP Address	Enter the Loopback-2 IP address.
Autonomous System Number	Enter the autonomous system number to uniquely identify the network.
Network Address	Enter the network address.
Inverse Mask	Enter the inverse mask.
IP address of Rendezvous-point	Enter the IP address of Rendezvous-point (RP), which acts as the meeting place for sources and receivers of multicast data.
Access List Number	Enter the access list number.
Multicast Network	Enter the multicast network address.
Multicast Inverse Mask	Enter the multicast inverse mask address.
<b>Other Setting</b>	
MSDP Core Switch IP Address to Configure IP Multicast Routing	Enter the Multicast Source Discovery Protocol (MSDP) to allow multicast sources for a group to be known to all rendezvous points (RPs) in different domains.
<b>Connecting to Distribution Layer</b>	
Port Channel Number	Enter the port channel number.
Port Channel IP Address	Enter the port channel IP address.
Port Channel Subnet Mask	Enter the port channel subnet mask.
TenGigabitEthernet First Interface Number	Enter the TenGigabitEthernet first interface number.
TenGigabitEthernet Second Interface Number	Enter the TenGigabitEthernet second interface number.

## Crypto Map Configuration-IOS

Use this option to configure IPSec on devices. You must configure the IKE and Transform configuration before configuring this template, and it can be downloaded only to VPN-enabled devices

The following table describes the Template Detail fields on **CLI Templates > System Templates - CLI > Crypto Map Configuration-IOS**.

**Table 1-87** *CLI Templates > System Templates - CLI > Crypto Map Configuration-IOS*

Field	Description
<b>Form View tab</b>	
Crypto Map Action	Select an option to add or remove the Cisco IOS configuration.

**Table 1-87** CLI Templates > System Templates - CLI > Crypto Map Configuration-IOS

Field	Description
Crypto Map Name	Enter the name for the crypto map.
Map Number	Enter the number for the crypto map. The value must be from 1 to 65535.
Map Type	Select the map type (manual or isakmp) for the crypto map. <ul style="list-style-type: none"> <li>Manual - Manual keying is usually only necessary when a Cisco device is configured to encrypt traffic to another vendor's device that does not support Internet Key Exchange (IKE).</li> <li>ISAKMP - The ISAKMP provides a framework for Internet key management and provides the specific protocol support for negotiation of security attributes.</li> </ul>
Map Description	Enter the description for the crypto map.
Crypto ACL	Enter the extended access list for crypto map.
IPSec Peer	Enter the IPsec peer hostname or IP address to be associated with the crypto map.
Transform Set Name	Enter the transform set name (see <a href="#">Security &gt; VPN Components &gt; Transform Sets, page 1-75</a> ) to be used with the crypto map.

## DNS Configuration-IOS

Use this option to configure Domain Name System (DNS) on Cisco IOS devices.

The following table describes the Template Detail fields on **CLI Templates > System Templates - CLI > DNS Configuration-IOS**.

**Table 1-88** CLI Templates > System Templates - CLI > DNS Configuration-IOS

Field	Description
<b>Form View tab</b>	
Add DNS Servers	Enter the IPv4 Address/IPv6 Address of DNS name server(s) that you want to add. Separate multiple addresses with commas. If the device accepts only one DNS server, then the first address will be considered.
Remove DNS Servers	Enter the IPv4 Address/IPv6 Address of DNS name server(s) that you want to remove. Separate multiple addresses with commas.
Remove Domain Name	Select this option to remove the domain names. If you do not want to make any change, select <b>No Change</b> .
Domain Name	Enter the IP addresses of DNS name server(s) that you want to remove. Separate multiple addresses with commas.
Domain Lookup	Select to enable or disable IP DNS-based hostname-to-address translation. If you do not want to make any change, select <b>No Change</b> .

**Table 1-88** *CLI Templates > System Templates - CLI > DNS Configuration-IOS (continued)*

Field	Description
CLNS NSAP	Select to enable or disable or make no change to the CLNS NSAP option. If this option is enabled, any packet with the specified CLNS NSAP prefix causes CLNS (Connectionless Network Service) protocol to behave as if no route were found.  If you do not want to make any change, select <b>No Change</b> .
OSPF	Select to enable or disable or make no change to the OSPF (Open Shortest Path First) protocol option.  If you do not want to make any change, select <b>No Change</b> .
Domain List Action	Select an option to add, remove, or make no change to the domain list.  If you do not want to make any change, select <b>No Change</b> .
Domain List	Enter domain names to complete unqualified hostnames, or add to the existing list.  Separate multiple domain names with commas.  Do not include an initial period before domain names.

## DNS Configuration-NAM

Use this option to configure Domain Name System (DNS) on NAM category devices.

The following table describes the Template Detail fields on **CLI Templates > System Templates - CLI > DNS Configuration-NAM**.

**Table 1-89** *CLI Templates > System Templates - CLI > DNS Configuration-NAM*

Field	Description
<b>Form View tab</b>	
Add DNS Servers	Enter the IPv4 Address addresses of DNS name server(s) that you want to add.  Separate multiple addresses with commas.  If the device accepts only one DNS server, then the first address will be considered.
Remove Domain Name	Select this option to remove the domain names.
Domain Name	Enter the IP addresses of DNS name server(s) that you want to remove.  Separate multiple addresses with commas.
Disable Name Servers	Select to disable domain name servers.

## DNS Configuration-Nexus

Use this option to configure Domain Name System - DNS on Nexus devices.

The following table describes the Template Detail fields on **CLI Templates > System Templates - CLI > DNS Configuration-Nexus**.

**Table 1-90** CLI Templates > System Templates - CLI > DNS Configuration-Nexus

Field	Description
<b>Form View tab</b>	
Add DNS Servers	Enter the IPv4 Address/IPv6 Address of DNS name server(s) that you want to add. Separate multiple addresses with commas. If the device accepts only one DNS server, then the first address will be considered.
Remove DNS Servers	Enter the IPv4 Address/IPv6 Address of DNS name server(s) that you want to remove. Separate multiple addresses with commas.
Remove Domain Name	Select this option to remove the domain names.
Domain Name	Enter the IP addresses of DNS name server(s) that you want to remove. Separate multiple addresses with commas.
Domain Lookup	Select to enable or disable IP DNS-based hostname-to-address translation. If you do not want to make any change, select <b>No Change</b> .
Domain List Action	Select an option to add, remove, or make no change to the domain list. If you do not want to make any change, select <b>No Change</b> .
Domain List	Enter domain names to complete unqualified hostnames, or add to the existing list. Separate multiple domain names with commas. Do not include an initial period before domain names.

## Distribution Layer-IOS

Use this option to configure the Platform, LAN Switch Universal Settings, Distribution Global Settings, and connect the devices to Access Layer and LAN Core or WAN Router.

The following table describes the Template Detail fields on **CLI Templates > System Templates - CLI > Distribution Layer-IOS**.

**Table 1-91** CLI Templates > System Templates - CLI > Distribution Layer-IOS

Field	Description
<b>Form View tab</b>	
Device Type	Deploys the template only on the selected device type. <b>Note</b> Do not edit this field to avoid deployment issues.
Device OID	Deploys the template only on the selected device OID. <b>Note</b> Do not edit this field to avoid deployment issues.
Switch Number	Enter the Switch number.
<b>LAN Switch Universal Configuration</b>	
Host name	Enter the hostname of the LAN Switch Universal Configuration.



**Table 1-91** *CLI Templates > System Templates - CLI > Distribution Layer-IOS (continued)*

Field	Description
IP Domain-name	Enter the default domain name that the Cisco IOS software uses to complete unqualified hostnames (names without a dotted-decimal domain name). Do not include the initial period that separates an unqualified name from the domain name.
SNMP-server community RO	Enter the SNMP-server community read-only access (RO) to set up the community access string to permit access to the Simple Network Management Protocol (SNMP).
SNMP-server community RW	Enter the SNMP-server community read-write access (RW) to set up the community access string to permit access to the Simple Network Management Protocol (SNMP).
Enable Secret Password	Enter the <b>enable secret password</b> command to provide encryption automatically.
Username Admin Password	Enter the Username Admin Password.
IP Address of Tacacs Server	Enter the IP address of the TACACS server.
TACACS Key	Enter the TACACS secret key to authenticate the switch to the TACACS server.
NTP Server IP Address	Enter the IP address of the NTP Server in order to keep the clocks in sync for applications and other desktop processes.
Time Zone	Enter the time zone to comply with the new Daylight Saving Time (DST) changes.
Hours offset from UTC	Select the number of hours behind or ahead from Coordinated Universal Time (UTC).
Minutes offset from UTC	Enter the number of minutes behind or ahead from Coordinated Universal Time (UTC).
Summer Time zone	Enter the Daylight Saving Time.
<b>Distribution Global Settings Configuration</b>	
Loopback-1 IP Address	Enter the Loopback-1 IP address.
IP address of Rendezvous-point	Enter the IP address of Rendezvous-point (RP), which acts as the meeting place for sources and receivers of multicast data.
Multicast Network Address	Enter the multicast network address.
Network Address	Enter the network address.
Inverse Mask	Enter the inverse mask address.
Autonomous System Number	Enter the autonomous system number to uniquely identify each network.
<b>Other Setting</b>	
Access List Number	Enter the access list number.
<b>Connecting to Access Layer</b>	
Data VLAN	Enter the data VLAN to carry only user-generated traffic.
Voice VLAN	Enter the voice VLAN to enable access ports to carry IP voice traffic from an IP phone.
Management VLAN	Enter the management VLAN for discovering, monitoring, auditing, and managing the IP address space used on a network.
Unused VLAN for Hopping	Enter the unused VLAN as native VLAN to prevent hopping.
Channel Group Number	Enter the channel group number to assign and configure an EtherChannel interface to an EtherChannel group.
Interface Type	Select the interface type from the drop-down list.

**Table 1-91** CLI Templates > System Templates - CLI > Distribution Layer-IOS (continued)

Field	Description
TenGigabitEthernet First Interface Number	Enter the TenGigabitEthernet first interface number.
TenGigabitEthernet Second Interface Number	Enter the TenGigabitEthernet second interface number.
DHCP Server IP Address	Enter the Dynamic Host Configuration Protocol (DHCP) IP Address to allocate the network device an IP address.
Data VLAN IP Address	Enter the data VLAN IP address.
Data VLAN IP Mask	Enter the data VLAN IP mask.
Voice VLAN IP Address	Enter the voice VLAN IP address.
Voice VLAN IP Mask	Enter the voice VLAN IP mask.
Management VLAN IP Address	Enter the Management VLAN IP address.
Management VLAN IP Mask	Enter the Management VLAN IP mask.
<b>Connecting to LAN Core or WAN Router</b>	
Port Channel Number	Enter the port channel number.
Port Channel IP Address	Enter the port channel IP address.
Port Channel Subnet Mask	Enter the port channel subnet mask.
Network Address	Enter the network address.
Network Subnet Mask	Enter the network subnet mask.
Interface Type	Select the interface type from the drop-down list.
Start Interface Number	Enter the starting interface number for connecting to LAN Core or WAN router.
End Interface Number	Enter the ending interface number for connecting to LAN Core or WAN router.

## EEM Environmental Variables-IOS

Use this option to configure Embedded Event Manager (EEM) Environmental variables used by the EEM TCL script policies on Cisco IOS devices.

The following table describes the Template Detail fields on **CLI Templates > System Templates - CLI > EEM Environmental Variables-IOS**.

**Table 1-92** CLI Templates > System Templates - CLI > EEM Environmental Variables-IOS

Field	Description
<b>Form View tab</b>	
Action	Select either: <ul style="list-style-type: none"> <li><b>Add</b>—to add one or more variables.</li> <li>or</li> <li><b>Remove</b>—to remove one or more variables.</li> </ul>

**Table 1-92** CLI Templates > System Templates - CLI > EEM Environmental Variables-IOS

Field	Description
Variable Name	Enter the name for the variable. Example: <code>my_counter</code> You can create a maximum of five variables at a time.
Variable Value	Enter the value for the variable. Example: <code>15</code> Now the variable <code>my_counter</code> will have the value <code>15</code> .

**Note**

Five variable names and variable values can be entered at one time. To enter more than five variable names and values, the template must be redeployed.

## Embedded Event Manager Configuration-IOS

Use this option to configure Embedded Event Manager (EEM) scripts or applets on the Cisco IOS devices.

The following table describes the Template Detail fields on **CLI Templates > System Templates - CLI > Embedded Event Manager Configuration-IOS**.

**Table 1-93** CLI Templates > System Templates - CLI > Embedded Event Manager Configuration-IOS

Field	Description
<b>Form View tab</b>	
EEM Configuration Action	Select <b>Register</b> or <b>Unregister</b> to register or unregister a script or applet.
EEM Configuration Policy Type	Select either <b>Script</b> or <b>Applet</b> as the policy. When you choose script as the policy type, enter the following fields: <ul style="list-style-type: none"> <li>Create New Directory</li> <li>Directory Name</li> <li>Enter the Server Name</li> <li>Enter the Script File Location with Name</li> </ul> When you choose Applet as the policy type, enter the following fields: <ul style="list-style-type: none"> <li>Enter the Applet Name</li> <li>Enter the Applet File Content</li> </ul>
Create New Directory	Check this option if you want to create a new directory on the device to copy the script. If you select this check box, the input given in the Directory Name text box is used to create a new directory.

**Table 1-93** CLI Templates > System Templates - CLI > Embedded Event Manager Configuration-IOS (continued)

Field	Description
Directory Name	Enter the absolute path of the directory where the file needs to be placed on the device.  Example: <b>disk0:/Testing</b> Here a new directory Testing is created in the device under the disk0 partition. Ensure that the selected directory has enough space before the script files are copied.
Enter the Server Name	Enter the TFTP server name.  <b>Note</b> The script file should be available in the TFTP boot folder.
Enter the Script File Location	Use this option to enter the file location to upload the scripts to deploy on the device. Ensure that you enter the absolute path along with the filename.  <b>Note</b> You can specify only single script file.
Enter the Applet Name	Enter the Applet Name if you have chosen <b>Unregister</b> as the EEM Configuration Action.
Enter the Applet File Content	Enter the Applet File Content if you have chosen <b>Register</b> as the EEM Configuration Action.

## Enable Password-IOS

Use this option to configure the enable or secret password and enter into the enable mode on Cisco IOS devices.

The following table describes the Template Detail fields on **CLI Templates > System Templates - CLI > Enable Password-IOS**.

**Table 1-94** CLI Templates > System Templates - CLI > Enable Password-IOS

Field	Description
<b>Form View tab</b>	
Action	Select an option to enable, disable, or make no change to the enable password. If you do not want to make any change, select <b>No Change</b> .
Enable Password	Enter the enable password.

**Table 1-94** CLI Templates > System Templates - CLI > Enable Password-IOS (continued)

Field	Description
Password Level	<p>Set the Enable Password level. The level can be from 1 to 15.</p> <p>For a Cisco IOS device, it is advisable not to disable both Enable Password and Enable Secret password as enabling the password will not allow the Cisco IOS device to go into the Enable mode. You can do this only if you have the console password for the device.</p> <p>If you have selected Enable Password as <b>No Change</b> in the Common Parameters pane, and selected Disable for Enable Secret in the IOS Parameters pane, then Enable Secret Password is updated in the Device and Credentials database.</p> <p>If you have selected Enable Password as <b>Disable</b> in the Common Parameters pane, and selected <b>No Change</b> for Enable Secret in the IOS Parameters pane, then Enable Password is updated in the Device and Credentials database.</p>
Encrypted	Select this option to encrypt the password.
Secret Action	Select an option to enable, disable or make no change to the secret password.
Secret Password	Enter the secret password.
Level	Set the password level. The level can be between 1 and 15.
Encrypted	Select this option to encrypt the password.

## GOLD Boot Level and Monitoring Test for Cat6k Devices-IOS

Use this option to configure GOLD Boot Level and Monitoring tests on Cat6k devices.

The following table describes the Template Detail fields on **CLI Templates > System Templates - CLI > GOLD Boot Level And Monitoring Test for Cat6k Devices-IOS**.

**Table 1-95** CLI Templates > System Templates-CLI > GOLD Boot Level and Monitoring Test for Cat6k Devices-IOS

Field	Description
Gold Boot Level Configuration Action	Select either <b>Enable</b> to enable the actions or <b>Disable</b> to disable the actions.
Gold Bootup Level	Select either <b>Complete</b> to set the boot level to Complete or <b>Minimal</b> to set the boot level to Minimal.
GOLD Monitoring Test Action	<p>Select any of the following:</p> <ul style="list-style-type: none"> <li>Addinterval —To add an interval.</li> <li>Nointerval —To not to add an interval.</li> </ul> <p>If you do not want to make any changes to the GOLD Monitoring Test Action, select <b>No Change</b>.</p>
GOLD Monitoring Test Module Number	Enter the Gold Monitoring Test Module Number that is in the selected device. You can enter one or more module numbers separated by commas.
Tests Details Action	<p>Select any of the following:</p> <ul style="list-style-type: none"> <li>All - Allows you to configure all diagnostic tests.</li> <li>Testnames —Allows you to manually enter the test names.</li> <li>TestRange —Allows you to enter a range for tests to be run.</li> </ul>

**Table 1-95** CLI Templates > System Templates-CLI > GOLD Boot Level and Monitoring Test for Cat6k Devices-IOS

Field	Description
Test Names	Enter one or more test names separated by comma. Do not add space in between commas. This field is mandatory if action is Testnames.
Range	Enter test ranges. This field is mandatory if action is TestRange.
No. of Days To Configure Health Monitoring Interval	Enter the number of days till which you require the tests to be run on the devices. The number of days can be any value from 0 to 20.
Begin Time To Configure Health Monitoring Interval	Enter the hours, minutes and seconds frequency at which the tests should be run.
Configuring Health Monitoring Interval in MilliSeconds	Enter the millisecond frequency at which the tests should be run. You can enter any value from 0 to 999 for the second.
Enable/Disable Health Monitoring Diagnostics Test Action	<p>Select any of the following:</p> <ul style="list-style-type: none"> <li>• Enable - To start the Health Monitoring tests.</li> <li>• Disable - To stop the running Health Monitoring tests.</li> </ul> <p>If you do not want to make any changes to the Health Monitoring test action, select <b>No Change</b>.</p>

## GOLD Monitoring Test for Non Stack Devices-IOS

Use this option to configure GOLD monitoring tests on nonstack devices.

The following table describes the Template Detail fields on **CLI Templates > System Templates - CLI > GOLD Monitoring Test for Non Stack Devices-IOS**.

**Table 1-96** CLI Templates > System Templates - CLI > GOLD Monitoring Test for Non Stack Devices-IOS

Field	Description
Non Stack Health Monitor Action	<p>Select any of the following:</p> <ul style="list-style-type: none"> <li>• Addinterval - To add an interval</li> <li>• Nointerval - To not to add an interval</li> </ul> <p>If you do not want to make any changes to the Non Stack Health Monitor Action, select <b>No Change</b>.</p>
Non Stack Tests Details Action	<p>Select any of the following:</p> <ul style="list-style-type: none"> <li>• All - Allows you to configure all diagnostic tests.</li> <li>• Testnames - Allows you to manually enter the test names.</li> <li>• TestRange - Allows you to enter a range for tests to be run.</li> </ul>



### Note

For similar field descriptions, refer [Table 1-95 on page 1-109](#).

## GOLD Monitoring Test for Stack Enabled Devices-IOS

Use this option to configure GOLD Monitoring tests on stack-enabled devices.

The following table describes the Template Detail fields on **CLI Templates > System Templates - CLI > GOLD Monitoring Test for Stack Enabled Devices-IOS**.

**Table 1-97** *CLI Templates > System Templates - CLI > GOLD Monitoring Test for Stack Enabled Devices-IOS*

Field	Description
Stack Health Monitor Action	<p>Select any of the following:</p> <ul style="list-style-type: none"> <li>Addinterval - To add an interval</li> <li>Nointerval - To not to add an interval</li> </ul> <p>If you do not want to make any changes to the Stack Health Monitor Action, select <b>No Change</b>.</p>
Stack Health Monitor Switch Id(s)	<p>Enter the Switch ID. You can enter a single switch ID or a number of switch IDs separated by comma. Example 1: Enter 2 if you want to include switch with ID 2. Example 2: Enter 3, 6 if you want to include switches with IDs 3 and 6.</p>
Stack Tests Details Action	<p>Select any of the following:</p> <ul style="list-style-type: none"> <li>All - Allows you to configure all diagnostic tests.</li> <li>Testnames - Allows you to manually enter the test names.</li> <li>TestRange - Allows you to enter a range for tests to be run.</li> </ul>



### Note

For similar field descriptions, refer The following table [Table 1-95 on page 1-109](#)

## HTTP-HTTPS Server and WSMA Configuration-IOS

Use this option to configure HTTP access on devices that, in turn, configure WSMA and VPN functionality.

The following table describes the Template Detail fields on **CLI Templates > System Templates - CLI > HTTP-HTTPS Server and WSMA Configuration-IOS**.

**Table 1-98** *CLI Templates > System Templates - CLI > HTTP-HTTPS Server and WSMA Configuration-IOS*

Field	Description
Server Action	<p>Select an option to enable or disable HTTP or HTTPs access on the device. Select <b>No Change</b> if you do not want to make changes to the server action.</p>
Port Number	<p>Specify the HTTP or HTTPs server port number from 1024 to 65535. Default HTTP prt number is 80 and default HTTPS port number is 443.</p>
Authentication Action	<p>Select an option to enable or disable authentication method. Select <b>No Change</b> if you do not want to make changes to the authentication action.</p>

**Table 1-98** CLI Templates > System Templates - CLI > HTTP-HTTPS Server and WSMA Configuration-IOS (continued)

Field	Description
Authentication Method	Select an authentication method: <ul style="list-style-type: none"> <li>• aaa</li> <li>• Enable</li> <li>• local</li> <li>• tacacs</li> </ul>
Access List Action	Select an option to enable or disable access list. Select <b>No Change</b> if you do not want to make changes to the Access List Action.
ACL Number/Name	Enter the Access Control List number or name to be used. The access list number must be from 1 to 99.
WSMA Action	Select an option to enable or disable WSMA action. Select <b>No Change</b> if you do not want to make changes to the WSMA Action.

To apply HTTP-HTTPS Server and WSMA Configuration-IOS template for Cisco IOS devices, do the following:

Create two instances for the template, that is, you can edit the given template and save the template as - HTTP-WSMA-For-ISR-ASR-Series (with WSMA as enable/disable) and then again edit the given template and save the template with a different name.

**Note**

You must enable the WSMA option for ISR, ISR-G2 and ASR series of routers. Keep the WSMA option as “No Change” for other routers.

## MAC Trap Configuration

Use this option to enable SNMPv1 or SNMPv2 MAC Notification Traps on switches.

The following table describes the Template Detail fields on **CLI Templates > System Templates - CLI > MAC Trap Configuration**.

**Table 1-99** CLI Templates > System Templates - CLI > MAC Trap Configuration

Field	Description
Device OID	Deploys the template only on the selected device OID. <b>Note</b> Do not edit this field to avoid deployment issues.
Notification Interval	Enter the time interval between traps from 0 to 2147483647 seconds.
Host Name/IP Address	Enter the hostname or IP address of the trap receiver.
SNMP Community	Enter the SNMP v1/v2c community string.
UDP Port	Enter the UDP port number on which the trap is received from 0 to 65535.
Interface Range	Enter the interface or interface range on which the trap must be configured.



## Mediatrace-Responder-Configuration

The following table describes the Template Detail fields on **CLI Templates > System Templates - CLI > -Responder-Configuration**.

**Table 1-100** *CLI Templates > System Templates - CLI > Mediatrace-Responder-Configuration*

Field	Description
Name Description	Enter a name for the template and an optional description.
Tags	Enter one or more tags.  Tags are used to group templates. There are two ways you can tag a template: <ul style="list-style-type: none"> <li>• Create the tags when you create the template.</li> <li>• Use the Tag icon located under the Templates search bar.</li> </ul>
Device Type	Choose <b>Routers</b> .
OS Version	Enter the OS Version for the selected device type. This must be at least the minimum Cisco IOS version shown in the following table. If this field is left empty, all available types for the chosen device type category (Family/Series/Type) will be displayed.

## Medianet-PerfMon

Use this option to configure performance monitoring for Medianet.

The following table describes the Template Detail fields on **CLI Templates > System Templates - CLI > Medianet-PerfMon**.

**Table 1-101** *CLI Templates > System Templates - CLI > Medianet-PerfMon*

Field	Description
Name Description	Enter a name for the template and an optional description.
Tags	Enter one or more tags.  Tags are used to group templates. There are two ways you can tag a template: <ul style="list-style-type: none"> <li>• Create the tags when you create the template.</li> <li>• Use the Tag icon located under the Templates search bar.</li> </ul>
Device Type	Select one of the Medianet PerfMon-compatible device types from the drop-down list.
OS Version	Enter the OS Version for the selected device type. This must be at least the minimum Cisco IOS version shown in the following table. If this field is left empty, all available types for the chosen device type category (Family/Series/Type) will be displayed.
Flow Exporter Name	A name for the NetFlow exporter on the device types you selected. This can be any collection of characters (for example: <code>EXPORTER-1</code> ).
Flow Exporter Address	The IP address of the Prime Infrastructure server.

**Table 1-101** CLI Templates > System Templates - CLI > Medianet-PerfMon (continued)

Field	Description
Flow Exporter Port	The port on which the NetFlow monitor will receive the exported data. Use the default 9991 port unless you have a special need to override it.
Performance Monitor Name	An arbitrary name for the Medianet Performance Monitor caching the data from the flow exporter (for example: MP-MONITOR-1).
Interface	The name of the interface on the device whose NetFlow data you want to monitor (for example: ethernet 0/0).
Flow Monitor Name	An arbitrary name for the NetFlow monitor caching the data from the flow exporter (for example: FLOW-MONITOR-1).

## RADIUS Configuration-IOS

Use this option to configure Single Radius Host and Radius Group for IOS devices.

The following table describes the Template Detail fields on CLI Templates > System Templates - CLI > Radius Configuration-IOS.

**Table 1-102** CLI Templates > System Templates - CLI > Radius Configuration-IOS

Field	Description
Radius Group Name	Enter the RADIUS group name.
Shared Key	Specify the authentication and encryption key to the RADIUS server.
Verify Shared Key	Specify the key for verification.
Server name or IP Address for Radius Group/Host	DNS name or IP address of the RADIUS server group/host. If you are entering a single RADIUS host, only the following fields must be entered: <ul style="list-style-type: none"> <li>• Shared Key</li> <li>• Verify Shared Key</li> <li>• Server name or IP address for Radius Group/Host</li> <li>• Authentication Port</li> <li>• Accounting Port</li> <li>• Enable for 802.1X / MAB AAA</li> <li>• Enable AAA for Web Authentication</li> </ul>
Authentication Port	Specify the port number for authentication requests. Authentication and Accounting port numbers cannot be the same. The host is not used for authentication if port number is set to 0. The default authorization port number is 1645.
Accounting Port	Specify the port number for accounting requests. Authentication and Accounting port numbers cannot be the same. The host is not used for accounting if the port number is set to 0. The default accounting port number is 1646.
Server name or IP Address for Radius Group Only	DNS name or IP address of the RADIUS server group.

**Table 1-102**      *CLI Templates > System Templates - CLI > Radius Configuration-IOS (continued)*

Field	Description
Authentication Port	Specify the port number for authentication requests. Authentication and Accounting port numbers cannot be the same. The host is not used for authentication if port number is set to 0. The default authorization port number is 1645.
Accounting Port	Specify the port number for accounting requests. Authentication and Accounting port numbers cannot be the same. The host is not used for accounting if the port number is set to 0. The default accounting port number is 1646.
Server name or IP Address for Radius Group Only	DNS name or IP address of the RADIUS server group.
Authentication Port	Specify the port number for authentication requests. Authentication and Accounting port numbers cannot be the same. The host is not used for authentication if port number is set to 0. The default authorization port number is 1645.
Accounting Port	Specify the port number for accounting requests. Authentication and Accounting port numbers cannot be the same. The host is not used for accounting if the port number is set to 0. The default accounting port number is 1646.
Server name or IP Address for Radius Group Only	DNS name or IP address of the RADIUS server group.
Authentication Port	Specify the port number for authentication requests. Authentication and Accounting port numbers cannot be the same. The host is not used for authentication if port number is set to 0. The default authorization port number is 1645.
Accounting Port	Specify the port number for accounting requests. Authentication and Accounting port numbers cannot be the same. The host is not used for accounting if the port number is set to 0. The default accounting port number is 1646.
Server name or IP Address for Radius Group Only	DNS name or IP address of the RADIUS server group.
Authentication Port	Specify the port number for authentication requests. Authentication and Accounting port numbers cannot be the same. The host is not used for authentication if port number is set to 0. The default authorization port number is 1645.
Accounting Port	Specify the port number for accounting requests. Authentication and Accounting port numbers cannot be the same. The host is not used for accounting if the port number is set to 0. The default accounting port number is 1646.
Enable for 802.1X / MAB AAA	Select the required option to enable or disable AAA for 802.1X and MAB authentication.
Enable AAA for Web Authentication	Select the required option to enable or disable AAA for Web-Based Authentication (WebAuth).

## Reload Configuration-IOS

Use this option to reload the Cisco IOS devices.

The following table describes the Template Detail fields on **CLI Templates > System Templates - CLI > Reload Configuration-IOS**.

**Table 1-103** CLI Templates > System Templates - CLI > Reload Configuration-IOS

Field	Description
Do not Save config before reload	Check this option if you do not want to save the configurations before reloading
Enter time to wait after reload	Enter the duration to wait after reload in minutes.

## Reload Configuration-NAM

Use this option to reload the NAM devices.

The following table describes the Template Detail fields on **CLI Templates > System Templates - CLI > Reload Configuration-NAM**.

**Table 1-104** CLI Templates > System Templates - CLI > Reload Configuration-NAM

Field	Description
Enter time to wait after reload	Enter the duration to wait after reload in minutes.

## Web User Configuration-NAM

Use this option to create, edit, and remove a local web user for NAM devices.

The following table describes the Template Detail fields on **CLI Templates > System Templates - CLI > Web User Configuration-NAM**.

**Table 1-105** CLI Templates > System Templates - CLI > Web User Configuration-NAM

Field	Description
Action	Select an option to add or remove web user group of fields. Select <b>No Change</b> , if you do not want to make changes to the action.
Username	Enter the username of the web user.
Enter DES encrypted WebUser Password	Enter the DES password for the username.
Account Management	Select the required option to enable or disable account management. Select <b>No Change</b> , if you do not want to make changes to account management.
System Config	Select the required option to enable or disable system configuration. Select <b>No Change</b> , if you do not want to make changes to system configuration.
Capture	Select the required option to enable or disable capture configuration. Select <b>No Change</b> , if you do not want to make changes to capture configuration.

**Table 1-105** *CLI Templates > System Templates - CLI > Web User Configuration-NAM (continued)*

Field	Description
Alarm Config	Select the required option to enable or disable alarm configuration. Select <b>No Change</b> , if you do not want to make changes to alarm configuration.
Collection Config	Select the required option to enable or disable collection configuration. Select <b>No Change</b> , if you do not want to make changes to collection configuration.

## User Defined Protocol Configuration-NAM

The following table describes the Template Detail fields on **User Defined Protocol Configuration-NAM**.

**Table 1-106** *User Defined Protocol Configuration-NAM Template Page Field Descriptions*

Field	Description
Action	Select an option to add, remove or replace the user-defined protocol.
Protocol	Select the protocol: <ul style="list-style-type: none"> <li>• TCP</li> <li>• UDP</li> </ul>
Port	Enter the port number. You can enter any port number in the range of 0 to 65535.
Name	Enter the name of the user-defined protocol.
Host	Select this option to enable host—Examines a stream of packets; produces a table of all network addresses observed in those packets (also known as the collection data). Each entry records the total number of packets and bytes sent and received by that host and the number of nonunicast packets sent by that host.
Conversations	Select this option to enable host conversations.
ART	Select this option to enable Application Response Time.

## Wireless Configuration Field Descriptions

The following topics contain field descriptions for pages found on **Design > Configuration > Wireless Configuration**.

- [Lightweight AP Configuration Templates, page 1-118](#)
- [Switch Location Configuration Template, page 1-125](#)
- [Switch Location Configuration Template, page 1-125](#)
- [Autonomous AP Migration Templates, page 1-126](#)
- [Controller Configuration Groups, page 1-128](#)
- [Plug and Play Profile Field Descriptions, page 1-129](#)

## Lightweight AP Configuration Templates

### Lightweight AP Configuration Templates > AP Parameters

The following table describes the Template Detail fields in **Design > Wireless Configuration > Lightweight AP Configuration Templates > AP Parameters**.

**Table 1-107**      *Lightweight AP Configuration Templates > AP Parameters*

Field	Description
Admin Status	<p>Select the <b>Admin and Enabled</b> check box to enable administrative status.</p> <p>To conserve energy, access points can be turned off at specified times during nonworking hours. Select the <b>Enabled</b> check box to allow access points to be enabled or disabled.</p>
AP Mode	<p>From the drop-down list, choose one of the following:</p> <ul style="list-style-type: none"> <li>• <b>Local</b>—Default</li> <li>• <b>Monitor</b>—Monitor mode only.</li> </ul> <p>Choose <b>Monitor</b> to enable this access point template for Cisco Adaptive wIPS. Once Monitor is selected, select the <b>Enhanced WIPS Engine</b> check box and the <b>Enabled</b> check box. Then select the <b>AP Monitor Mode Optimization</b> check box and choose WIPS from the AP Monitor Mode Optimization drop-down list.</p> <ul style="list-style-type: none"> <li>• <b>FlexConnect</b>—Cisco 1030 remote edge lightweight access point (REAP) used for Cisco 1030 IEEE 802.11a/b/g/n remote edge lightweight access points.</li> </ul> <p>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.</p> <ul style="list-style-type: none"> <li>• <b>Rogue Detector</b>—Monitors the rogue access points but does not transmit or contain rogue access points.</li> <li>• <b>Bridge</b></li> <li>• <b>Sniffer</b>—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.</li> </ul> <p>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 <a href="http://www.wildpackets.com">http://www.wildpackets.com</a>.</p> <ul style="list-style-type: none"> <li>• <b>SE-Connect</b>—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.</li> </ul> <p>This option is displayed only if the access point is CleanAir-capable.</p> <p>Changing the AP mode reboots the access point.</p>
Enhanced wIPS Engine	Select the <b>Enhanced wIPS engine</b> and the <b>Enabled</b> check box to enable.
AP Sub Mode	Choose an option from the drop-down list.

**Table 1-107 Lightweight AP Configuration Templates > AP Parameters (continued)**

Field	Description
Country Code	Select the appropriate country code from the drop-down list. <b>Note</b> Changing the country code might cause the access point to reboot.
AP Failover Priority	Choose <b>Low</b> , <b>Medium</b> , <b>High</b> , or <b>Critical</b> 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 Prime Infrastructure 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.
Domain Name Server IP Address	The DNS IP address and domain name can be configured only on access points that 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 <i>Cisco Wireless LAN Controller Configuration Guide</i> .
Telnet Access	An OfficeExtend access point might be connected directly to the WAN that 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.  <b>Note</b> 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 <b>Low</b> , <b>Medium</b> , <b>High</b> , or <b>Critical</b> from the drop-down list to indicate the access point failover priority. The default priority is low.
Controllers	Select the <b>Controllers</b> 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.

**Table 1-107**      **Lightweight AP Configuration Templates > AP Parameters (continued)**

Field	Description
Override Supplicant Credentials	<p>Select the <b>Override Supplicant Credentials</b> 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.</p> <ul style="list-style-type: none"> <li>In the Username, Password, and Confirm Password text boxes, enter the unique username and password that you want to assign to this access point.</li> </ul> <p><b>Note</b> The information that you enter is retained across controller and access point reboots and whenever the access point joins a new controller.</p>

## Lightweight AP Configuration Templates > Mesh

The following table describes the Template Detail fields in **Design > Wireless Configuration > Lightweight AP Configuration Templates > Mesh**.

**Table 1-108**      **Lightweight AP Configuration Templates > Mesh**

Field	Description
Bridge Group Name	<p>Enter a bridge group name (up to 10 characters) in the text box.</p> <p>Bridge groups are used to logically group the mesh access points to avoid two networks on the same channel from communicating with each other.</p> <p>For mesh access points to communicate, they must have the same bridge group name.</p> <p>For configurations with multiple RAPs, make sure that all RAPs have the same bridge group name to allow failover from one RAP to another.</p>
Data Rate (Mbps)	<p>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.</p> <p>This data rate is shared between the mesh access points and is fixed for the whole mesh network.</p> <p>Do not change the data rate for a deployed mesh networking solution.</p>
Ethernet Bridging	Select the <b>Enable</b> 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 ( <b>MAP</b> or <b>RAP</b> ). The default setting is MAP

## Lightweight AP Configuration Templates > 802.11a/n

The following table describes the Template Detail fields in **Design > Wireless Configuration > Lightweight AP Configuration Templates > 802.11a/n**.

**Table 1-109**      **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.



**Table 1-109**      *Lightweight AP Configuration Templates > 802.11a/n (continued)*

Field	Descriptions
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 <b>Antenna Type</b> 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.
Antenna Selection	Select the <b>Antenna Selection</b> check box, then select the appropriate antennas from the list.
CleanAir	Select to enable.

## Lightweight AP Configuration Templates > 802.11a SubBand

The following table describes the Template Detail fields in **Design > Wireless Configuration > Lightweight AP Configuration Templates > 802.11a SubBand**.

**Table 1-110**      *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. <b>Note</b> 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. <b>Note</b> The power level is validated against the radio list of supported power levels.
WLAN Override	Select the check box and then choose <b>Disable</b> or <b>Enable</b> from the drop-down list. <b>Note</b> 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.

## Lightweight AP Configuration Templates > 802.11b/g/n

The following table describes the Template Detail fields in **Design > Wireless Configuration > Lightweight AP Configuration Templates > 802.11b/g/n**.

**Table 1-111**      *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.

**Table 1-111** *Lightweight AP Configuration Templates > 802.11b/g/n (continued)*

Field	Descriptions
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 <b>Antenna Type</b> 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 <b>Antenna Selection</b> check box, then select the appropriate antennas from the list.
CleanAir	Select to enable.

## Lightweight AP Configuration Templates > CDP

The following table describes the Template Detail fields in **Design > Wireless Configuration > Lightweight AP Configuration Templates > 802.11b/g/n**.

**Table 1-112** *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.

## Lightweight AP Configuration Templates > FlexConnect

The following table describes the Template Detail fields in **Lightweight AP Template Details > FlexConnect**.

**Table 1-113** *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).
	<b>Note</b> These options are only available for access points in FlexConnect mode.

**Table 1-113**      **Lightweight AP Configuration Templates > FlexConnect (continued)**

Field	Description
OfficeExtend	<p>The default is Enabled.</p> <p>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 <b>Clear Config</b> 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.</p> <p>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.</p> <p>When you enable the OfficeExtend access point, you must configure at least one primary, secondary, and tertiary controller (including name and IP address).</p>
Least Latency Controller Join	<p>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.</p> <p>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.</p>
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 lists 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 lists to map to the WLAN ID specified.
Web Policy ACL Mapping	Choose a Web Policy ACL from the drop-down lists.
Local Split ACL Mapping	Choose a WLAN Profile and Local Split ACL from the drop-down lists to map to.

## Lightweight AP Configuration Templates > Select APs

The following table describes the Template Detail fields in **Lightweight AP Template Details > Select APs**.

**Table 1-114**      *Lightweight AP Configuration Templates > Select APs*

Field	Description
Search	<p>Use the Search APs drop-down list to search for and select the APs to which to apply the configuration template:</p> <ul style="list-style-type: none"> <li>• Last Applied AP(s)</li> <li>• Scheduled AP(s)</li> <li>• All</li> <li>• All Mesh MAP AP(s)</li> <li>• All Mesh RAP AP(s)</li> </ul> <p>You can also search by the following indices, and will be prompted for additional information as described in the fields below:</p> <ul style="list-style-type: none"> <li>• By Controller</li> <li>• By Controller Name</li> <li>• By Floor Area</li> <li>• By Outdoor Area</li> <li>• By Model</li> <li>• By AP MAC Address</li> <li>• By AP Name</li> <li>• By AP IP Address Range</li> </ul>
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

The following table describes the Template Detail fields in **Lightweight AP Template Details > Apply/Schedule**.

**Table 1-115** *Lightweight AP Configuration Templates > Select APs*

Field	Description
Schedule	Select the check box to enable scheduling
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.

## Lightweight AP Configuration Templates > Report

The following table describes the Template Detail fields in **Lightweight AP Template Details > Report**.

**Table 1-116** *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 <b>Details</b> 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.

## Switch Location Configuration Template

The following table describes the Template Detail fields on **Design > Wireless Configuration > Switch Location Configuration**.

**Table 1-117** *Design > Wireless Configuration > Switch Location Configuration*

Field	Description
<b>Map Location</b>	
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.
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.
<b>ELIN and Civic Location</b>	
ELIN	The Emergency Location Identification Number.

**Table 1-117**      *Design > Wireless Configuration > Switch Location Configuration (continued)*

Field	Description
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.

## Autonomous AP Migration Templates

The following table describes the Template Detail fields in **Design > Configuration > Wireless Configuration > Autonomous AP Migration Templates**.

**Table 1-118**      *Autonomous AP Migration Template Page*

Field	Description
Name	Template name.
Description	Template description.
AP Count	Number of APs.
Schedule Run	Scheduled run time.
Status	<p>Indicates one of the following:</p> <ul style="list-style-type: none"> <li>• Not initiated—The template is yet to start the migration and starts at the scheduled time.</li> <li>• Disabled—The template is disabled and does not run at the scheduled time. This is the default state for a template when it is created without selecting any autonomous access points.</li> <li>• Expired—The template did not run at the scheduled time (this might be due to the Prime Infrastructure server being down).</li> <li>• Enabled—The template is yet to start the migration and starts at the scheduled time.</li> <li>• In progress—The template is currently converting the selected autonomous access points to CAPWAP.</li> <li>• Success—The template has completed the migration of autonomous access point to CAPWAP successfully.</li> <li>• Failure—The template failed to migrate all the selected autonomous access point to CAPWAP. You can check the detailed status about the failures by using the View Migration Status page.</li> <li>• Partial Success—The template failed to migrate a subset of the selected autonomous access point to CAPWAP. You can check the detailed status about the failures by using the View Migration Status page.</li> </ul>

## Autonomous AP Migration Templates > Add Template

The following table describes the Template Detail fields in **Design > Configuration > Wireless Configuration > Autonomous AP Migration Templates**.

**Table 1-119 Autonomous AP Migration Templates**

Field	Description
<b>Upgrade Options</b>	
DHCP Support	Ensures that after the conversion every access point gets an IP from the DHCP server.
Retain AP HostName	<p>Allows you to retain the same hostname for this access point.</p> <p>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.</p> <p>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.</p>
Migrate over WANLink	<p>Increases the default timeouts for the CLI commands executed on the access point.</p> <p>If you enable this option, the <i>env_vars</i> 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 <i>env_vars</i> file to the access point.</p>
DNS Address	Enter the DNS address.
Domain Name	Enter the domain name.
<b>Controller Details</b>	
Controller IP	Enter controller IP address.
AP Manager IP	<p>Specify the controller the access point should join by entering the access point manager IP address.</p> <p>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.</p>
User Name	Enter the username.
Password	Enter the password for the username.
<b>TFTP Details</b>	
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 that 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).
<b>Schedule Details</b>	
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.

## Controller Configuration Groups

The following topics describe the fields in **Design > Wireless Configuration > Wireless Configuration > Controller Configuration Groups**.

- [Controller Configuration Groups > Add Config Group](#), page 1-128
- [Controller Configuration Groups > General](#), page 1-128
- [Controller Configuration Groups > Apply Schedule](#), page 1-129

### Controller Configuration Groups > Add Config Group

The following table describes the Template Detail fields in **Controller Configuration Groups > Add Config Group**.

**Table 1-120** *Wireless Configuration > Controller Configuration Groups*

Field	Description
Group Name	The group name must be unique across all groups.
Templates	<p>Other templates created in Prime Infrastructure can be assigned to a config group. The same WLAN template can be assigned to more than one config group. Choose from the following:</p> <ul style="list-style-type: none"> <li>• <b>Select and add later:</b> Add a template at a later time.</li> <li>• <b>Copy templates from a controller:</b> Copy templates from another controller. Choose a controller from a list of current controllers to copy its applied template to the new config group. Only the templates are copied.</li> </ul> <p><b>Note</b> The order of the templates is important when dealing with radio templates. For example, if the template list includes radio templates that require the radio network to be disabled prior to applying the radio parameters, the template to disable the radio network must be added to the template first.</p>

### Controller Configuration Groups > General

The following table describes the Template Detail fields in **Controller Configuration Groups > General**.

**Table 1-121** *Wireless Configuration > Controller Configuration Groups > General*

Field	Description
Enable Background Audit	<p>If selected, all the templates that are part of this group are audited against the controller during network and controller audits.</p> <p><b>Note</b> To enable this option, set the template-based audit option under <b>Administration &gt; System &gt; Audit</b>.</p>
Enable Enforcement	<p>If selected, the templates are automatically applied during the audit if any discrepancies are found.</p> <p><b>Note</b> To enable this option, set the template-based audit option under <b>Administration &gt; System &gt; Audit</b>.</p>
Enable Mobility Group	If selected, the mobility group name is pushed to all controllers in the group.



**Table 1-121**      **Wireless Configuration > Controller Configuration Groups > General (continued)**

Field	Description
Mobility Group Name	A name that is pushed to all controllers in the group. You can also use this field to change the group name. <b>Note</b> A controller can be part of multiple configuration groups.
Last Modified On	Date and time config group was last modified.
Last Applied On	Date and time last changes were applied.

## Controller Configuration Groups > Apply Schedule

The following table describes the Template Detail fields in **Controller Configuration Groups > Apply Schedule**.

**Table 1-122**      **Wireless Configuration > Controller Config Groups > Apply Schedule**

Field	Description
Apply	<b>Note</b> This option is available only when the <b>Schedule</b> option is <i>not</i> enabled.  Click <b>Apply</b> to start the provisioning of mobility groups, mobility members, and templates to all the controllers in the config group. After you apply, you can leave this page or log out of Prime Infrastructure. The process continues, and you can return later to this page to view a report. <b>Note</b> Do not perform any other configuration group functions during the apply provisioning.  The report appears in the <b>Recent Apply Report</b> page. It shows which mobility groups, mobility members, or templates were successfully applied to each of the controllers.
Schedule	Enabling the <b>Schedule</b> option disables the <b>Apply</b> option.
Start Date Start Time	Enter a starting date and time, then click <b>Schedule</b> .

## Plug and Play Profile Field Descriptions

The following topics contain field descriptions for Plug and Play profiles:

- [Design > Plug and Play Profiles, page 1-129](#)
- [Deploy > Plug and Play Profiles, page 1-130](#)

## Design > Plug and Play Profiles

The following table describes the field descriptions on **Design > Plug and Play Profiles > Plug and Play Profiles**.

**Table 1-123**     **Design > Plug and Play Profiles > Plug and Play Profiles**

Field	Description
Device Type	Choose the types of new devices that can use this profile.  In bulk deployments, the devices use the same deployment profile with the same set of images and configurations. To use the deployment profile for specific device IDs, do <i>not</i> select the Device Type.
Bootstrap Template	Choose the bootstrap CLI template from the drop-down list.
Software Image Image Location	Choose a software image from the drop-down list and specify the flash location on the device where the image is to be distributed.
Configuration Template	Choose the configuration template from the drop-down list.

## Deploy > Plug and Play Profiles

The following table describes the field descriptions on **Deploy > Plug and Play Profiles**.

**Table 1-124**     **Deploy > Plug and Play Profiles**

Field	Description
Device ID	For CNS ID-based deployments, this can be the hardware serial ID or the VUDI of the device.
Bootstrap Template Properties	Enter the username and password of the guest account, a description, the date and time, and the name of the attribute list.  Bootstrap Template properties appears in the profile parameters only if there is a bootstrap template defined in Design > Plug and Play. All the managed variables associated with the bootstrap template will be displayed under Bootstrap Template Properties.
Configuration Template Properties	Configuration Template properties appears in the profile parameters only if there is a configuration template defined in Design > Plug and Play. All the managed variables associated with the configuration template will be displayed under Configuration Template Properties and user can enter values for those variables and click Apply.
Image Properties	Image properties appears in the Profile Parameters if there is an image specified in the profile with the following details: <ul style="list-style-type: none"> <li>Image location</li> <li>Erase Flash</li> <li>Continue on Image Failure</li> <li>Activate Image</li> </ul>

Table 1-124 Deploy &gt; Plug and Play Profiles (continued)

Field	Description
Device Management Parameters	<p>Enter the IP address. In CNS-based deployments, if the IP address is not specified, the IP address that is supplied by the Prime Infrastructure Plug and Play gateway is used to add the device to the Prime Infrastructure device inventory.</p> <p>When the network is secured by firewalls and NAT, the IP address supplied by the Prime Infrastructure Plug and Play gateway server might not be the actual IP address of the device. If there are multiple devices behind that NAT that must be managed by Prime Infrastructure, an administrator can enter the device's IP address manually.</p> <p><b>Note</b> Cisco Prime Infrastructure does <i>not</i> deliver any device management parameters on the device; the device management parameters are used by Prime Infrastructure inventory to manage the device after the image and CLI configurations are applied. All configurations are performed only through the configuration templates in the profile.</p> <p><b>Note</b> If you want the management parameters configured on the device, add them to the configuration template included in the Plug and Play profile (see <a href="#">Creating Plug and Play Profiles</a> in the <i>Cisco Prime Infrastructure 2.0 User Guide</i>).</p>
SNMP Parameters	Enter the version, timeout, retries, and community name.
CLI Parameters	Select the protocol from the drop-down list, then enter the username, password, confirm password, enable password, confirm enable password, and timeout.

# Mobility Services Field Descriptions

The following topics contain field descriptions for designing the mobility services engine:

- [Mobility Services Engines, page 1-132](#)
- [High Availability, page 1-134](#)

## Mobility Services Engines

The following sections contain field description for pages found in **Design > Mobility Services > Mobility Services Engine**.

- [Mobility Services Engines > Select a command > Add Location Server, page 1-132](#)
- [Mobility Services Engines > Select a command > Add Mobility Services Engine, page 1-133](#)
- [Mobility Services Engines Database Synchronization, page 1-133](#)

### Mobility Services Engines > Select a command > Add Location Server

The following table describes the Template Detail fields in **Design > Mobility Services > Mobility Services Engines > Select a command > Add Location Server**.

**Table 1-125**      **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 the Prime Infrastructure communication username configured for MSE.
Password	The default password is admin. This is the 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 Engines > Select a command > Add Mobility Services Engine

The following table describes the Template Detail fields in **Design > Mobility Services > Mobility Services Engine > Select a command > Add a Mobility Services Engine**.

**Table 1-126**      *Add 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 the Prime Infrastructure communication username configured for MSE.
Password	The default password is admin. This is the 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 Engines Database Synchronization

The following table describes the Template Detail fields in **Design > Mobility Services > Mobility Services Engine > Select a command > Add Mobility Services Engine**.

**Table 1-127**      *Add 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 the Prime Infrastructure communication username configured for MSE.
Password	The default password is admin. This is the 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

The following table describes the Template Detail fields in **Design > Mobility Services > High Availability**.

**Table 1-128**      *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.
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.