Other Commands

capwap ap Commands

Use the **capwap ap** commands to configure CAPWAP access point settings.

capwap ap controller ip address

To configure the controller IP address into the CAPWAP access point from the access point's console port, use the **capwap ap controller ip address** command.

capwap ap controller ip address *A.B.C.D*

Syntax Description

A.B.C.D	IP address of the controller.

Command Default None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines This command must be entered from an access point's console port. This command is applicable for IPv4 addresses only.

Note The access point must be running Cisco IOS Release 12.3(11)JX1 or later releases.

The following example shows how to configure the controller IP address 10.23.90.81 into the CAPWAP access point:

```
ap_console >capwap ap controller ip address 10.23.90.81
```

capwap ap dot1x

To configure the dot1x username and password into the CAPWAP access point from the access point's console port, use the **capwap ap dot1x** command.

capwap ap dot1x username *user_name* **password** *password*

Syntax Description

user_name	Dot1x username.
password	Dot1x password.

Command Default None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

This command must be entered from an access point's console port.

Note The access point must be running Cisco Access Point IOS Release 12.3(11)JX1 or later releases.

This example shows how to configure the dot1x username ABC and password pass01:

```
ap_console >capwap ap dot1x username ABC password pass01
```

capwap ap hostname

To configure the access point host name from the access point's console port, use the **capwap ap hostname** command.

capwap ap hostname *host_name*

Syntax Description

host_name	Hostname of the access point.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

This command must be entered from an access point's console port.

Note The access point must be running Cisco IOS Release 12.3(11)JX1 or later releases. This command is available only for the Cisco Lightweight AP IOS Software recovery image (rcvk9w8) without any private-config. You can remove the private-config by using the **clear capwap private-config** command.

This example shows how to configure the hostname controller into the CAPWAP access point:

```
ap_console >capwap ap hostname controller
```

capwap ap controller ip address

To configure the controller IP address into the CAPWAP access point from the access point's console port, use the **capwap ap controller ip address** command.

capwap ap controller ip address *A.B.C.D*

Syntax Description		
	A.B.C.D	IP address of the controller.

Command Default None

Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines This command must be entered from an access point's console port. This command is applicable for IPv4 addresses only.

Note The access point must be running Cisco IOS Release 12.3(11)JX1 or later releases.

The following example shows how to configure the controller IP address 10.23.90.81 into the CAPWAP access point:

```
ap_console >capwap ap controller ip address 10.23.90.81
```

capwap ap ip default-gateway

To configure the default gateway from the access point's console port, use the **capwap ap ip default-gateway** command.

capwap ap ip default-gateway *A.B.C.D*

Syntax Description		
	A.B.C.D	Default gateway address of the capwap access point.

Command Default None

Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines This command must be entered from an access point's console port. This command supports only IPv4 address format.

Note The access point must be running Cisco Access Point IOS Release 12.3(11)JX1 or later releases.

This example shows how to configure the CAPWAP access point with the default gateway address 10.0.0.1:

```
ap_console >capwap ap ip default-gateway 10.0.0.1
```

capwap ap log-server

To configure the system log server to log all the CAPWAP errors, use the **capwap ap log-server** command.

capwap ap log-server *A.B.C.D*

Syntax Description

A.B.C.D	IP address of the syslog server.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

This command must be entered from an access point's console port. This command supports only IPv4 address format.

Note The access point must be running Cisco Access Point IOS Release 12.3(11)JX1 or later releases.

This example shows how to configure the syslog server with the IP address 10.0.0.1:

```
ap_console >capwap ap log-server 10.0.0.1
```

capwap ap ipv6 primary-base

To configure the primary controller name and IPv6 address into the CAPWAP access point from the Cisco Wave 1 access point's console port, use the **capwap ap ipv6 primary-base** command.

capwap ap ipv6 primary-base *WORD ipv6_addr*

Syntax Description

WORD	Name of the primary controller.
ipv6_addr	IPv6 address of the primary controller.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.0	This command supports IPv6 address format.

Usage Guidelines This command must be entered from the Cisco Wave 1 access point's console port in config mode.

This example shows how to configure the primary controller name WLC1 and primary controller IPv6 address 2001:DB8::1 into the CAPWAP access point:

```
ap_console >capwap ap ipv6 primary-base WLC1 2001:DB8::1
```

capwap ap primed-timer

To configure the primed timer into the CAPWAP access point, use the **capwap ap primed-timer** command.

capwap ap primed-timer {**enable** | **disable**}

Syntax Description

enable	Enables the primed timer settings
disable	Disables the primed timer settings.

Command Default None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines This command must be entered from an access point's console port.

Note The access point must be running Cisco Access Point IOS Release 12.3(11)JX1 or later releases.

This example shows how to enable the primed-timer settings:

```
ap_console >capwap ap primed-timer enable
```

capwap ap secondary-base

To configure the name and IP address of the secondary controller into the CAPWAP access point from the access point's console port, use the **capwap ap secondary-base** command.

capwap ap secondary-base *controller_name controller_ip_address*

Syntax Description

controller_name	Name of the secondary controller.
controller_ip_address	IP address of the secondary controller.

Command Default None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.0	This command supports only IPv4 address format.

Usage Guidelines

This command must be entered from an access point's console port. This command supports only IPv4 address format.

Note The access point must be running Cisco Access Point IOS Release 12.3(11)JX1 or later releases.

This example shows how to configure the secondary controller name as WLC2 and secondary controller IP address 209.165.200.226 into the CAPWAP access point:

```
ap_console >capwap ap secondary-base WLC2 209.165.200.226
```

capwap ap tertiary-base

To configure the name and IP address of the tertiary controller into the CAPWAP access point from the access point's console port, use the **capwap ap tertiary-base** command.

capwap ap tertiary-base *WORDA.B.C.D*

Syntax Description

WORD	Name of the tertiary controller.
A.B.C.D	IP address of the tertiary controller.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.0	This command supports only IPv4 address format.

Usage Guidelines

This command must be entered from an access point's console port. This command supports only IPv4 address format.

Note The access point must be running Cisco IOS Release 12.3(11)JX1 or later releases.

This example shows how to configure the tertiary controller with the name WLC3 and secondary controller IP address 209.165.200.227 into the CAPWAP access point:

```
ap_console >capwap ap tertiary-base WLC3 209.165.200.227
```

lwapp ap controller ip address

To configure the controller IP address into the FlexConnect access point from the access point's console port, use the **lwapp ap controller ip address** command.

lwapp ap controller ip address *A.B.C.D*

Syntax Description

A.B.C.D	IP address of the controller.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.0	This command supports only IPv4 address format.

Usage Guidelines

This command must be entered from an access point's console port. This command is applicable for IPv4 addresses only.

Prior to changing the FlexConnect configuration on an access point using the access point's console port, the access point must be in standalone mode (not connected to a controller) and you must remove the current LWAPP private configuration by using the **clear lwapp private-config** command.

Note The access point must be running Cisco IOS Release 12.3(11)JX1 or higher releases.

The following example shows how to configure the controller IP address 10.92.109.1 into the FlexConnect access point:

```
ap_console > lwapp ap controller ip address 10.92.109.1
```

save config

To save the controller configurations, use the **save config** command.

save config

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to save the controller settings:

```
(Cisco Controller) > save config
Are you sure you want to save? (y/n) y
Configuration Saved!
```

Clearing Configurations, Log files, and Other Actions

Use the **clear** command to clear existing configurations, log files, and other functions.

clear acl counters

To clear the current counters for an Access Control List (ACL), use the **clear acl counters** command.

clear acl counters *acl_name*

Syntax Description

acl_name	ACL name.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to clear the current counters for acl1:

```
(Cisco Controller) >clear acl counters acl1
```

clear ap config

To clear (reset to the default values) a lightweight access point's configuration settings, use the **clear ap config** command.

clear ap config *ap_name*

Syntax Description

ap_name	Access point name.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

Entering this command does not clear the static IP address of the access point.

The following example shows how to clear the access point's configuration settings for the access point named ap1240_322115:

```
(Cisco Controller) >clear ap config ap1240_322115
Clear ap-config will clear ap config and reboot the AP. Are you sure you want continue?
(y/n)
```

clear ap eventlog

To delete the existing event log and create an empty event log file for a specific access point or for all access points joined to the controller, use the **clear ap eventlog** command.

clear ap eventlog {**specific** *ap_name* | **all**}

Syntax Description

specific	Specifies a specific access point log file.
ap_name	Name of the access point for which the event log file is emptied.
all	Deletes the event log for all access points joined to the controller.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to delete the event log for all access points:

```
(Cisco Controller) >clear ap eventlog all
This will clear event log contents for all APs. Do you want continue? (y/n) :y
All AP event log contents have been successfully cleared.
```

clear ap join stats

To clear the join statistics for all access points or for a specific access point, use the **clear ap join stats** command.

clear ap join stats {**all** | *ap_mac*}

Syntax Description

all	Specifies all access points.
ap_mac	Access point MAC address.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to clear the join statistics of all the access points:

```
(Cisco Controller) >clear ap join stats all
```

clear ap tsm

To clear the Traffic Stream Metrics (TSM) statistics of clients associated to an access point, use the **clear ap tsm** command.

clear ap tsm {**802.11a** | **802.11b**} *cisco_ap* **all**

Syntax Description

802.11a	Clears 802.11a TSM statistics of clients associated to an access point.
802.11b	Clears 802.11b TSM statistics of clients associated to an access point.
cisco_ap	Cisco lightweight access point.
all	Clears TSM statistics of clients associated to the access point.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to clear 802.11a TSM statistics for all clients of an access point:

```
(Cisco Controller) >clear ap tsm 802.11a AP3600_1 all
```

clear config

To reset configuration data to factory defaults, use the **clear config** command.

clear config

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to reset the configuration data to factory defaults:

```
(Cisco Controller) >clear config
Are you sure you want to clear the configuration? (y/n)
n
Configuration not cleared!
```

Related Commands

clear transfer

clear download datatype

clear download filename

clear download mode

clear download serverip

clear download start

clear upload datatype

clear upload filename

clear upload mode

clear upload path

clear upload serverip

clear upload start

clear stats port

clear ext-webauth-url

To clear the external web authentication URL, use the **clear ext-webauth-url** command.

clear ext-webauth-url

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to clear the external web authentication URL:

```
(Cisco Controller) >clear ext-webauth-url
URL cleared.
```

Related Commands

clear transfer

clear download datatype

clear download filename

clear download mode

clear download serverip

clear download start

clear upload datatype

clear upload filename

clear upload mode

clear upload path

clear upload serverip

clear upload start

clear stats port

clear license agent

To clear the license agent's counter or session statistics, use the **clear license agent** command.

clear license agent {**counters** | **sessions**}

Syntax Description

counters	Clears the counter statistics.
sessions	Clears the session statistics.

Command Default None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to clear the license agent's counter settings:

```
(Cisco Controller) > clear license agent counters
```

Related Commands

config license agent

show license agent

license install

clear location rfid

To clear a specific Radio Frequency Identification (RFID) tag or all of the RFID tags in the entire database, use the **clear location rfid** command.

clear location rfid {*mac_address* | **all**}

Syntax Description

mac_address	MAC address of a specific RFID tag.
all	Specifies all the RFID tags in the database.

Command Default None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to clear all the RFID tags in the database:

```
(Cisco Controller) >clear location rfid all
```

Related Commands

clear location statistics rfid

config location

show location

show location statistics rfid

clear location statistics rfid

To clear Radio Frequency Identification (RFID) statistics, use the **clear location statistics rfid** command.

clear location statistics rfid

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to clear RFID statistics:

```
(Cisco Controller) >clear location statistics rfid
```

Related Commands

config location

show location

show location statistics rfid

clear locp statistics

To clear the Location Protocol (LOCP) statistics, use the **clear locp statistics** command.

clear locp statistics

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to clear the statistics related to LOCP:

```
(Cisco Controller) >clear locp statistics
```

Related Commands

clear nmsp statistics

config nmsp notify-interval measurement

show nmsp notify-interval summary

show nmsp statistics

show nmsp status

clear login-banner

To remove the login banner file from the controller, use the **clear login-banner** command.

clear login-banner

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to clear the login banner file:

```
(Cisco Controller) >clear login-banner
```

Related Commands

transfer download datatype

clear lwapp private-config

To clear (reset to default values) an access point's current Lightweight Access Point Protocol (LWAPP) private configuration, which contains static IP addressing and controller IP address configurations, use the **clear lwapp private-config** command.

clear lwapp private-config

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

Enter the command on the access point console port.

Prior to changing the FlexConnect configuration on an access point using the access point's console port, the access point must be in standalone mode (not connected to a controller) and you must remove the current LWAPP private configuration by using the **clear lwapp private-config** command.

Note The access point must be running Cisco Access Point IOS Release 12.3(11)JX1 or later releases.

The following example shows how to clear an access point's current LWAPP private configuration:

```
ap_console >clear lwapp private-config
removing the reap config file flash:/lwapp_reap.cfg
```

clear nmsp statistics

To clear the Network Mobility Services Protocol (NMSP) statistics, use the **clear nmsp statistics** command.

clear nmsp statistics

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to delete the NMSP statistics log file:

```
(Cisco Controller) >clear nmsp statistics
```

Related Commands

clear locp statistics

config nmsp notify-interval measurement

show nmsp notify-interval summary

show nmsp status

clear radius acct statistics

To clear the RADIUS accounting statistics on the controller, use the **clear radius acc statistics** command.

clear radius acct statistics [**index** | **all**]

Syntax Description

index	(Optional) Specifies the index of the RADIUS accounting server.

all	(Optional) Specifies all RADIUS accounting servers.

Command Default None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to clear the RADIUS accounting statistics:

```
(Cisco Controller) >clear radius acc statistics
```

Related Commands **show radius acct statistics**

clear tacacs auth statistics

To clear the RADIUS authentication server statistics in the controller, use the **clear tacacs auth statistics** command.

clear tacacs auth statistics [**index** | **all**]

Syntax Description

index	(Optional) Specifies the index of the RADIUS authentication server.
all	(Optional) Specifies all RADIUS authentication servers.

Command Default None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to clear the RADIUS authentication server statistics:

```
(Cisco Controller) >clear tacacs auth statistics
```

Related Commands **show tacacs auth statistics**

show tacacs summary

config tacacs auth

clear redirect-url

To clear the custom web authentication redirect URL on the Cisco Wireless LAN Controller, use the **clear redirect-url** command.

clear redirect-url

Syntax Description This command has no arguments or keywords.

Command Default None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to clear the custom web authentication redirect URL:

```
(Cisco Controller) >clear redirect-url
URL cleared.
```

Related Commands

clear transfer

clear download datatype

clear download filename

clear download mode

clear download path

clear download start

clear upload datatype

clear upload filename

clear upload mode

clear upload path

clear upload serverip

clear upload start

clear stats ap wlan

To clear the WLAN statistics, use the **clear stats ap wlan** command.

clear stats ap wlan *cisco_ap*

Syntax Description

cisco_ap	Selected configuration elements.

Command Default None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to clear the WLAN configuration elements of the access point cisco_ap:

```
(Cisco Controller) >clear stats ap wlan cisco_ap
WLAN statistics cleared.
```

clear stats local-auth

To clear the local Extensible Authentication Protocol (EAP) statistics, use the **clear stats local-auth** command.

clear stats local-auth

Syntax Description This command has no arguments or keywords.

Command Default None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to clear the local EAP statistics:

```
(Cisco Controller) >clear stats local-auth
Local EAP Authentication Stats Cleared.
```

Related Commands

config local-auth active-timeout

config local-auth eap-profile

config local-auth method fast

config local-auth user-credentials

debug aaa local-auth

show local-auth certificates

show local-auth config

show local-auth statistics

clear stats mobility

To clear mobility manager statistics, use the **clear stats mobility** command.

clear stats mobility

Syntax Description This command has no arguments or keywords.

Command Default None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to clear mobility manager statistics:

```
(Cisco Controller) >clear stats mobility

   Mobility stats cleared.
```

clear stats port

To clear statistics counters for a specific port, use the **clear stats port** command.

clear stats port *port*

Syntax Description

port	Physical interface port number.

Command Default None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to clear the statistics counters for port 9:

```
(Cisco Controller) >clear stats port 9
```

Related Commands

clear transfer

clear download datatype

clear download datatype

clear download filename

clear download mode

clear download serverip

clear download start

clear upload datatype

clear upload filename

clear upload mode

clear upload path

clear upload serverip

clear upload start

clear stats port

clear stats radius

To clear the statistics for one or more RADIUS servers, use the **clear stats radius** command.

clear stats radius {**auth** | **acct**} {**index** | **all**}

Syntax Description

auth	Clears statistics regarding authentication.
acct	Clears statistics regarding accounting.
index	Specifies the index number of the RADIUS server to be cleared.
all	Clears statistics for all RADIUS servers.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to clear the statistics for all RADIUS authentication servers:

```
(Cisco Controller) >clear stats radius auth all
```

Related Commands

clear transfer

clear download datatype

clear download filename

clear download mode

clear download serverip

clear download start

clear upload datatype

clear upload filename

clear upload mode

clear upload path

clear upload serverip

clear upload start

clear stats port

clear stats tacacs

To clear the TACACS+ server statistics on the controller, use the **clear stats tacacs** command.

clear stats tacacs [**auth** | **athr** | **acct**] [**index** | **all**]

Syntax Description

auth	(Optional) Clears the TACACS+ authentication server statistics.
athr	(Optional) Clears the TACACS+ authorization server statistics.
acct	(Optional) Clears the TACACS+ accounting server statistics.
index	(Optional) Specifies index of the TACACS+ server.
all	(Optional) Specifies all TACACS+ servers.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to clear the TACACS+ accounting server statistics for index 1:

```
(Cisco Controller) >clear stats tacacs acct 1
```

Related Commands

show tacacs summary

clear stats switch

To clear all switch statistics counters on a Cisco wireless LAN controller, use the **clear stats switch** command.

clear stats switch

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to clear all switch statistics counters:

```
(Cisco Controller) >clear stats switch
```

Related Commands

clear transfer
clear download datatype
clear download filename
clear download mode
clear download path
clear download start
clear upload datatype
clear upload filename
clear upload mode
clear upload path
clear upload serverip
clear upload start

clear transfer

To clear the transfer information, use the **clear transfer** command.

clear transfer

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to clear the transfer information:

```
(Cisco Controller) >clear transfer
Are you sure you want to clear the transfer information? (y/n) y
Transfer Information Cleared.
```

Related Commands

transfer upload datatype
transfer upload pac
transfer upload password
transfer upload port
transfer upload path
transfer upload username
transfer upload datatype
transfer upload serverip

transfer upload start

clear traplog

To clear the trap log, use the **clear traplog** command.

clear traplog

Syntax Description This command has no arguments or keywords.

Command Default None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to clear the trap log:

```
(Cisco Controller) >clear traplog
Are you sure you want to clear the trap log? (y/n) y
Trap Log Cleared.
```

Related Commands

clear transfer

clear download datatype

clear download filename

clear download mode

clear download path

clear download serverip

clear download start

clear upload filename

clear upload mode

clear upload path

clear upload serverip

clear upload start

clear webimage

To clear the custom web authentication image, use the **clear webimage** command.

clear webimage

Syntax Description This command has no arguments or keywords.

Command Default None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to clear the custom web authentication image:

```
(Cisco Controller) >clear webimage
```

Related Commands

clear transfer

clear download datatype

clear download filename

clear download mode

clear download path

clear download serverip

clear download start

clear upload filename

clear upload mode

clear upload path

clear upload serverip

clear upload start

clear webtitle

To clear the custom web authentication title, use the **clear webtitle** command.

clear webtitle

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to clear the custom web authentication title:

```
(Cisco Controller) >clear webtitle
Title cleared.
```

Related Commands

clear transfer

clear download datatype

clear download filename

clear download mode

clear download path

clear download serverip

clear download start

clear upload filename

clear upload mode

clear upload path

clear upload serverip

clear upload start

Resetting the System Reboot Time

Use the **reset** command to schedule a reboot of the controller and access points.

reset system at

To reset the system at a specified time, use the **reset system at** command.

reset system at YYYY-MM-DD HH : MM : SS image {**no-swap** | **swap**} **reset-aps** [**save-config**]

Syntax Description

YYYY-MM-DD	Specifies the date.
HH: MM: SS	Specifies the time in a 24-hour format.
image	Configures the image to be rebooted.
swap	Changes the active boot image; boots the non-active image and sets the default flag on it on the next reboot.
no-swap	Boots from the active image.
reset-aps	Resets all access points during the system reset.
save-config	(Optional) Saves the configuration before the system reset.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to reset the system at 2010-03-29 and 12:01:01 time:

```
(Cisco Controller) > reset system at 2010-03-29 12:01:01 image swap reset-aps save-config
```

reset system in

To specify the amount of time delay before the devices reboot, use the **reset system in** command.

reset system in HH : MM : SS image {**swap** | **no-swap**} **reset-aps save-config**

Syntax Description

HH :MM :SS	Specifies a delay in duration.
image	Configures the image to be rebooted.
swap	Changes the active boot image; boots the non-active image and sets the default flag on it on the next reboot.

reset-aps	Resets all access points during the system reset.
save-config	Saves the configuration before the system reset.

Command Default None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to reset the system after a delay of 00:01:01:

```
(Cisco Controller) > reset system in 00:01:01 image swap reset-aps save-config
```

reset system cancel

To cancel a scheduled reset, use the **reset system cancel** command.

reset system cancel

Syntax Description This command has no arguments or keywords.

Command Default None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to cancel a scheduled reset:

```
(Cisco Controller) > reset system cancel
```

reset system notify-time

To configure the trap generation prior to scheduled resets, use the **reset system notify-time** command.

reset system notify-time *minutes*

Syntax Description

minutes	Number of minutes before each scheduled reset at which to generate a trap.

Command Default The default time period to configure the trap generation prior to scheduled resets is 10 minutes.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the trap generation to 10 minutes before the scheduled resets:

```
(Cisco Controller) > reset system notify-time 55
```

reset peer-system

To reset the peer controller, use the **reset peer-system** command.

reset peer-system

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to reset the peer controller:

```
(Cisco Controller) >> reset peer-system
```

Uploading and Downloading Files and Configurations

Use the **transfer** command to transfer files to or from the Cisco Wireless LAN controller.

transfer download certpasswor

To set the password for the .PEM file so that the operating system can decrypt the web administration SSL key and certificate, use the **transfer download certpassword** command.

transfer download certpassword *private_key_password*

Syntax Description

private_key_password	Certificate's private key password.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to transfer a file to the switch with the certificate's private key password certpassword:

```
(Cisco Controller) > transfer download certpassword
Clearing password
```

transfer download datatype

To set the download file type, use the **transfer download datatype** command.

transfer download datatype {**avc-protocol-pack** | **code** | **config** | **eapdevcert** | **eapcacert** | **icon** | **image** | **ipseccacert** | **ipsecdevcert** | **login-banner** | **radius-avplist** | **signature** | **webadmincert** | **webauthbundle** | **webauthcert**}

Syntax Description

avc-protocol-pack	Downloads an AVC protocol pack to the system.
code	Downloads an executable image to the system.
config	Downloads the configuration file.
eapcacert	Downloads an EAP ca certificate to the system.
eapdevcert	Downloads an EAP dev certificate to the system.
icon	Downloads an executable image to the system.
image	Downloads a web page login to the system.

ipseccacert	Downloads an IPSec Certificate Authority (CA) certificate to the system.
ipsecdevcert	Downloads an IPSec dev certificate to the system.
login-banner	Downloads the controller login banner. Only text file is supported with a maximum of 1500 bytes.
radius-avplist	Downloads the RADIUS AVPs in the XML file format from the FTP server.
signature	Downloads a signature file to the system.
webadmincert	Downloads a certificate for web administration to the system.
webauthbundle	Downloads a custom webauth bundle to the system.
webauthcert	Downloads a web certificate for the web portal to the system.

Command Default None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.0	The **ipseccacert**, **ipsecdevcert**, and **radius-avplist** options were introduced.

The following example shows how to download an executable image to the system:

```
(Cisco Controller) > transfer download datatype code
```

transfer download filename

To download a specific file, use the **transfer download filename** command.

transfer download filename *filename*

Syntax Description

filename	Filename that contains up to 512 alphanumeric characters.

Command Default None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines You cannot use special characters such as \ : * ? " < > | for the filename.

The following example shows how to transfer a file named build603:

```
(Cisco Controller) > transfer download filename build603
```

transfer download mode

To set the transfer mode, use the **transfer download mode** command.

transfer upload mode {**ftp** | **tftp** | **sftp**}

Syntax Description

ftp	Sets the transfer mode to FTP.
tftp	Sets the transfer mode to TFTP.
sftp	Sets the transfer mode to SFTP.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to transfer a file using the TFTP mode:

```
(Cisco Controller) > transfer download mode tftp
```

transfer download password

To set the password for an FTP transfer, use the **transfer download password** command.

transfer download password *password*

Syntax Description

password	Password.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to set the password for FTP transfer to pass01:

```
(Cisco Controller) > transfer download password pass01
```

transfer download path

To set a specific FTP or TFTP path, use the **transfer download path** command.

transfer download path *path*

Syntax Description

path	Directory path.

Note Path names on a TFTP or FTP server are relative to the server's default or root directory. For example, in the case of the Solarwinds TFTP server, the path is "/".

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

You cannot use special characters such as \ : * ? " < > | for the file path.

The following example shows how to transfer a file to the path c:\install\version2:

```
(Cisco Controller) > transfer download path c:\install\version2
```

transfer download port

To specify the FTP port, use the **transfer download port** command.

transfer download port *port*

Syntax Description

port	FTP port.

Command Default

The default FTP *port* is 21.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to specify FTP port number 23:

```
(Cisco Controller) > transfer download port 23
```

transfer download serverip

To configure the IPv4 or IPv6 address of the TFTP server from which to download information, use the **transfer download serverip** command.

transfer download serverip *IP addr*

Syntax Description

IP addr	TFTP server IPv4 or IPv6 address.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.0	This command supports both IPv4 and IPv6 address formats.

The following example shows how to configure the IPv4 address of the TFTP server:

```
(Cisco Controller) > transfer download serverip 175.34.56.78
```

The following example shows how to configure the IPv6 address of the TFTP server:

```
(Cisco Controller) > transfer download serverip 2001:10:1:1::1
```

transfer download start

To initiate a download, use the **transfer download start** command.

transfer download start

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to initiate a download:

```
(Cisco Controller) > transfer download start
Mode..................................... TFTP
Data Type................................ Site Cert
TFTP Server IP........................... 172.16.16.78
TFTP Path................................ directory path
TFTP Filename............................ webadmincert_name
This may take some time.
Are you sure you want to start? (y/n) Y
TFTP Webadmin cert transfer starting.
```

```
Certificate installed.
Please restart the switch (reset system) to use the new certificate.
```

transfer download tftpMaxRetries

To specify the number of allowed TFTP packet retries, use the **transfer download tftpMaxRetries** command.

transfer download tftpMaxRetries *retries*

Syntax Description

retries	Number of allowed TFTP packet retries between 1 and 254 seconds.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to set the number of allowed TFTP packet retries to 55:

```
(Cisco Controller) > transfer download tftpMaxRetries 55
```

transfer download tftpPktTimeout

To specify the TFTP packet timeout, use the **transfer download tftpPktTimeout** command.

transfer download tftpPktTimeout *timeout*

Syntax Description

timeout	Timeout in seconds between 1 and 254.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to transfer a file with the TFTP packet timeout of 55 seconds:

```
(Cisco Controller) > transfer download tftpPktTimeout 55
```

transfer download username

To specify the FTP username, use the **transfer download username** command.

transfer download username *username*

Syntax Description		
	username	Username.

Command Default None

Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to set the FTP username to ftp_username:

```
(Cisco Controller) > transfer download username ftp_username
```

transfer encrypt

To configure encryption for configuration file transfers, use the **transfer encrypt** command.

transfer encrypt {**enable** | **disable** | **set-key** *key*}

Syntax Description		
	enable	Enables the encryption settings.
	disable	Disables the encryption settings.
	set-key	Specifies the encryption key for configuration file transfers.
	key	Encryption key for config file transfers.

Command Default None

Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the encryption settings:

```
(Cisco Controller) > transfer encrypt enable
```

transfer upload filename

To upload a specific file, use the **transfer upload filename** command.

transfer upload filename *filename*

Syntax Description		
	filename	Filename that contains up to 16 alphanumeric characters.

Command Default None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines You cannot use special characters such as \ : * ? " < > | for the filename.

The following example shows how to upload a file build603:

```
(Cisco Controller) > transfer upload filename build603
```

transfer upload password

To configure the password for FTP transfer, use the **transfer upload password** command.

Syntax Description

password	Password needed to access the FTP server.

transfer upload password *password*

Command Default None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the password for the FTP transfer to pass01:

```
(Cisco Controller) > transfer upload password pass01
```

transfer upload peer-start

To upload a file to the peer controller, use the **transfer upload peer-start** command.

transfer upload peer-start

Syntax Description This command has no arguments or keywords.

Command Default None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to start uploading a file to the peer controller:

```
(Cisco Controller) >transfer upload peer-start
Mode..................................... FTP
FTP Server IP.................................. 209.165.201.1
FTP Server Port................................ 21
FTP Path....................................... /builds/nimm/
FTP Filename................................... AS_5500_7_4_1_20.aes
FTP Username................................... wnbu
FTP Password................................... *********
Data Type...................................... Error Log

Are you sure you want to start upload from standby? (y/N) n

Transfer Canceled
```

transfer upload serverip

To configure the IPv4 or IPv6 address of the TFTP server to upload files to, use the **transfer upload serverip** command.

transfer upload serverip *IP addr*

Syntax Description

IP addr	TFTP Server IPv4 or IPv6 address.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.0	This command supports both IPv4 and IPv6 address formats.

The following example shows how to set the IPv4 address of the TFTP server to 175.31.56.78:

```
(Cisco Controller) > transfer upload serverip 175.31.56.78
```

The following example shows how to set the IPv6 address of the TFTP server to 175.31.56.78:

```
(Cisco Controller) > transfer upload serverip 2001:10:1:1::1
```

transfer upload datatype

To set the controller to upload specified log and crash files, use the **transfer upload datatype** command.

transfer upload datatype { **ap-crash-data** | **config** | **coredump** | **crashfile** | **debug-file** | **eapcacert** | **eapdevcert** | **errorlog** | **invalid-config** | **ipseccacert** | **ipsecdevcert** | **pac** | **packet-capture** | **panic-crash-file** | **radio-core-dump** | **radius-avplist** | **rrm-log** | **run-config** | **signature** | **systemtrace** | **traplog** | **watchdog-crash-file webadmincert** | **webauthbundle** | **webauthcert** | **webauth-ca-cert** | **yang-bundle** }

Syntax Description

ap-crash-data	Uploads the AP crash files.
config	Uploads the system configuration file.
coredump	Uploads the core-dump file.
crashfile	Uploads the system crash file.
debug-file	Uploads the system's debug log file.
eapcacert	Uploads an EAP CA certificate.
eapdevcert	Uploads an EAP Dev certificate.
errorlog	Uploads the system error log file.
invalid-config	Uploads the system invalid-config file.
ipseccacert	Uploads CA certificate file.
ipsecdevcert	Uploads device certificate file.
pac	Uploads a Protected Access Credential (PAC).
packet-capture	Uploads a packet capture file.
panic-crash-file	Uploads the kernel panic information file.
radio-core-dump	Uploads the system error log.
radius-avplist	Uploads the XML file from the controller to the RADIUS server.
rrm-log	Uploads the system's trap log.
run-config	Upload the controller's running configuration
signature	Uploads the system signature file.
systemtrace	Uploads the system trace file.
traplog	Uploads the system trap log.
watchdog-crash-file	Uploads a console dump file resulting from a software-watchdog-initiated controller reboot following a crash.
webadmincert	Uploads Web Admin certificate.
webauthbundle	Uploads a Web Auth bundle.
webauthcert	Upload a web certificate
webauth-ca-cert	Upload a Webhook CA certificate
yang-bundle	Upload the YANG files

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.0	The **ipseccacert**, **ipsecdevcert**, and **radius-avplist** options were introduced.
8.8	The **webauth-ca-cert** and **yang-bundle** options were introduced.

The following example shows how to upload the system error log file:

```
(Cisco Controller) > transfer upload datatype errorlog
```

transfer upload username

To specify the FTP username, use the **transfer upload username** command.

transfer upload username

Syntax Description

username	Username required to access the FTP server. The username can contain up to 31 characters.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to set the FTP username to ftp_username:

```
(Cisco Controller) > transfer upload username ftp_username
```

transfer upload mode

To configure the transfer mode, use the **transfer upload mode** command.

transfer upload mode {**ftp** | **tftp** | **sftp**}

Syntax Description

ftp	Sets the transfer mode to FTP.
tftp	Sets the transfer mode to TFTP.
sftp	Sets the transfer mode to SFTP.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to set the transfer mode to TFTP:

```
(Cisco Controller) > transfer upload mode tftp
```

transfer upload pac

To load a Protected Access Credential (PAC) to support the local authentication feature and allow a client to import the PAC, use the **transfer upload pac** command.

transfer upload pac *username validity password*

Syntax Description

username	User identity of the PAC.
validity	Validity period (days) of the PAC.
password	Password to protect the PAC.

Command Default None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines The client upload process uses a TFTP or FTP server.

The following example shows how to upload a PAC with the username user1, validity period 53, and password pass01:

```
(Cisco Controller) > transfer upload pac user1 53 pass01
```

transfer upload path

To set a specific upload path, use the **transfer upload path** command.

transfer upload path *path*

Syntax Description

path	Server path to file.

Command Default None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

You cannot use special characters such as \ : * ? " < > | for the file path.

The following example shows how to set the upload path to c:\install\version2:

```
(Cisco Controller) > transfer upload path c:\install\version2
```

transfer upload start

To initiate an upload, use the **transfer upload start** command.

transfer upload start

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to initiate an upload of a file:

```
(Cisco Controller) > transfer upload start
Mode..................................... TFTP
TFTP Server IP........................... 172.16.16.78
TFTP Path................................ c:\find\off/
TFTP Filename............................ wps_2_0_75_0.aes
Data Type................................ Code
Are you sure you want to start? (y/n) n
Transfer Cancelled
```

Installing and Modifying Licenses

Use the **license** commands to install, remove, modify, or rehost licenses.

Note Some license commands are available only on the Cisco 5500 Series Controller. Right to Use (RTU) licensing is not supported on Cisco 5500 Series Controllers.

Note For detailed information on installing and rehosting licenses on the Cisco 5500 Series Controller, see the "Installing and Configuring Licenses" section in Chapter 4 of the *Cisco Wireless LAN Controller Configuration Guide*.

license clear

To remove a license from the Cisco 5500 Series Controller, use the **license clear** command.

license clear *license_name*

Syntax Description

license_name	Name of the license.

Command Default None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines You can 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 controller.

The following example shows how to remove the license settings of the license named wplus-ap-count:

```
(Cisco Controller) > license clear wplus-ap-count
```

license comment

To add comments to a license or delete comments from a license on the Cisco 5500 Series Controller, use the **license comment** command.

license comment {**add** | **delete**} *license_name comment_string*

Syntax Description

add	Adds a comment.
delete	Deletes a comment.

license_name	Name of the license.
comment_string	License comment.

Command Default None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to add a comment “wplus ap count license” to the license name wplus-ap-count:

```
(Cisco Controller) > license comment add wplus-ap-count Comment for wplus ap count license
```

license install

To install a license on the Cisco 5500 Series Controller, use the **license install** command.

license install *url*

Syntax Description

url	URL of the TFTP server (tftp://server_ip/path/filename).

Command Default None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

We recommend that the access point count be the same for the base-ap-count and wplus-ap-count licenses installed on your controller. If your controller has a base-ap-count license of 100 and you install a wplus-ap-count license of 12, the controller supports up to 100 access points when the base license is in use but only a maximum of 12 access points when the wplus license is in use.

You cannot install a wplus license that has an access point count greater than the controller's base license. For example, you cannot apply a wplus-ap-count 100 license to a controller with an existing base-ap-count 12 license. If you attempt to register for such a license, an error message appears indicating that the license registration has failed. Before upgrading to a wplus-ap-count 100 license, you would first have to upgrade the controller to a base-ap-count 100 or 250 license.

The following example shows how to install a license on the controller from the URL tftp://10.10.10.10/path/license.lic:

```
(Cisco Controller) > license install tftp://10.10.10.10/path/license.lic
```

license modify priority

To raise or lower the priority of the base-ap-count or wplus-ap-count evaluation license on a Cisco 5500 Series Controller, use the **license modify priority** command.

license modify priority *license_name* {**high** | **low**}

Syntax Description

license_name	Ap-count evaluation license.
high	Modifies the priority of an ap-count evaluation license.
low	Modifies the priority of an ap-count evaluation license.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

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 controller 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, which forces the controller to use the permanent license.

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.

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.

Note To prevent disruptions in operation, the controller does not switch licenses when an evaluation license expires. You must reboot the controller in order to return to a permanent license. Following a reboot, the controller 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 controller uses a permanent license at another level or an unexpired evaluation license.

The following example shows how to set the priority of the wplus-ap-count to high:

```
(Cisco Controller) > license modify priority wplus-ap-count high
```

license revoke

To rehost a license on a Cisco 5500 Series Wireless Controller, use the **license revoke** command.

license revoke {*permission_ticket_url* | **rehost** *rehost_ticket_url*}

Syntax Description

permission_ticket_url	URL of the TFTP server (tftp://server_ip/path/filename) where you saved the permission ticket.
rehost	Specifies the rehost license settings.
rehost_ticket_url	URL of the TFTP server (tftp://server_ip/path/filename) where you saved the rehost ticket.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

Before you revoke a license, save the device credentials by using the **license save credential** *url* command.

You can rehost all permanent licenses except the permanent base image license. Evaluation licenses and the permanent base image license cannot be rehosted.

In order to rehost a license, you must generate credential information from the controller and use it to obtain a permission ticket to revoke the license from the Cisco licensing site, https://tools.cisco.com/SWIFT/LicensingUI/Quickstart. Next, you must obtain a rehost ticket and use it to obtain a license installation file for the controller on which you want to install the license.

For detailed information on rehosting licenses, see the "Installing and Configuring Licenses" section in the *Cisco Wireless LAN Controller Configuration Guide*.

The following example shows how to revoke the license settings from the saved permission ticket URL tftp://10.10.10.10/path/permit_ticket.lic:

```
(Cisco Controller) > license revoke tftp://10.10.10.10/path/permit_ticket.lic
```

The following example shows how to revoke the license settings from the saved rehost ticket URL tftp://10.10.10.10/path/rehost_ticket.lic:

```
(Cisco Controller) > license revoke rehost tftp://10.10.10.10/path/rehost_ticket.lic
```

license save

To save a backup copy of all installed licenses or license credentials on the Cisco 5500 Series Controller, use the **license save** command.

license save *credential url*

Syntax Description

credential	Device credential information.
url	URL of the TFTP server (tftp://server_ip/path/filename).

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

Save the device credentials before you revoke the license by using the **license revoke** command.

The following example shows how to save a backup copy of all installed licenses or license credentials on tftp://10.10.10.10/path/cred.lic:

```
(Cisco Controller) > license save credential tftp://10.10.10.10/path/cred.lic
```

Right to Use Licensing Commands

Use the **license** commands to configure Right to Use (RTU) licensing on Cisco Flex 7500 Series and 8500 Series controllers. This feature allows you to enable an AP license count on the controller without using any external tools after accepting an End User License Agreement (EULA).

license activate ap-count eval

To activate an evaluation access point license on the Cisco Flex 7500 Series and Cisco 8500 Series Wireless LAN Controllers, use the **license activate ap-count eval** command.

license activate ap-count eval

Syntax Description

This command has no arguments or keywords.

Command Default

By default, in release 7.3 Cisco Flex 7500 Series Controllers and Cisco 8500 Series Wireless LAN Controllers support 6000 APs.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

When you activate this license, the controller prompts you to accept or reject the End User License Agreement (EULA) for the given license. If you activate a license that supports a smaller number of APs than the current number of APs connected to the controller, the activation command fails.

The following example shows how to activate an evaluation AP-count license on a Cisco Flex 7500 Series controller:

```
(Cisco Controller) > license activate ap-count eval
```

license activate feature

To activate a feature license on Cisco Flex 7500 Series and Cisco 8500 Series Wireless LAN Controllers, use the **license activate feature** command.

license activate feature *license_name*

Syntax Description

license_name	Name of the feature license. The license name can be up to 50 case-sensitive characters.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to activate a data DTLS feature license on a Cisco Flex 7500 Series controller:

```
(Cisco Controller) > license activate feature data-DTLS
```

license add ap-count

To configure the number of access points (APs) that an AP license can support on Cisco Flex 7500 and 8500 Series Wireless LAN controllers, use the **license add ap-count** command.

license add ap-count *count*

Syntax Description

count	Number of APs that the AP license supports. The range is from 1 to the maximum number of APs that the controller can support. The count must be a multiple of 5.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

Right to Use (RTU) licensing allows you to enable a desired AP license count on the controller after accepting the End User License Agreement (EULA). You can now easily add AP counts on a controller without using external tools. RTU licensing is available only on Cisco Flex 7500 and 8500 series Wireless LAN controllers.

You can use this command to increase the count of an existing AP license. When you activate a license that supports a smaller number of APs than the current number of APs connected to the controller, the activation command fails.

The following example shows how to configure the count of an AP license on a Cisco Flex 7500 Series controller:

```
(Cisco Controller) > license add ap-count 5000
```

license add feature

To add a license for a feature on the Cisco 5520 Wireless Controller, Cisco Flex 7510 Wireless Controller, Cisco 8510 Wireless Controller, Cisco 8540 Wireless Controller, and Cisco Virtual Controller, use the **license add feature** command.

license add feature *license_name*

Syntax Description

license_name	Name of the feature license. The license name can be up to 50 case-sensitive characters. For example, data_encryption.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6. This command is applicable to Cisco Flex 7510 Wireless Controller and Cisco 8510 Wireless Controller.
8.1	This command is applicable to Cisco 5520 Wireless Controller, Cisco Flex 7510 Wireless Controller, Cisco 8510 Wireless Controller, Cisco 8540 Wireless Controller, and Cisco vWLC.

The following example shows how to add a data_encryption feature license:

```
(Cisco Controller) > license add feature data_encryption
```

license deactivate ap-count eval

To deactivate an evaluation access point license on the Cisco Flex 7500 Series and Cisco 8500 Series Wireless LAN Controllers, use the **license deactivate ap-count eval** command.

license deactivate ap-count eval

Syntax Description This command has no arguments or keywords.

Command Default None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to deactivate an evaluation AP license on a Cisco Flex 7500 Series controller:

```
(Cisco Controller) > license deactivate ap-count eval
```

license deactivate feature

To deactivate a feature license on Cisco Flex 7500 Series and Cisco 8500 Series Wireless LAN controllers, use the **license deactivate feature** command.

license deactivate feature *license_name*

Syntax Description

license_name	Name of the feature license. The license name can be up to 50 case-sensitive characters.

Command Default None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to deactivate a data DTLS feature license on a Cisco Flex 7500 Series controller:

```
(Cisco Controller) > license deactivate feature data_DTLS
```

license delete ap-count

To delete an access point (AP) count license on the Cisco Flex 7500 Series and Cisco 8500 Series Wireless LAN Controllers, use the **license delete ap-count** command.

license delete ap-count *count*

Syntax Description

count	Number of APs that the AP license supports. The range is from 1 to the maximum number of APs that the controller can support. The count must be a multiple of 5.

Command Default None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to delete an AP count license on a Cisco Flex 7500 Series controller:

```
(Cisco Controller) > license delete ap-count 5000
```

license delete feature

To delete a license for a feature on Cisco Flex 7500 Series and Cisco 8500 Series Wireless LAN controllers, use the **license delete feature** command.

license delete feature *license_name*

Syntax Description

license_name	Name of the feature license.

Command Default None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to delete the High Availability feature license on a Cisco Flex 7500 Series controller:

```
(Cisco Controller) > license delete feature high_availability
```

Integrated Management Module Commands in Cisco Flex 7500 Series Controllers

Use the **imm** commands to manage the Integrated Management Module (IMM) in the Cisco Flex 7500 Series Controllers.

imm address

To configure the static IP address of the IMM, use the **imm address** command.

imm address *ip-addr netmask gateway*

Syntax Description

ip-addr	IP address of the IMM
netmask	Netmask of the IMM
gateway	Gateway of the IMM

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.0	This command supports only IPv4 address format.

The following example shows how to set the static IP address of an IMM:

```
(Cisco Controller) >imm address 209.165.200.225 255.255.255.224 10.1.1.1
```

imm dhcp

To configure DHCP for the IMM, use the **imm dhcp** command.

imm dhcp {**enable** | **disable** | **fallback**}

Syntax Description

enable	Enables DHCP for the IMM
disable	Disables DHCP for the IMM
fallback	Enables DHCP for the IMM, but if it fails, then uses static IP of the IMM

Command Default

DHCP for IMM is enabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable DHCP for the IMM:

```
(Cisco Controller) >imm dhcp enable
```

imm mode

To configure the IMM mode, use the **imm mode** command.

imm mode {**shared** | **dedicated**}

Syntax Description

shared	Sets IMM in shared mode
dedicated	Sets IMM in dedicated mode

Command Default

Dedicated

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to set the IMM in shared mode:

```
(Cisco Controller) >imm mode
```

imm restart

To restart the IMM, use the **imm restart** command.

imm restart

Syntax Description

restart	Saves your settings and restarts the IMM

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

imm summary

To view the IMM parameters, use the **imm summary** command.

imm summary

Syntax Description

summary	Lists the IMM parameters

Command Default None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows a typical summary of the IMM:

```
(Cisco Controller) >imm summary
User ID.....................................username1
Mode.......................................... Shared
DHCP.......................................... Enabled
IP Address.................................... 209.165.200.225
Subnet Mask................................... 255.255.255.224
Gateway....................................... 10.1.1.1
```

imm username

To configure the logon credentials for an IMM user, use the **imm username** command.

imm username *username password*

Syntax Description

username	Username for the user
password	Password for the user

Command Default None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to set the logon credentials of an IMM user:

```
(Cisco Controller) >imm username username1 password1
```

Troubleshooting Commands

Use the **debug** commands to manage system debugging.

Caution Debug commands are reserved for use only under direction of Cisco personnel. Do not use these commands without direction from Cisco-certified staff.

Note Enabling all debug commands on a system with many clients authenticating may result in some debugs being lost.

debug aaa

To configure the debugging of AAA settings, use the **debug aaa** command.

debug aaa { [**all** | **detail** | **events** | **packet** | **local-auth** | **tacacs**] [**enable** | **disable**] }

Syntax Description

all	(Optional) Configures the debugging of all AAA messages.
avp-xml	(Optional) Configures debug of AAA Avp xml events.
detail	(Optional) Configures the debugging of AAA errors.
events	(Optional) Configures the debugging of AAA events.
packet	(Optional) Configures the debugging of AAA packets.
local-auth	(Optional) Configures the debugging of the AAA local Extensible Authentication Protocol (EAP) events.
tacacs	(Optional) Configures the debugging of the AAA TACACS+ events.
enable	(Optional) Enables the debugging.
disable	(Optional) Disables the debugging.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Related Commands

debug aaa local-auth eap

show running-config

debug aaa local-auth

To configure the debugging of AAA local authentication on the controller, use the **debug aaa local-auth** command.

debug aaa local-auth { **db** | **shim** | **eap** { **framework** | **method** } { **all** | **errors** | **events** | **packets** | **sm** } } { **enable** | **disable** }

Syntax Description

db	Configures the debugging of the AAA local authentication back-end messages and events.
shim	Configures the debugging of the AAA local authentication shim layer events.
eap	Configures the debugging of the AAA local Extensible Authentication Protocol (EAP) authentication.
framework	Configures the debugging of the local EAP framework.
method	Configures the debugging of local EAP methods.
all	Configures the debugging of local EAP messages.
errors	Configures the debugging of local EAP errors.
events	Configures the debugging of local EAP events.
packets	Configures the debugging of local EAP packets.
sm	Configures the debugging of the local EAP state machine.
enable	Starts the debugging.
disable	Stops the debugging.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the debugging of the AAA local EAP authentication:

```
(Cisco Controller) > debug aaa local-auth eap method all enable
```

Related Commands

clear stats local-auth

config local-auth active-timeout

config local-auth eap-profile

config local-auth method fast

config local-auth user-credentials

show local-auth certificates

show local-auth config

show local-auth statistics

debug airewave-director

To configure the debugging of Airewave Director software, use the **debug airwave-director** command.

debug airewave-director {**all** | **channel** | **detail** | **error** | **group** | **manager** | **message** | **packet** | **power** | **profile** | **radar** | **rf-change**} {**enable** | **disable**}

Syntax Description

all	Configures the debugging of all Airewave Director logs.
channel	Configures the debugging of the Airewave Director channel assignment protocol.
detail	Configures the debugging of the Airewave Director detail logs.
error	Configures the debugging of the Airewave Director error logs.
group	Configures the debugging of the Airewave Director grouping protocol.
manager	Configures the debugging of the Airewave Director manager.
message	Configures the debugging of the Airewave Director messages.
packet	Configures the debugging of the Airewave Director packets.
power	Configures the debugging of the Airewave Director power assignment protocol and coverage hole detection.
profile	Configures the debugging of the Airewave Director profile events.
radar	Configures the debugging of the Airewave Director radar detection/avoidance protocol.
rf-change	Configures the debugging of the Airewave Director rf changes.
enable	Enables the Airewave Director debugging.

disable	Disables the Airewave Director debugging.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the debugging of Airewave Director profile events:

```
(Cisco Controller) > debug airewave-director profile enable
```

Related Commands

debug disable-all

show sysinfo

debug ap

To configure the remote debugging of Cisco lightweight access points or to remotely execute a command on a lightweight access point, use the **debug ap** command.

debug ap {**enable** | **disable** | **command** *cmd*} *cisco_ap*

Syntax Description

enable	Enables the debugging on a lightweight access point. **Note** The debugging information is displayed only to the controller console and does not send output to a controller Telnet/SSH CLI session.
disable	Disables the debugging on a lightweight access point. **Note** The debugging information is displayed only to the controller console and does not send output to a controller Telnet/SSH CLI session.
command	Specifies that a CLI command is to be executed on the access point.
cmd	Command to be executed. **Note** The command to be executed must be enclosed in double quotes, such as **debug ap command "led flash 30" AP03**. The output of the command displays only to the controller console and does not send output to a controller Telnet/SSH CLI session.
cisco_ap	Name of a Cisco lightweight access point.

Command Default

The remote debugging of Cisco lightweight access points is disabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the remote debugging on access point AP01:

```
(Cisco Controller) >debug ap enable AP01
```

The following example shows how to execute the **config ap location** command on access point AP02:

```
(Cisco Controller) >debug ap command "config ap location "Building 1" AP02"
```

The following example shows how to execute the flash LED command on access point AP03:

```
(Cisco Controller) >debug ap command "led flash 30" AP03
```

debug ap enable

To configure the remote debugging of Cisco lightweight access points or to remotely execute a command on a lightweight access point, use the **debug ap enable** command.

debug ap {**enable** | **disable** | **command** *cmd*} *cisco_ap*

Syntax Description

enable	Enables the remote debugging. **Note** The debugging information is displayed only to the controller console and does not send output to a controller Telnet/SSH CLI session.
disable	Disables the remote debugging.
command	Specifies that a CLI command is to be executed on the access point.
cmd	Command to be executed. **Note** The command to be executed must be enclosed in double quotes, such as **debug ap command "led flash 30" AP03**. The output of the command displays only to the controller console and does not send output to a controller Telnet/SSH CLI session.
cisco_ap	Cisco lightweight access point name.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the remote debugging on access point AP01:

```
(Cisco Controller) >debug ap enable AP01
```

The following example shows how to disable the remote debugging on access point AP02:

```
(Cisco Controller) >debug ap disable AP02
```

The following example shows how to execute the flash LED command on access point AP03:

```
(Cisco Controller) >debug ap command "led flash 30" AP03
```

debug ap packet-dump

To configure the debugging of Packet Capture, use the **debug ap packet-dump** command.

debug ap packet-dump { **enable** | **disable** }

Syntax Description

enable	Enables the debugging of Packet Capture of an access point.
disable	Disables the debugging of Packet Capture of an access point.

Command Default

Debugging of Packet Capture is disabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

Packet Capture does not work during inter-controller roaming.

The controller does not capture packets created in the radio firmware and sent out of the access point, such as beacon or probe response. Only packets that flow through the radio driver in the Tx path will be captured.

The following example shows how to enable the debugging of Packet Capture from an access point:

```
(Cisco Controller) >debug ap packet-dump enable
```

debug ap show stats

To debug video messages and statistics of Cisco lightweight access points, use the **debug ap show stats** command.

debug ap show stats {**802.11a** | **802.11b**} *cisco_ap* {**tx-queue** | **packet** | **load** | **multicast** | **client** {*client_MAC* | **video** | **all**} | **video metrics**}

debug ap show stats video *cisco_ap* {**multicast mgid** *mgid_database_number* | **admission** | **bandwidth**}

Syntax Description

802.11a	Specifies the 802.11a network.
802.11b	Specifies the 802.11b/g network.
cisco_ap	Cisco lightweight access point name.
tx-queue	Displays the transmit queue traffic statistics of the AP.
packet	Displays the packet statistics of the AP.
load	Displays the QoS Basic Service Set (QBSS) and other statistics of the AP.
multicast	Displays the multicast supported rate statistics of the AP.
client	Displays the specified client metric statistics.
client_MAC	MAC address of the client.
video	Displays video statistics of all clients on the AP.
all	Displays statistics of all clients on the AP.
video metrics	Displays the video metric statistics.
mgid	Displays detailed multicast information for a single multicast group ID (MGID).
mgid_database_number	Layer 2 MGID database number.
admission	Displays video admission control on the AP.
bandwidth	Displays video bandwidth on the AP.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to troubleshoot the access point AP01's transmit queue traffic on an 802.11a network:

```
(Cisco Controller) >debug ap show stats 802.11a AP01 tx-queue
```

The following example shows how to troubleshoot the access point AP02's multicast supported rates on an 802.11b/g network:

```
(Cisco Controller) >debug ap show stats 802.11b AP02 multicast
```

The following example shows how to troubleshoot the metrics of a client identified by its MAC address, associated with the access point AP01 on an 802.11a network:

```
(Cisco Controller) >debug ap show stats 802.11a AP01 client 00:40:96:a8:f7:98
```

The following example shows how to troubleshoot the metrics of all clients associated with the access point AP01 on an 802.11a network:

```
(Cisco Controller) >debug ap show stats 802.11a AP01 client all
```

debug ap show stats video

To configure the debugging of video messages and statistics of Cisco lightweight access points, use the **debug ap show stats video** command.

debug ap show stats video *cisco_ap* {**multicast mgid** *mgid_value* | **admission** | **bandwidth**}

Syntax Description

cisco_ap	Cisco lightweight access point name.
multicast mgid	Displays multicast database related information for the specified MGID of an access point.
mgid_value	Layer 2 MGID database number from 1 to 4095.
admission	Displays the video admission control.
bandwidth	Displays the video bandwidth.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the debugging of an access point AP01's multicast group that is identified by the group's Layer 2 MGID database number:

```
(Cisco Controller) >debug ap show stats video AP01 multicast mgid 50
```

This example shows how to configure the debugging of an access point AP01's video bandwidth:

```
(Cisco Controller) >debug ap show stats video AP01 bandwidth
```

debug arp

To configure the debugging of Address Resolution Protocol (ARP) options, use the **debug arp** command.

debug arp {**all** | **detail** | **events** | **message**} {**enable** | **disable**}

Syntax Description

all	Configures the debugging of all ARP logs.
detail	Configures the debugging of ARP detail messages.
error	Configures the debugging of ARP errors.
message	Configures the debugging of ARP messages.
enable	Enables the ARP debugging.
disable	Disables the ARP debugging.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable ARP debug settings:

```
(Cisco Controller) > debug arp error enable
```

The following example shows how to disable ARP debug settings:

```
(Cisco Controller) > debug arp error disable
```

Related Commands

debug disable-all

show sysinfo

debug avc

To configure the debugging of Application Visibility and Control (AVC) options, use the **debug avc error** command.

debug avc {**events** | **error**} {**enable** | **disable**}

Syntax Description

events	Configures the debugging of AVC events.
error	Configures the debugging of AVC errors.
enable	Enables the debugging of AVC events or errors.
disable	Disables the debugging of AVC events or errors.

Command Default By default, the debugging of AVC options is disabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the debugging of AVC errors:

```
(Cisco Controller) > debug avc error enable
```

Related Commands

config avc profile delete

config avc profile rule

config wlan avc

show avc profile

show avc applications

show avc statistics

debug bcast

To configure the debugging of broadcast options, use the **debug bcast** command.

debug bcast {**all** | **error** | **message** | **igmp** | **detail**} {**enable** | **disable**}

Syntax Description

all	Configures the debugging of all broadcast logs.
error	Configures the debugging of broadcast errors.
message	Configures the debugging of broadcast messages.
igmp	Configures the debugging of broadcast IGMP messages.
detail	Configures the debugging of broadcast detailed messages.
enable	Enables the broadcast debugging.
disable	Disables the broadcast debugging.

Command Default None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the debugging of broadcast messages:

```
(Cisco Controller) > debug bcast message enable
```

The following example shows how to disable the debugging of broadcast mesages:

```
(Cisco Controller) > debug bcast message disable
```

Related Commands

debug disable-all

show sysinfo

debug cac

To configure the debugging of Call Admission Control (CAC) options, use the **debug cac** command.

debug cac {**all** | **event** | **packet**} {**enable** | **disable**}

Syntax Description

all	Configures the debugging options for all CAC messages.
event	Configures the debugging options for CAC events.
packet	Configures the debugging options for selected CAC packets.
kts	Configures the debugging options for KTS-based CAC messages.
enable	Enables the debugging of CAC settings.
disable	Disables the debugging of CAC settings.

Command Default

By default, the debugging of CAC options is disabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable debugging of CAC settings:

```
(Cisco Controller) > debug cac event enable
(Cisco Controller) > debug cac packet enable
```

Related Commands

config 802.11 cac video acm

config 802.11 cac video max-bandwidth

config 802.11 video roam-bandwidth

config 802.11 cac video tspec-inactivity-timeout

config 802.11 cac voice load-based

config 802.11 cac voice roam-bandwidth

config 802.11cac voice stream-size

config 802.11cac voice tspec-inactivity-timeout

debug call-control

To configure the debugging of the SIP call control settings, use the **debug call-control** command.

debug call-control {**all** | **event**} {**enable** | **disable**}

Syntax Description

all	Configures the debugging options for all SIP call control messages.
event	Configures the debugging options for SIP call control events.
enable	Enables the debugging of SIP call control messages or events.
disable	Disables the debugging of SIP call control messages or events.

Command Default

Disabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the debugging of all SIP call control messages:

```
(Cisco Controller) >debug call-control all enable
```

debug capwap

To configure the debugging of Control and Provisioning of Wireless Access Points (CAPWAP) settings, use the **debug capwap** command.

debug capwap {**detail** | **dtls-keepalive** | **errors** | **events** | **hexdump** | **info** | **packet** | **payload** | **mfp**} {**enable** | **disable**}

Syntax Description

detail	Configures the debugging for CAPWAP detail settings.
dtls-keepalive	Configures the debugging for CAPWAP DTLS data keepalive packets settings.
errors	Configures the debugging for CAPWAP error settings.
events	Configures the debugging for CAPWAP events settings.
hexdump	Configures the debugging for CAPWAP hexadecimal dump settings.
info	Configures the debugging for CAPWAP info settings.
packet	Configures the debugging for CAPWAP packet settings.
payload	Configures the debugging for CAPWAP payload settings.

mfp	Configures the debugging for CAPWAP mfp settings.
enable	Enables the debugging of the CAPWAP command.
disable	Disables the debugging of the CAPWAP command.

Command Default None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the debugging of CAPWAP details:

```
(Cisco Controller) >debug capwap detail enable
```

debug capwap reap

To configure the debugging of Control and Provisioning of Wireless Access Points (CAPWAP) settings on a FlexConnect access point, use the **debug capwap reap** command.

debug capwap reap [**mgmt** | **load**]

Syntax Description

mgmt	(Optional) Configures the debugging for client authentication and association messages.
load	(Optional) Configures the debugging for payload activities, which is useful when the FlexConnect access point boots up in standalone mode.

Command Default None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the debugging of FlexConnect client authentication and association messages:

```
(Cisco Controller) >debug capwap reap mgmt
```

debug client

To configure the debugging for a specific client, use the **debug client** command.

debug client *mac_address*

Syntax Description

mac_address	MAC address of the client.

Command Default None

Usage Guidelines After entering the **debug client** *mac_address* command, if you enter the **debug aaa events enable** command, then the AAA events logs are displayed for that particular client MAC address.

Command History

Release	Modification
7.6	This command was introduced.

The following example shows how to debug a specific client:

```
(Cisco Controller) > debug client 01:35:6x:yy:21:00
```

debug crypto

To configure the debugging of the hardware cryptographic options, use the **debug crypto** command.

debug crypto {**all** | **sessions** | **trace** | **warning**} {**enable** | **disable**}

Syntax Description

all	Configures the debugging of all hardware crypto messages.
sessions	Configures the debugging of hardware crypto sessions.
trace	Configures the debugging of hardware crypto sessions.
warning	Configures the debugging of hardware crypto sessions.
enable	Enables the debugging of hardware cryptographic sessions.
disable	Disables the debugging of hardware cryptographic sessions.

Command Default None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the debugging of hardware crypto sessions:

```
(Cisco Controller) > debug crypto sessions enable
```

Related Commands **debug disable-all**

show sysinfo

debug dhcp

To configure the debugging of DHCP, use the **debug dhcp** command.

debug dhcp {**message** | **packet**} {**enable** | **disable**}

Syntax Description

message	Configures the debugging of DHCP error messages.
packet	Configures the debugging of DHCP packets.
enable	Enables the debugging DHCP messages or packets.
disable	Disables the debugging of DHCP messages or packets.

Command Default None

The following example shows how to enable the debugging of DHCP messages:

```
(Cisco Controller) >debug dhcp message enable
```

debug dhcp service-port

To enable or disable debugging of the Dynamic Host Configuration Protocol (DHCP) packets on the service port, use the **debug dhcp service-port** command.

debug dhcp service-port {**enable** | **disable**}

Syntax Description

enable	Enables the debugging of DHCP packets on the service port.
disable	Disables the debugging of DHCP packets on the service port.

Command Default None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the debugging of DHCP packets on a service port:

```
(Cisco Controller) >debug dhcp service-port enable
```

debug disable-all

To disable all debug messages, use the **debug disable-all** command.

debug disable-all

Syntax Description This command has no arguments or keywords.

Command Default Disabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to disable all debug messages:

```
(Cisco Controller) > debug disable-all
```

debug dot11

To configure the debugging of 802.11 events, use the **debug dot11** command.

debug dot11 {**all** | **load-balancing** | **management** | **mobile** | **nmsp** | **probe** | **rldp** | **rogue** | **state**} {**enable** | **disable**}

Syntax Description

all	Configures the debugging of all 802.11 messages.
load-balancing	Configures the debugging of 802.11 load balancing events.
management	Configures the debugging of 802.11 MAC management messages.
mobile	Configures the debugging of 802.11 mobile events.
nmsp	Configures the debugging of the 802.11 NMSP interface events.
probe	Configures the debugging of probe.
rldp	Configures the debugging of 802.11 Rogue Location Discovery.
rogue	Configures the debugging of 802.11 rogue events.
state	Configures the debugging of 802.11 mobile state transitions.
enable	Enables the 802.11 debugging.
disable	Disables the 802.11 debugging.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the debugging of 802.11 settings:

```
(Cisco Controller) > debug dot11 state enable
(Cisco Controller) > debug dot11 mobile enable
```

debug dot11 mgmt interface

To configure debugging of 802.11 management interface events, use the **debug dot11 mgmt interface** command.

debug dot11 mgmt interface

Syntax Description This command has no arguments or keywords.

Command Default None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to debug 802.11 management interface events:

```
(Cisco Controller) >debug dot11 mgmt interface
```

debug dot11 mgmt msg

To configure debugging of 802.11 management messages, use the **debug dot11 mgmt msg** command.

debug dot11 mgmt msg

Syntax Description This command has no arguments or keywords.

Command Default None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

This example shows how to debug dot11 management messages:

```
(Cisco Controller) >debug dot11 mgmt msg
```

debug dot11 mgmt ssid

To configure debugging of 802.11 SSID management events, use the **debug dot11 mgmt ssid** command.

debug dot11 mgmt ssid

Syntax Description This command has no arguments or keywords.

Command Default None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the debugging of 802.11 SSID management events:

```
(Cisco Controller) >debug dot11 mgmt ssid
```

debug dot11 mgmt station

To configure the debugging of the management station settings, use the **debug dot11 mgmt station** command.

debug dot11 mgmt station

Syntax Description This command has no arguments or keywords.

Command Default None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the debugging of the management station settings:

```
(Cisco Controller) >debug dot11 mgmt station
```

debug dot1x

To configure debugging of the 802.1X options, use the **debug dot1x** command.

debug dot1x {**aaa** | **all** | **events** | **packets** | **states**} {**enable** | **disable**}

Syntax Description

aaa	Configures debugging of the 802.1X AAA interactions.
all	Configures debugging of all the 802.1X messages.
events	Configures debugging of the 802.1X events.
packets	Configures debugging of the 802.1X packets.
states	Configures debugging of the 802.1X state transitions.
enable	Enables debugging of the 802.1X options.
disable	Disables debugging of the 802.1X options.

Command Default None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable 802.1X state transitions debugging:

```
(Cisco Controller) > debug dot1x states enable
```

debug group

To configure the debugging of access point groups, use the **debug group** command.

debug group {**enable** | **disable**}

Syntax Description

enable	Enables the debugging of access point groups.
disable	Disables the debugging of access point groups.

Command Default None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the debugging of access point groups:

```
(Cisco Controller) >debug group enable
```

debug flexconnect aaa

To configure debugging of FlexConnect backup RADIUS server events or errors, use the **debug flexconnect aaa** command.

debug flexconnect aaa {**event** | **error**} {**enable** | **disable**}

Syntax Description

event	Configures the debugging for FlexConnect RADIUS server events.
error	Configures the debugging for FlexConnect RADIUS server errors.
enable	Enables the debugging of FlexConnect RADIUS server settings.
disable	Disables the debugging of FlexConnect RADIUS server settings.

Command Default None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the debugging of FlexConnect RADIUS server events:

```
(Cisco Controller) >debug flexconnect aaa event enable
```

debug flexconnect acl

Configures debugging of FlexConnect access control lists (ACLs), use the **debug flexconnect acl** command.

debug flexconnect acl {**enable** | **disable**}

Syntax Description

enable	Enables the debugging of FlexConnect ACLs.
disable	Disables the debugging of FlexConnect ACLs.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the debugging of FlexConnect ACLs:

```
(Cisco Controller) >debug flexconnect acl enable
```

debug flexconnect group

To configure debugging of FlexConnect access point groups, use the **debug flexconnect group** command.

debug flexconnect group {**enable** | **disable**}

Syntax Description

enable	Enables the debugging of FlexConnect access point groups.
disable	Disables the debugging of FlexConnect access point groups.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the debugging of FlexConnect access point groups:

```
(Cisco Controller) >debug flexconnect group enable
```

debug hotspot

To configure debugging of HotSpot events or packets, use the **debug hotspot** command.

debug hotspot {**events** | **packets**} {**enable** | **disable**} {**enable** | **disable**}

Syntax Description

events	Configures debugging of HotSpot events.
packets	Configures debugging of HotSpot packets.
enable	Enables the debugging of HotSpot options.
disable	Disables the debugging of HotSpot options.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable debugging of hotspot events:

```
(Cisco Controller) >debug hotspot events enable
```

debug hotspot packets

To configure the debugging of HotSpot packets, use the **debug hotspot packets** command.

debug hotspot packets {**enable** | **disable**}

Syntax Description

enable	Enables the debugging of HotSpot packets.
disable	Disables the debugging of HotSpot packets.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the debugging of HotSpot packets:

```
(Cisco Controller) >debug hotspot packets enable
```

debug l2age

To configure the debugging of Layer 2 age timeout messages, use the **debug l2age** command.

debug l2age {**enable** | **disable**}

Syntax Description

enable	Enables the debugging of Layer2 age settings.
disable	Disables the debugging Layer2 age settings.

Command Default None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the debugging of Layer2 age settings:

```
(Cisco Controller) > debug l2age enable
```

Related Commands **debug disable-all**

debug lwapp console cli

To configure the debugging of the access point console CLI, use the **debug lwapp console cli** command from the access point console port.

debug lwapp console cli

Syntax Description This command has no arguments or keywords.

Command Default None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines This access point CLI command must be entered from the access point console port.

The following example shows how to configure the debugging of the access point console:

```
AP# debug lwapp console cli
LWAPP console CLI allow/disallow debugging is on
```

debug mac

To configure the debugging of the client MAC address, use the **debug mac** command.

debug mac {**disable** | **addr** *MAC*}

Syntax Description

disable	Disables the debugging of the client using the MAC address.
addr	Configures the debugging of the client using the MAC address.

MAC	MAC address of the client.

Command Default None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the debugging of the client using the MAC address:

```
(Cisco Controller) > debug mac addr 00.0c.41.07.33.a6
```

Related Commands **debug disable-all**

debug media-stream

To configure the debugging of media stream, use the **debug media-stream** command.

debug media-stream {**admission** | **config** | **errors** | **event** | **history** | **rrc**} {**enable** | **disable**}

Syntax Description

admission	Configures the debugging of the media stream admission.
config	Configures the debugging of the media stream configuration.
errors	Configures the debugging of the media stream errors.
event	Configures the debugging of the media stream events.
history	Configures the debugging of the media stream history.
rrc	Configures the debugging of the media stream radio resource management.
enable	Enables the debugging of the media stream.
disable	Disables the debugging of the media stream.

Command Default None.

This example shows how to enable the debugging of the media stream history:

```
> debug media-stream history enable
```

Related Commands **show media-stream group summary**

config media-stream multicast direct

debug memory

To enable or disable the debugging of errors or events during the memory allocation of the controller, use the **debug memory** command.

debug memory { **errors** | **events** } { **enable** | **disable** }

Syntax Description

errors	Configures the debugging of memory leak errors.
events	Configures debugging of memory leak events.
enable	Enables the debugging of memory leak events.
disable	Disables the debugging of memory leak events.

Command Default

By default, the debugging of errors or events during the memory allocation of the controller is disabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the debugging of memory leak events:

```
(Cisco Controller) > debug memory events enable
```

Related Commands

config memory monitor errors

show memory monitor

config memory monitor leaks

debug mesh security

To configure the debugging of mesh security issues, use the **debug mesh security** command.

debug mesh security {**all** | **events** | **errors**} {**enable** | **disable**}

Syntax Description

all	Configures the debugging of all mesh security messages.
events	Configures the debugging of mesh security event messages.
errors	Configures the debugging of mesh security error messages.
enable	Enables the debugging of mesh security error messages.
disable	Disables the debugging of mesh security error messages.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the debugging of mesh security error messages:

```
(Cisco Controller) >debug mesh security errors enable
```

debug mobility

To configure the debugging of wireless mobility, use the **debug mobility** command.

debug mobility {**ap-list** | **config** | **directory** | **dtls** | **handoff** | **keep-alive** | **multicast** | **oracle** | **packet** | **peer-ip** *IP-address* | **pmk** | **pmtu-discovery** | **redha**} {**enable** | **disable**}

Syntax Description

ap-list	Configures the debugging of wireless mobility access point list.
config	Configures the debugging of wireless mobility configuration.
directory	Configures the debugging of wireless mobility error messages.
dtls	Configures the debugging of wireless mobility Datagram Transport Layer Security (DTLS) options.
handoff	Configures the debugging of wireless mobility handoff messages.
keep-alive	Configures the debugging of wireless mobility CAPWAP data DTLS keep-alive packets.
multicast	Configures the debugging of multicast mobility packets.
oracle	Starts the debugging of wireless mobility oracle options.
packet	Configures the debugging of wireless mobility packets.
peer-ip	Configures IP address of the mobility peer for which incoming and outgoing mobility messages should be displayed.
IP-address	IP address of the mobility peer for which incoming and outgoing mobility messages should be displayed.
pmk	Configures the debugging of wireless mobility pairwise master key (PMK).

pmtu-discovery	Configures the debugging of the wireless mobility path MTU discovery.
redha	Configures the debugging of the multicast mobility high availability.
enable	Enables the debugging of the wireless mobility feature.
disable	Disables the debugging of the wireless mobility feature.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.0	This command supports both IPv4 and IPv6 address formats.

The following example shows how to enable the debugging of wireless mobility packets.

```
(Cisco Controller) >debug mobility handoff enable
```

debug nmsp

To configure the debugging of the Network Mobility Services Protocol (NMSP), use the **debug nmsp** command.

debug nmsp {**all** | **connection** | **detail** | **error** | **event** | **message** | **packet**}

Syntax Description

all	Configures the debugging for all NMSP messages.
connection	Configures the debugging for NMSP connection events.
detail	Configures the debugging for NMSP events in detail.
error	Configures the debugging for NMSP error messages.
event	Configures the debugging for NMSP events.
message	Configures the debugging for NMSP transmit and receive messages.
packet	Configures the debugging for NMSP packet events.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the debugging of NMSP connection events:

```
(Cisco Controller) > debug nmsp connection
```

Related Commands

clear nmsp statistics

debug disable-all

config nmsp notify-interval measurement

debug ntp

To configure the debugging of the Network Time Protocol (NTP), use the **debug ntp** command.

debug ntp {**detail** | **low** | **packet**} {**enable** | **disable**}

Syntax Description

detail	Configures the debugging of detailed NTP messages.
low	Configures the debugging of NTP messages.
packet	Configures the debugging of NTP packets.
enable	Enables the NTP debugging.
disable	Disables the NTP debugging.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the debugging of NTP settings:

```
(Cisco Controller) > debug ntp packet enable
```

Related Commands

debug disable-all

debug packet error

To configure debugging of the packets sent to the controller CPU , use the **debug packet error** command.

debug packet error {**enable** | **disable**}

Syntax Description

enable	Enables debugging of the packets sent to the controller CPU.

disable	Disables debugging of the packets sent to the controller CPU.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the debugging of the packets sent to the controller CPU:

```
(Cisco Controller) > debug packet error enable
```

debug packet logging

To configure logging of the packets sent to the controller CPU, use the **debug packet logging** command.

debug packet logging {**acl** | **disable** | **enable** {**rx** | **tx** | **all**} *packet_count display_size* | **format** {**hex2pcap** | **text2pcap**}}

debug packet logging acl {**clear-all** | **driver** *rule_index action npu_encap port* | **eoip-eth** *rule_index action dst src type vlan* | **eoip-ip** *rule_index action src dst proto src_port dst_port* | **eth** *rule_index action dst src type vlan* | **ip** *rule_index action src dst proto src_port dst_port* | **lwapp-dot11***rule_index action dst src bssid type* | **lwapp-ip** *rule_index action src dst proto src_port dst_port*}

Syntax Description

acl	Filters the displayed packets according to a rule.
disable	Disables logging of all the packets.
enable	Enables logging of all the packets.
rx	Displays all the received packets.
tx	Displays all the transmitted packets.
all	Displays both the transmitted and the received packets.
packet_count	Maximum number of packets to be logged. The range is from 1 to 65535. The default value is 25.
display_size	Number of bytes to be displayed when printing a packet. By default, the entire packet is displayed.
format	Configures the format of the debug output.
hex2pcap	Configures the output format to be compatible with the hex2pcap format. The standard format used by Cisco IOS supports the use of hex2pcap and can be decoded using an HTML front end.

text2pcap	Configures the output format to be compatible with the text2pcap format. In this format, the sequence of packets can be decoded from the same console log file. .
clear-all	Clears all the existing rules pertaining to the packets.
driver	Filters the packets based on an incoming port or a Network Processing Unit (NPU) encapsulation type.
rule_index	Index of the rule that is a value between 1 and 6 (inclusive).
action	Action for the rule, which can be **permit**, **deny**, or **disable**.
npu_encap	NPU encapsulation type that determines how the packets are filtered. The possible values are *dhcp, dot11-mgmt, dot11-probe, dot1x, eoip-ping, iapp, ip, lwapp, multicast, orphan-from-sta, orphan-to-sta, rbcp, wired-guest,* or *any*.
port	Physical port for packet transmission or reception.
eoip-eth	Filters packets based on the Ethernet II header in the Ethernet over IP (EoIP) payload.
dst	Destination MAC address.
src	Source MAC address.
type	Two-byte type code, such as 0x800 for IP, 0x806 for Address Resolution Protocol (ARP). You can also enter a few common string values such as *ip* (for 0x800) or *arp* (for 0x806).
vlan	Two-byte VLAN identifier.
eoip-ip	Filters packets based on the IP header in the EoIP payload.
proto	Protocol. Valide values are: *ip, icmp, igmp, ggp, ipencap, st, tcp, egp, pup, udp, hmp, xns-idp, rdp, iso-tp4, xtp, ddp, idpr-cmtp, rspf, vmtp, ospf, ipip,* and *encap*.
src_port	User Datagram Protocol or Transmission Control Protocol (UDP or TCP) two-byte source port, such as *telnet, 23* , or *any*. The controller supports the following strings: *tcpmux, echo, discard, systat, daytime, netstat, qotd, msp, chargen, ftp-data, ftp, fsp, ssh, telnet, smtp, time, rlp, nameserver, whois, re-mail-ck, domain, mtp, bootps, bootpc, tftp, gopher, rje, finger, www, link, kerberos, supdup, hostnames, iso-tsap, csnet-ns, 3com-tsmux, rtelnet, pop-2, pop-3, sunrpc, auth, sftp, uucp-path, nntp, ntp, netbios-ns, netbios-dgm, netbios-ssn, imap2, snmp, snmp-trap, cmip-man, cmip-agent, xdmcp, nextstep, bgp, prospero, irc, smux, at-rtmp, at-nbp, at-echo, at-zis, qmtp, z3950, ipx, imap3, ulistserv, https, snpp, saft, npmp-local, npmp-gui,* and *hmmp-ind*.
dst_port	UDP or TCP two-byte destination port, such as *telnet, 23*, or *any*. The controller supports the same strings as those for the src_port.

eth	Filters packets based on the values in the Ethernet II header.
ip	Filters packets based on the values in the IP header.
lwapp-dot11	Filters packets based on the 802.11 header in the Lightweight Access Point Protocol (LWAPP) payload.
bssid	Basic Service Set Identifier of the VLAN.
lwapp-ip	Filters packets based on the IP header in the LWAPP payload.

Command Default None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable logging of a packet:

```
(Cisco Controller) > debug packet logging enable
```

debug pem

To configure debugging of the access policy manager, use the **debug pem** command.

debug pem {**events** | **state**} {**enable** | **disable**}

Syntax Description

events	Configures the debugging of the policy manager events.
state	Configures the debugging of the policy manager state machine.
enable	Enables the debugging of the access policy manager.
disable	Disables the debugging of the access policy manager.

Command Default None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the debugging of the access policy manager:

```
(Cisco Controller) >debug pem state enable
```

debug poe

To configure the debugging of Power over Ethernet (PoE), use the **debug poe** command.

debug poe {**detail** | **message** | **error**} {**enable** | **disable**}

Syntax Description

detail	Configures the debugging of PoE detail logs.
error	Configures the debugging of PoE error logs.
message	Configures the debugging of PoE messages.
enable	Enables the debugging of PoE logs.
disable	Disables the debugging of PoE logs.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the PoE debugging:

```
(Cisco Controller) > debug poe message enable
```

Related Commands

debug disable-all

debug profiling

To configure the debugging of client profiling, use the **debug profiling** command.

debug profiling {**enable** | **disable**}

Syntax Description

enable	Enables the debugging of client profiling (HTTP and DHCP profiling).
disable	Disables the debugging of client profiling (HTTP and DHCP profiling).

Command Default

Disabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the debugging of client profiling:

```
(Cisco Controller) >debug profiling enable
```

debug rbcp

To configure Router Blade Control (RBCP) debug options, use the **debug rbcp** command.

debug rbcp {**all** | **detail** | **errors** | **packet**} {**enable** | **disable**}

Syntax Description

all	Configures the debugging of RBCP.
detail	Configures the debugging of RBCP detail.
errors	Configures the debugging of RBCP errors.
packet	Configures the debugging of RBCP packet trace.
enable	Enables the RBCP debugging.
disable	Disables the RBCP debugging.

Command Default None

The following example shows how to enable the debugging of RBCP settings:

```
(Cisco Controller) > debug rbcp packet enable
```

Related Commands **debug disable-all**

debug rfac

To configure the debugging of the Redundancy Framework (RFAC), use the **debug rfac** command.

debug rfac {[**packet** | **events** | **errors** | **detail**] [**enable** | **disable**]}

Syntax Description

packet	Configures the debugging of Redundancy Framework packets.
events	Configures the debugging of Redundancy Framework events.
errors	Configures the debugging of Redundancy Framework errors.
detail	Configures the debugging of Redundancy Framework details.
enable	(Optional) Enables the debugging of Redundancy Framework.
disable	(Optional) Disables the debugging of Redundancy Framework.

Command Default None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the debugging of Redundancy Framework packets:

```
(Cisco Controller) >debug rfac packet enable
```

debug rfid

To configure radio frequency identification (RFID) debug options, use the **debug rfid** command.

debug rfid {**all** | **detail** | **errors** | **nmsp** | **receive**} {**enable** | **disable**}

Syntax Description

all	Configures the debugging of all RFID.
detail	Configures the debugging of RFID detail.
errors	Configures the debugging of RFID error messages.
nmsp	Configures the debugging of RFID Network Mobility Services Protocol (NMSP) messages.
receive	Configures the debugging of incoming RFID tag messages.
enable	Enables the RFID debugging.
disable	Disables the RFID debugging.

Command Default None

The following example shows how to enable the debugging of RFID error messages:

```
(Cisco Controller) > debug rfid errors enable
```

Related Commands **debug disable-all**

debug rmgr

To configure the debugging of Redundancy Manager (RMGR), use the **debug rmgr** command.

debug rmgr {**packet** | **events** | **errors** | **detail**} {**enable** | **disable**}

Syntax Description

packet	Configures the debugging of Redundancy Manager packets.
events	Configures the debugging of Redundancy Manager events.
errors	Configures the debugging of Redundancy Manager errors.
detail	Configures the debugging of Redundancy Manager details.
enable	Enables the debugging of Redundancy Manager.
disable	Disables the debugging of Redundancy Manager.

Command Default None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

Redundancy Manager determines the role of the Cisco WLCs, maintains the keepalive messages between the peers, and initiates the switchover.

The following example shows how to enable the debugging of Redundancy Manager packets:

```
(Cisco Controller) >debug rmgr packet enable
```

debug rsyncmgr

To configure the debugging of the Redundancy Sync Manager (RSYNCMGR), use the **debug rsyncmgr** command.

debug rsyncmgr {**packet** | **events** | **errors** | **detail**} {**enable** | **disable**}}

Syntax Description

packet	Configures the debugging of Redundancy Sync Manager packets.
events	Configures the debugging of Redundancy Sync Manager events.
errors	Configures the debugging of Redundancy Sync Manager errors.
detail	Configures the debugging of Redundancy Sync Manager details.
enable	Enables the debugging of Redundancy Sync Manager.
disable	Stops the debugging Redundancy Sync Manager.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

Redundancy Synchronization Manager synchronizes the configurations of the active and standby Cisco WLCs.

The following example shows how to enable the debugging of Redundancy Sync Manager packets:

```
(Cisco Controller) >debug rsyncmgr packet enable
```

debug service ap-monitor

To debug the access point monitor service, use the **debug service ap-monitor** command.

debug service ap-monitor {**all** | **error** | **event** | **nmsp** | **packet**} {**enable** | **disable**}

Syntax Description

all	Configures the debugging of all access point status messages.
error	Configures the debugging of access point monitor error events.
event	Configures the debugging of access point monitor events.
nmsp	Configures the debugging of access point monitor Network Mobility Services Protocol (NMSP) events.
packet	Configures the debugging of access point monitor packets.
enable	Enables the debugging for access point monitor service.
disable	Disables the debugging for access point monitor service.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the debugging of access point monitor NMSP events:

```
(Cisco Controller) >debug service ap-monitor events
```

debug snmp

To configure SNMP debug options, use the **debug snmp** command.

debug snmp {**agent** | **all** | **mib** | **trap**} {**enable** | **disable**}

Syntax Description

agent	Configures the debugging of the SNMP agent.
all	Configures the debugging of all SNMP messages.
mib	Configures the debugging of the SNMP MIB.
trap	Configures the debugging of SNMP traps.
enable	Enables the SNMP debugging.
disable	Disables the SNMP debugging.

Command Default None

The following example shows how to enable the SNMP debugging:

```
(Cisco Controller) > debug snmp trap enable
```

Related Commands **debug disable-all**

debug transfer

To configure transfer debug options, use the **debug transfer** command.

debug transfer {**all** | **tftp** | **trace**} {**enable** | **disable**}

Syntax Description

all	Configures the debugging of all transfer messages.
tftp	Configures the debugging of TFTP transfers.
trace	Configures the debugging of transfer messages.
enable	Enables the debugging of transfer messages.
disable	Disables the debugging of transfer messages.

Command Default None

The following example shows how to enable the debugging of transfer messages:

```
(Cisco Controller) > debug transfer trace enable
```

Related Commands **debug disable-all**

debug voice-diag

To trace call or packet flow, use the **debug voice-diag** command.

debug voice-diag {**enable** *client_mac1* [*client_mac2*] [**verbose**] | **disable**}

Syntax Description

enable	Enables the debugging of voice diagnostics for voice clients involved in a call.
client_mac1	MAC address of a voice client.
client_mac2	(Optional) MAC address of an additional voice client. **Note** Voice diagnostics can be enabled or disabled for a maximum of two voice clients at a time.

verbose	(Optional) Enables debug information to be displayed on the console. **Note** When voice diagnostics is enabled from the NCS or Prime Infrastructure, the verbose option is not available.
disable	Disables the debugging of voice diagnostics for voice clients involved in a call.

Command Default

None

Usage Guidelines

Follow these guidelines when you use the **debug voice-diag** command:

- When the command is entered, the validity of the clients is not checked.
- A few output messages of the command are sent to the NCS or Prime Infrastructure.
- The command expires automatically after 60 minutes.
- The command provides the details of the call flow between a pair of client MACs involved in an active call.

Note Voice diagnostics can be enabled for a maximum of two voice clients at a time.

The following example shows how to enable transfer/upgrade settings:

```
(Cisco Controller) > debug voice-diag enable 00:1a:a1:92:b9:5c 00:1a:a1:92:b5:9c verbose
```

Related Commands

show client voice-diag

show client calls

debug web-auth

To configure debugging of web-authenticated clients, use the **debug web-auth** command.

debug web-auth {**redirect** { **enable mac** *mac_address* | **disable**} | **webportal-server** {**enable** | **disable**} }

Syntax Description

redirect	Configures debugging of web-authenticated and redirected clients.
enable	Enables the debugging of web-authenticated clients.
mac	Configures the MAC address of the web-authenticated client.
mac_address	MAC address of the web-authenticated client.
disable	Disables the debugging of web-authenticated clients.
webportal-server	Configures the debugging of portal authentication of clients.

Command Default None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the debugging of a web authenticated and redirected client:

```
(Cisco Controller) > debug web-auth redirect enable mac xx:xx:xx:xx:xx:xx
```

debug wcp

To configure the debugging of WLAN Control Protocol (WCP), use the **debug wcp** command.

debug wcp {**events** | **packet**} {**enable** | **disable**}

Syntax Description

events	Configures the debugging of WCP events.
packet	Configures the debugging of WCP packets.
enable	Enables the debugging of WCP settings.
disable	Disables the debugging of WCP settings.

Command Default None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the debugging of WCP settings:

```
(Cisco Controller) >debug wcp packet enable
```

debug wps sig

To configure the debugging of Wireless Provisioning Service (WPS) signature settings, use the **debug wps sig** command.

debug wps sig {**enable** | **disable**}

Syntax Description

enable	Enables the debugging for WPS settings.
disable	Disables the debugging for WPS settings.

Command Default None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the debugging of WPS signature settings:

```
(Cisco Controller) > debug wps sig enable
```

Related Commands

debug wps mfp

debug disable-all

debug wps mfp

To configure the debugging of WPS Management Frame Protection (MFP) settings, use the **debug wps mfp** command.

debug wps mfp {**client** | **capwap** | **detail** | **report** | **mm**} {**enable** | **disable**}

Syntax Description

client	Configures the debugging for client MFP messages.
capwap	Configures the debugging for MFP messages between the controller and access points.
detail	Configures the detailed debugging for MFP messages.
report	Configures the debugging for MFP reporting.
mm	Configures the debugging for MFP mobility (inter-controller) messages.
enable	Enables the debugging for WPS MFP settings.
disable	Disables the debugging for WPS MFP settings.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the debugging of WPS MFP settings:

```
(Cisco Controller) > debug wps mfp detail enable
```

Related Commands

debug disable-all

debug wps sig

eping

To test the mobility Ethernet over IP (EoIP) data packet communication between two controllers, use the **eping** command.

eping *mobility_peer_IP_address*

Syntax Description

mobility_peer_IP_address	IP address of a controller that belongs to a mobility group.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.0	This command supports only IPv4 address format.

Usage Guidelines

This command tests the mobility data traffic over the management interface.

Note This ping test is not Internet Control Message Protocol (ICMP) based. The term “ping” is used to indicate an echo request and an echo reply message.

The IPv6 address format for this command is not supported.

The following example shows how to test EoIP data packets and to set the IP address of a controller that belongs to a mobility group to 172.12.35.31:

```
(Cisco Controller) >eping 172.12.35.31
```

mping

To test mobility UDP control packet communication between two controllers, use the **mping** command.

mping *mobility_peer_IP_address*

Syntax Description

mobility_peer_IP_address	IP address of a controller that belongs to a mobility group.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Release	Modification
8.0	This command supports both IPv4 and IPv6 address formats.

Usage Guidelines

This test runs over mobility UDP port 16666. It tests whether the mobility control packet can be reached over the management interface.

Note This ping test is not Internet Control Message Protocol (ICMP) based. The term “ping” is used to indicate an echo request and an echo reply message.

The following example shows how to test mobility UDP control packet communications and to set the IP address of a controller that belongs to a mobility group to 172.12.35.31:

```
(Cisco Controller) >mping 172.12.35.31
```