



Management Tab

This tab on the menu bar enables you to access the Cisco WLC management details. Use the left navigation pane to access specific management parameters. Making this selection from the menu bar opens the [Summary](#) page.

Summary

Choose **MANAGEMENT > Summary** to navigate to the Summary page. This page displays the network summary.

Table 7-1 Summary Parameters

Parameter	Description
SNMP Protocols	SNMP protocols supported.
Syslog	Log of system events.
HTTP Mode	Access mode for web and secure web.
HTTPS Mode	Status of the HTTPS Secure Shell (SSL) interface that uses secure certificate authentication.
New Telnet Sessions Allowed	Whether or not additional Telnet sessions are permitted.
New SSH Sessions Allowed	Whether or not additional SSH-enabled sessions are permitted.
Management via Wireless	Whether Cisco WLC management from a wireless client is enabled or disabled.

SNMP System Summary

Choose **MANAGEMENT > SNMP > General** to navigate to the SNMP System Summary page. This page enables you to change some of the SNMP system parameters.

Table 7-2 SNMP System Parameters

Parameter	Description
Name	Customer-definable name of the Cisco WLC.
Location	Customer-definable Cisco WLC location.

Table 7-2 *SNMP System Parameters*

Parameter	Description
Contact	Customer-definable contact details.
System Description	Read-only Cisco WLC description.
System Object ID	Read-only object ID.
SNMP Port Number	Read-only SNMP port number.
Trap Port Number	Definable trap port number; the default value is 162.
SNMP v1 Mode	SNMP v1 mode that you can enable or disable; The default is disabled state.
SNMP v2c Mode	SNMP v2c mode that you can enable or disable; the default is enabled. This parameter should be modified if remote management is desired.
SNMP v3 Mode	SNMP v3 mode that you can enable or disable; the default is enabled. This parameter should be modified if remote management is desired.

Click **Apply** to send data to the Cisco WLC, but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

SNMP V3 Users

Choose **MANAGEMENT > SNMP > SNMP V3 Users** to navigate to the SNMP V3 Users page. This page provides a summary of the SNMP users.

Table 7-3 *SNMP User Summary Parameters*

Parameter	Range
User Name	Name of the user profile.
Access Level	Read-only or read-write.
Auth Protocol	None, HMAC-MD5, or HMAC-SHA.
Privacy Protocol	None, CBC-DES, or CFB-AES-128.

To remove a user profile, click the blue arrow adjacent the desired profile and choose **Remove**. You are prompted for confirmation of the user removal.

Click **New** to add a new SNMP user (see the [Adding SNMP V3 Users](#) topic).

Adding SNMP V3 Users

Choose **MANAGEMENT > SNMP > SNMP V3 Users** and then click **New** to navigate to the SNMP V3 Users > New page. This page provides a summary of the SNMP users.

Table 7-4 *SNMP User Details Parameters*

Parameter	Range
User Profile Name	Name of the user profile.
Access Mode	Read-only or read-write.

Table 7-4 *SNMP User Details Parameters*

Parameter	Range
Authentication Protocol	None, HMAC-MD5, or HMAC-SHA (default). For HMAC-MD5 or HMAC-SHA, enter and confirm an authentication password.
Privacy Protocol	None, CBC-DES, or CFB-AES-128 (default). For CBC-DES, enter and confirm a Privacy Password.

If you select an authentication or privacy protocol, you must enter a password for each.

Click **Apply** to send data to the Cisco WLC, but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

SNMP Communities

Choose **MANAGEMENT > SNMP > Communities** to navigate to the **SNMP v1 / v2c Community** page.

Edit a user profile by choosing **Edit** (see the [Editing SNMP v1/v2c Community](#) topic).

To remove a community, click the blue arrow adjacent the desired community and choose **Remove**. You are prompted to confirm the removal of the community. This page provides a summary of the SNMP community.

Table 7-5 *SNMP Community Summary Parameters*

Parameter	Range
Community Name	Community string to which this entry grants access. A valid entry is a case-sensitive, alphanumeric string of up to 16 characters. Each row of this table must contain a unique community name.
IP Address (IPv4/IPv6)	IP address from which this device accepts SNMP packets with the associated community. An AND operation is performed between the requesting entity's IP address and the subnet mask before being compared to the IP address. From Release 8.0, SNMP community supports IPv4 and IPv6. Note If the subnet mask is set to 0.0.0.0, an IP address of 0.0.0.0 matches all IP addresses. The default value is 0.0.0.0.
IP Mask/Prefix Length	The subnet mask/ prefix length assigned to IPv4/IPv6 address Mask that must be an operand in the AND operation with the requesting entity's IP address before the IP addresses are compared. If the IP addresses match, then the address is an authenticated IP address. For example, if the IP address is 9.47.128.0 and the corresponding subnet mask is 255.255.255.0, a range of incoming IP addresses would match. The incoming IP address could equal 9.47.128.0 to 9.47.128.255. The default value is 0.0.0.0.

Table 7-5 *SNMP Community Summary Parameters*

Parameter	Range
Access Mode	Access level for this community string. This mode may be specified by choosing read/write or read only from the drop-down list.
Status	Status of this community access entry. When this object is set to enabled, if the community name for this row is not unique among all valid rows, the set request is rejected.

Click **New** to add a new community user profile (see the [Adding SNMP v1/v2c Community](#) topic).

Adding SNMP v1/v2c Community

Choose **MANAGEMENT > SNMP > Communities** and then click **New** to navigate to the **SNMP v1 / v2c Community > New** page. This page enables you to add a new SNMP community profile.



Note

There is no IPSec support for IPv6.

Table 7-6 *SNMP Community Summary Parameters*

Parameter	Range
Community Name	Community string to which this entry grants access. A valid entry is a case-sensitive, alphanumeric string of up to 16 characters. Each row of this table must contain a unique community name.
IP Address (IPv4/IPv6)	<p>IP address from which this device accepts SNMP packets with the associated community. An AND operation is performed between the requesting entity's IP address and the subnet mask before being compared to the IP address.</p> <p>From Release 8.0, SNMP community supports IPv4 and IPv6.</p> <p>Note If the subnet mask is set to 0.0.0.0, an IP address of 0.0.0.0 matches all IP addresses. The default value is 0.0.0.0.</p>
IP Mask/Prefix Length	<p>The subnet mask/ prefix length assigned to IPv4/IPv6 address.</p> <p>Mask that must be the AND operand with the requesting entity's IP address before the IP addresses are compared. If the IP addresses match, then the address is an authenticated IP address.</p> <p>For example, if the IP address is 9.47.128.0 and the corresponding subnet mask is 255.255.255.0, a range of incoming IP addresses would match, that is, the incoming IP address could equal 9.47.128.0 to 9.47.128.255. The default value is 0.0.0.0.</p> <p>Note For IPv6 input, enter Prefix Length.</p>
Access Mode	Access level for this community string. This mode, may be specified by selecting read/write or read-only from the drop-down list.

Table 7-6 SNMP Community Summary Parameters

Parameter	Range
Status	Status of this community access entry. When this object is set to enabled, if the community name for this row is not unique among all valid rows, the set request is rejected. Community names may be made invalid by choosing disable.
IPSec Parameters	
IPSec	Check box that allows you to enable or disable the IP Security mechanism.
IPSec Profile Name	Choose the IPSec profile name from the drop-down list. To create an IPSec profile, see “IPSEC” section on page 7-14 .

Click **Apply** to send data to the Cisco WLC, but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

Editing SNMP v1/v2c Community

Choose **MANAGEMENT > SNMP > Communities** and then click **Edit** to navigate to the **SNMP v1 / v2c Community > Edit** page.

This page allows you to enable or disable an SNMP community profile. All fields are read-only except the Status text box.



Note

There is no IPSec support for IPv6.

Table 7-7 SNMP Community Summary Parameters

Parameter	Range
Community Name	Community string to which this entry grants access. A valid entry is a case-sensitive, alphanumeric string of up to 16 characters. Each row of this table must contain a unique community name.
IP Address (IPv4/IPv6)	<p>IP address from which this device accepts SNMP packets with the associated community. An AND operation is performed between the requesting entity's IP address and the subnet mask before being compared to the IP address.</p> <p>From Release 8.0, SNMP community supports IPv4 and IPv6.</p> <p>Note If the subnet mask is set to 0.0.0.0, an IP address of 0.0.0.0 matches all IP addresses. The default value is 0.0.0.0.</p>

Table 7-7 *SNMP Community Summary Parameters*

Parameter	Range
IP Mask/Prefix Length	<p>The subnet mask/ prefix length assigned to IPv4/IPv6 address.</p> <p>Mask that must be the AND operand with the requesting entity's IP address before the IP addresses are compared. If the IP addresses match, then the address is an authenticated IP address.</p> <p>For example, if the IP address is 9.47.128.0 and the corresponding subnet mask is 255.255.255.0, a range of incoming IP addresses would match, that is, the incoming IP address could equal 9.47.128.0 to 9.47.128.255. The default value is 0.0.0.0.</p> <p>Note For IPv6 input, enter Prefix Length.</p>
Access Mode	Access level for this community string. This mode may be specified by selecting read/write or read-only from the drop-down list.
Status	Status of this community access entry. When this object is set to enabled, if the community name for this row is not unique among all valid rows, the set request is rejected. Community names may be made invalid by choosing disable.
IPSec Parameters	
IPSec	Check box that allows you to enable or disable the IP Security mechanism.
IPSec Profile Name	Choose the IPSec profile name from the drop-down list. To create an IPSec profile, see “IPSEC” section on page 7-14 .

Click **Apply** to send data to the Cisco WLC, but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

SNMP Trap Receiver

Choose **MANAGEMENT > SNMP > Trap Receivers** to navigate to the **SNMP Trap Receiver** page.

Edit a user profile by choosing **Edit** (see the [Editing SNMP Trap Receivers](#) topic).

Remove a user profile by choosing **Remove**. You are prompted for confirmation of the trap removal. This page provides a summary of existing SNMP trap receivers.

Table 7-8 *SNMP Trap Receiver Summary Parameters*

Parameter	Range
Community Name	Name of the server where the traps are sent.
IP Address (IPv4/IPv6)	IP address of the server. From Release 8.0, SNMP trap receiver support IPv4 and IPv6.
Status	Status that must be enabled for the SNMP traps to be sent to the server.
IPSec	Check box that allows you to enable or disable the IP Security mechanism.
IPSec Profile Name	Choose the IPSec profile name from the drop-down list. To create an IPSec profile, see “IPSEC” section on page 7-14 .

Click **New** to add a new trap receiver (see the [Adding SNMP Trap Receivers](#) topic).

Adding SNMP Trap Receivers

Choose **MANAGEMENT > SNMP > Trap Receivers** and then click **New** to navigate to the **SNMP Trap Receiver > New** page.

This page enables you to add a server to receive SNMP traps from this Cisco WLC.

Table 7-9 SNMP Trap Receiver Detail Parameters

Parameter	Range
Community Name	Name of the server where the traps are sent.
IP Address (IPv4/IPv6)	IP address of the server. From Release 8.0, SNMP trap receiver support IPv4 and IPv6.
Status	Status that you must enable for the SNMP traps to be sent to the receiver. The default is enabled.
IPSec	Check box that allows you to enable or disable the IP Security mechanism.
IPSec Profile Name	Choose the IPSec profile name from the drop-down list. To create an IPSec profile, see “IPSEC” section on page 7-14 .



Note

There is no IPSec support for IPv6.

Click **Apply** to send data to the Cisco WLC, but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

Editing SNMP Trap Receivers

Choose **MANAGEMENT > SNMP > Trap Receivers** and then click the Community Name to edit an SNMP trap receivers and its IPSec details.



Note

There is no IPSec support for IPv6.

This page enables you to configure sending traps to a particular server. Only the Status text box can be modified.

Click **Apply** to send data to the Cisco WLC, but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

SNMP Trap Controls

Choose **MANAGEMENT > SNMP > Trap Controls** to navigate to the SNMP Trap Controls page.

This page enables you to select which traps logs should be captured. Choose the applicable logs and choose **Apply**.



Note

Select the **Select All** check box to enable all traps on a tab. Unselect the **Select All** check box to disable all traps on a tab.

General Tab**Table 7-10** *General Tab Parameters*

Trap Name	Description
Link (Port) Up/Down	Port changes status from up or down.
Spanning Tree ¹	Spanning tree traps. Refer to the STP specifications for descriptions of individual parameters.
Config Save	Notification sent when the configuration is modified.
RFID Limit Reached	Notification sent when the number of RFID tags on the Cisco WLC exceeds the threshold limit defined in the Threshold field.
Threshold	Threshold number of the RFID tags on the Cisco WLC to trigger a trap.

1. The Cisco 5500 Series Controllers do not support the Spanning Tree Protocol.

Client Tab**Table 7-11** *Client Tab Parameters*

Trap Name	Description
802.11 Association	Associate notification sent when the client sends an association frame.
802.11 Disassociation	Disassociate notification sent when the client sends a disassociation frame.
802.11 Deauthentication	Deauthenticate notification sent when the client sends a deauthentication frame.
802.11 Failed Authentication	Authenticate failure notification sent when the client sends an authentication frame with a status code other than successful.
802.11 Failed Association	Associate failure notification sent when the client sends an association frame with a status code other than successful.
Exclusion	Associate failure notification sent when a client is Exclusion Listed (blacklisted).
Authentication	Authentication notification sent when a client is successfully authenticated.
Max Clients Limit Reached	Notification sent when the maximum number of clients, defined in the Threshold field, have been associated with the Cisco WLC.
NAC Alert	Alert that is sent when a client joins an SNMP NAC-enabled WLAN. This notification is generated when clients on NAC-enabled SSIDs complete Layer 2 authentication. This trap is to inform the NAC appliance about the client's presence.
Association with Stats	Associate notification sent with data statistics when a client associates with the Cisco WLC or roams. The data statistics include transmitted and received bytes and packets.
Disassociation with Stats	Disassociate notification sent with data statistics when a client disassociates from the Cisco WLC. The data statistics include transmitted and received bytes and packets, SSID, and session ID.

AP Tab**Table 7-12** *AP Tab Parameters*

Trap Name	Description
AP Register	Notification sent when the access point associates or disassociates with the Cisco WLC.
AP Interface Up/Down	Notification sent when the access point interface (802.11a/n or 802.11b/g/n) status changes to up or down.
AP Authorization	AP authorization that you can enable or disable. The default is enabled.
AP SSID Key Conflict	Notification sent when two SSIDs on an AP have the same cipher key.
AP Mode Change	Notification sent when the access point mode changes.
AP Time Sync Failure	Notification sent when the heartbeat (for example, 60s) between the Cisco WLC and the AP is lost or the connection breaks.

Security Tab**Table 7-13** *Security Tab Parameters*

Trap Name	Description
AAA Traps	
User Authentication	Trap to inform that a client RADIUS authentication failure has occurred.
RADIUS Servers Not Responding	Trap to indicate that no RADIUS server(s) are responding to authentication requests sent by the RADIUS client.
802.11 Security Traps	
WEP/WPA Decrypt Error	Trap to inform that an error has occurred while a WEP/WPA entity is being decrypted.
IDS Signature Attack	IDS Signature attack that you can enable or disable. The default is enabled.
Rogues	
Rogue AP	Trap that is sent with its MAC address whenever a rogue access point is detected. When a rogue access point that was detected earlier no longer exists, this trap is sent.
Adjacent Channel Rogue	Notification sent when a rogue AP is detected in the adjacent channels and if it has been removed from the network.
Management Traps	
SNMP Authentication	SNMPv2 entity that has received a protocol message that is not properly authenticated.
Multiple Users	Two users that log in with the same login ID.
Strong Password	Strong password check that you enable or disable.

Auto RF Tab**Table 7-14** *Auto RF Tab Parameters*

Trap Name	Description
Auto RF Profile	
Load Profile	Notification sent when the Load Profile state changes between PASS and FAIL.
Noise Profile	Notification sent when the Noise Profile state changes between PASS and FAIL.
Interference Profile	Notification sent when the Interference Profile state changes between PASS and FAIL.
Coverage Profile	Notification sent when the Coverage Profile state changes between PASS and FAIL.
Auto RF Update Traps	
Channel Update	Notification sent when the access point's dynamic channel algorithm is updated.
Tx Power Update	Notification sent when the access point's dynamic transmit power algorithm is updated.

Mesh Tab**Table 7-15** *Mesh Tab Parameters*

Trap Name	Description
Child Excluded Parent	Notification sent when the child access point marks a parent access point for exclusion. When the child fails to authenticate at the Cisco WLC after a fixed number of times, the child marks the parent for exclusion. The child remembers the excluded MAC address and informs the Cisco WLC when it joins the network. The child access point marks the MAC address and excludes it for the time determined by MAP node so that it does not try to join this excluded node. The child MAC address is sent as part of the index.
Parent Change	Notification sent when a child moves to another parent. The alarm includes the MAC addresses of the former and current parents.
Authfailure Mesh	Notification sent when the access point tries to join the mesh but fails to authenticate because it is not in the MAC filter list. The trap contains the MAC address of the AP that failed authorization.
Child Moved	Notification sent when the parent access point loses connection with its child.
Excessive Parent Change	Notification sent when the number of parent changes for a given mesh access point exceeds the threshold. Each access point keeps count of the number of parent changes within a fixed time. If the count exceeds the threshold defined by c1MeshExcessiveParentChangeThreshold, then the child access point informs the Cisco WLC.
Excessive Children	Notification sent when the child count of an access point exceeds 10 (default) children. RAP and MAP need to be handled separately. RAP allows more than 10 (default) children up to 20 (default) children.

Table 7-15 Mesh Tab Parameters

Trap Name	Description
Poor SNR	Notification sent when the child access point detects a signal-to-noise ratio (SNR) below 12 dB on the backhaul link. The alarm includes the SNR value and the MAC addresses of the parent and child.
Console Login	Notification sent when a login on the MAP console is successful or when a failure occurs after three attempts.
Excessive Association	Notification sent when the MAP access point associates more than 5 times within 60 minutes.
Default Bridge Group Name	Notification sent when a MAP mesh node joins parent using the “default” bridge group name.
Excessive Hopcount	Notification sent when the number of hops from the Mesh access point (MAP) node to the root access point (RAP) exceeds the threshold defined by <code>clMeshExcessiveHopCountThreshold</code> .
Secondary Backhaul Change	Notification sent when the MAP changes the backhaul from primary to secondary.
PSK Auth Failure	Notification sent when WPA/WPA2-PSK authentication failure occurs.

Click **Apply** to send data to the Cisco WLC, but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

SNMP Trap Logs

Choose **MANAGEMENT > SNMP > Trap Logs** to navigate to the **Trap Logs** page.

This page enables you to view the trap logs that have been captured by the Cisco WLC. Each trap entry includes the log number, system time, and trap description.

This page also displays the number of traps since the last reset and number of traps since log last viewed.



Note

Review the following client reason and status codes. You are likely to encounter them when reviewing the trap logs.

Client Reason Code Descriptions

Table 7-16 Client Reason Code Parameters

Client Reason Code	Description	Meaning
0	noReasonCode	Normal operation.
1	unspecifiedReason	Client associated but no longer authorized.
2	previousAuthNotValid	Client associated but not authorized.
3	deauthenticationLeaving	Access point went offline; deauthenticating the client.

Table 7-16 *Client Reason Code Parameters*

Client Reason Code	Description	Meaning
4	disassociationDueToInactivity	Client session timeout exceeded.
5	disassociationAPBusy	Access point is busy.
6	class2FrameFromNonAuthStation	Client attempted to transfer data before it was authenticated.
7	class2FrameFromNonAssStation	Client attempted to transfer data before it was associated.
8	disassociationStaHasLeft	Operating system moved the client to another access point using nonaggressive load balancing.
9	staReqAssociationWithoutAuth	Client not authorized yet; still attempting to associate with an access point.
99	missingReasonCode	Client momentarily in an unknown state.

Client Status Code Descriptions

Table 7-17 *Client Status Code Parameters*

Client Status Code	Description	Meaning
0	idle	Normal operation; no rejections of client association requests.
1	aaaPending	Completing an AAA transaction.
2	authenticated	802.11 authentication is completed.
3	associated	802.11 association is completed.
4	powersave	Client is in powersave mode.
5	disassociated	802.11 disassociation is completed.
6	tobedeleted	Client is deleted after disassociation.
7	probing	Client not associated or authorized yet.
8	disabled	Automatically disabled by the operating system for an operator-defined time.

Click **Clear Log** to delete all log entries. You are prompted for confirmation to delete the logs.

HTTP-HTTPS Configuration

Choose **MANAGEMENT > HTTP-HTTPS** to navigate to the HTTP-HTTPS Configuration page.

This page enables you to configure the following settings for Web Mode or Secure Web Mode:

- **HTTP Access**—HTTP Web User Interface that is accessible using a login and password. If you disable HTTP Web Mode, you must enable Secure Web Mode or you must use the CLI or Cisco Wireless Control System interface to configure the Cisco WLC. If you disable Web Mode and Secure Web Mode, you must use the CLI interface to configure the Cisco WLC.
- **HTTPS Access**—HTTPS Secure Shell (SSL) interface that is accessible using secure certificate authentication (configured below). This is the default access. If you disable HTTPS Secure Web Mode, you must enable Web Mode or you must use the CLI or Cisco Wireless Control System interface to configure the Cisco WLC.
- **Web Session Timeout**—Amount of inactivity (in minutes) before the session times out.
- **Current Certificate**—Name, Type, Serial Number, Valid, Subject Name, Issuer Name, MD5 Fingerprint, and SHA1 Fingerprint.
- **Download SSL Certificate**—Certificate that you use to download an SSL Web Admin Certificate from a local TFTP server. Select the **Download SSL Certificate** check box to display the following entries:
 - **Server IP Address**—IP address of the local TFTP server.
 - **Maximum Retries**—Maximum number of times each download can be attempted.
 - **Timeout**—Amount of time allowed for each download.
 - **Certificate File Path**—Usually either \ or /, as most TFTP servers automatically determine the path to their default file location. Otherwise, use the TFTP server absolute file path.
 - **Certificate File Name**—Web Administration Certificate filename in encrypted PEM (Privacy Enhanced Mail) format.
 - **Certificate Password**—SSL certificate password that is used to decrypt the SSL Web Admin Certificate.

**Note**

The TFTP server cannot run on the same computer because the Cisco Prime Infrastructure and the TFTP server use the same communication port.

**Caution**

Each certificate has a variable-length embedded RSA key. The RSA key length varies from 512 bits, which is relatively insecure, to thousands of bits, which is very secure. When you are obtaining a new certificate from a Certificate Authority (such as the Microsoft CA), make sure the RSA key embedded in the certificate is at least 768 bits.

Click **Apply** and **Yes** to download the SSL Web Admin Certificate. The operating system informs you of the file transfer and the certificate installation progress.

The SSL password decrypts the certificate, and the certificate is used for Secure Web Mode access when activated.

**Note**

You must save the configuration changes and reboot the Cisco WLC after changing the SSL certificate.

Click **Apply** to send data or a download SSL certificate request to the Cisco WLC, but the result is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

Click **Delete Certificate** to instruct the operating system to delete the current SSL certificate.

Click **Regenerate Certificate** to instruct the operating system to generate a new SSL certificate to replace any existing certificate; the Web User Interface displays the “Successfully Generated SSL Web Admin Certificate” message when done.

IPSEC

Choose **MANAGEMENT > IPSEC** to navigate to the **IPSEC Profile Name** page.

Click **New** to create a new IPSEC profile.

On the **IPSEC Profile Name** page, click an IPSEC profile name to edit the profile.

Table 7-18 *IPSEC Profile Parameters*

Parameter	Range
IPSec Profile Name	Name of the IPSec profile that you created.
IKE Version	IKE version: 1 or 2.
Encryption	IP security encryption mechanism used.
Authentication	IP security authentication protocol used.
IKE DH Group	Set the IKE Diffie-Hellman Group. The options are as follows: <ul style="list-style-type: none">• Group 14 (2048 bits)• Group 19 (256 bits)• Group 20 (384 bits) Diffie-Hellman techniques are used by two devices to generate a symmetric key where they can publicly exchange values and generate the same symmetric key.
IKE Lifetime	IKE lifetime in seconds. Valid range is between 1800 and 57600. Default value is 28800 seconds.
IPSec Lifetime	IPSec lifetime in seconds. Valid range is between 1800 and 57600. Default value is 1800 seconds.
IKE Phase1	Internet Key Exchange protocol (IKE). Options are as follows: <ul style="list-style-type: none">• Aggressive• Main IKE Phase1 is used to negotiate how IKE should be protected. Aggressive mode passes more information in fewer packets, with a slightly faster connection, at the cost of transmitting the identities of the security gateways in the clear.
IKE Peer Identification	IKE peer identification mode. Options include: <ul style="list-style-type: none">• FQDN• User FQDN• CN• IP
IKE Peer Value	Peer value for IKE that you can specify.

Table 7-18 IPSEC Profile Parameters

Parameter	Range
IKE Authentication Mode	IKE authentication method as either PSK or Certificate.
Shared Secret Format	Format of the shared secret that you set to either ASCII or Hex.
Shared Secret	RADIUS Server login Shared Secret.
Confirm Shared Secret	RADIUS Server login Shared Secret.

Telnet-SSH Configuration

Choose **MANAGEMENT > Telnet-SSH** to navigate to the Telnet-SSH Configuration page.

**Note**

Only FIPS approved algorithm 128-cbc is supported when using SSH to control WLANs.

This page enables you to modify the following settings for Telnet accessibility to the Cisco WLC:

- **Session Timeout (minutes)**—Number of minutes that a Telnet session is allowed to remain inactive before being logged off. A zero means there is no timeout. The timeout may be specified as a number from 0 to 160. The default is 5 minutes.
- **Maximum Number of Telnet Sessions**—Values from 0 to 5. This object indicates the number of simultaneous Telnet sessions allowed. The default is 5.
- **Allow New Telnet Sessions**—Whether new Telnet sessions are not allowed on the DS port when set to no. The default is no.

**Note**

New Telnet sessions are allowed or disallowed on both the DS (network) port and the Service port using the Allow New Telnet Sessions parameter.

- **Allow New SSH Sessions**—Whether new Secure Shell Telnet sessions are not allowed when set to no. The default value is yes.

Click **Apply** to send data to the Cisco WLC, but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

Serial Port Configuration

Choose **MANAGEMENT > Serial Port** to navigate to the Serial Port Configuration page. This page enables you to modify configurable serial session properties.

This table describes the serial port configuration parameters.

Table 7-19 *Serial Port Configuration Parameters*

Parameter	Description	Range
Serial Port Login Timeout (Seconds)	Time, in minutes, of inactivity on a serial port connection, after which the Cisco WLC closes the connection.	Any numeric value between 0 and 9600 is allowed. The default is 5. A value of 0 disables the timeout.
Baud Rate (bps)	Default baud rate at which the serial port tries to connect.	The available values are 1200, 2400, 4800, 9600, 19200, 38400, 57600, and 115200 baud. The default is 9600 baud.
Character Size (bits)	Number of bits in a character.	8 (read-only).
Flow Control	Whether hardware flow control is enabled or disabled.	Disabled (read-only).
Stop Bits	Number of stop bits per character.	1 (read-only).
Parity	Parity method used on the serial port.	None (read-only).

Click **Apply** to send data to the Cisco WLC, but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

Local Management Users

Choose **MANAGEMENT > Local Management Users** to navigate to the Local Management Users page.

This page lists current management user logins on the Cisco WLC and the users' access privileges.

You may remove a user account by click the blue arrow adjacent the desired account and choose **Remove**.



Caution

Removing the default admin user prohibits both web and CLI access to the Cisco WLC. Therefore, you must create a user with administrative (read/write) privileges before you remove the default user.

- Click **New** to add a new management user. For more information, see the [Adding Local Management Users](#) topic.

Adding Local Management Users

Choose **MANAGEMENT > Local Management Users** and then click **New** to navigate to the **Local Management Users > New** page.

This page enables you to add management user accounts on the Cisco WLC and the user's access privileges.

The settings for the Management User Details parameters depends on the settings that you make in the Password Policy page. The following requirements are enforced on the password:

- The password should contain characters from at least three of the following classes: lowercase letters, uppercase letters, digits, and special characters.
- No character in the password can be repeated more than three times consecutively.
- The password should not contain a management username or the reverse letters of a username.
- The password should not contain words like Cisco, oscic, admin, nimda, or any variant obtained by changing the capitalization of letters by substituting l, I, or ! or substituting 0 for o or substituting \$ for s.

This table describes the management user details parameters.

Table 7-20 *Management User Details Parameters*

Parameter	Description
User Name	Login username.
Password	User password. The default is admin.
Confirm Password	User password that you confirm. The default is admin.
User Access Mode	User privilege assignment (Read-Only, Read-Write, or Lobby Admin) that you create for Guest User Accounts.
Telnet Capable	Check box that you can select to enable local management users to Telnet to the Cisco WLC. By default, this feature is enabled. You must enable global Telnet to enable this feature. SSH connection is not affected when you enable this option.

Click **Apply** to send data to the Cisco WLC, but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

Guest User Accounts

The first step in creating guest user accounts is for the system administrator to set up a lobby administrator account, also known as a Lobby Ambassador account. A Lobby Ambassador account has limited configuration privileges and has access only to the pages that are used to configure and manage guest user accounts. This feature enables a nontechnical person to create and manage guest user accounts on the Cisco WLC.

A guest user account can provide a user account for a limited amount of time. The Lobby Ambassador is able to configure a specific time frame for the guest user account to be active. After the specified time period, the guest user account automatically expires.

To create a guest user account, log out of the Cisco WLC and log back in again as Lobby Administrator. You will view the guest user accounts you create on the Cisco WLC (and all others) on the local net user's page (see the [Local Net Users](#) topic).

Lobby Ambassador Account Setup

-
- Step 1** Go to **Management > Local Management Users > New**.
- Step 2** Create a username for the Lobby Ambassador account and enter it in the User Name text box.
- Step 3** Create a password for the Lobby Ambassador account and enter it in the Password text box.

- Step 4** Reenter the Lobby Ambassador account password in the Confirm Password text box.
- Step 5** Select **LobbyAdmin** in the User Access Mode box.
- Step 6** Click **Apply**. The Local Management Users page opens and displays all registered users, including the new username that you just created, identified as LobbyAdmin. You may create additional new users from this page, or remove any except the admin user.
-

Adding Guest User Accounts

- Step 1** Log into the Cisco WLC user as Lobby Ambassador.
- Step 2** Click **Configure > Controller Templates** to display the NTP Server Templates page.
- Step 3** From the left navigation, choose **Security**, and then choose **Guest Users** to display the Guest Users page.
- Step 4** From the Select a Command drop-down list, choose **Add Template** and click **GO**.
- Step 5** On the Guest User > New Template page, follow these steps to add a new guest user account:
- Enter the guest username. The maximum is 24 characters.
 - Select the check box to generate an automatic password or enter a password. If you enter a password, enter it twice to confirm. The generated password is automatically entered into the password text box.



Note Passwords are case sensitive.

- From the drop-down list, choose an SSID (WLAN Service Set Identifier). The SSID that this guest user applies must be a WLAN that has a Layer 3 web authentication policy configured. Your administrator can advise which SSID to use.
 - Enter a description of the guest user account.
 - From the drop-down list, choose days, hours, or minutes for the lifetime of this guest user account. The maximum is 30 days. A value of zero (0) implies infinity and will be a permanent account.
- Step 6** Click **Save** to save your changes or click **Cancel** to leave the settings unchanged. When you click Save, the screen refreshes and includes the following:
- Save—Save your changes.
 - Apply to Controllers—The Apply to Controller page appears. Select the check box for the Cisco WLC or Config Group name that the guest user account applies to and click **OK**. If you do not want to apply to Cisco WLCs, click **Cancel**. If you click OK, the Apply to Controllers page refreshes and shows the operation status. If the operation status shows as successful, the guest user account has been completed and can be used immediately.
 - The Account Expiry page displays the Cisco WLC to which the guest user account was applied and the seconds remaining before the guest user account expires.
 - Delete—Deletes the displayed guest user template.
 - Cancel—Disregards any settings or changes.
-

User Sessions

Choose **MANAGEMENT > User Sessions** to navigate to the **CLI Sessions** page. This page provides a list of open CLI sessions.

Table 7-21 CLI Session Details Parameters

Parameter	Description
ID	Session identification.
User Name	Login username.
Login Type	Telnet or serial session.
Connection From	Name of the client computer system or the physical port.
Idle time	Elapsed inactive session time.
Session Time	Elapsed active session time.

To stop an existing Telnet session, click the blue arrow adjacent the desired session and choose **Close**.

Syslog Configuration

Choose **MANAGEMENT > Logs > Config** to navigate to the Syslog Configuration page.

This page enables you to configure system logs.

If you enable system logs, enter the IP address of the server to which to send the syslog messages and click **Add**. You can add up to three syslog servers to the Cisco WLC. The list of syslog servers that have already been added to the Cisco WLC appears below this field.

Syslog Server

Table 7-22 *Syslog Server Parameters*

Parameter	Description
Syslog Server IP Address (IPv4/IPv6)	Enter the IPv4/ IPv6 address of the Syslog server address. Note You can only add a maximum of 3 Syslog servers.

Table 7-22 Syslog Server Parameters

Parameter	Description
Syslog Level	<p>Severity level for filtering syslog messages to the syslog servers:</p> <ul style="list-style-type: none"> • Emergencies—Severity level 0 • Alerts—Severity level 1 (default value) • Critical—Severity level 2 • Errors—Severity level 3 • Warnings—Severity level 4 • Notifications—Severity level 5 • Informational—Severity level 6 • Debugging—Severity level 7 <p>Note If you set a logging level, only those messages whose severity is equal to or less than that level are logged by the Cisco WLC. For example, if you set the logging level to Warnings (severity level 4), only those messages whose severity is between 0 and 4 are logged.</p>
Syslog Facility	<p>Facility for outgoing syslog messages to the syslog servers:</p> <ul style="list-style-type: none"> • Kernel—Facility level 0 • User Process—Facility level 1 • Mail—Facility level 2 • System Daemons—Facility level 3 • Authorization—Facility level 4 • Syslog—Facility level 5 (default value) • Line Printer—Facility level 6 • USENET—Facility level 7 • Unix-to-Unix Copy—Facility level 8 • Cron—Facility level 9 • FTP Daemon—Facility level 11 • System Use 1—Facility level 12 • System Use 2—Facility level 13 • System Use 3—Facility level 14 • System Use 4—Facility level 15 • Local Use 0—Facility level 16 • Local Use 1—Facility level 17 • Local Use 2—Facility level 18 • Local Use 3—Facility level 19 • Local Use 4—Facility level 20 • Local Use 5—Facility level 21 • Local Use 6—Facility level 22 • Local Use 7—Facility level 23

Msg Log Configuration

Table 7-23 Msg Log Configuration Parameters

Parameter	Description
Buffered Log Level	Severity level for logging messages to the Cisco WLC buffer and console: <ul style="list-style-type: none">• Emergencies—Severity level 0• Alerts—Severity level 1• Critical—Severity level 2• Errors—Severity level 3 (default value)• Warnings—Severity level 4• Notifications—Severity level 5• Informational—Severity level 6• Debugging—Severity level 7• Disable—Disable console logging
Console Log Level	
File Info	Information about the source file. The default is enabled.
Trace Info	Traceback information. The default is disabled state.

Click **Apply** to send data to the Cisco WLC, but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

Message Logs

Choose **MANAGEMENT > Logs > Message logs** to navigate to the Message Logs page.

This page enables you to view the message logs that have been captured by the Cisco WLC, by the last to the first message. Each trap entry includes the system time, filename and line, message type and message.

Click **Clear** to purge the existing message log..

Management Via Wireless

Choose **MANAGEMENT > Mgmt Via Wireless** to navigate to the Management Via Wireless page. This page enables you to configure access to the Cisco WLC management interface from wireless clients using IPv4 and IPv6 methods. The default is disabled state.



Note

Due to IPsec limitations, the Management Via Wireless feature is available only if you log in across WPA, Static WEP, or VPN Pass Through WLANs. The Management feature is not available if you attempt to log on through an IPsec WLAN.

Click **Apply** to send data to the Cisco WLC, but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

Cloud Services

Choose **MANAGEMENT > Cloud Services** to navigate to the **Cloud Services** page. This page enables you to configure the CMX Cloud in the Cisco WLC. HTTPS protocol is used to connect the Cisco WLC and the CMX cloud.

Server

Table 7-24 Cloud Server Configuration Parameters

Parameter	Description
URL	The CMX server URL.
Id-Token	Cloud server Id-token issued for Cisco WLC.

CMX

Table 7-25 Cloud CMX Configuration Parameters

Parameter	Description
Service Status	CMX service that you can enable or disable.
Connectivity Mode	Communication protocol used to connect the Cisco WLC with the CMX server (read-only).
Link Status	The current status of the link (read-only).

Installing and Configuring Licenses

You can order Cisco 5508 Wireless Controllers with support for 12, 25, 50, 100, 250 or 500 access points as the Cisco WLC's base capacity. You can add additional access point capacity through capacity adder licenses available at 25, 50, 100, and 250 access point capacities. You can add the capacity adder licenses to any base license in any combination to arrive at the maximum capacity of 500 access points. The base and adder licenses are supported through both rehosting and RMAs.

The base license supports the standard base software set and, for 6.0196.0 and later releases, the premium software set is included as part of the base feature set, which includes this functionality:

- Datagram Transport Layer Security (DTLS) data encryption for added security across remote WAN and LAN links.

About the availability of data DTLS for the 7.0.116.0 release:

- Cisco 5500 Series Controller—The Cisco 5500 Series Controller will be available with two licensing options: one with data DTLS capabilities and another image without data DTLS.

- Cisco 7500, 2500, WiSM2—These platforms by default will not contain DTLS. To turn on data DTLS, a license must be installed. That is, these platforms will have a single image with data DTLS turned off. To use data DTLS you must have a license.
- Support for OfficeExtend Access Points, which are used for secure mobile telecommuting. For more information about OfficeExtend access points, see [OfficeExtend Access Points](#).

All features included in a Wireless LAN Controller WPLUS license are now included in the base license; this change is introduced in release 6.0.196.0. There are no changes to WCS BASE and PLUS licensing. These WPLUS license features are included in the base license:

- OfficeExtend AP
- Enterprise Mesh
- CAPWAP Data Encryption

The licensing change can affect features on your wireless LAN when you upgrade or downgrade software releases, so you should be aware of these guidelines:

- If you have a WPLUS license and you upgrade from 6.0.x.x to 7.0.98.0, your license file contains both Basic and WPLUS license features. You will not see any disruption in feature availability and operation.
- If you have a WPLUS license and you downgrade from 7.0.98.0 to 6.0.196.0 or 6.0.188 or 6.0.182, your license file contains only base license, and you will lose all WPLUS features.
- If you have a base license and downgrade from 6.0.196.0 to 6.0.188 or 6.0.182, when you downgrade, you lose all WPLUS features.

To view the Cisco WLC trap log, choose **Monitor** and click **View All** under “Most Recent Traps” on the Cisco WLC GUI.



Note You can also view traps by using SNMP-based management tools.

The ap-count licenses and their corresponding image-based licenses are installed together. The Cisco WLC keeps track of the licensed access point count and does not allow more than the number of access points to associate to it.

The Cisco 5500 Series Controller is shipped with both permanent and evaluation base and base-ap-count licenses. If desired, you can activate the evaluation licenses, which are designed for temporary use and set to expire after 60 days.

No licensing steps are required after you receive your Cisco 5500 Series Controller because the licenses you ordered are installed at the factory. In addition, licenses and product authorization keys (PAKs) are preregistered to serial numbers. However, as your wireless network evolves, you might want to add support for additional access points or upgrade from the standard software set to the base software set. To do so, you need to obtain and install an upgrade license.

Obtaining an Upgrade License

A certificate with a product authorization key (PAK) is required before you can obtain an upgrade license.

You can use the capacity adder licenses to increase the number of access points supported by the Cisco WLC up to a maximum of 500 access points. The capacity adder licenses are available in access point capacities of 10, 25, 50, 100 and 250 access points. You can add these licenses to any of the base capacity licenses of 12, 25, 50, 100 and 250 access points.

For example, if your Cisco WLC was initially ordered with support for 100 access points (base license AIR-CT5508-100-K9), you could increase the capacity to 500 access points by purchasing a 250 access point, 100 access point, and a 50 access point additive capacity license (LIC-CT5508-250A, LIC-CT5508-100A, and LIC-CT5508-50A).

You can find more information on ordering capacity adder licenses at this URL:

<http://www.cisco.com/c/en/us/products/wireless/5500-series-wireless-controllers/datasheet-listing.html>

If you skip any tiers when upgrading (for example, if you do not install the -25U and -50U licenses along with the -100U), the license registration fails.

For a single Cisco WLC, you can order different upgrade licenses in one transaction (for example, -25U, -50U, -100U, and -250U), for which you receive one PAK with one license. Then you have only one license (instead of four) to install on your Cisco WLC.

If you have multiple Cisco WLCs and want to upgrade all of them, you can order multiple quantities of each upgrade license in one transaction (for example, you can order 10 each of the -25U, -50U, -100U, and -250 upgrade licenses), for which you receive one PAK with one license. You can continue to register the PAK for multiple Cisco WLCs until it is exhausted.

Base license SKUs for the Cisco Flex 7500 Series Controllers are as follows:

- AIR-CT7510-300-K9
- AIR-CT7510-500-K9
- AIR-CT7510-1K-K9
- AIR-CT7510-2K-K9

Base license SKUs for the Cisco 5500 Series Controllers are as follows:

- AIR-CT5508-12-K9
- AIR-CT5508-25-K9
- AIR-CT5508-50-K9
- AIR-CT5508-100-K9
- AIR-CT5508-250-K9
- AIR-CT5508-500-K9

The capacity adder SKUs are as follows:

- LIC-CT5508-10A
- LIC-CT5508-25A
- LIC-CT5508-50A
- LIC-CT5508-100A
- LIC-CT5508-250A

Base license SKUs for the Cisco 2500 Series Controllers are as follows:

- AIR-CT2504-5-K9
- AIR-CT2504-15-K9
- AIR-CT2504-25-K9
- AIR-CT2504-50-K9

Base license SKUs for the Cisco WiSM2 Controllers are as follows:

- WS-SVC-WISM2-1-K9—WiSM2 with 100 AP support

- WS-SVC-WISM2-3-K9—WiSM2 with 300 AP support
- WS-SVC-WISM2-5-K9—WiSM2

To obtain and register a PAK certificate, follow these steps:

Step 1 Order the PAK certificate for an upgrade license through your Cisco channel partner or your Cisco sales representative, or order it online at this URL:

<http://www.cisco.com/web/ordering/root/index.html>

Step 2 If you are ordering online, begin by choosing the primary upgrade SKU L-LIC-CT5508-UPG or LIC CT5508-UPG. Then, choose any number of the following options to upgrade one or more Cisco WLCs under one PAK.

This table describes the controller configuration parameters.

Table 7-26 License Agent Configuration Parameters

Type	Part Number	Description
email	L-LIC-CT5508-UPG	Primary upgrade SKU: Pick any number or combination of the following options under this SKU to upgrade one or many Cisco WLCs under one product authorization key
	L-LIC-CT5508-25A	25 AP Adder License for the Cisco 5508 Controllers (eDelivery)
	L-LIC-CT5508-50A	50 AP Adder License for the Cisco 5508 Controllers (eDelivery)
	L-LIC-CT5508-100A	100 AP Adder License for the Cisco 5508 Controllers (eDelivery)
	L-LIC-CT5508-250A	250 AP Adder License for the Cisco 5508 Controllers (eDelivery)
	L-LIC-CT2504-UPG	Primary upgrade SKU: Pick any number or combination of the following options under this SKU to upgrade one or many Cisco WLCs under one product authorization key
	L-LIC-CT2504-5A	5 AP Adder License for Cisco 2504 Wireless Controller (e-Delivery)
	L-LiC-CT2504-25A	25 AP Adder License for Cisco 2504 Wireless Controller (E-Delivery)

Table 7-26 License Agent Configuration Parameters

Type	Part Number	Description
paper	LIC-CT5508-UPG	Primary upgrade SKU: Pick any number or combination of the following options under this SKU, to upgrade one or many Cisco WLCs under one product authorization key
	LIC-CT5508-25A	25 AP Adder License for the Cisco 5508 Controller
	LIC-CT5508-50A	50 AP Adder License for the Cisco 5508 Controller
	LIC-CT5508-100A	100 AP Adder License for the Cisco 5508 Controller
	LIC-CT5508-250A	250 AP Adder License for the Cisco 5508 Controller
	LIC-CT2504-UPG	Primary upgrade SKU: Pick any number or combination of the following options under this sku to upgrade one or many Cisco WLCs under one product authorization key
	LIC-CT2504-5A	5 AP Adder License for Cisco 2504 Controller (Paper Certificate -US Mail)
	LIC-CT2504-25A	25 AP Adder License for Cisco 2504 Controller (Paper Certificate - US Mail)

**Note**

If you require a paper certificate for Customs, order it without the “L-” in the SKU (for example, LIC-CT5508-250A) and choose to ship it using the U.S. mail.

Step 3

After you receive the certificate, use one of two methods to register the PAK:

- Cisco License Manager (CLM)—This method automates the process of obtaining licenses and deploying them on Cisco devices. For deployments with more than five Cisco WLCs, we recommend using CLM to register PAKs and install licenses. You can also use CLM to rehost or RMA a license.

**Note**

You can download the CLM software and access user documentation at <http://www.cisco.com/c/en/us/products/cloud-systems-management/license-manager/index.html>

- Licensing portal—This alternative method enables you to manually obtain and install licenses on your Cisco WLC. If you want to use the licensing portal to register the PAK, follow the instructions in [Step 4](#).

Step 4 Use the licensing portal to register the PAK as follows:

- a. Go to <http://tools.cisco.com/SWIFT/Licensing/PrivateRegistrationServlet>
- b. On the main Product License Registration page, enter the PAK mailed with the certificate in the Product Authorization Key (PAK) text box and click **Submit**.
- c. On the Validate Features page, enter the number of licenses that you want to register in the Qty text box and click **Update**.
- d. To determine the Cisco WLC's product ID and serial number, choose **Controller > Inventory** on the Cisco WLC GUI or enter the **show license udi** command on the Cisco WLC CLI.



Note To determine the Cisco WLC's product ID and serial number, see the [Inventory](#) page.

- e. On the Designate Licensee page, enter the product ID and serial number of the Cisco WLC on which you plan to install the license, read and accept the conditions of the end-user license agreement (EULA), complete the rest of the text boxes on this page, and click **Submit**.
 - f. On the Finish and Submit page, verify that all information is correct and click **Submit**.
 - g. When a message appears indicating that the registration is complete, click **Download License**. The license is emailed within 1 hour to the address that you specified.
 - h. When the e-mail arrives, follow the instructions provided.
 - i. Copy the license file to your TFTP server.
 - j. Follow the instructions in the "Installing a License" section below to install the license on your Cisco WLC.
-

Installing a License

For installation instructions, see the [Install License](#) section on the [License Commands](#) page.

Licenses



Note To use Cisco Smart Software License supported on certain [supported models](#), see [License Type](#) and [Smart-License](#) sections.

Choose **MANAGEMENT > Software Activation > Licenses** to navigate to the Licenses page.

This page enables you to view all of the following types of information about the licenses installed on the Cisco WLC:

- License—Name of the license.
- Type—Permanent, evaluation, or extension.
- Time (expires)—How long until the license expires.
- HBL Count—Maximum number of access points allowed for the adder license. This field appears only for Cisco Flex 7500 Series and 8500 Series Controllers.
- Non HBL Count—Maximum number of access points allowed for the CDK license. This field appears only for Cisco Flex 7500 Series and 8500 Series Controllers.

- **Count**—Maximum number of access points allowed for this license. This field does not appear for Cisco Flex 7500 Series and 8500 Series Controllers.
- **Priority**—Low, medium, or high.
- **Status**—In use, not in use, inactive, or End User License Agreement (EULA) not accepted.

If you ever want to remove a license from the Cisco WLC, click the blue arrow adjacent the desired license and choose **Remove**. For example, you might want to delete an expired evaluation license or any unused license. You cannot delete unexpired evaluation licenses, the permanent base image license, or licenses that are in use by the Cisco WLC.

For Cisco Flex 7500 Series and 8500 Series Controllers, honor-based licensing also called Right to Use licensing was introduced in Cisco WLC Release 7.3. This feature allows you to add and activate an AP-count license on the Cisco WLC without using any external tools after accepting an End User License Agreement (EULA).

To add an AP-count license for Cisco Flex 7500 Series and 8500 Series Controllers follow these steps:

-
- Step 1** Enter the count in the License Count text box.
- Step 2** Choose **Add** from the License Count drop-down list.
- Step 3** Click **Set Count**.
- Step 4** When the end-user license agreement (EULA) appears, read the terms of the agreement and then click **Accept**.
- The ap-count permanent license is active now.
-

To delete an AP-count license or reduce the count for Cisco Flex 7500 Series and 8500 Series Controllers follow these steps:

-
- Step 1** Enter the count in the License Count text box.
- Step 2** Choose **Delete** from the License Count drop-down list.
- Step 3** Click **Set Count**.
- Step 4** When the end-user license agreement (EULA) appears, read the terms of the agreement and then click **Accept**.

If the count is equal to the HBL count of the license, the license is removed from the list. If the count is less than the HBL count, the license appears with the decremented count.

To view more details for a particular license, click the link for the desired license. The [License Detail](#) page appears.

License Detail

Choose **MANAGEMENT > Software Activation > License** and then click a license name to navigate to the License Detail page.

This page shows the following additional information for the license:

- License name

- License type
The license type can be permanent, evaluation, or extension.
- License version
- Comment
You can enter a comment for this license in the Comment text box and click **Apply**.
- Status
Status of the license. It can be one of the following:
 - In use
 - Not in use
 - Inactive
 - End user license agreement not accepted
- Current Status
This field appears only for Cisco Flex 7500 Series and 8500 Series Controllers. It indicates the current status of the license. It can be one of the following:
 - In use
 - Not in use
 - Inactive
 - End user license agreement not accepted
- Expires
Length of time before the license expires



Note Permanent licenses never expire.

- License Status
This field appears only for Cisco Flex 7500 Series and 8500 Series Controllers. You can activate or deactivate the license by choosing **Activate** or **Deactivate** from the drop-down list.
- Built-in License
Whether the license is a built-in license.
- Maximum Count
Maximum number of access points allowed for this license. This field does not appear for Cisco Flex 7500 Series and 8500 Series Controllers.
- Counts Used
Number of access points currently using this license. This field does not appear for Cisco Flex 7500 Series and 8500 Series Controllers.
- Priority
To activate an ap-count evaluation license, you must change its priority to high. If you no longer want to have this higher capacity, you can lower the priority of the ap-count evaluation license, which forces the controller to use the permanent license. This field does not appear for Cisco Flex 7500 Series and 8500 Series Controllers.



Note You can set the priority only for ap-count evaluation licenses. AP-count permanent licenses always have a medium priority, which cannot be configured.

Activating an AP-Count Evaluation License

If you are considering upgrading to a license with a higher access point count, you can try an evaluation license before upgrading to a permanent version of the license. For example, if you are using a permanent license with a 50 access point count and want to try an evaluation license with a 100 access point count, you can try out the evaluation license for 60 days.

AP-count evaluation licenses are set to low priority by default so that the Cisco WLC uses the ap-count permanent license. If you want to try an evaluation license with an increased access point count, you must change its priority to high. If you no longer want to have this higher capacity, you can lower the priority of the ap-count evaluation license, forcing the Cisco WLC to use the permanent license.



Note If the ap-count evaluation license is a wplus license and the ap-count permanent license is a base license, you must also change the feature set to wplus. See the [License Level](#) page for instructions.



Note To prevent disruptions in operation, the Cisco WLC does not switch licenses when an evaluation license expires. You must reboot the Cisco WLC in order to return to a permanent license. Following a reboot, the Cisco WLC defaults to the same feature set level as the expired evaluation license. If no permanent license at the same feature set level is installed, the Cisco WLC uses a permanent license at another level or an unexpired evaluation license.

To activate an ap-count evaluation license, follow these steps:

- Step 1** Choose **High** from the Priority drop-down list and click **Set Priority**.
- Step 2** Click **OK** when prompted to confirm your decision about changing the priority of the license.
- Step 3** When the end-user license agreement (EULA) appears, read the terms of the agreement and then click **Accept**.
- Step 4** When prompted to reboot the Cisco WLC, click **OK**.
- Step 5** Reboot the Cisco WLC in order for the priority change to take effect.
- Step 6** Click [Licenses](#) to open the Licenses page and verify that the ap-count evaluation license now has a high priority and is in use. You can use the evaluation license until it expires.

If you decide to stop using the ap-count evaluation license and want to revert to using an ap-count permanent license, follow these steps:

- Step 1** Choose **Low** from the Priority drop-down list and click **Set Priority**.
- Step 2** Click **OK** when prompted to confirm your decision about changing the priority of the license.
- Step 3** When the end-user license agreement (EULA) appears, read the terms of the agreement and then click **Accept**.
- Step 4** When prompted to reboot the Cisco WLC, click **OK**.

- Step 5** Reboot the Cisco WLC in order for the priority change to take effect.
- Step 6** Click [Licenses](#) to open the Licenses page and verify that the ap-count evaluation license now has a low priority and is not in use. Instead, the ap-count permanent license should be in use.
-

License Level

Choose **MANAGEMENT > Software Activation > License Usage** to navigate to the License Level page.

This page enables you to configure the Cisco WLC to specify which feature set it uses (base or wplus). Only the base or wplus license can be active at a time. The currently active license determines the feature set and number of access points supported on the Cisco WLC.

This page shows the current license level (base or wplus) and the level to be used after the next Cisco WLC reboot. It also shows the maximum number of access points allowed by the license on the Cisco WLC, the number of access points currently joined to the Cisco WLC, and the number of access points that can still join the Cisco WLC.

**Note**

To learn more about the available license levels, click the **base** or **wplus** license level link to open the Licenses page. This page shows the licenses applicable to this level and the list of features supported. Click **Back** to return to the License Level page.

To change the license level, follow these steps:

- Step 1** Choose the license level to be used on the next reboot: **base**, **wplus**, or **auto**. If you choose auto, the licensing software automatically chooses the license level to use on the next reboot. It chooses permanent licenses over evaluation licenses and wplus licenses over base licenses.

**Note**

If you are considering upgrading from a base license to a wplus license, you can try an evaluation wplus license before upgrading to a permanent wplus license. To activate the evaluation license, you need to set the image level to **wplus** in order for the Cisco WLC to use the wplus evaluation license instead of the base permanent license. If no valid licenses are installed, the Cisco WLC can always operate in base level.

**Note**

To prevent disruptions in operation, the Cisco WLC does not switch licenses when an evaluation license expires. You must reboot the Cisco WLC in order to return to a permanent license. Following a reboot, the Cisco WLC defaults to the same feature set level as the expired evaluation license. If no permanent license at the same feature set level is installed, the Cisco WLC uses a permanent license at another level or an unexpired evaluation license.

- Step 2** Click **Activate**.
- Step 3** Click **OK** when prompted to confirm your decision to change the license level on the next reboot.
- Step 4** If the end-user license agreement (EULA) appears, read the terms of the agreement and then click **Accept**. The Next Boot Level text box now shows the license level that you specified as the level to be used after the next Cisco WLC reboot.

- Step 5** Reboot the Cisco WLC for the specified license level to take effect.
-

License Commands

Choose > **Software Activation** > **Commands** to navigate to the License Commands page.

From this page, you can install, save, or rehost licenses, and save device credentials.

Install License



Note

For information about obtaining an upgrade license, see the [Obtaining an Upgrade License](#) topic.

- Step 1** From the Action drop-down list, choose **Install License**. The Install license from a file section appears.
- Step 2** In the File Name to Install text box, enter the path to the license (*.lic) on the TFTP server.
- Step 3** Click **Install License**. A message appears to show whether the license was installed successfully. If the installation fails, the message provides the reason for the failure, such as the license is an existing license, the path was not found, the license does not belong to this device, you do not have correct permissions for the license, and so on.
- Step 4** If the end-user license agreement (EULA) acceptance window appears, read the agreement and click **Accept** to accept the terms of the agreement.



Note

Typically you are prompted to accept the end-user license agreement (EULA) for evaluation, extension, and rehost licenses. The EULA is also required for permanent licenses, but it is accepted during license generation.

- Step 5** Reboot the Cisco WLC.
-

Save License

- Step 1** From the Action drop-down list, choose **Save License**. This saves all the licenses to a file, except the evaluation license section that appears.
- Step 2** In the File Name to Save text box, enter the path on the TFTP server where you want the licenses to be saved.



Note

You cannot save evaluation licenses.

- Step 3** Click **Save Licenses**.
- Step 4** Reboot the Cisco WLC.
-

Save Credentials

To save device credential information to a file, enter the path on the TFTP server where you want the device credentials to be saved and click **Save Credentials**. You need to save the device credentials to rehost a license.

Rehost

Revoking a license from one Cisco WLC and installing it on another is called *rehosting*. You might want to rehost a license to change the purpose of a Cisco WLC. For example, if you want to move your OfficeExtend or indoor mesh access points to a different Cisco WLC, you could transfer the wplus license from one Cisco WLC to another.

In order to rehost a license, you must generate credential information from the Cisco WLC and use it to obtain a permission ticket to revoke the license from the Cisco licensing site. Next, you must obtain a rehost ticket and use it to obtain a license installation file for the Cisco WLC on which you want to install the license.

Evaluation licenses and the permanent base image license cannot be rehosted.



Note

A revoked license cannot be reinstalled on the same Cisco WLC.

To rehost a license, follow these steps:

- Step 1** In the File Name to Save Credentials text box, enter the path on the TFTP server where you want the device credentials to be saved and click **Save Credentials**.
- Step 2** Obtain a permission ticket to revoke the license as follows:
 - a. Click **Cisco Licensing** (<https://tools.cisco.com/SWIFT/Licensing/PrivateRegistrationServlet>). The Product License Registration page appears.
 - b. Under Manage Licenses, click **Look Up a License**.
 - c. Enter the product ID and serial number for your Cisco WLC.



Note

To determine the Cisco WLC's product ID and serial number, see the [Inventory](#) page.

- d. Open the device credential information file that you saved in [Step 1](#) and copy and paste the contents of the file into the Device Credentials text box.
- e. Enter the security code in the blank box and click **Continue**.
- f. Choose the licenses that you want to revoke from this Cisco WLC and click **Start License Transfer**.
- g. On the Rehost Quantities page, enter the number of licenses that you want to revoke in the To Rehost box and click **Continue**.
- h. On the Designate Licensee page, enter the product ID and serial number of the Cisco WLC for which you plan to revoke the license, read and accept the conditions of the end-user license agreement (EULA), complete the rest of the text boxes on this page, and click **Continue**.
- i. On the Review and Submit page, verify that all information is correct and click **Submit**.
- j. When a message appears indicating that the registration is complete, click **Download Permission Ticket**. The rehost permission ticket is e-mailed within 1 hour to the address that you specified.
- k. After the e-mail arrives, copy the rehost permission ticket to your TFTP server.

- Step 3** Use the rehost permission ticket to revoke the license from this Cisco WLC and generate a rehost ticket as follows:
- In the Cisco WLC GUI Enter Saved Permission Ticket File Name text box, enter the TFTP path and filename (*.lic) for the rehost permission ticket that you generated in [Step 2](#).
 - In the Rehost Ticket File Name text box, enter the TFTP path and filename (*.lic) for the ticket that will be used to rehost this license on another Cisco WLC.
 - Click **Generate Rehost Ticket**.
 - When the EULA acceptance page appears, read the agreement and click **Accept** to accept the terms of the agreement.
- Step 4** Use the rehost ticket that you generated in [Step 3](#) to obtain a license installation file, which can then be installed on another Cisco WLC as follows:
- Click **Cisco Licensing** (<http://www.cisco.com/go/license>)
 - On the Product License Registration page, click **Upload Rehost Ticket** under Manage Licenses.
 - On the Upload Ticket page, enter the rehost ticket that you generated in [Step 3](#) in the Enter Rehost Ticket text box and click **Continue**.
 - On the Validate Features page, verify that the license information for your Cisco WLC is correct, enter the rehost quantity, and click **Continue**.
 - On the Designate Licensee page, enter the product ID and serial number of the Cisco WLC on which you plan to use the license, read and accept the conditions of the EULA, complete the rest of the text boxes on this page, and click **Continue**.
 - On the Review and Submit page, verify that all information is correct and click **Submit**.
 - When a message appears indicating that the registration is complete, click **Download License**. The rehost license key is e-mailed within 1 hour to the address you specified.
 - After the e-mail arrives, copy the rehost license key to your TFTP server.
 - Follow the instructions from the [Install License](#) page to install this license on another Cisco WLC.
-

License Type

This section is applicable to platforms that support both **RTU** and **Smart Licensing** mechanisms.

To choose the license type that should be used, follow these steps:



Note

The device must be rebooted to activate the changed license mechanism.

- Step 1** Choose **Management > Software Activation > License Type**.
- Step 2** From the **Licensing Type** drop-down list, choose from the following options:
- RTU**
 - Smart-Licensing**
- Step 3** Enter the **DNS Server IP address** in IPv4 format.
- Step 4** Click **Apply**.

Step 5 Reboot Cisco WLC to activate the selected license mechanism.

Smart-License

Cisco Smart Software Licensing is a secured mechanism designed to provide flexible licensing of next generation Cisco software products in your network.

Cisco Smart Software Licensing feature is currently supported only on the following Cisco WLC models:

- Cisco 5520 WLC (AIR-CT5520-K9)
- Cisco 8540 WLC (AIR-CT8540-K9)
- Cisco vWLC (L-AIR-CTVM-5-K9)

Device Registration

Step 1 Choose **Management > Smart-License > Device registration** to open the **Device Registration** page.

Step 2 To register a new device, follow these steps:

- a. From the **Action** drop-down list, choose **Registration** to register a new device.
- b. In the **Smart License registration in the field** area, enter the token ID of the device in the **Token-id** box.
- c. Check the **Force** check box to push for the registration of this device token ID with the central system for activation.



Note

To de-register the device, choose **De-registration** from the **Action** drop-down list to remove the registered device.

Step 3 Click **Apply**.

Status

Step 1 Choose **Management > Smart-license > Status** to open the **Status** page


Step 2 To view the **Smart-Licensing Parameters**, choose from the following options in the drop-down list:

- Status—displays the license status
- Summary—displays a brief summary of all licenses
- all—displays the information on all the licenses
- Udi—displays the unique device identifier (UDI) for the licenses
- Usage—displays entitled licenses in use
- Tech-support—displays information to help troubleshoot issues

Call-home Configuration

Choose **Management > Smart-License > Call-home > Configuration** to open the **Call-Home Configuration** page.

Table 7-27 Call-Home Configuration Parameters

Parameter	Description
Events	Options: <ul style="list-style-type: none"> Enabled—enables the Call-home reporting Disabled—disables the Call-home reporting
Reporting Data-privacy-level	Options: <ul style="list-style-type: none"> Normal—scrubs normal level commands High—scrubs all normal level commands, IP domain name and IP address commands
Reporting Hostname	Enter the Hostname
HTTP-Proxy	To enable proxy, enter the IP-address and port number.
TAC Profile Name	Displays the TAC profile name
TAC Profile Status	Options: <ul style="list-style-type: none"> Enabled—enables the TAC profile Disabled—disables the TAC profile
Contact person's email address	Enter the contact person's email address
Profile	
Name	Name of the new profile
Status	Options: <ul style="list-style-type: none"> Enabled—enables the new profile Disabled—disables the profile
Module	Options: <ul style="list-style-type: none"> sm-license-data—reporting of smart license data all—reporting of smart license and call-home data call-home-data—reporting of call-home data
Reporting Format	Options: <ul style="list-style-type: none"> short-text—data reporting in short-text format long-text—data reporting in long-text format xml—data reporting in XML format <div>  </div> <div> Note Currently, only XML format is supported. </div>
URL	Enter the URL, depending on your preference either the Cisco URL or your custom satellite URL.

System Resource Information

Choose **MANAGEMENT > Tech Support > System Resource Information** to navigate to the System Resource Information page.

This page enables you to view the settings for the current Cisco WLC CPU usage, system buffers, and web server buffers.

For Cisco 5500 Series Controllers, the System Resource Information page also shows the Individual CPU usage, which is the percentage of the CPU in use and the percentage of the CPU time spent at the interrupt level.

Controller Crash Information

Choose **MANAGEMENT > Tech Support > Controller Crash** to navigate to the Controller Crash Information page.

This page displays the most recent Cisco WLC CPU crash files from most to least recent.

Core Dump

Choose **MANAGEMENT > Tech Support > Core Dump** to navigate to the Core Dump page.

You can configure the following settings so that the Cisco WLC can automatically upload a core dump file of the Cisco WLC:

- Core Dump Transfer—Setting to enable or disable the Cisco WLC to generate a core dump file following a crash.
- Transfer Mode—Transfer mode type. Choose FTP. The default is FTP.
- IP Address—IP address of the FTP server to which the core dump file is uploaded.
- File Name—Name that the Cisco WLC uses to label the core dump file.
- User Name—Username to log on to FTP.
- Password—Password to log on to FTP.

Click **Apply** to send data to the Cisco WLC, but the data is not preserved across a power cycle; these parameters are stored temporarily in volatile RAM.

AP Crash Logs

Choose **MANAGEMENT > Tech Support > AP Crash Log** to navigate to the AP Crash Logs page.

This page enables you to view the following settings for the most recent access point log:

- AP Name—Access point name
- AP ID—Access point ID
- MAC Address—MAC address of the access point
- Admin Status—Admin status of the access point
- Operational Status—Operational status of the access point

- Port—Port number
- FileName—Name of the crash log file
- FileSize—Size of the crash log file
- TimeStamp—Crash Timestamp

