



## Security Commands

---

- [clear acl counters](#), on page 6
- [clear radius acct statistics](#), on page 7
- [clear tacacs auth statistics](#), on page 8
- [clear stats local-auth](#), on page 9
- [clear stats radius](#), on page 10
- [clear stats tacacs](#), on page 11
- [config 802.11b preamble](#), on page 12
- [config aaa auth](#), on page 13
- [config aaa auth mgmt](#), on page 14
- [config acl apply](#), on page 15
- [config acl counter](#), on page 16
- [config acl create](#), on page 17
- [config acl cpu](#), on page 18
- [config acl delete](#), on page 19
- [config acl rule](#), on page 20
- [config auth-list add](#), on page 22
- [config auth-list ap-policy](#), on page 23
- [config auth-list delete](#), on page 24
- [config advanced eap](#), on page 25
- [config advanced timers auth-timeout](#), on page 27
- [config advanced timers eap-timeout](#), on page 28
- [config advanced timers eap-identity-request-delay](#), on page 29
- [config cts sxp](#), on page 30
- [config database size](#), on page 31
- [config dhcp opt-82 format](#), on page 32
- [config dhcp opt-82 remote-id](#), on page 33
- [config exclusionlist](#), on page 34
- [config ldap](#), on page 35
- [config local-auth active-timeout](#), on page 37
- [config local-auth eap-profile](#), on page 38
- [config local-auth method fast](#), on page 40
- [config local-auth user-credentials](#), on page 42
- [config ipv6 acl](#), on page 43

- [config netuser add](#) , on page 45
- [config netuser delete](#), on page 47
- [config netuser description](#), on page 48
- [config network bridging-shared-secret](#), on page 49
- [config network web-auth captive-bypass](#), on page 50
- [config network web-auth port](#), on page 51
- [config network web-auth proxy-redirect](#), on page 52
- [config network web-auth secureweb](#), on page 53
- [config network webmode](#), on page 54
- [config network web-auth](#), on page 55
- [config radius acct](#), on page 56
- [config radius acct ipsec authentication](#), on page 59
- [config radius acct ipsec disable](#), on page 60
- [config radius acct ipsec enable](#), on page 61
- [config radius acct ipsec encryption](#), on page 62
- [config radius acct ipsec ike](#), on page 63
- [config radius acct mac-delimiter](#), on page 64
- [config radius acct network](#), on page 65
- [config radius acct retransmit-timeout](#), on page 66
- [config radius auth](#), on page 67
- [config radius auth callStationIdType](#), on page 69
- [config radius auth IPsec authentication](#), on page 71
- [config radius auth ipsec disable](#), on page 72
- [config radius auth ipsec encryption](#), on page 73
- [config radius auth ipsec ike](#), on page 74
- [config radius auth keywrap](#), on page 76
- [config radius auth mac-delimiter](#), on page 77
- [config radius auth management](#), on page 78
- [config radius auth mgmt-retransmit-timeout](#), on page 79
- [config radius auth network](#), on page 80
- [config radius auth retransmit-timeout](#), on page 81
- [config radius auth rfc3576](#), on page 82
- [config radius auth retransmit-timeout](#), on page 83
- [config radius aggressive-failover disabled](#), on page 84
- [config radius backward compatibility](#), on page 85
- [config radius callStationIdCase](#), on page 86
- [config radius callStationIdType](#), on page 87
- [config radius fallback-test](#), on page 89
- [config rogue adhoc](#), on page 91
- [config rogue ap classify](#), on page 94
- [config rogue ap friendly](#), on page 96
- [config rogue ap rldp](#), on page 98
- [config rogue ap ssid](#), on page 100
- [config rogue ap timeout](#), on page 102
- [config rogue auto-contain level](#), on page 103
- [config rogue ap valid-client](#), on page 105

- [config rogue client](#), on page 107
- [config rogue detection](#), on page 109
- [config rogue detection min-rssi](#), on page 110
- [config rogue detection monitor-ap](#), on page 111
- [config rogue rule](#), on page 113
- [config tacacs acct](#), on page 117
- [config tacacs athr](#), on page 119
- [config tacacs athr mgmt-server-timeout](#), on page 121
- [config tacacs auth](#), on page 122
- [config tacacs auth mgmt-server-timeout](#), on page 124
- [config wps ap-authentication](#), on page 125
- [config wps auto-immune](#), on page 126
- [config wps cids-sensor](#), on page 127
- [config wps client-exclusion](#), on page 129
- [config wps mfp](#), on page 130
- [config wps shun-list re-sync](#), on page 131
- [config wps signature](#), on page 132
- [config wps signature frequency](#), on page 134
- [config wps signature interval](#), on page 135
- [config wps signature mac-frequency](#), on page 136
- [config wps signature quiet-time](#), on page 137
- [config wps signature reset](#), on page 138
- [debug 11w-pmf](#), on page 139
- [debug aaa](#), on page 140
- [debug aaa local-auth](#), on page 141
- [debug bcast](#), on page 143
- [debug cckm](#), on page 144
- [debug cts xp](#), on page 145
- [debug dot1x](#), on page 146
- [debug dtls](#), on page 147
- [debug nac](#), on page 148
- [debug pm](#), on page 149
- [debug web-auth](#), on page 151
- [debug wips](#), on page 152
- [debug wps sig](#), on page 153
- [debug wps mfp](#), on page 154
- [show 802.11](#), on page 155
- [show aaa auth](#), on page 157
- [show acl](#), on page 158
- [show advanced eap](#), on page 160
- [show database summary](#), on page 161
- [show exclusionlist](#), on page 162
- [show ike](#), on page 163
- [show IPsec](#), on page 164
- [show ipv6 acl](#), on page 166
- [show ipv6 summary](#), on page 167

- [show l2tp](#), on page 168
- [show ldap](#), on page 169
- [show ldap statistics](#), on page 170
- [show ldap summary](#), on page 171
- [show local-auth certificates](#), on page 172
- [show local-auth config](#), on page 173
- [show local-auth statistics](#), on page 175
- [show nac statistics](#), on page 177
- [show nac summary](#), on page 178
- [show netuser](#), on page 179
- [show netuser guest-roles](#), on page 180
- [show network](#), on page 181
- [show network summary](#), on page 182
- [show ntp-keys](#), on page 184
- [show radius acct statistics](#), on page 185
- [show radius auth statistics](#), on page 186
- [show radius summary](#), on page 187
- [show rules](#), on page 188
- [show switchconfig](#), on page 189
- [show rogue adhoc custom summary](#), on page 190
- [show rogue adhoc detailed](#), on page 191
- [show rogue adhoc friendly summary](#) , on page 192
- [show rogue adhoc malicious summary](#), on page 193
- [show rogue adhoc unclassified summary](#) , on page 194
- [show rogue adhoc summary](#), on page 195
- [show rogue ap custom summary](#) , on page 196
- [show rogue ap clients](#), on page 198
- [show rogue ap detailed](#), on page 200
- [show rogue ap summary](#), on page 203
- [show rogue ap friendly summary](#), on page 206
- [show rogue ap malicious summary](#), on page 208
- [show rogue ap unclassified summary](#), on page 210
- [show rogue auto-contain](#), on page 211
- [show rogue client detailed](#), on page 212
- [show rogue client summary](#), on page 213
- [show rogue ignore-list](#), on page 214
- [show rogue rule detailed](#), on page 216
- [show rogue rule summary](#), on page 218
- [show tacacs acct statistics](#), on page 219
- [show tacacs athr statistics](#), on page 220
- [show tacacs auth statistics](#), on page 221
- [show tacacs summary](#), on page 222
- [show wps ap-authentication summary](#), on page 223
- [show wps cids-sensor](#), on page 224
- [show wps mfp](#), on page 225
- [show wps shun-list](#), on page 226

- [show wps signature detail, on page 227](#)
- [show wps signature events, on page 228](#)
- [show wps signature summary, on page 230](#)
- [show wps summary, on page 232](#)
- [show wps wips statistics, on page 234](#)
- [show wps wips summary, on page 235](#)

## 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*

<b>Syntax Description</b>	<i>acl_name</i>	ACL name.
<b>Command Default</b>	None	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	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 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**]

<b>Syntax Description</b>	<b>index</b>	(Optional) Specifies the index of the RADIUS accounting server.
	<b>all</b>	(Optional) Specifies all RADIUS accounting servers.

**Command Default** None

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	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**]

<b>Syntax Description</b>	<b>index</b>	(Optional) Specifies the index of the RADIUS authentication server.
	<b>all</b>	(Optional) Specifies all RADIUS authentication servers.
<b>Command Default</b>	None	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	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 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

---

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	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 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		
	<b>auth</b>	Clears statistics regarding authentication.
	<b>acct</b>	Clears statistics regarding accounting.
	<b>index</b>	Specifies the index number of the RADIUS server to be cleared.
	<b>all</b>	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		
<b>auth</b>	(Optional) Clears the TACACS+ authentication server statistics.	
<b>athr</b>	(Optional) Clears the TACACS+ authorization server statistics.	
<b>acct</b>	(Optional) Clears the TACACS+ accounting server statistics.	
<b>index</b>	(Optional) Specifies index of the TACACS+ server.	
<b>all</b>	(Optional) Specifies all TACACS+ servers.	
<b>Command Default</b>	None	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	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**

## config 802.11b preamble

To change the 802.11b preamble as defined in subclause 18.2.2.2 to **long** (slower, but more reliable) or **short** (faster, but less reliable), use the **config 802.11b preamble** command.

**config 802.11b preamble** {long | short}

Syntax Description		
	<b>long</b>	Specifies the long 802.11b preamble.
	<b>short</b>	Specifies the short 802.11b preamble.

**Command Default** The default 802.11b preamble value is short.

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

### Usage Guidelines



**Note** You must reboot the Cisco Wireless LAN Controller (reset system) with save to implement this command.

This parameter must be set to **long** to optimize this Cisco wireless LAN controller for some clients, including SpectraLink NetLink telephones.

This command can be used any time that the CLI interface is active.

The following example shows how to change the 802.11b preamble to short:

```
(Cisco Controller) >config 802.11b preamble short
(Cisco Controller) >(reset system with save)
```

## config aaa auth

To configure the AAA authentication search order for management users, use the **config aaa auth** command.

```
config aaa auth mgmt [aaa_server_type1 | aaa_server_type2]
```

<b>Syntax Description</b>	<p><b>mgmt</b> Configures the AAA authentication search order for controller management users by specifying up to three AAA authentication server types. The order that the server types are entered specifies the AAA authentication search order.</p> <hr/> <p><i>aaa_server_type</i> (Optional) AAA authentication server type (<b>local</b>, <b>radius</b>, or <b>tacacs</b>). The <b>local</b> setting specifies the local database, the <b>radius</b> setting specifies the RADIUS server, and the <b>tacacs</b> setting specifies the TACACS+ server.</p>				
<b>Command Default</b>	None				
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>7.6</td> <td>This command was introduced in a release earlier than Release 7.6.</td> </tr> </tbody> </table>	Release	Modification	7.6	This command was introduced in a release earlier than Release 7.6.
Release	Modification				
7.6	This command was introduced in a release earlier than Release 7.6.				
<b>Usage Guidelines</b>	<p>You can enter two AAA server types as long as one of the server types is <b>local</b>. You cannot enter <b>radius</b> and <b>tacacs</b> together.</p> <p>The following example shows how to configure the AAA authentication search order for controller management users by the authentication server type local:</p> <pre>(Cisco Controller) &gt; config aaa auth radius local</pre>				
<b>Related Commands</b>	<b>show aaa auth</b>				

## config aaa auth mgmt

To configure the order of authentication when multiple databases are configured, use the **config aaa auth mgmt** command.

**config aaa auth mgmt** [**radius** | **tacacs**]

<b>Syntax Description</b>	<b>radius</b>	(Optional) Configures the order of authentication for RADIUS servers.
	<b>tacacs</b>	(Optional) Configures the order of authentication for TACACS servers.
<b>Command Default</b>	None	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the order of authentication for the RADIUS server:

```
(Cisco Controller) > config aaa auth mgmt radius
```

The following example shows how to configure the order of authentication for the TACACS server:

```
(Cisco Controller) > config aaa auth mgmt tacacs
```

**Related Commands**    **show aaa auth order**

# config acl apply

To apply an access control list (ACL) to the data path, use the **config acl apply** command.

**config acl apply** *rule\_name*

<b>Syntax Description</b>	<i>rule_name</i>	ACL name that contains up to 32 alphanumeric characters.
<b>Command Default</b>	None	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.

## Example

The following example shows how to apply an ACL to the data path:

```
(Cisco Controller) > config acl apply acl01
```

## config acl counter

To see if packets are hitting any of the access control lists (ACLs) configured on your controller, use the **config acl counter** command.

**config acl counter** { **start** | **stop** }

Syntax Description		
	<b>start</b>	Enables ACL counters on your controller.
	<b>stop</b>	Disables ACL counters on your controller.

**Command Default** None

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

**Usage Guidelines** ACL counters are available only on the following controllers: 4400 series, Cisco WiSM, and Catalyst 3750G Integrated Wireless LAN Controller Switch.

The following example shows how to enable ACL counters on your controller:

```
(Cisco Controller) > config acl counter start
```

**Related Commands**

- clear acl counters**
- show acl detailed**

# config acl create

To create a new access control list (ACL), use the **config acl create** command.

**config acl create** *rule\_name*

<b>Syntax Description</b>	<i>rule_name</i>	ACL name that contains up to 32 alphanumeric characters.
<b>Command Default</b>	None	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.
<b>Usage Guidelines</b>	<p>For a Cisco 2100 Series Wireless LAN Controller, you must configure a preauthentication ACL on the wireless LAN for the external web server. This ACL should then be set as a wireless LAN preauthentication ACL under Web Policy. However, you do not need to configure any preauthentication ACL for Cisco 4400 Series Wireless LAN Controllers.</p> <p>The following example shows how to create a new ACL:</p> <pre>(Cisco Controller) &gt; config acl create ac101</pre>	
<b>Related Commands</b>	show acl	

# config acl cpu

To create a new access control list (ACL) rule that restricts the traffic reaching the CPU, use the **config acl cpu** command.

```
config acl cpu rule_name { wired | wireless | both }
```

Syntax Description		
	<i>rule_name</i>	Specifies the ACL name.
	<b>wired</b>	Specifies an ACL on wired traffic.
	<b>wireless</b>	Specifies an ACL on wireless traffic.
	<b>both</b>	Specifies an ACL on both wired and wireless traffic.

**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 allows you to control the type of packets reaching the CPU.

The following example shows how to create an ACL named `acl101` on the CPU and apply it to wired traffic:

```
(Cisco Controller) > config acl cpu acl101 wired
```

**Related Commands** `show acl cpu`

# config acl delete

To delete an access control list (ACL), use the **config acl delete** command.

**config acl delete** *rule\_name*

<b>Syntax Description</b>	<i>rule_name</i>	ACL name that contains up to 32 alphanumeric characters.
<b>Command Default</b>	None	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.
<b>Usage Guidelines</b>	<p>For a Cisco 2100 Series Wireless LAN Controller, you must configure a preauthentication ACL on the wireless LAN for the external web server. This ACL should then be set as a wireless LAN preauthentication ACL under Web Policy. However, you do not need to configure any preauthentication ACL for Cisco 4400 Series Wireless LAN Controllers.</p> <p>The following example shows how to delete an ACL named acl101 on the CPU:</p> <pre>(Cisco Controller) &gt; config acl delete acl101</pre>	
<b>Related Commands</b>	show acl	

## config acl rule

To configure ACL rules, use the **config acl rule** command.

```
config acl rule { action rule_name rule_index { permit | deny } | add rule_name rule_index |
change index rule_name old_index new_index | delete rule_name rule_index | destination address
rule_name rule_index ip_address netmask | destination port range rule_name rule_index start_port
end_port | direction rule_name rule_index { in | out | any } | dscp rule_name rule_index dscp
| protocol rule_name rule_index protocol | source address rule_name rule_index ip_address netmask
| source port range rule_name rule_index start_port end_port | swap index rule_name index_1 index_2 }
```

### Syntax Description

<b>action</b>	Configures whether to permit or deny access.
<i>rule_name</i>	ACL name that contains up to 32 alphanumeric characters.
<i>rule_index</i>	Rule index between 1 and 32.
<b>permit</b>	Permits the rule action.
<b>deny</b>	Denies the rule action.
<b>add</b>	Adds a new rule.
<b>change</b>	Changes a rule's index.
<b>index</b>	Specifies a rule index.
<b>delete</b>	Deletes a rule.
<b>destination address</b>	Configures a rule's destination IP address and netmask.
<b>destination port range</b>	Configure a rule's destination port range.
<i>ip_address</i>	IP address of the rule.
<i>netmask</i>	Netmask of the rule.
<i>start_port</i>	Start port number (between 0 and 65535).
<i>end_port</i>	End port number (between 0 and 65535).
<b>direction</b>	Configures a rule's direction to in, out, or any.
<b>in</b>	Configures a rule's direction to in.
<b>out</b>	Configures a rule's direction to out.
<b>any</b>	Configures a rule's direction to any.
<b>dscp</b>	Configures a rule's DSCP.

<i>dscp</i>	Number between 0 and 63, or <b>any</b> .
<b>protocol</b>	Configures a rule's DSCP.
<i>protocol</i>	Number between 0 and 255, or <b>any</b> .
<b>source address</b>	Configures a rule's source IP address and netmask.
<b>source port range</b>	Configures a rule's source port range.
<b>swap</b>	Swaps two rules' indices.

**Command Default**

None

**Command History**

<b>Release</b>	<b>Modification</b>
7.6	This command was introduced in a release earlier than Release 7.6.

**Usage Guidelines**

For a Cisco 2100 Series Wireless LAN Controller, you must configure a preauthentication ACL on the wireless LAN for the external web server. This ACL should then be set as a wireless LAN pre-authentication ACL under Web Policy. However, you do not need to configure any preauthentication ACL for Cisco 4400 Series Wireless LAN Controllers.

The following example shows how to configure an ACL to permit access:

```
(Cisco Controller) > config acl rule action lab1 4 permit
```

**Related Commands**

show acl

## config auth-list add

To create an authorized access point entry, use the **config auth-list add** command.

```
config auth-list add { mic | ssc } AP_MAC [AP_key]
```

Syntax Description	mic	Specifies that the access point has a manufacture-installed certificate.
	ssc	Specifies that the access point has a self-signed certificate.
	AP_MAC	MAC address of a Cisco lightweight access point.
	AP_key	(Optional) Key hash value that is equal to 20 bytes or 40 digits.
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 create an authorized access point entry with a manufacturer-installed certificate on MAC address 00:0b:85:02:0d:20:

```
(Cisco Controller) > config auth-list add 00:0b:85:02:0d:20
```

Related Commands	config auth-list delete
	config auth-list ap-policy

## config auth-list ap-policy

To configure an access point authorization policy, use the **config auth-list ap-policy** command.

```
config auth-list ap-policy {authorize-ap {enable | disable} | ssc {enable | disable}}
```

Syntax Description		
<b>authorize-ap enable</b>		Enables the authorization policy.
<b>authorize-ap disable</b>		Disables the AP authorization policy.
<b>ssc enable</b>		Allows the APs with self-signed certificates to connect.
<b>ssc disable</b>		Disallows the APs with self-signed certificates to connect.
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 an access point authorization policy:

```
(Cisco Controller) > config auth-list ap-policy authorize-ap enable
```

The following example shows how to enable an access point with a self-signed certificate to connect:

```
(Cisco Controller) > config auth-list ap-policy ssc disable
```

Related Commands
<b>config auth-list delete</b>
<b>config auth-list add</b>

## config auth-list delete

To delete an access point entry, use the **config auth-list delete** command.

**config auth-list delete** *AP\_MAC*

<b>Syntax Description</b>	<i>AP_MAC</i>	MAC address of a Cisco lightweight access point.
<b>Command Default</b>	None	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to delete an access point entry for MAC address 00:1f:ca:cf:b6:60:

```
(Cisco Controller) > config auth-list delete 00:1f:ca:cf:b6:60
```

<b>Related Commands</b>	<b>config auth-list delete</b>
	<b>config auth-list add</b>
	<b>config auth-list ap-policy</b>

## config advanced eap

To configure advanced extensible authentication protocol (EAP) settings, use the **config advanced eap** command.

```
config advanced eap { bcast-key-interval seconds | eapol-key-timeout timeout | eapol-key-retries
retries | identity-request-timeout timeout | identity-request-retries retries | key-index index |
max-login-ignore-identity-response { enable | disable } request-timeout timeout | request-retries
retries } }
```

Syntax Description		
<b>bcast-key-interval</b> <i>seconds</i>		Specifies the EAP-broadcast key renew interval time in seconds.  The range is from 120 to 86400 seconds.
<b>eapol-key-timeout</b> <i>timeout</i>		Specifies the amount of time (200 to 5000 milliseconds) that the controller waits before retransmitting an EAPOL (WPA) key message to a wireless client using EAP or WPA/WPA-2 PSK.  The default value is 1000 milliseconds.
<b>eapol-key-retries</b> <i>retries</i>		Specifies the maximum number of times (0 to 4 retries) that the controller retransmits an EAPOL (WPA) key message to a wireless client.  The default value is 2.
<b>identity-request- timeout</b> <i>timeout</i>		Specifies the amount of time (1 to 120 seconds) that the controller waits before retransmitting an EAP Identity Request message to a wireless client.  The default value is 30 seconds.
<b>identity-request- retries</b>		Specifies the maximum number of times (0 to 4 retries) that the controller retransmits an EAPOL (WPA) key message to a wireless client.  The default value is 2.
<b>key-index</b> <i>index</i>		Specifies the key index (0 or 3) used for dynamic wired equivalent privacy (WEP).

<b>max-login-ignore-identity-response</b>	<p>When enabled, this command ignores the limit set for the number of devices that can be connected to the controller with the same username using 802.1x authentication. When disabled, this command limits the number of devices that can be connected to the controller with the same username. This option is not applicable for Web auth user.</p> <p>Use the command <b>config netuser maxUserLogin</b> to set the limit of maximum number of devices per same username</p>
<b>enable</b>	<p>Ignores the same username reaching the maximum EAP identity response.</p>
<b>disable</b>	<p>Checks the same username reaching the maximum EAP identity response.</p>
<b>request-timeout</b>	<p>For EAP messages other than Identity Requests or EAPOL (WPA) key messages, specifies the amount of time (1 to 120 seconds) that the controller waits before retransmitting the message to a wireless client.</p> <p>The default value is 30 seconds.</p>
<b>request-retries</b>	<p>(Optional) For EAP messages other than Identity Requests or EAPOL (WPA) key messages, specifies the maximum number of times (0 to 20 retries) that the controller retransmits the message to a wireless client.</p> <p>The default value is 2.</p>

**Command Default** None

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the key index used for dynamic wired equivalent privacy (WEP):

```
(Cisco Controller) > config advanced eap key-index 0
```

## config advanced timers auth-timeout

To configure the authentication timeout, use the **config advanced timers auth-timeout** command.

**config advanced timers auth-timeout** *seconds*

<b>Syntax Description</b>	<i>seconds</i>	Authentication response timeout value in seconds between 10 and 600.
<b>Command Default</b>	The default authentication timeout value is 10 seconds.	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the authentication timeout to 20 seconds:

```
(Cisco Controller) >config advanced timers auth-timeout 20
```

## config advanced timers eap-timeout

To configure the Extensible Authentication Protocol (EAP) expiration timeout, use the **config advanced timers eap-timeout** command.

**config advanced timers eap-timeout** *seconds*

<b>Syntax Description</b>	<i>seconds</i>	EAP timeout value in seconds between 8 and 120.
<b>Command Default</b>	None	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the EAP expiration timeout to 10 seconds:

```
(Cisco Controller) >config advanced timers eap-timeout 10
```

## config advanced timers eap-identity-request-delay

To configure the advanced Extensible Authentication Protocol (EAP) identity request delay in seconds, use the **config advanced timers eap-identity-request-delay** command.

**config advanced timers eap-identity-request-delay** *seconds*

<b>Syntax Description</b>	<i>seconds</i>	Advanced EAP identity request delay in number of seconds between 0 and 10.
<b>Command Default</b>	None	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the advanced EAP identity request delay to 8 seconds:

```
(Cisco Controller) >config advanced timers eap-identity-request-delay 8
```

## config cts sxp

To configure Cisco TrustSec SXP (CTS) connections on the controller, use the **config cts sxp** command.

```
config cts sxp {enable | disable | connection {delete | peer} | default password password |
retry period time-in-seconds}
```

Syntax Description		
<b>enable</b>		Enables CTS connections on the controller.
<b>disable</b>		Disables CTS connections on the controller.
<b>connection</b>		Configures CTS connection on the controller.
<b>delete</b>		Deletes the CTS connection on the controller.
<b>peer</b>		Configures the next hop switch with which the controller is connected.
<i>ip-address</i>		Only IPv4 address of the peer.
<b>default password</b>		Configures the default password for MD5 authentication of SXP messages.
<i>password</i>		Default password for MD5 Authentication of SXP messages. The password should contain a minimum of six characters.
<b>retry period</b>		Configures the SXP retry period.
<i>time-in-seconds</i>		Time after which a CTS connection should be again tried for after a failure to connect.

**Command Default** None

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

**Usage Guidelines** For release 8.0, only IPv4 is supported for TrustSec SXP configuration.

The following example shows how to enable CTS on the controller:

```
(Cisco Controller) > config cts sxp enable
```

The following example shows how to configure a peer for a CTS connection:

```
> config cts sxp connection peer 209.165.200.224
```

**Related Commands** **debug cts sxp**

## config database size

To configure the local database, use the **config database size** command.

**config database size** *count*

<b>Syntax Description</b>	<i>count</i>	Database size value between 512 and 2040
<b>Command Default</b>	None	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.
<b>Usage Guidelines</b>	<p>Use the <b>show database</b> command to display local database configuration.</p> <p>The following example shows how to configure the size of the local database:</p> <pre>(Cisco Controller) &gt; config database size 1024</pre>	
<b>Related Commands</b>	<b>show database</b>	

## config dhcp opt-82 format

To configure the DHCP option 82 format, use the **config dhcp opt-82 format** command.

```
config dhcp opt-82 format { binary | ascii }
```

<b>Syntax Description</b>	<i>binary</i>	Specifies the DHCP option 82 format as binary.
	<i>ascii</i>	Specifies the DHCP option 82 format as ASCII.
<b>Command Default</b>	None	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the format of DHCP option 82 payload:

```
(Cisco Controller) > config dhcp opt-82 format binary
```

## config dhcp opt-82 remote-id

To configure the format of the DHCP option 82 payload, use the **config dhcp opt-82 remote-id** command.

```
config dhcp opt-82 remote-id {ap_mac | ap_mac:ssid | ap-ethmac | apname:ssid | ap-group-name
| flex-group-name | ap-location | apmac-vlan-id | apname-vlan-id | ap-ethmac-ssid}
```

Syntax	Description
<i>ap_mac</i>	Specifies the radio MAC address of the access point to the DHCP option 82 payload.
<i>ap_mac:ssid</i>	Specifies the radio MAC address and SSID of the access point to the DHCP option 82 payload.
<i>ap-ethmac</i>	Specifies the Ethernet MAC address of the access point to the DHCP option 82 payload.
<i>apname:ssid</i>	Specifies the AP name and SSID of the access point to the DHCP option 82 payload.
<i>ap-group-name</i>	Specifies the AP group name to the DHCP option 82 payload.
<i>flex-group-name</i>	Specifies the FlexConnect group name to the DHCP option 82 payload.
<i>ap-location</i>	Specifies the AP location to the DHCP option 82 payload.
<i>apmac-vlan-id</i>	Specifies the radio MAC address of the access point and the VLAN ID to the DHCP option 82 payload.
<i>apname-vlan-id</i>	Specifies the AP name and its VLAN ID to the DHCP option 82 payload.
<i>ap-ethmac-ssid</i>	Specifies the Ethernet MAC address of the access point and the SSID to the DHCP option 82 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 configure the remote ID of DHCP option 82 payload:

```
(Cisco Controller) > config dhcp opt-82 remote-id apgroup1
```

## config exclusionlist

To create or delete an exclusion list entry, use the **config exclusionlist** command.

```
config exclusionlist {add MAC [description] | delete MAC | description MAC [description] }
```

### Syntax Description

<b>config exclusionlist</b>	Configures the exclusion list.
<b>add</b>	Creates a local exclusion-list entry.
<b>delete</b>	Deletes a local exclusion-list entry
<b>description</b>	Specifies the description for an exclusion-list entry.
<i>MAC</i>	MAC address of the local Excluded entry.
<i>description</i>	(Optional) Description, up to 32 characters, for an excluded entry.

### 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 create a local exclusion list entry for the MAC address `xx:xx:xx:xx:xx:xx`:

```
(Cisco Controller) > config exclusionlist add xx:xx:xx:xx:xx:xx lab
```

The following example shows how to delete a local exclusion list entry for the MAC address `xx:xx:xx:xx:xx:xx`:

```
(Cisco Controller) > config exclusionlist delete xx:xx:xx:xx:xx:xx lab
```

### Related Commands

**show exclusionlist**

# config ldap

To configure the Lightweight Directory Access Protocol (LDAP) server settings, use the **config ldap** command.

```
config ldap {add | delete | enable | disable | retransmit-timeout | retry | user | simple-bind} index
```

```
config ldap add index server_ip_address port user_base user_attr user_type [ ]
```

```
config ldap retransmit-timeout index retransmit-timeout
```

```
config ldap retry attempts
```

```
config ldap user {attr index user-attr | base index user-base | typeindex user-type}
```

```
config ldap simple-bind {anonymous index | authenticated index username password}
```

## Syntax Description

<b>add</b>	Specifies that an LDAP server is being added.
<b>delete</b>	Specifies that an LDAP server is being deleted.
<b>enable</b>	Specifies that an LDAP server is enabled.
<b>disable</b>	Specifies that an LDAP server is disabled.
<b>retransmit-timeout</b>	Changes the default retransmit timeout for an LDAP server.
<b>retry</b>	Configures the retry attempts for an LDAP server.
<b>user</b>	Configures the user search parameters.
<b>simple-bind</b>	Configures the local authentication bind method.
<b>anonymous</b>	Allows anonymous access to the LDAP server.
<b>authenticated</b>	Specifies that a username and password be entered to secure access to the LDAP server.
<i>index</i>	LDAP server index. The range is from 1 to 17.
<i>server_ip_address</i>	IP address of the LDAP server.
<i>port</i>	Port number.
<i>user_base</i>	Distinguished name for the subtree that contains all of the users.
<i>user_attr</i>	Attribute that contains the username.
<i>user_type</i>	ObjectType that identifies the user.

<i>retransmit-timeout</i>	Retransmit timeout for an LDAP server. The range is from 2 to 30.
<i>attempts</i>	Number of attempts that each LDAP server is retried.
<b>attr</b>	Configures the attribute that contains the username.
<b>base</b>	Configures the distinguished name of the subtree that contains all the users.
<b>type</b>	Configures the user type.
<i>username</i>	Username for the authenticated bind method.
<i>password</i>	Password for the authenticated bind method.

**Command Default**

None

**Command History**

<b>Release</b>	<b>Modification</b>
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable LDAP server index 10:

```
(Cisco Controller) > config ldap enable 10
```

**Related Commands**

**config ldap add**  
**config ldap simple-bind**  
**show ldap summary**

## config local-auth active-timeout

To specify the amount of time in which the controller attempts to authenticate wireless clients using local Extensible Authentication Protocol (EAP) after any pair of configured RADIUS servers fails, use the **config local-auth active-timeout** command.

**config local-auth active-timeout** *timeout*

<b>Syntax Description</b>	<i>timeout</i>	Timeout measured in seconds. The range is from 1 to 3600.
<b>Command Default</b>	The default timeout value is 100 seconds.	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to specify the active timeout to authenticate wireless clients using EAP to 500 seconds:

```
(Cisco Controller) > config local-auth active-timeout 500
```

<b>Related Commands</b>	<b>clear stats local-auth</b> <b>config local-auth eap-profile</b> <b>config local-auth method fast</b> <b>config local-auth user-credentials</b> <b>debug aaa local-auth</b> <b>show local-auth certificates</b> <b>show local-auth config</b> <b>show local-auth statistics</b>
-------------------------	--

## config local-auth eap-profile

To configure local Extensible Authentication Protocol (EAP) authentication profiles, use the **config local-auth eap-profile** command.

```
config local-auth eap-profile { [add | delete] profile_name | cert-issuer { cisco | vendor } |
method method local-cert { enable | disable } profile_name | method method client-cert { enable |
disable } profile_name | method method peer-verify ca-issuer { enable | disable } | method method
peer-verify cn-verify { enable | disable } | method method peer-verify date-valid { enable | disable }
```

### Syntax Description

<b>add</b>	(Optional) Specifies that an EAP profile or method is being added.
<b>delete</b>	(Optional) Specifies that an EAP profile or method is being deleted.
<i>profile_name</i>	EAP profile name (up to 63 alphanumeric characters). Do not include spaces within a profile name.
<b>cert-issuer</b>	(For use with EAP-TLS, PEAP, or EAP-FAST with certificates) Specifies the issuer of the certificates that will be sent to the client. The supported certificate issuers are Cisco or a third-party vendor.
<b>cisco</b>	Specifies the Cisco certificate issuer.
<b>vendor</b>	Specifies the third-party vendor.
<b>method</b>	Configures an EAP profile method.
<i>method</i>	EAP profile method name. The supported methods are leap, fast, tls, and peap.
<b>local-cert</b>	(For use with EAP-FAST) Specifies whether the device certificate on the controller is required for authentication.
<b>enable</b>	Specifies that the parameter is enabled.
<b>disable</b>	Specifies that the parameter is disabled.
<b>client-cert</b>	(For use with EAP-FAST) Specifies whether wireless clients are required to send their device certificates to the controller in order to authenticate.
<b>peer-verify</b>	Configures the peer certificate verification options.
<b>ca-issuer</b>	(For use with EAP-TLS or EAP-FAST with certificates) Specifies whether the incoming certificate from the client is to be validated against the Certificate Authority (CA) certificates on the controller.

<b>cn-verify</b>	(For use with EAP-TLS or EAP-FAST with certificates) Specifies whether the common name (CN) in the incoming certificate is to be validated against the CA certificates' CN on the controller.
<b>date-valid</b>	(For use with EAP-TLS or EAP-FAST with certificates) Specifies whether the controller is to verify that the incoming device certificate is still valid and has not expired.

**Command Default**

None

**Command History**

<b>Release</b>	<b>Modification</b>
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to create a local EAP profile named FAST01:

```
(Cisco Controller) > config local-auth eap-profile add FAST01
```

The following example shows how to add the EAP-FAST method to a local EAP profile:

```
(Cisco Controller) > config local-auth eap-profile method add fast FAST01
```

The following example shows how to specify Cisco as the issuer of the certificates that will be sent to the client for an EAP-FAST profile:

```
(Cisco Controller) > config local-auth eap-profile method fast cert-issuer cisco
```

The following example shows how to specify that the incoming certificate from the client be validated against the CA certificates on the controller:

```
(Cisco Controller) > config local-auth eap-profile method fast peer-verify ca-issuer enable
```

**Related Commands**

**config local-auth active-timeout**  
**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**

## config local-auth method fast

To configure an EAP-FAST profile, use the **config local-auth method fast** command.

```
config local-auth method fast {anon-prov [enable | disable] | authority-id auth_id pac-ttl days
| server-key key_value}
```

Syntax Description		
<b>anon-prov</b>		Configures the controller to allow anonymous provisioning, which allows PACs to be sent automatically to clients that do not have one during Protected Access Credentials (PAC) provisioning.
<b>enable</b>		(Optional) Specifies that the parameter is enabled.
<b>disable</b>		(Optional) Specifies that the parameter is disabled.
<b>authority-id</b>		Configures the authority identifier of the local EAP-FAST server.
<i>auth_id</i>		Authority identifier of the local EAP-FAST server (2 to 32 hexadecimal digits).
<b>pac-ttl</b>		Configures the number of days for the Protected Access Credentials (PAC) to remain viable (also known as the time-to-live [TTL] value).
<i>days</i>		Time-to-live value (TTL) value (1 to 1000 days).
<b>server-key</b>		Configures the server key to encrypt or decrypt PACs.
<i>key_value</i>		Encryption key value (2 to 32 hexadecimal digits).
<b>Command Default</b>	None	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to disable the controller to allows anonymous provisioning:

```
(Cisco Controller) > config local-auth method fast anon-prov disable
```

The following example shows how to configure the authority identifier 0125631177 of the local EAP-FAST server:

```
(Cisco Controller) > config local-auth method fast authority-id 0125631177
```

The following example shows how to configure the number of days to 10 for the PAC to remain viable:

```
(Cisco Controller) > config local-auth method fast pac-ttl 10
```

---

**Related Commands**

**clear stats local-auth**  
**config local-auth eap-profile**  
**config local-auth active-timeout**  
**config local-auth user-credentials**  
**debug aaa local-auth**  
**show local-auth certificates**  
**show local-auth config**  
**show local-auth statistics**

## config local-auth user-credentials

To configure the local Extensible Authentication Protocol (EAP) authentication database search order for user credentials, use the **config local-auth user-credentials** command.

```
config local-auth user-credentials { local [ldap] | ldap [local] }
```

<b>Syntax Description</b>	<b>local</b>	Specifies that the local database is searched for the user credentials.
	<b>ldap</b>	(Optional) Specifies that the Lightweight Directory Access Protocol (LDAP) database is searched for the user credentials.

<b>Command Default</b>	None
------------------------	------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.

**Usage Guidelines** The order of the specified database parameters indicate the database search order.

The following example shows how to specify the order in which the local EAP authentication database is searched:

```
(Cisco Controller) > config local-auth user credentials local lda
```

In the above example, the local database is searched first and then the LDAP database.

<b>Related Commands</b>	<b>clear stats local-auth</b>
	<b>config local-auth eap-profile</b>
	<b>config local-auth method fast</b>
	<b>config local-auth active-timeout</b>
	<b>debug aaa local-auth</b>
	<b>show local-auth certificates</b>
	<b>show local-auth config</b>
<b>show local-auth statistics</b>	

## config ipv6 acl

To create or delete an IPv6 ACL on the Cisco wireless LAN controller, apply ACL to data path, and configure rules in the IPv6 ACL, use the **config ipv6 acl** command.

```

config ipv6 acl [apply | cpu | create | delete | rule]
config ipv6 acl apply name
config ipv6 acl cpu {name | none}
config ipv6 acl create name
config ipv6 acl delete name
config ipv6 acl rule [action | add | change | delete | destination | direction | dscp | protocol
| source | swap ]
config ipv6 acl rule action name index {permit | deny}
config ipv6 acl rule add name index
config ipv6 acl rule change index name old_index new_index
config ipv6 acl rule delete name index
config ipv6 acl rule destination {address name index ip_address prefix-len | port range name index }
config ipv6 acl rule direction name index {in | out | any}
config ipv6 acl rule dscp name dscp
config ipv6 acl rule protocol name index protocol
config ipv6 acl rule source {address name index ip_address prefix-len | port range name index
start_port end_port}
config ipv6 acl rule swap index name index_1 index_2

```

Syntax	Description
<b>apply</b> <i>name</i>	Applies an IPv6 ACL. An IPv6 ACL can contain up to 32 alphanumeric characters.
<b>cpu</b> <i>name</i>	Applies the IPv6 ACL to the CPU.
<b>cpu none</b>	Configure none if you wish not to have a IPv6 ACL.
<b>create</b>	Creates an IPv6 ACL.
<b>delete</b>	Deletes an IPv6 ACL.
<b>rule</b> ( <b>action</b> ) ( <i>name</i> ) ( <i>index</i> )	Configures rules in the IPv6 ACL to either permit or deny access. IPv6 ACL name can contain up to 32 alphanumeric characters and IPv6 ACL rule index can be between 1 and 32.
{ <b>permit</b>   <b>deny</b> }	Permit or deny the IPv6 rule action.
<b>add</b> <i>name index</i>	Adds a new rule and rule index.
<b>change</b> <i>name old_index</i> <i>new_index</i>	Changes a rule's index.
<b>delete</b> <i>name index</i>	Deletes a rule and rule index.
<b>destination</b> <b>address</b> <i>name</i> <i>index ip_addr prefix-len</i>	Configures a rule's destination IP address and prefix length (between 0 and 128).

<b>destination port</b> <i>name index</i>	Configure a rule's destination port range. Enter IPv6 ACL name and set an rule index for it.
<b>direction</b> <i>name index</i> { <b>in</b>   <b>out</b>   <b>any</b> }	Configures a rule's direction to in, out, or any.
<b>dscp</b> <i>name index dscp</i>	Configures a rule's DSCP. For rule index of DSCP, select a number between 0 and 63, or <b>any</b> .
<b>protocol</b> <i>name index protocol</i>	Configures a rule's protocol. Enter a name and set an index between 0 and 255 or <b>any</b> .
<b>source address</b> <i>name index</i> <i>ip_address prefix-len</i>	Configures a rule's source IP address and netmask.
<b>source port range</b> <i>name index</i> <i>start_port end_port</i>	Configures a rule's source port range.
<b>swap index</b> <i>name index_1</i> <i>index_2</i>	Swap's two rules' indices.

**Command Default**

After adding an ACL, the **config ipv6 acl cpu** is by default configured as **enabled**.

**Command History**

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6..
8.0	This command was updated by adding <b>cpu</b> and <b>none</b> keywords and the <i>ipv6_acl_name</i> variable.

**Usage Guidelines**

For a Cisco 2100 Series Wireless LAN Controller, you must configure a preauthentication ACL on the wireless LAN for the external web server. This ACL should then be set as a wireless LAN preauthentication ACL under Web Policy. However, you do not need to configure any preauthentication ACL for Cisco 4400 Series Wireless LAN Controllers.

The following example shows how to configure an IPv6 ACL to permit access:

```
(Cisco Controller) >config ipv6 acl rule action lab1 4 permit
```

The following example shows how to configure an interface ACL:

```
(Cisco Controller) > config ipv6 interface acl management IPv6-Acl
```

**Related Commands**

**show ipv6 acl detailed**  
**show ipv6 acl cpu**

# config netuser add

To add a guest user on a WLAN or wired guest LAN to the local user database on the controller, use the **config netuser add** command.

```
config netuser add username password { wlan wlan_id | guestlan guestlan_id } userType guest lifetime lifetime description description
```

Syntax Description		
<i>username</i>		Guest username. The username can be up to 50 alphanumeric characters.
<i>password</i>		User password. The password can be up to 24 alphanumeric characters.
<b>wlan</b>		Specifies the wireless LAN identifier to associate with or zero for any wireless LAN.
<i>wlan_id</i>		Wireless LAN identifier assigned to the user. A zero value associates the user with any wireless LAN.
<b>guestlan</b>		Specifies the guest LAN identifier to associate with or zero for any wireless LAN.
<i>guestlan_id</i>		Guest LAN ID.
<b>userType</b>		Specifies the user type.
<b>guest</b>		Specifies the guest for the guest user.
<b>lifetime</b>		Specifies the lifetime.
<i>lifetime</i>		Lifetime value (60 to 259200 or 0) in seconds for the guest user. <b>Note</b> A value of 0 indicates an unlimited lifetime.
<i>description</i>		Short description of user. The description can be up to 32 characters enclosed in double-quotes.

**Command Default** None

**Command History**

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

**Usage Guidelines** Local network usernames must be unique because they are stored in the same database.

The following example shows how to add a permanent username Jane to the wireless network for 1 hour:

```
(Cisco Controller) > config netuser add jane able2 1 wlan_id 1 userType permanent
```

The following example shows how to add a guest username George to the wireless network for 1 hour:

```
(Cisco Controller) > config netuser add george able1 guestlan 1 3600
```

---

**Related Commands**

**show netuser**

**config netuser delete**

# config netuser delete

To delete an existing user from the local network, use the **config netuser delete** command.

**config netuser delete** *username*

<b>Syntax Description</b>	<i>username</i>	Network username. The username can be up to 24 alphanumeric characters.
<b>Command Default</b>	None	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.
<b>Usage Guidelines</b>	Local network usernames must be unique because they are stored in the same database.  The following example shows how to delete an existing username named able1 from the network:  (Cisco Controller) > <b>config netuser delete able1</b> Deleted user able1	
<b>Related Commands</b>	<b>show netuser</b>	

# config netuser description

To add a description to an existing net user, use the **config netuser description** command.

**config netuser description** *username description*

## Syntax Description

*username*

Network username. The username can contain up to 24 alphanumeric characters.

*description*

(Optional) User description. The description can be up to 32 alphanumeric characters enclosed in double quotes.

## 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 user description “HQ1 Contact” to an existing network user named able 1:

```
(Cisco Controller) > config netuser description able1 "HQ1 Contact"
```

## Related Commands

**show netuser**

# config network bridging-shared-secret

To configure the bridging shared secret, use the **config network bridging-shared-secret** command.

```
config network bridging-shared-secret shared_secret
```

<b>Syntax Description</b>	<i>shared_secret</i>	Bridging shared secret string. The string can contain up to 10 bytes.
<b>Command Default</b>	The bridging shared secret is enabled by default.	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.
<b>Usage Guidelines</b>	This command creates a secret that encrypts backhaul user data for the mesh access points that connect to the switch. The zero-touch configuration must be enabled for this command to work. The following example shows how to configure the bridging shared secret string “shhh1”:  (Cisco Controller) > <b>config network bridging-shared-secret shhh1</b>	
<b>Related Commands</b>	<b>show network summary</b>	

## config network web-auth captive-bypass

To configure the controller to support bypass of captive portals at the network level, use the **config network web-auth captive-bypass** command.

```
config network web-auth captive-bypass {enable | disable}
```

### Syntax Description

<b>enable</b>	Allows the controller to support bypass of captive portals.
<b>disable</b>	Disallows the controller to support bypass of captive portals.

### Command Default

None

The following example shows how to configure the controller to support bypass of captive portals:

```
(Cisco Controller) > config network web-auth captive-bypass enable
```

### Related Commands

**show network summary**  
**config network web-auth cmcc-support**

# config network web-auth port

To configure an additional port to be redirected for web authentication at the network level, use the **config network web-auth port** command.

**config network web-auth port** *port*

<b>Syntax Description</b>	<i>port</i>	Port number. The valid range is from 0 to 65535.
<b>Command Default</b>	None	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure an additional port number 1200 to be redirected for web authentication:

```
(Cisco Controller) > config network web-auth port 1200
```

**Related Commands**    **show network summary**

# config network web-auth proxy-redirect

To configure proxy redirect support for web authentication clients, use the **config network web-auth proxy-redirect** command.

**config network web-auth proxy-redirect** {enable | disable}

<b>Syntax Description</b>	<b>enable</b>	Allows proxy redirect support for web authentication clients.
	<b>disable</b>	Disallows proxy redirect support for web authentication clients.
<b>Command Default</b>	None	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable proxy redirect support for web authentication clients:

```
(Cisco Controller) > config network web-auth proxy-redirect enable
```

**Related Commands**    **show network summary**

## config network web-auth secureweb

To configure the secure web (https) authentication for clients, use the **config network web-auth secureweb** command.

**config network web-auth secureweb** { **enable** | **disable** }

<b>Syntax Description</b>	<b>enable</b>	Allows secure web (https) authentication for clients.
	<b>disable</b>	Disallows secure web (https) authentication for clients. Enables http web authentication for clients.
<b>Command Default</b>	The default secure web (https) authentication for clients is enabled.	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.
<b>Usage Guidelines</b>	<p>If you configure the secure web (https) authentication for clients using the <b>config network web-auth secureweb disable</b> command, then you must reboot the Cisco WLC to implement the change.</p> <p>The following example shows how to enable the secure web (https) authentication for clients:</p> <pre>(Cisco Controller) &gt; config network web-auth secureweb enable</pre>	
<b>Related Commands</b>	<b>show network summary</b>	

# config network webmode

To enable or disable the web mode, use the **config network webmode** command.

```
config network webmode {enable | disable}
```

## Syntax Description

<b>enable</b>	Enables the web interface.
<b>disable</b>	Disables the web interface.

## Command Default

The default value for the web mode is **enable**.

## 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 the web interface mode:

```
(Cisco Controller) > config network webmode disable
```

## Related Commands

**show network summary**

# config network web-auth

To configure the network-level web authentication options, use the **config network web-auth** command.

**config network web-auth** {port *port-number*} | {proxy-redirect {enable | disable}}

Syntax Description		
<b>port</b>		Configures additional ports for web authentication redirection.
<i>port-number</i>		Port number (between 0 and 65535).
<b>proxy-redirect</b>		Configures proxy redirect support for web authentication clients.
<b>enable</b>		Enables proxy redirect support for web authentication clients.  <b>Note</b> Web-auth proxy redirection will be enabled for ports 80, 8080, and 3128, along with user defined port 345.
<b>disable</b>		Disables proxy redirect support for web authentication clients.

**Command Default** The default network-level web authentication value is disabled.

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

**Usage Guidelines** You must reset the system for the configuration to take effect.

The following example shows how to enable proxy redirect support for web authentication clients:

```
(Cisco Controller) > config network web-auth proxy-redirect enable
```

**Related Commands**

- show network summary
- show run-config
- config qos protocol-type

## config radius acct

To configure settings for a RADIUS accounting server for the Cisco wireless LAN controller, use the **config radius acct** command.

```
config radius acct {
  {add index IP addr port {ascii | hex} secret} | delete index | disable index
  | enable index | ipsec {authentication {hmac-md5 index | hmac-sha1 index} | disable index
  | enable index | encryption {256-aes | 3des | aes | des} index | ike {auth-mode
  {pre-shared-key index type shared_secret_key | certificate index} | dh-group { 2048bit-group-14
  | group-1 | group-2 | group-5} index | lifetime seconds index | phase1 {aggressive | main}
  index } } | {mac-delimiter {colon | hyphen | none | single-hyphen}} | {network index
  {disable | enable}} | {region {group | none | provincial}} | retransmit-timeout index
  seconds | realm {add | delete} index realm-string}
```

### Syntax Description

<b>add</b>	Adds a RADIUS accounting server (IPv4 or IPv6).
<i>index</i>	RADIUS server index (1 to 17).
<i>IP addr</i>	RADIUS server IP address (IPv4 or IPv6).
<i>port</i>	RADIUS server's UDP port number for the interface protocols.
<b>ascii</b>	Specifies the RADIUS server's secret type: <b>ascii</b> .
<b>hex</b>	Specifies the RADIUS server's secret type: <b>hex</b> .
<i>secret</i>	RADIUS server's secret.
<b>enable</b>	Enables a RADIUS accounting server.
<b>disable</b>	Disables a RADIUS accounting server.
<b>delete</b>	Deletes a RADIUS accounting server.
<b>ipsec</b>	Enables or disables IPsec support for an accounting server. <b>Note</b> IPsec is not supported for IPv6.
<b>authentication</b>	Configures IPsec Authentication.
<b>hmac-md5</b>	Enables IPsec HMAC-MD5 authentication.
<b>hmac-sha1</b>	Enables IPsec HMAC-SHA1 authentication.
<b>disable</b>	Disables IPsec support for an accounting server.
<b>enable</b>	Enables IPsec support for an accounting server.
<b>encryption</b>	Configures IPsec encryption.
<b>256-aes</b>	Enables IPsec AES-256 encryption.

<b>3des</b>	Enables IPsec 3DES encryption.
<b>aes</b>	Enables IPsec AES-128 encryption.
<b>des</b>	Enables IPsec DES encryption.
<b>ike</b>	Configures Internet Key Exchange (IKE).
<b>auth-mode</b>	Configures IKE authentication method.
<b>pre-shared-key</b>	Pre-shared key for authentication.
<b>certificate</b>	Certificate used for authentication.
<b>dh-group</b>	Configures IKE Diffie-Hellman group.
<b>2048bit-group-14</b>	Configures DH group 14 (2048 bits).
<b>group-1</b>	Configures DH group 1 (768 bits).
<b>group-2</b>	Configures DH group 2 (1024 bits).
<b>group-5</b>	Configures DH group 5 (1536 bits).
<b>lifetime</b> <i>seconds</i>	Configures IKE lifetime in seconds. The range is from 1800 to 57600 seconds and the default is 28800.
<b>phase1</b>	Configures IKE phase1 mode.
<b>aggressive</b>	Enables IKE aggressive mode.
<b>main</b>	Enables IKE main mode.
<b>mac-delimiter</b>	Configures MAC delimiter for caller station ID and calling station ID.
<b>colon</b>	Sets the delimiter to colon (For example: xx:xx:xx:xx:xx:xx).
<b>hyphen</b>	Sets the delimiter to hyphen (For example: xx-xx-xx-xx-xx-xx).
<b>none</b>	Disables delimiters (For example: xxxxxxxxxx).
<b>single-hyphen</b>	Sets the delimiters to single hyphen (For example: xxxxxx-xxxxxx).
<b>network</b>	Configures a default RADIUS server for network users.
<b>group</b>	Specifies RADIUS server type group.
<b>none</b>	Specifies RADIUS server type none.
<b>provincial</b>	Specifies RADIUS server type provincial.

<b>retransmit-timeout</b>	Changes the default retransmit timeout for the server.
<i>seconds</i>	The number of seconds between retransmissions.
<b>realm</b>	Specifies radius acct realm.
<b>add</b>	Adds radius acct realm.
<b>delete</b>	Deletes radius acct realm.

**Command Default** When adding a RADIUS server, the port number defaults to 1813 and the state is **enabled**.

**Usage Guidelines** IPsec is not supported for IPv6.

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure a priority 1 RADIUS accounting server at *10.10.10.10* using port *1813* with a login password of *admin*:

```
(Cisco Controller) > config radius acct add 1 10.10.10.10 1813 ascii admin
```

The following example shows how to configure a priority 1 RADIUS accounting server at *2001:9:6:40::623* using port *1813* with a login password of *admin*:

```
(Cisco Controller) > config radius acct add 1 2001:9:6:40::623 1813 ascii admin
```

### Related Topics

[show radius acct statistics](#), on page 185

## config radius acct ipsec authentication

To configure IPsec authentication for the Cisco wireless LAN controller, use the **config radius acct ipsec authentication** command.

**config radius acct ipsec authentication** { **hmac-md5** | **hmac-sha1** } *index*

Syntax Description	hmac-md5	hmac-sha1	index
	Enables IPsec HMAC-MD5 authentication.	Enables IPsec HMAC-SHA1 authentication.	RADIUS server index.
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 IPsec hmac-md5 authentication service on the RADIUS accounting server index 1:

```
(Cisco Controller) > config radius acct ipsec authentication hmac-md5 1
```

**Related Commands**    **show radius acct statistics**

## config radius acct ipsec disable

To disable IPsec support for an accounting server for the Cisco wireless LAN controller, use the **config radius acct ipsec disable** command.

**config radius acct ipsec disable** *index*

<b>Syntax Description</b>	<i>index</i>	RADIUS server index.
<b>Command Default</b>	None	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to disable the IPsec support for RADIUS accounting server index 1:

```
(Cisco Controller) > config radius acct ipsec disable 1
```

**Related Commands**    **show radius acct statistics**

# config radius acct ipsec enable

To enable IPsec support for an accounting server for the Cisco wireless LAN controller, use the **config radius acct ipsec enable** command.

**config radius acct ipsec enable** *index*

<b>Syntax Description</b>	<i>index</i>	RADIUS server index.
<b>Command Default</b>	None	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.

## Examples

The following example shows how to enable the IPsec support for RADIUS accounting server index 1:

```
(Cisco Controller) > config radius acct ipsec enable 1
```

**Related Commands**    **show radius acct statistics**

## config radius acct ipsec encryption

To configure IPsec encryption for an accounting server for the Cisco wireless LAN controller, use the **config radius acct ipsec encryption** command.

**config radius acct ipsec encryption** {3des | aes | des} *index*

Syntax Description		
	256-aes	Enables IPsec AES-256 encryption.
	3des	Enables IPsec 3DES encryption.
	aes	Enables IPsec AES encryption.
	des	Enables IPsec DES encryption.
	<i>index</i>	RADIUS server index value of between 1 and 17.
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 IPsec 3DES encryption for RADIUS server index value 3:

```
(Cisco Controller) > config radius acct ipsec encryption 3des 3
```

## config radius acct ipsec ike

To configure Internet Key Exchange (IKE) for the Cisco WLC, use the **config radius acct ipsec ike** command.

```
config radius acct ipsec ike dh-group { group-1 | group-2 | group-5 } | lifetime seconds | phase1
{ aggressive | main } } index
```

Syntax Description		
<b>dh-group</b>	Specifies the Dixie-Hellman (DH) group.	
<b>group-1</b>	Configures the DH Group 1 (768 bits).	
<b>group-2</b>	Configures the DH Group 2 (1024 bits).	
<b>group-5</b>	Configures the DH Group 5 (1024 bits).	
<b>lifetime</b>	Configures the IKE lifetime.	
<i>seconds</i>	IKE lifetime in seconds.	
<b>phase1</b>	Configures the IKE phase1 node.	
<b>aggressive</b>	Enables the aggressive mode.	
<b>main</b>	Enables the main mode.	
<i>index</i>	RADIUS server index.	
<b>Command Default</b>	None	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure an IKE lifetime of 23 seconds for RADIUS server index 1:

```
(Cisco Controller) > config radius acct ipsec ike lifetime 23 1
```

**Related Commands**    **show radius acct statistics**

## config radius acct mac-delimiter

To specify the delimiter to be used in the MAC addresses that are sent to the RADIUS accounting server, use the **config radius acct mac-delimiter** command.

**config radius acct mac-delimiter** { **colon** | **hyphen** | **single-hyphen** | **none** }

### Syntax Description

<b>colon</b>	Sets the delimiter to a colon (for example, xx:xx:xx:xx:xx:xx).
<b>hyphen</b>	Sets the delimiter to a hyphen (for example, xx-xx-xx-xx-xx-xx).
<b>single-hyphen</b>	Sets the delimiter to a single hyphen (for example, xxxxxx-xxxxxx).
<b>none</b>	Disables the delimiter (for example, xxxxxxxxxxxx).

### Command Default

The default delimiter is a hyphen.

### 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 delimiter hyphen to be used in the MAC addresses that are sent to the RADIUS accounting server for the network users:

```
(Cisco Controller) > config radius acct mac-delimiter hyphen
```

### Related Commands

**show radius acct statistics**

# config radius acct network

To configure a default RADIUS server for network users, use the **config radius acct network** command.

**config radius acct network** *index* { **enable** | **disable** }

Syntax Description		
<i>index</i>	RADIUS server index.	
<b>enable</b>	Enables the server as a network user's default RADIUS server.	
<b>disable</b>	Disables the server as a network user's default RADIUS server.	
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 a default RADIUS accounting server for the network users with RADIUS server index1:

```
(Cisco Controller) > config radius acct network 1 enable
```

**Related Commands**    **show radius acct statistics**

## config radius acct retransmit-timeout

To change the default transmission timeout for a RADIUS accounting server for the Cisco wireless LAN controller, use the **config radius acct retransmit-timeout** command.

**config radius acct retransmit-timeout** *index timeout*

<b>Syntax Description</b>	<i>index</i>	RADIUS server index.
	<i>timeout</i>	Number of seconds (from 2 to 30) between retransmissions.
<b>Command Default</b>	None	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure retransmission timeout value 5 seconds between the retransmission:

```
(Cisco Controller) > config radius acct retransmit-timeout 5
```

**Related Commands**    **show radius acct statistics**

## config radius auth

To configure settings for a RADIUS authentication server for the Cisco wireless LAN controller, use the `config radius auth` command.

```
config radius auth {add index IP addr portascii/hexsecret} | | delete index | disable index |
enable index | framed-mtu mtu | { ipsec {authentication {hmac-md5 index | hmac-sha1 index
} | disable index | enable index | encryption {256-aes | 3des | aes | des} index | ike
{auth-mode {pre-shared-key index ascii/hex shared_secret | certificate index } | dh-group {
2048bit-group-14 | group-1 | group-2 | group-5} index | lifetime seconds index | phase1
{aggressive | main} index } } | { { keywrap {add ascii/hex kek mack index } | delete index
| disable | enable} } | {mac-delimiter {colon | hyphen | none | single-hyphen}} |
{{management index {enable | disable}} | {mgmt-retransmit-timeout index Retransmit Timeout
} | {network index {enable | disable}} | {realm {add | delete} radius-index realm-string}
} | {region {group | none | provincial}} | {retransmit-timeout index Retransmit Timeout}
| {rfc3576 {enable | disable} index }
```

### Syntax Description

<b>enable</b>	Enables a RADIUS authentication server.
<b>disable</b>	Disables a RADIUS authentication server.
<b>delete</b>	Deletes a RADIUS authentication server.
<i>index</i>	RADIUS server index. The controller begins the search with 1. The server index range is from 1 to 17.
<b>add</b>	Adds a RADIUS authentication server. See the “Defaults” section.
<i>IP addr</i>	IP address (IPv4 or IPv6) of the RADIUS server.
<i>port</i>	RADIUS server’s UDP port number for the interface protocols.
<i>ascii/hex</i>	Specifies RADIUS server’s secret type: <b>ascii</b> or <b>hex</b> .
<i>secret</i>	RADIUS server’s secret.
<b>callStationIdType</b>	Configures Called Station Id information sent in RADIUS authentication messages.
<b>framed-mtu</b>	Configures the Framed-MTU for all the RADIUS servers. The framed-mtu range is from 64 to 1300 bytes.
<b>ipsec</b>	Enables or disables IPSEC support for an authentication server.  <b>Note</b> IPsec is not supported for IPv6.
<b>keywrap</b>	Configures RADIUS keywrap.

<i>ascii/hex</i>	Specifies the input format of the keywrap keys.
<i>kek</i>	Enters the 16-byte key-encryption-key.
<i>mack</i>	Enters the 20-byte message-authenticator-code-key.
<b>mac-delimiter</b>	Configures MAC delimiter for caller station ID and calling station ID.
<b>management</b>	Configures a RADIUS Server for management users.
<b>mgmt-retransmit-timeout</b>	Changes the default management login retransmission timeout for the server.
<b>network</b>	Configures a default RADIUS server for network users.
<b>realm</b>	Configures radius auth realm.
<b>region</b>	Configures RADIUS region property.
<b>retransmit-timeout</b>	Changes the default network login retransmission timeout for the server.
<b>rfc3576</b>	Enables or disables RFC-3576 support for an authentication server.

**Command Default** When adding a RADIUS server, the port number defaults to 1812 and the state is **enabled**.

**Usage Guidelines** IPsec is not supported for IPv6.

#### 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 a priority 3 RADIUS authentication server at *10.10.10.10* using port *1812* with a login password of *admin*:

```
(Cisco Controller) > config radius auth add 3 10.10.10.10 1812 ascii admin
```

The following example shows how to configure a priority 3 RADIUS authentication server at *2001:9:6:40::623* using port *1812* with a login password of *admin*:

```
(Cisco Controller) > config radius auth add 3 2001:9:6:40::623 1812 ascii admin
```

#### Related Topics

[show radius auth statistics](#), on page 186

## config radius auth callStationIdType

To configure the RADIUS authentication server, use the **config radius auth callStationIdType** command.

```
config radius auth callStationIdType { | ap-group-name | ap-label-address | ap-label-address-ssid |
ap-location | ap-macaddr-only | ap-macaddr-ssid | ap-name | ap-name-ssid | flex-group-name
| ipaddr | macaddr | vlan-id }
```

Syntax Description		
<b>ipaddr</b>		Configures the Call Station ID type to use the IP address (only Layer 3).
<b>macaddr</b>		Configures the Call Station ID type to use the system's MAC address (Layers 2 and 3).
<b>ap-macaddr-only</b>		Configures the Call Station ID type to use the access point's MAC address (Layers 2 and 3).
<b>ap-macaddr-ssid</b>		Configures the Call Station ID type to use the access point's MAC address (Layers 2 and 3) in the format <i>AP MAC address:SSID</i> .
<b>ap-group-name</b>		Configures the Call Station ID type to use the AP group name. If the AP is not part of any AP group, default-group is taken as the AP group name.
<b>flex-group-name</b>		Configures the Call Station ID type to use the FlexConnect group name. If the FlexConnect AP is not part of any FlexConnect group, the system MAC address is taken as the Call Station ID.
<b>ap-name</b>		Configures the Call Station ID type to use the access point's name.
<b>ap-name-ssid</b>		Configures the Call Station ID type to use the access point's name in the format <i>AP name:SSID</i>
<b>ap-location</b>		Configures the Call Station ID type to use the access point's location.
<b>vlan-id</b>		Configures the Call Station ID type to use the system's VLAN-ID.

**Command Default** The MAC address of the system.

**Usage Guidelines** The controller sends the Called Station ID attribute to the RADIUS server in all authentication and accounting packets. The Called Station ID attribute can be used to classify users to different groups based on the attribute value. The command is applicable only for the Called Station and not for the Calling Station.

You cannot send only the SSID as the Called-Station-ID, you can only combine the SSID with either the access point MAC address or the access point name.

Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.
	7.6	The <b>ap-ethmac-only</b> and <b>ap-ethmac-ssid</b> keywords were added to support the access point's Ethernet MAC address.  The <b>ap-label-address</b> and <b>ap-label-address-ssid</b> keywords were added.
	8.0	This command supports both IPv4 and IPv6 address formats.

The following example shows how to configure the call station ID type to use the IP address:

```
(Cisco Controller) > config radius auth callStationIdType ipAddr
```

The following example shows how to configure the call station ID type to use the system's MAC address:

```
(Cisco Controller) > config radius auth callStationIdType macAddr
```

The following example shows how to configure the call station ID type to use the access point's MAC address:

```
(Cisco Controller) > config radius auth callStationIdType ap-macAddr
```

## config radius auth IPsec authentication

To configure IPsec support for an authentication server for the Cisco wireless LAN controller, use the **config radius auth IPsec authentication** command.

**config radius auth IPsec authentication** { **hmac-md5** | **hmac-sha1** } *index*

Syntax Description	hmac-md5	hmac-sha1	index
	Enables IPsec HMAC-MD5 authentication.	Enables IPsec HMAC-SHA1 authentication.	RADIUS server index.
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 IPsec hmac-md5 support for RADIUS authentication server index 1:

```
(Cisco Controller) > config radius auth IPsec authentication hmac-md5 1
```

**Related Commands**    **show radius acct statistics**

## config radius auth ipsec disable

To disable IPsec support for an authentication server for the Cisco wireless LAN controller, use the **config radius auth IPsec disable** command.

**config radius auth ipsec** {enable | disable} *index*

Syntax Description		
	<b>enable</b>	Enables the IPsec support for an authentication server.
	<b>disable</b>	Disables the IPsec support for an authentication server.
	<i>index</i>	RADIUS server index.

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 enable the IPsec support for RADIUS authentication server index 1:

```
(Cisco Controller) > config radius auth ipsec enable 1
```

This example shows how to disable the IPsec support for RADIUS authentication server index 1:

```
(Cisco Controller) > config radius auth ipsec disable 1
```

Related Commands	<b>show radius acct statistics</b>
------------------	------------------------------------

## config radius auth ipsec encryption

To configure IPsec encryption support for an authentication server for the Cisco wireless LAN controller, use the **config radius auth ipsec encryption** command.

**config radius auth IPsec encryption** {**3des** | **aes** | **des**} *index*

Syntax Description		
	<b>3des</b>	Enables the IPsec 3DES encryption.
	<b>aes</b>	Enables the IPsec AES encryption.
	<b>des</b>	Enables the IPsec DES encryption.
	<i>index</i>	RADIUS server index.
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 IPsec 3des encryption RADIUS authentication server index 3:

```
(Cisco Controller) > config radius auth ipsec encryption 3des 3
```

**Related Commands**    **show radius acct statistics**

## config radius auth ipsec ike

To configure Internet Key Exchange (IKE) for the Cisco wireless LAN controller, use the **config radius auth IPsec ike** command.

```
config radius auth ipsec ike {auth-mode {pre-shared-keyindex {ascii | hex shared-secret} | certificate index} dh-group {2048bit-group-14 | group-1 | group-2 | group-5} | lifetime seconds | phase1 {aggressive | main}} index
```

Syntax	Description
<b>auth-mode</b>	Configures the IKE authentication method.
<b>pre-shared-key</b>	Configures the preshared key for IKE authentication method.
<i>index</i>	RADIUS server index between 1 and 17.
<b>ascii</b>	Configures RADIUS IPsec IKE secret in an ASCII format.
<b>hex</b>	Configures RADIUS IPsec IKE secret in a hexadecimal format.
<i>shared-secret</i>	Configures the shared RADIUS IPsec secret.
<b>certificate</b>	Configures the certificate for IKE authentication.
<b>dh-group</b>	Configures the IKE Diffie-Hellman group.
<b>2048bit-group-14</b>	Configures the DH Group14 (2048 bits).
<b>group-1</b>	Configures the DH Group 1 (768 bits).
<b>group-2</b>	Configures the DH Group 2 (1024 bits).
<b>group-5</b>	Configures the DH Group 2 (1024 bits).
<b>lifetime</b>	Configures the IKE lifetime.
<i>seconds</i>	IKE lifetime in seconds. The range is from 1800 to 57600 seconds.
<b>phase1</b>	Configures the IKE phase1 mode.
<b>aggressive</b>	Enables the aggressive mode.
<b>main</b>	Enables the main mode.
<i>index</i>	RADIUS server index.

**Command Default** By default, preshared key is used for IPsec sessions and IKE lifetime is 28800 seconds.

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 IKE lifetime of 23 seconds for RADIUS authentication server index 1:

```
(Cisco Controller) > config radius auth ipsec ike lifetime 23 1
```

**Related Commands**    **show radius acct statistics**

## config radius auth keywrap

To enable and configure Advanced Encryption Standard (AES) key wrap, which makes the shared secret between the controller and the RADIUS server more secure, use the **config radius auth keywrap** command.

**config radius auth keywrap** { **enable** | **disable** | **add** { **ascii** | **hex** } *kek mack* | **delete** } *index*

Syntax Description		
<b>enable</b>	Enables AES key wrap.	
<b>disable</b>	Disables AES key wrap.	
<b>add</b>	Configures AES key wrap attributes.	
<b>ascii</b>	Configures key wrap in an ASCII format.	
<b>hex</b>	Configures key wrap in a hexadecimal format.	
<i>kek</i>	16-byte Key Encryption Key (KEK).	
<i>mack</i>	20-byte Message Authentication Code Key (MACK).	
<b>delete</b>	Deletes AES key wrap attributes.	
<i>index</i>	Index of the RADIUS authentication server on which to configure the AES key wrap.	
<b>Command Default</b>	None	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the AES key wrap for a RADIUS authentication server:

```
(Cisco Controller) > config radius auth keywrap enable
```

**Related Commands**    **show radius auth statistics**

# config radius auth mac-delimiter

To specify a delimiter to be used in the MAC addresses that are sent to the RADIUS authentication server, use the **config radius auth mac-delimiter** command.

**config radius auth mac-delimiter** { **colon** | **hyphen** | **single-hyphen** | **none** }

Syntax Description	Option	Description
	<b>colon</b>	Sets a delimiter to a colon (for example, xx:xx:xx:xx:xx:xx).
	<b>hyphen</b>	Sets a delimiter to a hyphen (for example, xx-xx-xx-xx-xx-xx).
	<b>single-hyphen</b>	Sets a delimiter to a single hyphen (for example, xxxxxx-xxxxxx).
	<b>none</b>	Disables the delimiter (for example, xxxxxxxxxxxx).

**Command Default** The default delimiter is a hyphen.

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 a delimiter hyphen to be used for a RADIUS authentication server:

```
(Cisco Controller) > config radius auth mac-delimiter hyphen
```

**Related Commands** **show radius auth statistics**

# config radius auth management

To configure a default RADIUS server for management users, use the **config radius auth management** command.

**config radius auth management** *index* {**enable** | **disable**}

Syntax Description		
<i>index</i>	RADIUS server index.	
<b>enable</b>	Enables the server as a management user's default RADIUS server.	
<b>disable</b>	Disables the server as a management user's default RADIUS server.	
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 a RADIUS server for management users:

```
(Cisco Controller) > config radius auth management 1 enable
```

- Related Commands**
- show radius acct statistics
  - config radius acct network
  - config radius auth mgmt-retransmit-timeout

## config radius auth mgmt-retransmit-timeout

To configure a default RADIUS server retransmission timeout for management users, use the **config radius auth mgmt-retransmit-timeout** command.

**config radius auth mgmt-retransmit-timeout** *index retransmit-timeout*

Syntax Description		
	<i>index</i>	RADIUS server index.
	<i>retransmit-timeout</i>	Timeout value. The range is from 1 to 30 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 configure a default RADIUS server retransmission timeout for management users:

```
(Cisco Controller) > config radius auth mgmt-retransmit-timeout 1 10
```

**Related Commands** [config radius auth management](#)

# config radius auth network

To configure a default RADIUS server for network users, use the **config radius auth network** command.

**config radius auth network** *index* {**enable** | **disable**}

Syntax Description		
<i>index</i>	RADIUS server index.	
<b>enable</b>	Enables the server as a network user default RADIUS server.	
<b>disable</b>	Disables the server as a network user default RADIUS server.	
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 a default RADIUS server for network users:

```
(Cisco Controller) > config radius auth network 1 enable
```

**Related Commands**

- show radius acct statistics**
- config radius acct network**

## config radius auth retransmit-timeout

To change a default transmission timeout for a RADIUS authentication server for the Cisco wireless LAN controller, use the **config radius auth retransmit-timeout** command.

**config radius auth retransmit-timeout** *index timeout*

<b>Syntax Description</b>	<i>index</i>	RADIUS server index.
	<i>timeout</i>	Number of seconds (from 2 to 30) between retransmissions.
<b>Command Default</b>	None	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure a retransmission timeout of 5 seconds for a RADIUS authentication server:

```
(Cisco Controller) > config radius auth retransmit-timeout 5
```

**Related Commands**    **show radius auth statistics**

## config radius auth rfc3576

To configure RADIUS RFC-3576 support for the authentication server for the Cisco WLC, use the **config radius auth rfc3576** command.

**config radius auth rfc3576** {enable | disable} *index*

Syntax Description		
	<b>enable</b>	Enables RFC-3576 support for an authentication server.
	<b>disable</b>	Disables RFC-3576 support for an authentication server.
	<i>index</i>	RADIUS server index.

**Command Default** Disabled

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

**Usage Guidelines** RFC 3576, which is an extension to the RADIUS protocol, allows dynamic changes to a user session. RFC 3576 includes support for disconnecting users and changing authorizations applicable to a user session. Disconnect messages cause a user session to be terminated immediately; CoA messages modify session authorization attributes such as data filters.

The following example shows how to enable the RADIUS RFC-3576 support for a RADIUS authentication server:

```
(Cisco Controller) > config radius auth rfc3576 enable 2
```

**Related Commands**

- show radius auth statistics**
- show radius summary**
- show radius rfc3576**

## config radius auth retransmit-timeout

To configure a retransmission timeout value for a RADIUS accounting server, use the **config radius auth server-timeout** command.

**config radius auth retransmit-timeout** *index timeout*

Syntax Description		
	<i>index</i>	RADIUS server index.
	<i>timeout</i>	Timeout value. The range is from 2 to 30 seconds.

**Command Default** The default timeout is 2 seconds.

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 a server timeout value of 2 seconds for RADIUS authentication server index 10:

```
(Cisco Controller) > config radius auth retransmit-timeout 2 10
```

**Related Commands**

- show radius auth statistics
- show radius summary

# config radius aggressive-failover disabled

To configure the controller to mark a RADIUS server as down (not responding) after the server does not reply to three consecutive clients, use the **config radius aggressive-failover disabled** command.

## **config radius aggressive-failover disabled**

---

**Syntax Description** This command has no arguments or keywords.

---

**Command Default** None

---

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.

---

The following example shows how to configure the controller to mark a RADIUS server as down:

```
(Cisco Controller) > config radius aggressive-failover disabled
```

---

**Related Commands** **show radius summary**

## config radius backward compatibility

To configure RADIUS backward compatibility for the Cisco wireless LAN controller, use the **config radius backward compatibility** command.

**config radius backward compatibility** {enable | disable}

Syntax Description	enable	enable
	enable	Enables RADIUS vendor ID backward compatibility.
	disable	Disables RADIUS vendor ID backward compatibility.

**Command Default** 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 the RADIUS backward compatibility settings:

```
(Cisco Controller) > config radius backward compatibility disable
```

**Related Commands** **show radius summary**

## config radius callStationIdCase

To configure callStationIdCase information sent in RADIUS messages for the Cisco WLC, use the **config radius callStationIdCase** command.

**config radius callStationIdCase** { **legacy** | **lower** | **upper** }

Syntax Description		
	<b>legacy</b>	Configures Call Station IDs for Layer 2 authentication to RADIUS in uppercase.
	<b>lower</b>	Configures all Call Station IDs to RADIUS in lowercase.
	<b>upper</b>	Configures all Call Station IDs to RADIUS in uppercase.
Command Default	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 send the call station ID in lowercase:

```
(Cisco Controller) > config radius callStationIdCase lower
```

**Related Commands**    **show radius summary**

## config radius callStationIdType

To configure the Called Station ID type information sent in RADIUS accounting messages for the Cisco wireless LAN controller, use the **config radius callStationIdType** command.

```
config radius callStationIdType { | ap-group-name | ap-label-address | ap-label-address-ssid |
ap-location | ap-macaddr-only | ap-macaddr-ssid | ap-name | ap-name-ssid | flex-group-name
| ipaddr | macaddr | vlan-id }
```

Syntax Description		
<b>ipaddr</b>		Configures the Call Station ID type to use the IP address (only Layer 3).
<b>macaddr</b>		Configures the Call Station ID type to use the system's MAC address (Layers 2 and 3).
<b>ap-macaddr-only</b>		Configures the Call Station ID type to use the access point's MAC address (Layers 2 and 3).
<b>ap-macaddr-ssid</b>		Configures the Call Station ID type to use the access point's MAC address (Layers 2 and 3) in the format <i>AP MAC address:SSID</i> .
<b>ap-group-name</b>		Configures the Call Station ID type to use the AP group name. If the AP is not part of any AP group, default-group is taken as the AP group name.
<b>flex-group-name</b>		Configures the Call Station ID type to use the FlexConnect group name. If the FlexConnect AP is not part of any FlexConnect group, the system MAC address is taken as the Call Station ID.
<b>ap-name</b>		Configures the Call Station ID type to use the access point's name.
<b>ap-name-ssid</b>		Configures the Call Station ID type to use the access point's name in the format <i>AP name:SSID</i>
<b>ap-location</b>		Configures the Call Station ID type to use the access point's location.
<b>ap-mac-ssid-ap-group</b>		Sets Called Station ID type to the format <AP MAC address>:<SSID>:<AP Group>
<b>vlan-id</b>		Configures the Call Station ID type to use the system's VLAN-ID.

**Command Default** The IP address of the system.

**Usage Guidelines** The controller sends the Called Station ID attribute to the RADIUS server in all authentication and accounting packets. The Called Station ID attribute can be used to classify users to different groups based on the attribute value. The command is applicable only for the Called Station and not for the Calling Station.

You cannot send only the SSID as the Called-Station-ID, you can only combine the SSID with either the access point MAC address or the access point name.

Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.
	7.6	The <b>ap-ethmac-only</b> and <b>ap-ethmac-ssid</b> keywords were added to support the access point's Ethernet MAC address.  The <b>ap-label-address</b> and <b>ap-label-address-ssid</b> keywords were added.
	8.0	This command supports both IPv4 and IPv6 address formats.

The following example shows how to configure the call station ID type to use the IP address:

```
(Cisco Controller) > config radius callStationIdType ipaddr
```

The following example shows how to configure the call station ID type to use the system's MAC address:

```
(Cisco Controller) > config radius callStationIdType macaddr
```

The following example shows how to configure the call station ID type to use the access point's MAC address:

```
(Cisco Controller) > config radius callStationIdType ap-macaddr-only
```

### Related Topics

[show radius summary](#), on page 187

## config radius fallback-test

To configure the RADIUS server fallback behavior, use the **config radius fallback-test** command.

```
config radius fallback-test mode {off | passive | active} | username username | {interval interval}
```

Syntax	Description
<b>mode</b>	Specifies the mode.
<b>off</b>	Disables RADIUS server fallback.
<b>passive</b>	Causes the controller to revert to a preferable server (with a lower server index) from the available backup servers without using extraneous probe messages. The controller ignores all inactive servers for a time period and retries later when a RADIUS message needs to be sent.
<b>active</b>	Causes the controller to revert to a preferable server (with a lower server index) from the available backup servers by using RADIUS probe messages to proactively determine whether a server that has been marked inactive is back online. The controller ignores all inactive servers for all active RADIUS requests.
<b>username</b>	Specifies the username.
<i>username</i>	Username. The username can be up to 16 alphanumeric characters.
<b>interval</b>	Specifies the probe interval value.
<i>interval</i>	Probe interval. The range is 180 to 3600.

**Command Default** The default probe interval is 300.

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 the RADIUS accounting server fallback behavior:

```
(Cisco Controller) > config radius fallback-test mode off
```

The following example shows how to configure the controller to revert to a preferable server from the available backup servers without using the extraneous probe messages:

```
(Cisco Controller) > config radius fallback-test mode passive
```

The following example shows how to configure the controller to revert to a preferable server from the available backup servers by using RADIUS probe messages:

```
(Cisco Controller) > config radius fallback-test mode active
```

---

**Related Commands**

**config advanced probe filter**

**config advanced probe limit**

**show advanced probe**

**show radius acct statistics**

## config rogue adhoc

To globally or individually configure the status of an Independent Basic Service Set (IBSS or *ad-hoc*) rogue access point, use the **config rogue adhoc** command.

```
config rogue adhoc { enable | disable | external rogue_MAC | alert { rogue_MAC | all } | auto-contain [monitor_ap] | contain rogue_MAC 1234_aps | }
```

```
config rogue adhoc { delete { all | mac-address mac-address } | classify { friendly state { external | internal } mac-address | malicious state { alert | contain } mac-address | unclassified state { alert | contain } mac-address }
```

Syntax	Description
<b>enable</b>	Globally enables detection and reporting of ad-hoc rogues.
<b>disable</b>	Globally disables detection and reporting of ad-hoc rogues.
<b>external</b>	Configure external state on the rogue access point that is outside the network and poses no threat to WLAN security. The controller acknowledges the presence of this rogue access point.
<i>rogue_MAC</i>	MAC address of the ad-hoc rogue access point.
<b>alert</b>	Generates an SNMP trap upon detection of the ad-hoc rogue, and generates an immediate alert to the system administrator for further action.
<b>all</b>	Enables alerts for all ad-hoc rogue access points.
<b>auto-contain</b>	Contains all wired ad-hoc rogues detected by the controller.
<i>monitor_ap</i>	(Optional) IP address of the ad-hoc rogue access point.
<b>contain</b>	Contains the offending device so that its signals no longer interfere with authorized clients.
<i>1234_aps</i>	Maximum number of Cisco access points assigned to actively contain the ad-hoc rogue access point (1 through 4, inclusive).
<b>delete</b>	Deletes ad-hoc rogue access points.
<b>all</b>	Deletes all ad-hoc rogue access points.
<b>mac-address</b>	Deletes ad-hoc rogue access point with the specified MAC address.
<i>mac-address</i>	MAC address of the ad-hoc rogue access point.

<b>classify</b>	Configures ad-hoc rogue access point classification.
<b>friendly state</b>	Classifies ad-hoc rogue access points as friendly.
<b>internal</b>	Configures alert state on rogue access point that is inside the network and poses no threat to WLAN security. The controller trusts this rogue access point.
<b>malicious state</b>	Classifies ad-hoc rogue access points as malicious.
<b>alert</b>	Configures alert state on the rogue access point that is not in the neighbor list or in the user configured friendly MAC list. The controller forwards an immediate alert to the system administrator for further action.
<b>contain</b>	Configures contain state on the rogue access point. Controller contains the offending device so that its signals no longer interfere with authorized clients.
<b>unclassified state</b>	Classifies ad-hoc rogue access points as unclassified.

**Command Default**

The default for this command is **enabled** and is set to **alert**. The default for auto-containment is **disabled**.

**Command History**

<b>Release</b>	<b>Modification</b>
7.6	This command was introduced in a release earlier than Release 7.6.

**Usage Guidelines**

The controller continuously monitors all nearby access points and automatically discovers and collects information on rogue access points and clients. When the controller discovers a rogue access point, it uses RLDP to determine if the rogue is attached to your wired network.

**Note**

RLDP is not supported for use with Cisco autonomous rogue access points. These access points drop the DHCP Discover request sent by the RLDP client. Also, RLDP is not supported if the rogue access point channel requires dynamic frequency selection (DFS).

When you enter any of the containment commands, the following warning appears:

```
Using this feature may have legal consequences. Do you want to continue? (y/n) :
```

The 2.4- and 5-GHz frequencies in the Industrial, Scientific, and Medical (ISM) band are open to the public and can be used without a license. As such, containing devices on another party's network could have legal consequences.

Enter the **auto-contain** command with the *monitor\_ap* argument to monitor the rogue access point without containing it. Enter the **auto-contain** command without the optional *monitor\_ap* to automatically contain all wired ad-hoc rogues detected by the controller.

The following example shows how to enable the detection and reporting of ad-hoc rogues:

```
(Cisco Controller) > config rogue adhoc enable
```

The following example shows how to enable alerts for all ad-hoc rogue access points:

```
(Cisco Controller) > config rogue adhoc alert all
```

The following example shows how to classify an ad-hoc rogue access point as friendly and configure external state on it:

```
(Cisco Controller) > config rogue adhoc classify friendly state internal 11:11:11:11:11:11
```

---

**Related Commands**

**config rogue auto-contain level**

**show rogue ignore-list**

**show rogue rule detailed**

**show rogue rule summary**

## config rogue ap classify

To classify the status of a rogue access point, use the **config rogue ap classify** command.

```
config rogue ap classify {friendly state {internal | external} ap_mac }
```

```
config rogue ap classify {malicious | unclassified} state {alert | contain} ap_mac
```

Syntax Description		
<b>friendly</b>		Classifies a rogue access point as friendly.
<b>state</b>		Specifies a response to classification.
<b>internal</b>		Configures the controller to trust this rogue access point.
<b>external</b>		Configures the controller to acknowledge the presence of this access point.
<i>ap_mac</i>		MAC address of the rogue access point.
<b>malicious</b>		Classifies a rogue access point as potentially malicious.
<b>unclassified</b>		Classifies a rogue access point as unknown.
<b>alert</b>		Configures the controller to forward an immediate alert to the system administrator for further action.
<b>contain</b>		Configures the controller to contain the offending device so that its signals no longer interfere with authorized clients.

**Command Default** These commands are disabled by default. Therefore, all unknown access points are categorized as **unclassified** by default.

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

**Usage Guidelines** A rogue access point cannot be moved to the unclassified class if its current state is contain.

When you enter any of the containment commands, the following warning appears: “Using this feature may have legal consequences. Do you want to continue?” The 2.4- and 5-GHz frequencies in the Industrial, Scientific, and Medical (ISM) band are open to the public and can be used without a license. As such, containing devices on another party’s network could have legal consequences.

The following example shows how to classify a rogue access point as friendly and can be trusted:

```
(Cisco Controller) > config rogue ap classify friendly state internal 11:11:11:11:11:11
```

The following example shows how to classify a rogue access point as malicious and to send an alert:

```
(Cisco Controller) > config rogue ap classify malicious state alert 11:11:11:11:11:11
```

The following example shows how to classify a rogue access point as unclassified and to contain it:

```
(Cisco Controller) > config rogue ap classify unclassified state contain 11:11:11:11:11:11
```

---

**Related Commands**

- config rogue adhoc**
- config rogue ap friendly**
- config rogue ap rldp**
- config rogue ap ssid**
- config rogue ap timeout**
- config rogue ap valid-client**
- config rogue client**
- config trapflags rogueap**
- show rogue ap clients**
- show rogue ap detailed**
- show rogue ap summary**
- show rogue ap friendly summary**
- show rogue ap malicious summary**
- show rogue ap unclassified summary**
- show rogue client detailed**
- show rogue client summary**
- show rogue ignore-list**
- show rogue rule detailed**
- show rogue rule summary**

# config rogue ap friendly

To add a new friendly access point entry to the friendly MAC address list, or delete an existing friendly access point entry from the list, use the **config rogue ap friendly** command.

**config rogue ap friendly** { **add** | **delete** } *ap\_mac*

Syntax Description		
<b>add</b>		Adds this rogue access point from the friendly MAC address list.
<b>delete</b>		Deletes this rogue access point from the friendly MAC address list.
<i>ap_mac</i>		MAC address of the rogue access point that you want to add or delete.
<b>Command Default</b>	None	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to add a new friendly access point with MAC address 11:11:11:11:11:11 to the friendly MAC address list.

```
(Cisco Controller) > config rogue ap friendly add 11:11:11:11:11:11
```

Related Commands	
	<b>config rogue adhoc</b>
	<b>config rogue ap classify</b>
	<b>config rogue ap rldp</b>
	<b>config rogue ap ssid</b>
	<b>config rogue ap timeout</b>
	<b>config rogue ap valid-client</b>
	<b>config rogue client</b>
	<b>config trapflags rogueap</b>
	<b>show rogue ap clients</b>
	<b>show rogue ap detailed</b>
	<b>show rogue ap summary</b>
	<b>show rogue ap friendly summary</b>
	<b>show rogue ap malicious summary</b>
	<b>show rogue ap unclassified summary</b>

**show rogue client detailed**  
**show rogue client summary**  
**show rogue ignore-list**  
**show rogue rule detailed**  
**show rogue rule summary**

## config rogue ap rldp

To enable, disable, or initiate the Rogue Location Discovery Protocol (RLDP), use the **config rogue ap rldp** command.

**config rogue ap rldp enable** { **alarm-only** | **auto-contain** } [*monitor\_ap\_only*]

**config rogue ap rldp initiate** *rogue\_mac\_address*

**config rogue ap rldp disable**

Syntax Description		
<b>alarm-only</b>		When entered without the optional argument <i>monitor_ap_only</i> , enables RLDP on all access points.
<b>auto-contain</b>		When entered without the optional argument <i>monitor_ap_only</i> , automatically contains all rogue access points.
<i>monitor_ap_only</i>		(Optional) RLDP is enabled (when used with <b>alarm-only</b> keyword), or automatically contained (when used with <b>auto-contain</b> keyword) is enabled only on the designated monitor access point.
<b>initiate</b>		Initiates RLDP on a specific rogue access point.
<i>rogue_mac_address</i>		MAC address of specific rogue access point.
<b>disable</b>		Disables RLDP on all access points.

**Command Default** None

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

**Usage Guidelines** When you enter any of the containment commands, the following warning appears: “Using this feature may have legal consequences. Do you want to continue?” The 2.4- and 5-GHz frequencies in the Industrial, Scientific, and Medical (ISM) band are open to the public and can be used without a license. As such, containing devices on another party’s network could have legal consequences.

The following example shows how to enable RLDP on all access points:

```
(Cisco Controller) > config rogue ap rldp enable alarm-only
```

The following example shows how to enable RLDP on monitor-mode access point ap\_1:

```
(Cisco Controller) > config rogue ap rldp enable alarm-only ap_1
```

The following example shows how to start RLDP on the rogue access point with MAC address 123.456.789.000:

```
(Cisco Controller) > config rogue ap rldp initiate 123.456.789.000
```

The following example shows how to disable RLDP on all access points:

```
(Cisco Controller) > config rogue ap rldp disable
```

---

**Related Commands**

- config rogue adhoc**
- config rogue ap classify**
- config rogue ap friendly**
- config rogue ap ssid**
- config rogue ap timeout**
- config rogue ap valid-client**
- config rogue client**
- config trapflags rogueap**
- show rogue ap clients**
- show rogue ap detailed**
- show rogue ap summary**
- show rogue ap friendly summary**
- show rogue ap malicious summary**
- show rogue ap unclassified summary**
- show rogue client detailed**
- show rogue client summary**
- show rogue ignore-list**
- show rogue rule detailed**
- show rogue rule summary**

## config rogue ap ssid

To generate an alarm only, or to automatically contain a rogue access point that is advertising your network's service set identifier (SSID), use the **config rogue ap ssid** command.

**config rogue ap ssid** { **alarm** | **auto-contain** }

Syntax Description	alarm	auto-contain
	Generates only an alarm when a rogue access point is discovered to be advertising your network's SSID.	Automatically contains the rogue access point that is advertising your network's SSID.

**Command Default** None

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

**Usage Guidelines** When you enter any of the containment commands, the following warning appears: "Using this feature may have legal consequences. Do you want to continue?" The 2.4- and 5-GHz frequencies in the Industrial, Scientific, and Medical (ISM) band are open to the public and can be used without a license. As such, containing devices on another party's network could have legal consequences.

The following example shows how to automatically contain a rogue access point that is advertising your network's SSID:

```
(Cisco Controller) > config rogue ap ssid auto-contain
```

Related Commands
<b>config rogue adhoc</b>
<b>config rogue ap classify</b>
<b>config rogue ap friendly</b>
<b>config rogue ap rldp</b>
<b>config rogue ap timeout</b>
<b>config rogue ap valid-client</b>
<b>config rogue client</b>
<b>config trapflags rogueap</b>
<b>show rogue ap clients</b>
<b>show rogue ap detailed</b>
<b>show rogue ap summary</b>
<b>show rogue ap friendly summary</b>

**show rogue ap malicious summary**  
**show rogue ap unclassified summary**  
**show rogue client detailed**  
**show rogue client summary**  
**show rogue ignore-list**  
**show rogue rule detailed**  
**show rogue rule summary**

## config rogue ap timeout

To specify the number of seconds after which the rogue access point and client entries expire and are removed from the list, use the **config rogue ap timeout** command.

**config rogue ap timeout** *seconds*

<b>Syntax Description</b>	<i>seconds</i>	Value of 240 to 3600 seconds (inclusive), with a default value of 1200 seconds.
<b>Command Default</b>	The default number of seconds after which the rogue access point and client entries expire is 1200 seconds.	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to set an expiration time for entries in the rogue access point and client list to 2400 seconds:

```
(Cisco Controller) > config rogue ap timeout 2400
```

<b>Related Commands</b>	<ul style="list-style-type: none"> <li>config rogue ap classify</li> <li>config rogue ap friendly</li> <li>config rogue ap rldp</li> <li>config rogue ap ssid</li> <li>config rogue rule</li> <li>config trapflags rogueap</li> <li>show rogue ap clients</li> <li>show rogue ap detailed</li> <li>show rogue ap summary</li> <li>show rogue ap friendly summary</li> <li>show rogue ap malicious summary</li> <li>show rogue ap unclassified summary</li> <li>show rogue ignore-list</li> <li>show rogue rule detailed</li> <li>show rogue rule summary</li> </ul>
-------------------------	---

# config rogue auto-contain level

To configure rogue the auto-containment level, use the **config rogue auto-contain level** command.

**config rogue auto-contain level** *level* [**monitor\_ap\_only**]

<b>Syntax Description</b>	<i>level</i>	Rogue auto-containment level in the range of 1 to 4.
	<b>monitor_ap_only</b>	(Optional) Configures auto-containment using only monitor AP mode.

**Note** Up to four APs can be used to auto-contain when a rogue AP is moved to contained state through any of the auto-containment policies.

**Command Default** The default auto-containment level is 1.

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.

**Usage Guidelines** The controller continuously monitors all nearby access points and automatically discovers and collects information on rogue access points and clients. When the controller discovers a rogue access point, it uses any of the configured auto-containment policies to start autocontainment. The policies for initiating autocontainment are rogue on wire (detected through RLDP or rogue detector AP), rogue using managed SSID, Valid client on Rogue AP, and AdHoc Rogue.



**Note** RLDP is not supported for use with Cisco autonomous rogue access points. These access points drop the DHCP Discover request sent by the RLDP client. Also, RLDP is not supported if the rogue access point channel requires dynamic frequency selection (DFS).

When you enter any of the containment commands, the following warning appears:

```
Using this feature may have legal consequences. Do you want to continue? (y/n) :
```

The 2.4-GHz and 5-GHz frequencies in the Industrial, Scientific, and Medical (ISM) band are open to the public and can be used without a license. As such, containing devices on another party's network could have legal consequences.

The following example shows how to configure the auto-contain level to 3:

```
(Cisco Controller) > config rogue auto-contain level 3
```

**Related Commands** **config rogue adhoc**

**show rogue adhoc summary**

**show rogue client summary**

**show rogue ignore-list**

**show rogue rule summary**

# config rogue ap valid-client

To generate an alarm only, or to automatically contain a rogue access point to which a trusted client is associated, use the **config rogue ap valid-client** command.

**config rogue ap valid-client** { **alarm** | **auto-contain** }

<b>Syntax Description</b>	<b>alarm</b>	Generates only an alarm when a rogue access point is discovered to be associated with a valid client.
	<b>auto-contain</b>	Automatically contains a rogue access point to which a trusted client is associated.
<b>Command Default</b>	None	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.
<b>Usage Guidelines</b>	<p>When you enter any of the containment commands, the following warning appears: “Using this feature may have legal consequences. Do you want to continue?” The 2.4- and 5-GHz frequencies in the Industrial, Scientific, and Medical (ISM) band are open to the public and can be used without a license. As such, containing devices on another party’s network could have legal consequences.</p> <p>The following example shows how to automatically contain a rogue access point that is associated with a valid client:</p> <pre>(Cisco Controller) &gt; config rogue ap valid-client auto-contain</pre>	
<b>Related Commands</b>	<ul style="list-style-type: none"> <li>config rogue ap classify</li> <li>config rogue ap friendly</li> <li>config rogue ap rldp</li> <li>config rogue ap timeout</li> <li>config rogue ap ssid</li> <li>config rogue rule</li> <li>config trapflags rogueap</li> <li>show rogue ap clients</li> <li>show rogue ap detailed</li> <li>show rogue ap summary</li> <li>show rogue ap friendly summary</li> <li>show rogue ap malicious summary</li> </ul>	

**show rogue ap unclassified summary**

**show rogue ignore-list**

**show rogue rule detailed**

**show rogue rule summary**



**show rogue ap clients**  
**show rogue ap detailed**  
**show rogue client summary**  
**show rogue ignore-list**  
**show rogue rule detailed**  
**show rogue rule summary**

# config rogue detection

To enable or disable rogue detection, use the **config rogue detection** command.



**Note** If an AP itself is configured with the keyword **all**, the **all access points** case takes precedence over the AP that is with the keyword **all**.

```
config rogue detection {enable | disable} {cisco_ap | all}
```

## Syntax Description

<b>enable</b>	Enables rogue detection on this access point.
<b>disable</b>	Disables rogue detection on this access point.
<i>cisco_ap</i>	Cisco access point.
<b>all</b>	Specifies all access points.

## Command Default

The default rogue detection value is enabled.

## Command History

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

## Usage Guidelines

Rogue detection is enabled by default for all access points joined to the controller except for OfficeExtend access points. OfficeExtend access points are deployed in a home environment and are likely to detect a large number of rogue devices.

The following example shows how to enable rogue detection on the access point Cisco\_AP:

```
(Cisco Controller) > config rogue detection enable Cisco_AP
```

## Related Commands

- config rogue rule
- config trapflags rogueap
- show rogue client detailed
- show rogue client summary
- show rogue ignore-list
- show rogue rule detailed
- show rogue rule summary

## config rogue detection min-rssi

To configure the minimum Received Signal Strength Indicator (RSSI) value at which APs can detect rogues and create a rogue entry in the controller, use the **config rogue detection min-rssi** command.

**config rogue detection min-rssi** *rssi-in-dBm*

<b>Syntax Description</b>	<i>rssi-in-dBm</i>	Minimum RSSI value. The valid range is from $-70$ dBm to $-128$ dBm, and the default value is $-128$ dBm.
---------------------------	--------------------	---

<b>Command Default</b>	The default RSSI value to detect rogues in APs is $-128$ dBm.
------------------------	---

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.

**Usage Guidelines** This feature is applicable to all the AP modes.

There can be many rogues with very weak RSSI values that do not provide any valuable information in rogue analysis. Therefore, you can use this option to filter rogues by specifying the minimum RSSI value at which APs should detect rogues.

The following example shows how to configure the minimum RSSI value:

```
(Cisco Controller) > config rogue detection min-rssi -80
```

<b>Related Commands</b>	<b>config rogue detection</b> <b>show rogue ap clients</b> <b>config rogue rule</b> <b>config trapflags rogueap</b> <b>show rogue client detailed</b> <b>show rogue client summary</b> <b>show rogue ignore-list</b> <b>show rogue rule detailed</b> <b>show rogue rule summary</b>
-------------------------	---

# config rogue detection monitor-ap

To configure the rogue report interval for all monitor mode Cisco APs, use the **config rogue detection monitor-ap** command.

```
config rogue detection monitor-ap {report-interval | transient-rogue-interval} time-in-seconds
```

Syntax Description	Parameter	Description
	<b>report-interval</b>	Specifies the interval at which rogue reports are sent.
	<b>transient-rogue-interval</b>	Specifies the interval at which rogues are consistently scanned for by APs after the first time the rogues are scanned.
	<i>time-in-seconds</i>	Time in seconds. The valid range is as follows: <ul style="list-style-type: none"> <li>• 10 to 300 for <b>report-interval</b></li> <li>• 120 to 1800 for <b>transient-rogue-interval</b></li> </ul>
Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

## Usage Guidelines

This feature is applicable to APs that are in monitor mode only.

Using the transient interval values, you can control the time interval at which APs should scan for rogues. APs can also filter the rogues based on their transient interval values.

This feature has the following advantages:

- Rogue reports from APs to the controller are shorter.
- Transient rogue entries are avoided in the controller.
- Unnecessary memory allocation for transient rogues are avoided.

The following example shows how to configure the rogue report interval to 60 seconds:

```
(Cisco Controller) > config rogue detection monitor-ap report-interval 60
```

The following example shows how to configure the transient rogue interval to 300 seconds:

```
(Cisco Controller) > config rogue detection monitor-ap transient-rogue-interval 300
```

## Related Commands

**config rogue detection**  
**config rogue detection min-rssi**  
**config rogue rule**  
**config trapflags rogueap**

**show rogue ap clients**  
**show rogue client detailed**  
**show rogue client summary**  
**show rogue ignore-list**  
**show rogue rule detailed**  
**show rogue rule summary**

## config rogue rule

To add and configure rogue classification rules, use the **config rogue rule** command.

```
config rogue rule {add ap priority classify {custom severity-score classification-name | friendly
| malicious} notify {all | global | none | local} state {alert | contain | internal | external}
rule_name | classify {custom severity-score classification-name | friendly | malicious} rule_name
| condition ap {set | delete} condition_type condition_value rule_name | {enable | delete |
disable} {all | rule_name} | match {all | any} | priority priority | notify {all | global |
none | local} rule_name | state {alert | contain | internal | external} rule_name}
```

### Syntax Description

<b>add ap priority</b>	Adds a rule with match any criteria and the priority that you specify.
<i>priority</i>	Priority of this rule within the list of rules.
<b>classify</b>	Specifies the classification of a rule.
<b>custom</b>	Classifies devices matching the rule as custom.
<i>severity-score</i>	Custom classification severity score of the rule. The range is from 1 to 100.
<i>classification-name</i>	Custom classification name. The name can be up to 32 case-sensitive, alphanumeric characters.
<b>friendly</b>	Classifies a rule as friendly.
<b>malicious</b>	Classifies a rule as malicious.
<b>notify</b>	Configures type of notification upon rule match.
<b>all</b>	Notifies the controller and a trap receiver such as Cisco Prime Infrastructure.
<b>global</b>	Notifies only a trap receiver such as Cisco Prime Infrastructure.
<b>local</b>	Notifies only the controller.
<b>none</b>	Notifies neither the controller nor a trap receiver such as Cisco Prime Infrastructure.
<b>state</b>	Configures state of the rogue access point after a rule match.
<b>alert</b>	Configures alert state on the rogue access point that is not in the neighbor list or in the user configured friendly MAC list. The controller forwards an immediate alert to the system administrator for further action.

<b>contain</b>	Configures contain state on the rogue access point. Controller contains the offending device so that its signals no longer interfere with authorized clients.
<b>external</b>	Configures external state on the rogue access point that is outside the network and poses no threat to WLAN security. The controller acknowledges the presence of this rogue access point.
<b>internal</b>	Configures alert state on rogue access point that is inside the network and poses no threat to WLAN security. The controller trusts this rogue access point.
<i>rule_name</i>	Rule to which the command applies, or the name of a new rule.
<b>condition ap</b>	Specifies the conditions for a rule that the rogue access point must meet.
<b>set</b>	Adds conditions to a rule that the rogue access point must meet.
<b>delete</b>	Removes conditions to a rule that the rogue access point must meet.
<i>condition_type</i>	Type of the condition to be configured. The condition types are listed below: <ul style="list-style-type: none"> <li>• <b>client-count</b>—Requires that a minimum number of clients be associated to a rogue access point. The valid range is 1 to 10 (inclusive).</li> <li>• <b>duration</b>—Requires that a rogue access point be detected for a minimum period of time. The valid range is 0 to 3600 seconds (inclusive).</li> <li>• <b>managed-ssid</b>—Requires that a rogue access point's SSID be known to the controller.</li> <li>• <b>no-encryption</b>—Requires that a rogue access point's advertised WLAN does not have encryption enabled.</li> <li>• <b>rssi</b>—Requires that a rogue access point have a minimum RSSI value. The range is from -95 to -50 dBm (inclusive).</li> <li>• <b>ssid</b>—Requires that a rogue access point have a specific SSID.</li> </ul>
<i>condition_value</i>	Value of the condition. This value is dependent upon the <i>condition_type</i> . For instance, if the condition type is <i>ssid</i> , then the condition value is either the SSID name or <i>all</i> .

<b>enable</b>	Enables all rules or a single specific rule.
<b>delete</b>	Deletes all rules or a single specific rule.
<b>disable</b>	Deletes all rules or a single specific rule.
<b>match</b>	Specifies whether a detected rogue access point must meet all or any of the conditions specified by the rule in order for the rule to be matched and the rogue access point to adopt the classification type of the rule.
<b>all</b>	Specifies all rules defined.
<b>any</b>	Specifies any rule meeting certain criteria.
<b>priority</b>	Changes the priority of a specific rule and shifts others in the list accordingly.

**Command Default** No rogue rules are configured.

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.

**Usage Guidelines** For your changes to be effective, you must enable the rule. You can configure up to 64 rules. Reclassification of rogue APs according to the RSSI condition of the rogue rule occurs only when the RSSI changes more than +/- 2 dBm of the configured RSSI value. Manual and automatic classification override custom rogue rules. Rules are applied to manually changed rogues if their class type changes to unclassified and state changes to alert. Adhoc rogues are classified and do not go to the pending state. You can have up to 50 classification types.

The following example shows how to create a rule called rule\_1 with a priority of 1 and a classification as friendly.

```
(Cisco Controller) > config rogue rule add ap priority 1 classify friendly rule_1
```

The following example shows how to enable rule\_1.

```
(Cisco Controller) > config rogue rule enable rule_1
```

The following example shows how to change the priority of the last command.

```
(Cisco Controller) > config rogue rule priority 2 rule_1
```

The following example shows how to change the classification of the last command.

```
(Cisco Controller) > config rogue rule classify malicious rule_1
```

The following example shows how to disable the last command.

```
(Cisco Controller) > config rogue rule disable rule_1
```

The following example shows how to delete SSID\_2 from the user-configured SSID list in rule-5.

```
(Cisco Controller) > config rogue rule condition ap delete ssid ssid_2 rule-5
```

The following example shows how to create a custom rogue rule.

```
(Cisco Controller) > config rogue rule classify custom 1 VeryMalicious rule6
```

### Related Topics

- [config rogue adhoc](#), on page 91
- [config rogue auto-contain level](#), on page 103
- [config rogue client](#), on page 107
- [config rogue detection](#), on page 109
- [show rogue ignore-list](#), on page 214
- [show rogue rule detailed](#), on page 216
- [show rogue rule summary](#), on page 218

## config tacacs acct

To configure TACACS+ accounting server settings, use the **config tacacs acct** command.

**config tacacs acct** {**add** *1-3 IP addr port ascii/hex secret* | **delete** *1-3* | **disable** *1-3* | **enable** *1-3* | **server-timeout** *1-3 seconds*}

Syntax	Description						
<b>add</b>	Adds a new TACACS+ accounting server.						
<i>1-3</i>	Specifies TACACS+ accounting server index from 1 to 3.						
<i>IP addr</i>	Specifies IPv4 or IPv6 address of the TACACS+ accounting server.						
<i>port</i>	Specifies TACACS+ Server's TCP port.						
<i>ascii/hex</i>	Specifies type of TACACS+ server's secret being used (ASCII or HEX).						
<i>secret</i>	Specifies secret key in ASCII or hexadecimal characters.						
<b>delete</b>	Deletes a TACACS+ server.						
<b>disable</b>	Disables a TACACS+ server.						
<b>enable</b>	Enables a TACACS+ server.						
<b>server-timeout</b>	Changes the default server timeout for the TACACS+ server.						
<i>seconds</i>	Specifies the number of seconds before the TACACS+ server times out. The server timeout range is from 5 to 30 seconds.						
<b>Command Default</b>	None						
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>7.6</td> <td>This command was introduced in a release earlier than Release 7.6.</td> </tr> <tr> <td>8.0</td> <td>This command supports both IPv4 and IPv6 address formats.</td> </tr> </tbody> </table>	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.
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 add a new TACACS+ accounting server index 1 with the IPv4 address 10.0.0.0, port number 49, and secret key 12345678 in ASCII:

```
(Cisco Controller) > config tacacs acct add 1 10.0.0.0 10 ascii 12345678
```

The following example shows how to add a new TACACS+ accounting server index 1 with the IPv6 address 2001:9:6:40::623, port number 49, and secret key 12345678 in ASCII:

```
(Cisco Controller) > config tacacs acct add 1 2001:9:6:40::623 10 ascii 12345678
```

The following example shows how to configure the server timeout of 5 seconds for the TACACS+ accounting server:

```
(Cisco Controller) > config tacacs acct server-timeout 1 5
```

### Related Topics

[show tacacs acct statistics](#), on page 219

[show tacacs summary](#), on page 222

## config tacacs athr

To configure TACACS+ authorization server settings, use the **config tacacs athr** command.

**config tacacs athr** {**add** *1-3 IP addr port ascii/hex secret* | **delete** *1-3* | **disable** *1-3* | **enable** *1-3* | **mgmt-server-timeout** *1-3 seconds* | **server-timeout** *1-3 seconds*}

Syntax	Description
<b>add</b>	Adds a new TACACS+ authorization server (IPv4 or IPv6).
<i>1-3</i>	TACACS+ server index from 1 to 3.
<i>IP addr</i>	TACACS+ authorization server IP address (IPv4 or IPv6).
<i>port</i>	TACACS+ server TCP port.
<i>ascii/hex</i>	Type of secret key being used (ASCII or HEX).
<i>secret</i>	Secret key in ASCII or hexadecimal characters.
<b>delete</b>	Deletes a TACACS+ server.
<b>disable</b>	Disables a TACACS+ server.
<b>enable</b>	Enables a TACACS+ server.
<b>mgmt-server-timeout</b> <i>1-3seconds</i>	Changes the default management login server timeout for the server. The number of seconds before server times out is from 1 to 30 seconds.
<b>server-timeout</b> <i>1-3 seconds</i>	Changes the default network login server timeout for the server. The number of seconds before server times out is from 5 to 30 seconds.

**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 add a new TACACS+ authorization server index 1 with the IPv4 address 10.0.0.0, port number 49, and secret key 12345678 in ASCII:

```
(Cisco Controller) > config tacacs athr add 1 10.0.0.0 49 ascii 12345678
```

The following example shows how to add a new TACACS+ authorization server index 1 with the IPv6 address 2001:9:6:40::623, port number 49, and secret key 12345678 in ASCII:

```
(Cisco Controller) > config tacacs athr add 1 2001:9:6:40::623 49 ascii 12345678
```

The following example shows how to configure the retransmit timeout of 5 seconds for the TACACS+ authorization server:

```
(Cisco Controller) > config tacacs athr server-timeout 1 5
```

### Related Topics

[show tacacs athr statistics](#), on page 220

[show tacacs summary](#), on page 222

## config tacacs athr mgmt-server-timeout

To configure a default TACACS+ authorization server timeout for management users, use the **config tacacs athr mgmt-server-timeout** command.

```
config tacacs athr mgmt-server-timeout index timeout
```

<b>Syntax Description</b>	<i>index</i>	TACACS+ authorization server index.
	<i>timeout</i>	Timeout value. The range is 1 to 30 seconds.

<b>Command Default</b>	None
------------------------	------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure a default TACACS+ authorization server timeout for management users:

```
(Cisco Controller) > config tacacs athr mgmt-server-timeout 1 10
```

## config tacacs auth

To configure TACACS+ authentication server settings, use the **config tacacs auth** command.

**config tacacs auth** { **add** *1-3 IP addr port ascii/hex secret* | **delete** *1-3* | **disable** *1-3* | **enable** *1-3* | **mgmt-server-timeout** *1-3 seconds* | **server-timeout** *1-3seconds* }

Syntax Description		
<b>add</b>		Adds a new TACACS+ accounting server.
<i>1-3</i>		TACACS+ accounting server index from 1 to 3.
<i>IP addr</i>		IP address for the TACACS+ accounting server.
<i>port</i>		Controller port used for the TACACS+ accounting server.
<i>ascii/hex</i>		Type of secret key being used (ASCII or HEX).
<i>secret</i>		Secret key in ASCII or hexadecimal characters.
<b>delete</b>		Deletes a TACACS+ server.
<b>disable</b>		Disables a TACACS+ server.
<b>enable</b>		Enables a TACACS+ server.
<b>mgmt-server-timeout</b> <i>1-3 seconds</i>		Changes the default management login server timeout for the server. The number of seconds before server times out is from 1 to 30 seconds.
<b>server-timeout</b> <i>1-3 seconds</i>		Changes the default network login server timeout for the server. The number of seconds before server times out is from 5 to 30 seconds.

**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 add a new TACACS+ authentication server index 1 with the IPv4 address 10.0.0.3, port number 49, and secret key 12345678 in ASCII:

```
(Cisco Controller) > config tacacs auth add 1 10.0.0.3 49 ascii 12345678
```

The following example shows how to add a new TACACS+ authentication server index 1 with the IPv6 address 2001:9:6:40::623, port number 49, and secret key 12345678 in ASCII:

```
(Cisco Controller) > config tacacs auth add 1 2001:9:6:40::623 49 ascii 12345678
```

The following example shows how to configure the server timeout for TACACS+ authentication server:

```
(Cisco Controller) > config tacacs auth server-timeout 1 5
```

### Related Topics

[show tacacs auth statistics](#), on page 221

[show tacacs summary](#), on page 222

## config tacacs auth mgmt-server-timeout

To configure a default TACACS+ authentication server timeout for management users, use the **config tacacs auth mgmt-server-timeout** command.

**config tacacs auth mgmt-server-timeout** *index timeout*

Syntax Description		
	<i>index</i>	TACACS+ authentication server index.
	<i>timeout</i>	Timeout value. The range is 1 to 30 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 configure a default TACACS+ authentication server timeout for management users:

```
(Cisco Controller) > config tacacs auth mgmt-server-timeout 1 10
```

**Related Commands** **config tacacs auth**

## config wps ap-authentication

To configure access point neighbor authentication, use the **config wps ap-authentication** command.

**config wps ap-authentication** [**enable** | **disable threshold** *threshold\_value*]

Syntax Description		
<b>enable</b>		(Optional) Enables WMM on the wireless LAN.
<b>disable</b>		(Optional) Disables WMM on the wireless LAN.
<b>threshold</b>		(Optional) Specifies that WMM-enabled clients are on the wireless LAN.
<i>threshold_value</i>		Threshold value (1 to 255).
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 access point neighbor authentication:

```
(Cisco Controller) > config wps ap-authentication threshold 25
```

**Related Commands**    **show wps ap-authentication summary**

## config wps auto-immune

To enable or disable protection from Denial of Service (DoS) attacks, use the **config wps auto-immune** command.

**config wps auto-immune** { **enable** | **disable** | **stop** }

Syntax Description		
	<b>enable</b>	Enables the auto-immune feature.
	<b>disable</b>	Disables the auto-immune feature.
	<b>stop</b>	Stops dynamic auto-immune feature.

Command Default	Disabled
-----------------	----------

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

**Usage Guidelines**

A potential attacker can use specially crafted packets to mislead the Intrusion Detection System (IDS) into treating a legitimate client as an attacker. It causes the controller to disconnect this legitimate client and launch a DoS attack. The auto-immune feature, when enabled, is designed to protect against such attacks. However, conversations using Cisco 792x phones might be interrupted intermittently when the auto-immune feature is enabled. If you experience frequent disruptions when using 792x phones, you might want to disable this feature.

The following example shows how to configure the auto-immune mode:

```
(Cisco Controller) > config wps auto-immune enable
```

The following example shows how to stop the auto-immune mode:

```
(Cisco Controller) > config wps auto-immune stop
Dynamic Auto Immune by WIPS is stopped
```

**Related Commands**    **show wps summary**

## config wps cids-sensor

To configure Intrusion Detection System (IDS) sensors for the Wireless Protection System (WPS), use the `config wps cids-sensor` command.

```
config wps cids-sensor { [add index ip_address username password] | [delete index] | [enable index] | [disable index] | [port index port] | [interval index query_interval] | [fingerprint sha1 fingerprint] }
```

Syntax Description	
<b>add</b>	(Optional) Configures a new IDS sensor.
<i>index</i>	IDS sensor internal index.
<i>ip_address</i>	IDS sensor IP address.
<i>username</i>	IDS sensor username.
<i>password</i>	IDS sensor password.
<b>delete</b>	(Optional) Deletes an IDS sensor.
<b>enable</b>	(Optional) Enables an IDS sensor.
<b>disable</b>	(Optional) Disables an IDS sensor.
<b>port</b>	(Optional) Configures the IDS sensor's port number.
<i>port</i>	Port number.
<b>interval</b>	(Optional) Specifies the IDS sensor's query interval.
<i>query_interval</i>	Query interval setting.
<b>fingerprint</b>	(Optional) Specifies the IDS sensor's TLS fingerprint.
<b>sha1</b>	(Optional) Specifies the TLS fingerprint.
<i>fingerprint</i>	TLS fingerprint.

**Command Default** Command defaults are listed below as follows:

Port	443
Query interval	60
Certification fingerprint	00:00
Query state	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 configure the intrusion detection system with the IDS index 1, IDS sensor IP address 10.0.0.51, IDS username Sensor\_user0doc1, and IDS password passowrd01:

```
(Cisco Controller) > config wps cids-sensor add 1 10.0.0.51 Sensor_user0doc1 password01
```

**Related Commands**    `show wps cids-sensor detail`

# config wps client-exclusion

To configure client exclusion policies, use the **config wps client-exclusion** command.

```
config wps client-exclusion {802.11-assoc | 802.11-auth | 802.11x-auth | ip-theft | web-auth
| all} {enable | disable}
```

Syntax	Description
<b>802.11-assoc</b>	Specifies that the controller excludes clients on the sixth 802.11 association attempt, after five consecutive failures.
<b>802.11-auth</b>	Specifies that the controller excludes clients on the sixth 802.11 authentication attempt, after five consecutive failures.
<b>802.11x-auth</b>	Specifies that the controller excludes clients on the sixth 802.11X authentication attempt, after five consecutive failures.
<b>ip-theft</b>	Specifies that the control excludes clients if the IP address is already assigned to another device.
<b>web-auth</b>	Specifies that the controller excludes clients on the fourth web authentication attempt, after three consecutive failures.
<b>all</b>	Specifies that the controller excludes clients for all of the above reasons.
<b>enable</b>	Enables client exclusion policies.
<b>disable</b>	Disables client exclusion policies.

**Command Default** All policies are 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 disable clients on the 802.11 association attempt after five consecutive failures:

```
(Cisco Controller) > config wps client-exclusion 802.11-assoc disable
```

**Related Commands** `show wps summary`

## config wps mfp

To configure Management Frame Protection (MFP), use the **config wps mfp** command.

```
config wps mfp { infrastructure | ap-impersonation } { enable | disable }
```

Syntax Description		
	<b>infrastructure</b>	Configures the MFP infrastructure.
	<b>ap-impersonation</b>	Configures ap impersonation detection by MFP.
	<b>enable</b>	Enables the MFP feature.
	<b>disable</b>	Disables the MFP feature.
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 infrastructure MFP:

```
(Cisco Controller) > config wps mfp infrastructure enable
```

**Related Commands**    **show wps mfp**

## config wps shun-list re-sync

To force the controller to synchronization with other controllers in the mobility group for the shun list, use the **config wps shun-list re-sync** command.

**config wps shun-list re-sync**

---

**Syntax Description** This command has no arguments or keywords.

---

**Command Default** None

---

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.

---

The following example shows how to configure the controller to synchronize with other controllers for the shun list:

```
(Cisco Controller) > config wps shun-list re-sync
```

---

**Related Commands** **show wps shun-list**

## config wps signature

To enable or disable Intrusion Detection System (IDS) signature processing, or to enable or disable a specific IDS signature, use the **config wps signature** command.

```
config wps signature { standard | custom } state signature_id { enable | disable }
```

Syntax Description		
<b>standard</b>		Configures a standard IDS signature.
<b>custom</b>		Configures a standard IDS signature.
<b>state</b>		Specifies the state of the IDS signature.
<i>signature_id</i>		Identifier for the signature to be enabled or disabled.
<b>enable</b>		Enables the IDS signature processing or a specific IDS signature.
<b>disable</b>		Disables IDS signature processing or a specific IDS signature.

**Command Default** IDS signature processing is enabled by default.

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

**Usage Guidelines** If IDS signature processing is disabled, all signatures are disabled, regardless of the state configured for individual signatures.

The following example shows how to enable IDS signature processing, which enables the processing of all IDS signatures:

```
(Cisco Controller) > config wps signature enable
```

The following example shows how to disable a standard individual IDS signature:

```
(Cisco Controller) > config wps signature standard state 15 disable
```

Related Commands	
	<b>config wps signature frequency</b>
	<b>config wps signature interval</b>
	<b>config wps signature mac-frequency</b>
	<b>config wps signature quiet-time</b>
	<b>config wps signature reset</b>
	<b>show wps signature events</b>

**show wps signature summary**

**show wps summary**

## config wps signature frequency

To specify the number of matching packets per interval that must be identified at the individual access point level before an attack is detected, use the **config wps signature frequency** command.

**config wps signature frequency** *signature\_id* *frequency*

<b>Syntax Description</b>	<i>signature_id</i>	Identifier for the signature to be configured.
	<i>frequency</i>	Number of matching packets per interval that must be at the individual access point level before an attack is detected. The range is 1 to 32,000 packets per interval.

**Command Default** The *frequency* default value varies per signature.

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.

**Usage Guidelines** If IDS signature processing is disabled, all signatures are disabled, regardless of the state configured for individual signatures.

The following example shows how to set the number of matching packets per interval per access point before an attack is detected to 1800 for signature ID 4:

```
(Cisco Controller) > config wps signature frequency 4 1800
```

**Related Commands**

- config wps signature frequency
- config wps signature interval
- config wps signature quiet-time
- config wps signature reset
- show wps signature events
- show wps signature summary
- show wps summary

# config wps signature interval

To specify the number of seconds that must elapse before the signature frequency threshold is reached within the configured interval, use the **config wps signature interval** command.

**config wps signature interval** *signature\_id interval*

Syntax Description	<i>signature_id</i>	Identifier for the signature to be configured.
	<i>interval</i>	Number of seconds that must elapse before the signature frequency threshold is reached. The range is 1 to 3,600 seconds.

**Command Default** The default value of *interval* varies per signature.

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

**Usage Guidelines** If IDS signature processing is disabled, all signatures are disabled, regardless of the state configured for individual signatures.

The following example shows how to set the number of seconds to elapse before reaching the signature frequency threshold to 200 for signature ID 1:

```
(Cisco Controller) > config wps signature interval 1 200
```

Related Commands
<b>config wps signature frequency</b>
<b>config wps signature</b>
<b>config wps signature mac-frequency</b>
<b>config wps signature quiet-time</b>
<b>config wps signature reset</b>
<b>show wps signature events</b>
<b>show wps signature summary</b>
<b>show wps summary</b>

## config wps signature mac-frequency

To specify the number of matching packets per interval that must be identified per client per access point before an attack is detected, use the **config wps signature mac-frequency** command.

**config wps signature mac-frequency** *signature\_id mac\_frequency*

Syntax Description		
	<i>signature_id</i>	Identifier for the signature to be configured.
	<i>mac_frequency</i>	Number of matching packets per interval that must be identified per client per access point before an attack is detected. The range is 1 to 32,000 packets per interval.

**Command Default** The *mac\_frequency* default value varies per signature.

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

**Usage Guidelines** If IDS signature processing is disabled, all signatures are disabled, regardless of the state configured for individual signatures.

The following example shows how to set the number of matching packets per interval per client before an attack is detected to 50 for signature ID 3:

```
(Cisco Controller) > config wps signature mac-frequency 3 50
```

**Related Commands**

- config wps signature frequency
- config wps signature interval
- config wps signature
- config wps signature quiet-time
- config wps signature reset
- show wps signature events
- show wps signature summary
- show wps summary

## config wps signature quiet-time

To specify the length of time after which no attacks have been detected at the individual access point level and the alarm can stop, use the **config wps signature quiet-time** command.

```
config wps signature quiet-time signature_id quiet_time
```

Syntax Description		
	<i>signature_id</i>	Identifier for the signature to be configured.
	<i>quiet_time</i>	Length of time after which no attacks have been detected at the individual access point level and the alarm can stop. The range is 60 to 32,000 seconds.

**Command Default** The default value of *quiet\_time* varies per signature.

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

**Usage Guidelines** If IDS signature processing is disabled, all signatures are disabled, regardless of the state configured for individual signatures.

The following example shows how to set the number of seconds after which no attacks have been detected per access point to 60 for signature ID 1:

```
(Cisco Controller) > config wps signature quiet-time 1 60
```

Related Commands	
	<b>config wps signature</b>
	<b>config wps signature frequency</b>
	<b>config wps signature interval</b>
	<b>config wps signature mac-frequency</b>
	<b>config wps signature reset</b>
	<b>show wps signature events</b>
	<b>show wps signature summary</b>
	<b>show wps summary</b>

## config wps signature reset

To reset a specific Intrusion Detection System (IDS) signature or all IDS signatures to default values, use the **config wps signature reset** command.

```
config wps signature reset {signature_id | all}
```

<b>Syntax Description</b>	<i>signature_id</i>	Identifier for the specific IDS signature to be reset.
	<b>all</b>	Resets all IDS signatures.

**Command Default** None

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.

**Usage Guidelines** If IDS signature processing is disabled, all signatures are disabled, regardless of the state configured for individual signatures.

The following example shows how to reset the IDS signature 1 to default values:

```
(Cisco Controller) > config wps signature reset 1
```

**Related Commands**

- config wps signature**
- config wps signature frequency**
- config wps signature interval**
- config wps signature mac-frequency**
- config wps signature quiet-time**
- show wps signature events**
- show wps signature summary**
- show wps summary**

## debug 11w-pmf

To configure the debugging of 802.11w, use the **debug 11w-pmf** command.

```
debug 11w-pmf {all | events| keys} {enable | disable}
```

Syntax Description		
<b>all</b>	Configures the debugging of all 802.11w messages.	
<b>keys</b>	Configures the debugging of 802.11w keys.	
<b>events</b>	Configures the debugging of 802.11w events.	
<b>enable</b>	Enables the debugging of 802.1w options.	
<b>disable</b>	Disables the debugging of 802.1w 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 the debugging of 802.11w keys:

```
(Cisco Controller) >debug 11w-pmf keys enable
```

## debug aaa

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

```
debug aaa { [all | avp-xml | detail | events | packet | ldap | local-auth | tacacs] [enable | disable] }
```

### Syntax Description

<b>all</b>	(Optional) Configures the debugging of all AAA messages.
<b>avp-xml</b>	(Optional) Configures debug of AAA Avp xml events.
<b>detail</b>	(Optional) Configures the debugging of AAA errors.
<b>events</b>	(Optional) Configures the debugging of AAA events.
<b>packet</b>	(Optional) Configures the debugging of AAA packets.
<b>ldap</b>	(Optional) Configures the debugging of the AAA Lightweight Directory Access Protocol (LDAP) events.
<b>local-auth</b>	(Optional) Configures the debugging of the AAA local Extensible Authentication Protocol (EAP) events.
<b>tacacs</b>	(Optional) Configures the debugging of the AAA TACACS+ events.
<b>enable</b>	(Optional) Enables the debugging.
<b>disable</b>	(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.

The following example shows how to enable the debugging of AAA LDAP events:

```
(Cisco Controller) > debug aaa ldap enable
```

### Related Commands

**debug aaa local-auth eap**  
**show running-config**

## debug aaa local-auth

To configure the debugging of AAA local authentication on the Cisco WLC, 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		
	<b>db</b>	Configures the debugging of the AAA local authentication back-end messages and events.
	<b>shim</b>	Configures the debugging of the AAA local authentication shim layer events.
	<b>eap</b>	Configures the debugging of the AAA local Extensible Authentication Protocol (EAP) authentication.
	<b>framework</b>	Configures the debugging of the local EAP framework.
	<b>method</b>	Configures the debugging of local EAP methods.
	<b>all</b>	Configures the debugging of local EAP messages.
	<b>errors</b>	Configures the debugging of local EAP errors.
	<b>events</b>	Configures the debugging of local EAP events.
	<b>packets</b>	Configures the debugging of local EAP packets.
	<b>sm</b>	Configures the debugging of the local EAP state machine.
	<b>enable</b>	Starts the debugging.
	<b>disable</b>	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 bcast

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

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

Syntax Description		
	<b>all</b>	Configures the debugging of all broadcast logs.
	<b>error</b>	Configures the debugging of broadcast errors.
	<b>message</b>	Configures the debugging of broadcast messages.
	<b>igmp</b>	Configures the debugging of broadcast IGMP messages.
	<b>detail</b>	Configures the debugging of broadcast detailed messages.
	<b>enable</b>	Enables the broadcast debugging.
	<b>disable</b>	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 messages:

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

**Related Commands**

- debug disable-all**
- show sysinfo**

# debug cckm

To configure the debugging of the Cisco Centralized Key Management options, use the **debug cckm**

**debug cckm** { **client** | **detailed** } { **enable** | **disable** }

## Syntax Description

<b>client</b>	Configures debugging of the Cisco Centralized Key Management of clients.
<b>detailed</b>	Configures detailed debugging of Cisco Centralized Key Management.
<b>enable</b>	Enables debugging of Cisco Centralized Key Management.
<b>disable</b>	Disables debugging of Cisco Centralized Key Management.

## 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 detailed debugging of Cisco Centralized Key Management:

```
(Cisco Controller) > debug cckm detailed enable
```

# debug cts sxp

To configure debugging of Cisco TrustSec SXP options, use the **debug cts sxp** command.

**debug cts sxp** { **all** | **errors** | **events** | **framework** | **message** } { **enable** | **disable** }

## Syntax Description

<b>all</b>	Configures debugging of all the CTS SXP options
<b>errors</b>	Configures debugging of the CTS SXP errors
<b>events</b>	Configures debugging of the CTS SXP events
<b>framework</b>	Configures debugging of the CTS SXP framework
<b>message</b>	Configures debugging of the CTS SXP messages
<b>enable</b>	Enables debugging
<b>disable</b>	Disables debugging

## Command Default

None

## Command History

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

## Related Topics

[config cts sxp](#), on page 30

# 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

<b>aaa</b>	Configures debugging of the 802.1X AAA interactions.
<b>all</b>	Configures debugging of all the 802.1X messages.
<b>events</b>	Configures debugging of the 802.1X events.
<b>packets</b>	Configures debugging of the 802.1X packets.
<b>states</b>	Configures debugging of the 802.1X state transitions.
<b>enable</b>	Enables debugging of the 802.1X options.
<b>disable</b>	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
```

## Related Topics

[config wlan security 802.1X](#)

[config wlan security wpa akm 802.1x](#)

# debug dtls

To configure debugging of the Datagram Transport Layer Security (DTLS) options, use the **debug dtls** command.

**debug dtls** {all | event | packet | trace} {enable | disable}

## Syntax Description

<b>all</b>	Configures debugging of all the DTLS messages.
<b>event</b>	Configures debugging of the DTLS events.
<b>packet</b>	Configures debugging of the DTLS packets.
<b>trace</b>	Configures debugging of the DTLS trace messages.
<b>enable</b>	Enables debugging of the DTLS options.
<b>disable</b>	Disables debugging of the DTLS options.

## Command Default

None

## Command History

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

## Usage Guidelines

The debug actions described here are used in conjunction with CAPWAP troubleshooting.

The following example shows how to enable DTLS packet debugging:

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

## Related Topics

[show dtls connections](#)

# debug nac

To configure the debugging of Network Access Control (NAC), use the **debug nac** command.

**debug nac** { **events** | **packet** } { **enable** | **disable** }

Syntax Description		
	<b>events</b>	Configures the debugging of NAC events.
	<b>packet</b>	Configures the debugging of NAC packets.
	<b>enable</b>	Enables the NAC debugging.
	<b>disable</b>	Disables the NAC 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 NAC settings:

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

Related Commands	
	<b>show nac statistics</b>
	<b>show nac summary</b>
	<b>config guest-lan nac</b>
	<b>config wlan nac</b>

# debug pm

To configure the debugging of the security policy manager module, use the **debug pm** command.

```
debug pm {all disable | {config | hwcrypto | ikemsg | init | list | message | pki | rng
| rules | sa-export | sa-import | ssh-l2tp | ssh-appgw | ssh-engine | ssh-int | ssh-pmgr
| ssh-ppp | ssh-tcp} {enable | disable}}
```

Syntax Description		
<b>all disable</b>		Disables all debugging in the policy manager module.
<b>config</b>		Configures the debugging of the policy manager configuration.
<b>hwcrypto</b>		Configures the debugging of hardware offload events.
<b>ikemsg</b>		Configures the debugging of Internet Key Exchange (IKE) messages.
<b>init</b>		Configures the debugging of policy manager initialization events.
<b>list</b>		Configures the debugging of policy manager list mgmt.
<b>message</b>		Configures the debugging of policy manager message queue events.
<b>pki</b>		Configures the debugging of Public Key Infrastructure (PKI) related events.
<b>rng</b>		Configures the debugging of random number generation.
<b>rules</b>		Configures the debugging of Layer 3 policy events.
<b>sa-export</b>		Configures the debugging of SA export (mobility).
<b>sa-import</b>		Configures the debugging of SA import (mobility).
<b>ssh-l2tp</b>		Configures the debugging of policy manager Layer 2 Tunneling Protocol (L2TP) handling.
<b>ssh-appgw</b>		Configures the debugging of application gateways.
<b>ssh-engine</b>		Configures the debugging of the policy manager engine.
<b>ssh-int</b>		Configures the debugging of the policy manager interceptor.
<b>ssh-pmgr</b>		Configures the debugging of the policy manager.

<b>ssh-ppp</b>	Configures the debugging of policy manager Point To Point Protocol (PPP) handling.
<b>ssh-tcp</b>	Configures the debugging of policy manager TCP handling.
<b>enable</b>	Enables the debugging.
<b>disable</b>	Disables the debugging.

**Command Default**

None

**Command History**

<b>Release</b>	<b>Modification</b>
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the debugging of PKI-related events:

```
(Cisco Controller) > debug pm pki enable
```

**Related Commands****debug disable-all**

# 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		
<b>redirect</b>		Configures debugging of web-authenticated and redirected clients.
<b>enable</b>		Enables the debugging of web-authenticated clients.
<b>mac</b>		Configures the MAC address of the web-authenticated client.
<i>mac_address</i>		MAC address of the web-authenticated client.
<b>disable</b>		Disables the debugging of web-authenticated clients.
<b>webportal-server</b>		Configures the debugging of portal authentication of clients.
<b>Command Default</b>	None	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	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 wips

To configure debugging of wireless intrusion prevention system (WIPS), use the **debug wips** command.

**debug wips** {all | error | event | nmsp | packet} {enable | disable}

## Syntax Description

<b>all</b>	Configures debugging of all WIPS messages.
<b>error</b>	Configures debugging of WIPS errors.
<b>event</b>	Configures debugging of WIPS events.
<b>nmsp</b>	Configures debugging of WIPS Network Mobility Services Protocol (NMSP) events.
<b>packet</b>	Configures debugging of WIPS packets.
<b>enable</b>	Enables debugging of WIPS.
<b>disable</b>	Disables debugging of WIPS.

## 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 all WIPS messages:

```
(Cisco Controller) > debug wips all enable
```

## Related Commands

**debug client**  
**debug dot11 rogue**  
**show wps summary**  
**show wps wips**

# 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	enable
	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		
	<b>client</b>	Configures the debugging for client MFP messages.
	<b>capwap</b>	Configures the debugging for MFP messages between the controller and access points.
	<b>detail</b>	Configures the detailed debugging for MFP messages.
	<b>report</b>	Configures the debugging for MFP reporting.
	<b>mm</b>	Configures the debugging for MFP mobility (inter-Cisco WLC) messages.
	<b>enable</b>	Enables the debugging for WPS MFP settings.
	<b>disable</b>	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

# show 802.11

To display basic 802.11a, 802.11b/g, or 802.11h network settings, use the **show 802.11** command.

**show 802.11{a | b | h}**

Syntax Description		
<b>a</b>		Specifies the 802.11a network.
<b>b</b>		Specifies the 802.11b/g network.
<b>h</b>		Specifies the 802.11h network.

**Command Default** None.

This example shows to display basic 802.11a network settings:

```
> show 802.11a
802.11a Network..... Enabled
11nSupport..... Enabled
    802.11a Low Band..... Enabled
    802.11a Mid Band..... Enabled
    802.11a High Band..... Enabled
802.11a Operational Rates
    802.11a 6M Rate..... Mandatory
    802.11a 9M Rate..... Supported
    802.11a 12M Rate..... Mandatory
    802.11a 18M Rate..... Supported
    802.11a 24M Rate..... Mandatory
    802.11a 36M Rate..... Supported
    802.11a 48M Rate..... Supported
    802.11a 54M Rate..... Supported
802.11n MCS Settings:
MCS 0..... Supported
MCS 1..... Supported
MCS 2..... Supported
MCS 3..... Supported
MCS 4..... Supported
MCS 5..... Supported
MCS 6..... Supported
MCS 7..... Supported
MCS 8..... Supported
MCS 9..... Supported
MCS 10..... Supported
MCS 11..... Supported
MCS 12..... Supported
MCS 13..... Supported
MCS 14..... Supported
MCS 15..... Supported
802.11n Status:
A-MPDU Tx:
    Priority 0..... Enabled
    Priority 1..... Disabled
    Priority 2..... Disabled
    Priority 3..... Disabled
    Priority 4..... Disabled
    Priority 5..... Disabled
    Priority 6..... Disabled
```

```

        Priority 7..... Disabled
Beacon Interval..... 100
CF Pollable mandatory..... Disabled
CF Poll Request mandatory..... Disabled
--More-- or (q)uit
CFP Period..... 4
CFP Maximum Duration..... 60
Default Channel..... 36
Default Tx Power Level..... 0
DTPC Status..... Enabled
Fragmentation Threshold..... 2346
TI Threshold..... -50
Legacy Tx Beamforming setting..... Disabled
Traffic Stream Metrics Status..... Enabled
Expedited BW Request Status..... Disabled
World Mode..... Enabled
EDCA profile type..... default-wmm
Voice MAC optimization status..... Disabled
Call Admission Control (CAC) configuration
Voice AC:
  Voice AC - Admission control (ACM)..... Disabled
  Voice max RF bandwidth..... 75
  Voice reserved roaming bandwidth..... 6
  Voice load-based CAC mode..... Disabled
  Voice tspec inactivity timeout..... Disabled
  Voice Stream-Size..... 84000
  Voice Max-Streams..... 2
Video AC:
  Video AC - Admission control (ACM)..... Disabled
  Video max RF bandwidth..... Infinite
  Video reserved roaming bandwidth..... 0

```

This example shows how to display basic 802.11h network settings:

```

> show 802.11h
802.11h ..... powerconstraint : 0
802.11h ..... channelswitch : Disable
802.11h ..... channelswitch mode : 0

```

## Related Commands

**show ap stats**

**show ap summary**

**show client summary**

**show network**

**show network summary**

**show port**

**show wlan**

# show aaa auth

To display the configuration settings for the AAA authentication server database, use the **show aaa auth** command.

## show aaa 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 display the configuration settings for the AAA authentication server database:

```
(Cisco Controller) > show aaa auth
Management authentication server order:
 1..... local
 2..... tacacs
```

**Related Commands**

- config aaa auth**
- config aaa auth mgmt**

# show acl

To display the access control lists (ACLs) that are configured on the controller, use the **show acl** command.

```
show acl {cpu | detailed acl_name | summary}
```

Syntax Description		
<b>cpu</b>		Displays the ACLs configured on the Cisco WLC's central processing unit (CPU).
<b>detailed</b>		Displays detailed information about a specific ACL.
<i>acl_name</i>		ACL name. The name can be up to 32 alphanumeric characters.
<b>summary</b>		Displays a summary of all ACLs configured on 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 display the access control lists on the CPU.

```
(Cisco Controller) >show acl cpu

CPU Acl Name.....
Wireless Traffic..... Disabled
Wired Traffic..... Disabled
Applied to NPU..... No
```

The following example shows how to display a summary of the access control lists.

```
(Cisco Controller) > show acl summary

ACL Counter Status          Disabled
-----
IPv4 ACL Name                Applied
-----
acl1                          Yes
acl2                          Yes
acl3                          Yes
-----
IPv6 ACL Name                Applied
-----
acl6                          No
```

The following example shows how to display the detailed information of the access control lists.

```
(Cisco Controller) > show acl detailed acl_name
```

	Source	Destination	Source Port	Dest Port		DSCP
I Dir	IP Address/Netmask	IP Address/Netmask	Prot	Range	Range	Action Counter
1	Any 0.0.0.0/0.0.0.0	0.0.0.0/0.0.0.0	Any	0-65535	0-65535	0 Deny 0
2	In 0.0.0.0/0.0.0.0	200.200.200.0/ 255.255.255.0	6	80-80	0-65535	Any Permit 0
DenyCounter :		0				



**Note** The Counter field increments each time a packet matches an ACL rule, and the DenyCounter field increments each time a packet does not match any of the rules.

#### Related Commands

```
clear acl counters
config acl apply
config acl counter
config acl cpu
config acl create
config acl delete
config interface acl
config acl rule
```

## show advanced eap

To display Extensible Authentication Protocol (EAP) settings, use the **show advanced eap** command.

### show advanced eap

**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 display the EAP settings:

```
(Cisco Controller) > show advanced eap
EAP-Identity-Request Timeout (seconds)..... 1
EAP-Identity-Request Max Retries..... 20
EAP Key-Index for Dynamic WEP..... 0
EAP Max-Login Ignore Identity Response..... enable
EAP-Request Timeout (seconds)..... 1
EAP-Request Max Retries..... 20
EAPOL-Key Timeout (milliseconds)..... 1000
EAPOL-Key Max Retries..... 2
```

**Related Commands**

- config advanced eap**
- config advanced timers eap-identity-request-delay**
- config advanced timers eap-timeout**

# show database summary

To display the maximum number of entries in the database, use the **show database summary** command.

## show database summary

**Syntax Description** This command has no arguments or keywords.

**Command Default** None

The following is a sample output of the **show database summary** command:

```
(Cisco Controller) > show database summary
Maximum Database Entries..... 2048
Maximum Database Entries On Next Reboot..... 2048
Database Contents
  MAC Filter Entries..... 2
  Exclusion List Entries..... 0
  AP Authorization List Entries..... 1
  Management Users..... 1
  Local Network Users..... 1
    Local Users..... 1
    Guest Users..... 0
  Total..... 5
```

**Related Commands** [config database size](#)

# show exclusionlist

To display a summary of all clients on the manual exclusion list from associating with the controller, use the **show exclusionlist** command.

## show exclusionlist

**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 command displays all manually excluded MAC addresses.

The following example shows how to display the exclusion list:

```
(Cisco Controller) > show exclusionlist
No manually disabled clients.
Dynamically Disabled Clients
-----
  MAC Address           Exclusion Reason           Time Remaining (in secs)
  -----
00:40:96:b4:82:55     802.1X Failure            51
```

**Related Commands** **config exclusionlist**

# show ike

To display active Internet Key Exchange (IKE) security associations (SAs), use the **show ike** command.

```
show ike { brief | detailed } IP_or_MAC_address
```

Syntax Description		
<b>brief</b>		Displays a brief summary of all active IKE SAs.
<b>detailed</b>		Displays a detailed summary of all active IKE SAs.
<i>IP_or_MAC_address</i>		IP or MAC address of active IKE SA.
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 display the active Internet Key Exchange security associations:

```
(Cisco Controller) > show ike brief 209.165.200.254
```

# show IPsec

To display active Internet Protocol Security (IPsec) security associations (SAs), use the **show IPsec** command.

**show IPsec** { **brief** | **detailed** } *IP\_or\_MAC\_address*

<b>Syntax Description</b>	<b>brief</b>	Displays a brief summary of active IPsec SAs.
	<b>detailed</b>	Displays a detailed summary of active IPsec SAs.
	<i>IP_or_MAC_address</i>	IP address or MAC address of a device.
<b>Command Default</b>	None	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display brief information about the active Internet Protocol Security (IPsec) security associations (SAs):

```
(Cisco Controller) > show IPsec brief 209.165.200.254
```

<b>Related Commands</b>	<b>config radius acct ipsec authentication</b>
	<b>config radius acct ipsec disable</b>
	<b>config radius acct ipsec enable</b>
	<b>config radius acct ipsec encryption</b>
	<b>config radius auth IPsec encryption</b>
	<b>config radius auth IPsec authentication</b>
	<b>config radius auth IPsec disable</b>
	<b>config radius auth IPsec encryption</b>
	<b>config radius auth IPsec ike</b>
	<b>config trapflags IPsec</b>
	<b>config wlan security IPsec disable</b>
	<b>config wlan security IPsec enable</b>
	<b>config wlan security IPsec authentication</b>
	<b>config wlan security IPsec encryption</b>
<b>config wlan security IPsec config</b>	
<b>config wlan security IPsec ike authentication</b>	

```
config wlan security IPsec ike dh-group
config wlan security IPsec ike lifetime
config wlan security IPsec ike phase1
config wlan security IPsec ike contivity
```

## show ipv6 acl

To display the IPv6 access control lists (ACLs) that are configured on the controller, use the **show ipv6 acl** command.

**show ipv6 acl detailed** { *acl\_name* | **summary** }

<b>Syntax Description</b>	<i>acl_name</i>	IPv6 ACL name. The name can be up to 32 alphanumeric characters.
	<b>detailed</b>	Displays detailed information about a specific ACL.
<b>Command Default</b>	None	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display the detailed information of the access control lists:

```
(Cisco Controller) >show ipv6 acl detailed acl6
Rule Index..... 1
Direction..... Any
IPv6 source prefix..... ::/0
IPv6 destination prefix..... ::/0
Protocol..... Any
Source Port Range..... 0-65535
Destination Port Range..... 0-65535
DSCP..... Any
Flow label..... 0
Action..... Permit
Counter..... 0
Deny Counter..... 0
```

# show ipv6 summary

To display the IPv6 configuration settings, use the **show ipv6 summary** command.

## show ipv6 summary

<b>Syntax Description</b>	This command has no arguments or keywords.
---------------------------	--

<b>Command Default</b>	None
------------------------	------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example displays the output of the **show ipv6 summary** command:

```
(Cisco Controller) >show ipv6 summary
Global Config..... Enabled
Reachable-lifetime value..... 30
Stale-lifetime value..... 300
Down-lifetime value..... 300
RA Throttling..... Disabled
RA Throttling allow at-least..... 1
RA Throttling allow at-most..... no-limit
RA Throttling max-through..... 5
RA Throttling throttle-period..... 600
RA Throttling interval-option..... ignore
NS Multicast CacheMiss Forwarding..... Enabled
NA Multicast Forwarding..... Enabled
IPv6 Capwap UDP Lite..... Enabled
Operating System IPv6 state ..... Enabled
```

# show l2tp

To display Layer 2 Tunneling Protocol (L2TP) sessions, use the **show l2tp** command.

**show l2tp** { **summary** | *ip\_address* }

<b>Syntax Description</b>	<b>summary</b>	Displays all L2TP sessions.
	<i>ip_address</i>	IP address.
<b>Command Default</b>	None	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display a summary of all L2TP sessions:

```
(Cisco Controller) > show l2tp summary
LAC_IPaddr LTid LSid RTid RSid ATid ASid State
-----
```

# show ldap

To display the Lightweight Directory Access Protocol (LDAP) server information for a particular LDAP server, use the **show ldap** command.

**show ldap** *index*

<b>Syntax Description</b>	<i>index</i>	LDAP server index. Valid values are from 1 to 17.
<b>Command Default</b>	None	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display the detailed LDAP server information:

```
(Cisco Controller) > show ldap 1
Server Index..... 1
Address..... 2.3.1.4
Port..... 389
Enabled..... Yes
User DN..... name1
User Attribute..... attr1
User Type..... username1
Retransmit Timeout..... 3 seconds
Bind Method ..... Anonymous
```

<b>Related Commands</b>	<b>config ldap</b> <b>config ldap add</b> <b>config ldap simple-bind</b> <b>show ldap statistics</b> <b>show ldap summary</b>
-------------------------	---

## show ldap statistics

To display all Lightweight Directory Access Protocol (LDAP) server information, use the **show ldap statistics** command.

### show ldap statistics

#### Syntax Description

This command has no arguments or keywords.

#### Command History

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

The following example shows how to display the LDAP server statistics:

```
(Cisco Controller) > show ldap statistics
Server Index..... 1
Server statistics:
  Initialized OK..... 0
  Initialization failed..... 0
  Initialization retries..... 0
  Closed OK..... 0
Request statistics:
  Received..... 0
  Sent..... 0
  OK..... 0
  Success..... 0
  Authentication failed..... 0
  Server not found..... 0
  No received attributes..... 0
  No passed username..... 0
  Not connected to server..... 0
  Internal error..... 0
  Retries..... 0
Server Index..... 2
...
```

#### Related Commands

**config ldap**  
**config ldap add**  
**config ldap simple-bind**  
**show ldap**  
**show ldap summary**

# show ldap summary

To display the current Lightweight Directory Access Protocol (LDAP) server status, use the **show ldap summary** command.

**show ldap summary**

**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 display a summary of configured LDAP servers:

```
(Cisco Controller) > show ldap summary
Idx  Server Address  Port  Enabled
---  -
1    2.3.1.4         389   Yes
2    10.10.20.22    389   Yes
```

**Related Commands**

- config ldap**
- config ldap add**
- config ldap simple-bind**
- show ldap statistics**
- show ldap**

## show local-auth certificates

To display local authentication certificate information, use the **show local-auth certificates** command:

```
show local-auth certificates
```

---

**Syntax Description** This command has no arguments or keywords.

---

**Command Default** None

---

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.

---

The following example shows how to display the authentication certificate information stored locally:

```
(Cisco Controller) > show local-auth certificates
```

---

**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**
- debug aaa local-auth**
- show local-auth config**
- show local-auth statistics**

# show local-auth config

To display local authentication configuration information, use the **show local-auth config** command.

## show local-auth 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 display the local authentication configuration information:

```
(Cisco Controller) > show local-auth config
User credentials database search order:
Primary ..... Local DB
Configured EAP profiles:
Name ..... fast-test
Certificate issuer ..... default
Enabled methods ..... fast
Configured on WLANs ..... 2
EAP Method configuration:
EAP-TLS:
Certificate issuer ..... default
Peer verification options:
  Check against CA certificates ..... Enabled
  Verify certificate CN identity .... Disabled
  Check certificate date validity ... Enabled
EAP-FAST:
TTL for the PAC ..... 3 600
Initial client message ..... <none>
Local certificate required ..... No
Client certificate required ..... No
Vendor certificate required ..... No
Anonymous provision allowed ..... Yes
Authenticator ID ..... 7b7fffffff000000000000000000000000
Authority Information ..... Test
EAP Profile..... tls-prof
Enabled methods for this profile ..... tls
Active on WLANs ..... 1
3EAP Method configuration:
EAP-TLS:
Certificate issuer used ..... cisco
Peer verification options:
  Check against CA certificates ..... disabled
```

```
Verify certificate CN identity .... disabled  
Check certificate date validity ... disabled
```

---

**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**  
**debug aaa local-auth**  
**show local-auth certificates**  
**show local-auth statistics**

## show local-auth statistics

To display local Extensible Authentication Protocol (EAP) authentication statistics, use the **show local-auth statistics** command:

**show local-auth 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 display the local authentication certificate statistics:

```
(Cisco Controller) > show local-auth statistics
Local EAP authentication DB statistics:
Requests received ..... 14
Responses returned ..... 14
Requests dropped (no EAP AVP) ..... 0
Requests dropped (other reasons) ..... 0
Authentication timeouts ..... 0
Authentication statistics:
  Method          Success      Fail
  -----
  Unknown         0            0
  LEAP             0            0
  EAP-FAST        2            0
  EAP-TLS         0            0
  PEAP            0            0
Local EAP credential request statistics:
Requests sent to LDAP DB ..... 0
Requests sent to File DB ..... 2
Requests failed (unable to send) ..... 0
Authentication results received:
  Success ..... 2
  Fail ..... 0
Certificate operations:
Local device certificate load failures ..... 0
Total peer certificates checked ..... 0
Failures:
  CA issuer check ..... 0
  CN name not equal to identity ..... 0
  Dates not valid or expired ..... 0
```

**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**  
**debug aaa local-auth**  
**show local-auth config**  
**show local-auth certificates**

# show nac statistics

To display detailed Network Access Control (NAC) information about a Cisco wireless LAN controller, use the **show nac statistics** command.

## show nac 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 display detailed statistics of network access control settings:

```
(Cisco Controller) > show nac statistics
Server Index..... 1
Server Address.....
xxx.xxx.xxx.xxx
Number of requests sent..... 0
Number of retransmissions..... 0
Number of requests received..... 0
Number of malformed requests received..... 0
Number of bad auth requests received..... 0
Number of pending requests..... 0
Number of timed out requests..... 0
Number of misc dropped request received..... 0
Number of requests sent..... 0
```

**Related Commands**

- show nac summary**
- config guest-lan nac**
- config wlan nac**
- debug nac**

## show nac summary

To display NAC summary information for a Cisco wireless LAN controller, use the **show nac summary** command.

### show nac summary

**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 display a summary information of network access control settings:

```
(Cisco Controller) > show nac summary
NAC ACL Name .....
Index  Server Address                               Port      State
-----  -
1      xxx.xxx.xxx.xxx                                   13336     Enabled
```

**Related Commands**

- show nac statistics
- config guest-lan nac
- config wlan nac
- debug nac

# show netuser

To display the configuration of a particular user in the local user database, use the **show netuser** command.

**show netuser** { **detail** *user\_name* | **guest-roles** | **summary** }

Syntax Description	detail	Displays detailed information about the specified network user.
	<i>user_name</i>	Network user.
	<b>guest_roles</b>	Displays configured roles for guest users.
	<b>summary</b>	Displays a summary of all users in the local user database.

**Command Default** None

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

The following is a sample output of the **show netuser summary** command:

```
(Cisco Controller) > show netuser summary
Maximum logins allowed for a given username .....Unlimited
```

The following is a sample output of the **show netuser detail** command:

```
(Cisco Controller) > show netuser detail john10
username..... abc
WLAN Id..... Any
Lifetime..... Permanent
Description..... test user
```

Related Commands
<b>config netuser add</b>
<b>config netuser delete</b>
<b>config netuser description</b>
<b>config netuser guest-role apply</b>
<b>config netuser wlan-id</b>
<b>config netuser guest-roles</b>

# show netuser guest-roles

To display a list of the current quality of service (QoS) roles and their bandwidth parameters, use the **show netuser guest-roles** command.

**show netuser guest-roles**

**Syntax Description** This command has no arguments or keywords.

**Command Default** None

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.

This example shows how to display a QoS role for the guest network user:

```
(Cisco Controller) > show netuser guest-roles
Role Name..... Contractor
Average Data Rate..... 10
Burst Data Rate..... 10
Average Realtime Rate..... 100
Burst Realtime Rate..... 100
Role Name..... Vendor
Average Data Rate..... unconfigured
Burst Data Rate..... unconfigured
Average Realtime Rate..... unconfigured
Burst Realtime Rate..... unconfigured
```

**Related Commands**

- config netuser add**
- config netuser delete**
- config netuser description**
- config netuser guest-role apply**
- config netuser wlan-id**
- show netuser guest-roles**
- show netuser**

# show network

To display the current status of 802.3 bridging for all WLANs, use the **show network** command.

## **show network**

---

**Syntax Description** This command has no arguments or keywords.

---

**Command Default** None.

This example shows how to display the network details:

```
(Cisco Controller) > show network
```

---

**Related Commands**

- config network**
- show network summary**
- show network multicast mgid detail**
- show network multicast mgid summary**

## show network summary

To display the network configuration of the Cisco wireless LAN controller, use the **show network summary** command.

### show network summary

**Syntax Description** This command has no arguments or keywords.

**Command Default** None.

This example shows how to display a summary configuration:

```
(Cisco Controller) >show network summary
RF-Network Name..... RF
Web Mode..... Disable
Secure Web Mode..... Enable
Secure Web Mode Cipher-Option High..... Disable
Secure Web Mode Cipher-Option SSLv2..... Disable

OCSP..... Disabled
OCSP responder URL.....
Secure Shell (ssh)..... Enable
Telnet..... Enable
Ethernet Multicast Mode..... Disable   Mode: Ucast
Ethernet Broadcast Mode..... Disable
Ethernet Multicast Forwarding..... Disable
Ethernet Broadcast Forwarding..... Disable
AP Multicast/Broadcast Mode..... Unicast
IGMP snooping..... Disabled
IGMP timeout..... 60 seconds
IGMP Query Interval..... 20 seconds
MLD snooping..... Disabled
MLD timeout..... 60 seconds
MLD query interval..... 20 seconds
User Idle Timeout..... 300 seconds
AP Join Priority..... Disable
ARP Idle Timeout..... 300 seconds
ARP Unicast Mode..... Disabled
Cisco AP Default Master..... Disable
Mgmt Via Wireless Interface..... Disable
Mgmt Via Dynamic Interface..... Disable
Bridge MAC filter Config..... Enable
Bridge Security Mode..... EAP
Over The Air Provisioning of AP's..... Enable
Apple Talk ..... Disable
Mesh Full Sector DFS..... Enable
AP Fallback ..... Disable
Web Auth CMCC Support ..... Disabled
Web Auth Redirect Ports ..... 80
Web Auth Proxy Redirect ..... Disable
Web Auth Captive-Bypass ..... Disable
Web Auth Secure Web ..... Enable
Fast SSID Change ..... Disabled
AP Discovery - NAT IP Only ..... Enabled
IP/MAC Addr Binding Check ..... Enabled
CCX-lite status ..... Disable
oep-600 dual-rlan-ports ..... Disable
```

```
oeap-600 local-network ..... Enable
mDNS snooping..... Disabled
mDNS Query Interval..... 15 minutes

Web Color Theme..... Default
CAPWAP Prefer Mode..... IPv4
```

# show ntp-keys

To display network time protocol authentication key details, use the **show ntp-keys** command.

## show ntp-keys

**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 display NTP authentication key details:

```
(Cisco Controller) > show ntp-keys
Ntp Authentication Key Details.....
  Key Index
  -----
      1
      3
```

**Related Commands** `config time ntp`

# show radius acct statistics

To display the RADIUS accounting server statistics for the Cisco wireless LAN controller, use the **show radius acct statistics** command.

## show radius acct 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 display RADIUS accounting server statistics:

```
(Cisco Controller) > show radius acct statistics
Accounting Servers:
Server Index..... 1
Server Address..... 10.1.17.10
Msg Round Trip Time..... 0 (1/100 second)
First Requests..... 0
Retry Requests..... 0
Accounting Responses..... 0
Malformed Msgs..... 0
Bad Authenticator Msgs..... 0
Pending Requests..... 0
Timeout Requests..... 0
Unknowntype Msgs..... 0
Other Drops..... 0
```

**Related Commands**

- config radius acct**
- config radius acct ipsec authentication**
- config radius acct ipsec disable**
- config radius acct network**
- show radius auth statistics**
- show radius summary**

## show radius auth statistics

To display the RADIUS authentication server statistics for the Cisco wireless LAN controller, use the **show radius auth statistics** command.

### show radius auth statistics

This command has no arguments or keyword.

#### 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 display RADIUS authentication server statistics:

```
(Cisco Controller) > show radius auth statistics
Authentication Servers:
  Server Index..... 1
  Server Address..... 209.165.200.10
  Msg Round Trip Time..... 0 (1/100 second)
  First Requests..... 0
  Retry Requests..... 0
  Accept Responses..... 0
  Reject Responses..... 0
  Challenge Responses..... 0
  Malformed Msgs..... 0
  Bad Authenticator Msgs..... 0
  Pending Requests..... 0
  Timeout Requests..... 0
  Unknowntype Msgs..... 0
  Other Drops..... 0
```

#### Related Commands

**config radius auth**  
**config radius auth management**  
**config radius auth network**  
**show radius summary**

# show radius summary

To display the RADIUS authentication and accounting server summary, use the **show radius summary** command.

## show radius summary

**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 display a RADIUS authentication server summary:

```
(Cisco Controller) > show radius summary
Vendor Id Backward Compatibility..... Disabled
Credentials Caching..... Disabled
Call Station Id Type..... IP Address
Administrative Authentication via RADIUS..... Enabled
Authentication Servers
Index Type Server Address Port State Tout RFC-3576 IPsec -
AuthMod
e/Phase1/Group/Lifetime/Auth/Encr
-----
Accounting Servers
Index Type Server Address Port State Tout RFC-3576 IPsec -
AuthMod
e/Phase1/Group/Lifetime/Auth/Encr
-----
```

**Related Commands** **show radius auth statistics**

**show radius acct statistics**

# show rules

To display the active internal firewall rules, use the **show rules** command.

## show rules

**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 display active internal firewall rules:

```
(Cisco Controller) > show rules
-----
Rule ID.....: 3
Ref count.....: 0
Precedence.....: 99999999
Flags.....: 00000001 ( PASS )
Source IP range:
    (Local stack)
Destination IP range:
    (Local stack)
-----
Rule ID.....: 25
Ref count.....: 0
Precedence.....: 99999999
Flags.....: 00000001 ( PASS )
Service Info
    Service name.....: GDB
    Protocol.....: 6
    Source port low.....: 0
    Source port high.....: 0
    Dest port low.....: 1000
    Dest port high.....: 1000
Source IP range:
IP High.....: 0.0.0.0
    Interface.....: ANY
Destination IP range:
    (Local stack)
-----
```

# show switchconfig

To display parameters that apply to the Cisco wireless LAN controller, use the **show switchconfig** command.

## show switchconfig

**Syntax Description** This command has no arguments or keywords.

**Command Default** Enabled.

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

This example shows how to display parameters that apply to the Cisco wireless LAN controller:

```
(Cisco Controller) >> show switchconfig
802.3x Flow Control Mode..... Disabled
FIPS prerequisite features..... Enabled
Boot Break..... Enabled
secret obfuscation..... Enabled
Strong Password Check Features:
  case-check .....Disabled
  consecutive-check ...Disabled
  default-check .....Disabled
  username-check .....Disabled
```

**Related Commands**

- config switchconfig mode**
- config switchconfig secret-obfuscation**
- config switchconfig strong-pwd**
- config switchconfig flowcontrol**
- config switchconfig fips-prerequisite**
- show stats switch**

# show rogue adhoc custom summary

To display information about custom rogue ad-hoc rogue access points, use the **show rogue adhoc custom summary** command.

**show rogue adhoc custom summary**

**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 display details of custom rogue ad-hoc rogue access points:

```
(Cisco Controller) > show rogue adhoc custom summary
Number of Adhocs.....0

MAC Address          State                # APs # Clients Last Heard
-----
-----
```

**Related Commands**

- show rogue adhoc detailed
- show rogue adhoc summary
- show rogue adhoc friendly summary
- show rogue adhoc malicious summary
- show rogue adhoc unclassified summary
- config rogue adhoc

# show rogue adhoc detailed

To display details of an ad-hoc rogue access point detected by the Cisco wireless LAN controller, use the **show rogue adhoc client detailed** command.

**show rogue adhoc detailed** *MAC\_address*

<b>Syntax Description</b>	<i>MAC_address</i>	Adhoc rogue MAC address.
<b>Command Default</b>	None	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display detailed ad-hoc rogue MAC address information:

```
(Cisco Controller) > show rogue adhoc client detailed 02:61:ce:8e:a8:8c
Adhoc Rogue MAC address..... 02:61:ce:8e:a8:8c
Adhoc Rogue BSSID..... 02:61:ce:8e:a8:8c
State..... Alert
First Time Adhoc Rogue was Reported..... Tue Dec 11 20:45:45
2007
Last Time Adhoc Rogue was Reported..... Tue Dec 11 20:45:45
2007
Reported By
AP 1
MAC Address..... 00:14:1b:58:4a:e0
Name..... AP0014.1ced.2a60
Radio Type..... 802.11b
SSID..... rf4k3ap
Channel..... 3
RSSI..... -56 dBm
SNR..... 15 dB
Encryption..... Disabled
ShortPreamble..... Disabled
WPA Support..... Disabled
Last reported by this AP..... Tue Dec 11 20:45:45 2007
```

<b>Related Commands</b>	<b>config rogue adhoc</b>
	<b>show rogue ignore-list</b>
	<b>show rogue rule summary</b>
	<b>show rogue rule detailed</b>
	<b>config rogue rule</b>
	<b>show rogue adhoc summary</b>

## show rogue adhoc friendly summary

To display information about friendly rogue ad-hoc rogue access points, use the **show rogue adhoc friendly summary** command.

**show rogue adhoc friendly summary**

**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 display information about friendly rogue ad-hoc rogue access points:

```
(Cisco Controller) > show rogue adhoc friendly summary
```

```
Number of Adhocs.....0
```

```
MAC Address          State                # APs # Clients Last Heard
-----
```

**Related Commands** **show rogue adhoc custom summary**

**show rogue adhoc detailed**

**show rogue adhoc summary**

**show rogue adhoc malicious summary**

**show rogue adhoc unclassified summary**

**config rogue adhoc**

# show rogue adhoc malicious summary

To display information about malicious rogue ad-hoc rogue access points, use the **show rogue adhoc malicious summary** command.

**show rogue adhoc malicious summary**

**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 display details of malicious rogue ad-hoc rogue access points:

```
(Cisco Controller) > show rogue adhoc malicious summary
Number of Adhocs.....0

MAC Address          State                # APs # Clients Last Heard
-----
-----
```

**Related Commands**

- show rogue adhoc custom summary**
- show rogue adhoc detailed**
- show rogue adhoc summary**
- show rogue adhoc friendly summary**
- show rogue adhoc unclassified summary**
- config rogue adhoc**

# show rogue adhoc unclassified summary

To display information about unclassified rogue ad-hoc rogue access points, use the **show rogue adhoc unclassified summary** command.

**show rogue adhoc unclassified summary**

**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 display information about unclassified rogue ad-hoc rogue access points:

```
(Cisco Controller) > show rogue adhoc unclassified summary
```

```
Number of Adhocs.....0
```

```
MAC Address          State                # APs # Clients Last Heard
-----
```

**Related Commands**

- show rogue adhoc custom summary**
- show rogue adhoc detailed**
- show rogue adhoc summary**
- show rogue adhoc friendly summary**
- show rogue adhoc malicious summary**
- config rogue adhoc**

# show rogue adhoc summary

To display a summary of the ad-hoc rogue access points detected by the Cisco wireless LAN controller, use the **show rogue adhoc summary** command.

## show rogue adhoc summary

**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 display a summary of all ad-hoc rogues:

```
(Cisco Controller) > show rogue adhoc summary
Detect and report Ad-Hoc Networks..... Enabled
Client MAC Address      Adhoc BSSID      State # APs      Last Heard
-----
xx:xx:xx:xx:xx:xx      super            Alert  1              Sat Aug  9 21:12:50
 2004
xx:xx:xx:xx:xx:xx                        Alert  1              Aug  9 21:12:50
2003
xx:xx:xx:xx:xx:xx                        Alert  1              Sat Aug  9 21:10:50
2003
```

**Related Commands**

- config rogue adhoc**
- show rogue ignore-list**
- show rogue rule summary**
- show rogue rule detailed**
- config rogue rule**
- show rogue adhoc detailed**

## show rogue ap custom summary

To display information about custom rogue ad-hoc rogue access points, use the **show rogue ap custom summary** command.

**show rogue ap custom summary**

**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 display details of custom rogue ad-hoc rogue access points:

```
(Cisco Controller) > show rogue ap custom summary
```

```
Number of APs.....0
```

```
MAC Address          State                # APs # Clients Last Heard
-----
```

### Related Commands

- config rogue adhoc
- config rogue ap classify
- config rogue ap friendly
- config rogue ap rldp
- config rogue ap timeout
- config rogue ap valid-client
- config rogue client
- config trapflags rogueap
- show rogue ap clients
- show rogue ap detailed
- show rogue ap summary
- show rogue ap malicious summary
- show rogue ap unclassified summary
- show rogue client detailed
- show rogue client summary
- show rogue ignore-list

**show rogue rule detailed**

**show rogue rule summary**

## show rogue ap clients

To display details of rogue access point clients detected by the Cisco wireless LAN controller, use the **show rogue ap clients** command.

**show rogue ap clients** *ap\_mac\_address*

<b>Syntax Description</b>	<i>ap_mac_address</i>	Rogue access point MAC address.
<b>Command Default</b>	None	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display details of rogue access point clients:

```
(Cisco Controller) > show rogue ap clients xx:xx:xx:xx:xx:xx
MAC Address State # APs Last Heard
-----
00:bb:cd:12:ab:ff Alert 1 Fri Nov 30 11:26:23 2007
```

<b>Related Commands</b>	<b>config rogue adhoc</b> <b>config rogue ap classify</b> <b>config rogue ap friendly</b> <b>config rogue ap rldp</b> <b>config rogue ap timeout</b> <b>config rogue ap valid-client</b> <b>config rogue client</b> <b>config trapflags rogueap</b> <b>show rogue ap detailed</b> <b>show rogue ap summary</b> <b>show rogue ap friendly summary</b> <b>show rogue ap malicious summary</b> <b>show rogue ap unclassified summary</b> <b>show rogue client detailed</b> <b>show rogue client summary</b> <b>show rogue ignore-list</b> <b>show rogue rule detailed</b>
-------------------------	--

**show rogue rule summary**

## show rogue ap detailed

To display details of a rogue access point detected by the Cisco wireless LAN controller, use the **show rogue-ap detailed** command.

**show rogue ap detailed** *ap\_mac\_address*

<b>Syntax Description</b>	<i>ap_mac_address</i>	Rogue access point MAC address.
<b>Command Default</b>	None	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display detailed information of a rogue access point:

```
(Cisco Controller) > show rogue ap detailed xx:xx:xx:xx:xx:xx
Rogue BSSID..... 00:0b:85:63:d1:94
Is Rogue on Wired Network..... No
Classification..... Unclassified
State..... Alert
First Time Rogue was Reported..... Fri Nov 30 11:24:56
2007
Last Time Rogue was Reported..... Fri Nov 30 11:24:56
2007
Reported By
AP 1
MAC Address..... 00:12:44:bb:25:d0
Name..... flexconnect
Radio Type..... 802.11g
SSID..... edu-eap
Channel..... 6
RSSI..... -61 dBm
SNR..... -1 dB
Encryption..... Enabled
ShortPreamble..... Enabled
WPA Support..... Disabled
Last reported by this AP..... Fri Nov 30 11:24:56 2007
```

This example shows how to display detailed information of a rogue access point with a customized classification:

```
(Cisco Controller) > show rogue ap detailed xx:xx:xx:xx:xx:xx
Rogue BSSID..... 00:17:0f:34:48:a0
Is Rogue on Wired Network..... No
Classification..... custom
```

```

Severity Score ..... 1
Class Name.....VeryMalicious
Class Change by..... Rogue Rule
Classified at ..... -60 dBm
Classified by..... c4:0a:cb:a1:18:80

State..... Contained
State change by..... Rogue Rule
First Time Rogue was Reported..... Mon Jun  4 10:31:18
2012
Last Time Rogue was Reported..... Mon Jun  4 10:31:18
2012
Reported By
  AP 1
    MAC Address..... c4:0a:cb:a1:18:80
    Name..... SHIELD-3600-2027
    Radio Type..... 802.11g
    SSID..... sri
    Channel..... 11
    RSSI..... -87 dBm
    SNR..... 4 dB
    Encryption..... Enabled
    ShortPreamble..... Enabled
    WPA Support..... Enabled
    Last reported by this AP..... Mon Jun  4 10:31:18
2012

```

**Related Commands**

```

config rogue adhoc
config rogue ap classify
config rogue ap friendly
config rogue ap rldp
config rogue ap timeout
config rogue ap valid-client
config rogue client
config trapflags rogueap
show rogue ap clients
show rogue ap summary
show rogue ap friendly summary
show rogue ap malicious summary
show rogue ap unclassified summary
show rogue client detailed
show rogue client summary

```

■ show rogue ap detailed

show rogue ignore-list  
show rogue rule detailed  
show rogue rule summary

# show rogue ap summary

To display a summary of the rogue access points detected by the Cisco wireless LAN controller, use the **show rogue-ap summary** command.

**show rogue ap summary** {ssid | channel}

<b>Syntax Description</b>	<i>ssid</i>	Displays specific user-configured SSID of the rogue access point.
	<i>channel</i>	Displays specific user-configured radio type and channel of the rogue access point.
<b>Command Default</b>	None	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.
	8.0	The new keywords <b>SSID</b> and <b>channel</b> are added.

The following example shows how to display a summary of all rogue access points:

```
(Cisco Controller) > show rogue ap summary

Rogue Location Discovery Protocol..... Disabled
Rogue ap timeout..... 1200
Rogue on wire Auto-Contain..... Disabled
Rogue using our SSID Auto-Contain..... Disabled
Valid client on rogue AP Auto-Contain..... Disabled
Rogue AP timeout..... 1200
Rogue Detection Report Interval..... 10
Rogue Detection Min Rssi..... -128
Rogue Detection Transient Interval..... 0
Rogue Detection Client Num Thershold..... 0
Total Rogues (AP+Ad-hoc) supported..... 2000
Total Rogues classified..... 729

MAC Address          Classification      # APs # Clients Last Heard
-----
xx:xx:xx:xx:xx:xx   friendly          1     0     Thu Aug  4 18:57:11 2005
xx:xx:xx:xx:xx:xx   malicious         1     0     Thu Aug  4 19:00:11 2005
xx:xx:xx:xx:xx:xx   malicious         1     0     Thu Aug  4 18:57:11 2005
xx:xx:xx:xx:xx:xx   malicious         1     0     Thu Aug  4 18:57:11 2005
```

The following example shows how to display a summary of all rogue access points with SSID as extended parameter.

```
(Cisco Controller) > show rogue ap summary ssid

MAC Address          Class           State      SSID  Security
-----
xx:xx:xx:xx:xx:xx   Unclassified   Alert     xxx   Open
```

**show rogue ap summary**

```

xx:xx:xx:xx:xx:xx  Unclassified  Alert  xxx  Open
xx:xx:xx:xx:xx:xx  Pending      Pending xxx  Open
xx:xx:xx:xx:xx:xx  Unclassified Alert  xxx  WEP/WPA

```

The following example shows how to display a summary of all rogue access points with channel as extended parameter.

```
(Cisco Controller) > show rogue ap summary channel
```

MAC Address	Class	State	Det	RadioType	Channel	RSSIlast/Max)
xx:xx:xx:xx:xx:xx	Unclassified	Alert	802.11g		11	-53 / -48
xx:xx:xx:xx:xx:xx	Unclassified	Alert	802.11g		11	-53 / -48
xx:xx:xx:xx:xx:xx	Unclassified	Alert	802.11a		149	-74 / -69
xx:xx:xx:xx:xx:xx	Unclassified	Alert	802.11a		149	-74 / -69
xx:xx:xx:xx:xx:xx	Unclassified	Alert	802.11a		149	-74 / -69

The following example shows how to display a summary of all rogue access points with both SSID and channel as extended parameters.

```
(Cisco Controller) > show rogue ap summary ssid channel
```

MAC Address	Class	State	SSID	Security	Det	RadioType
Channel	RSSI (last/Max)					
xx:xx:xx:xx:xx:xx	Unclassified	Alert	dd	WEP/WPA	802.11n5G	
56	-73 / -62					
xx:xx:xx:xx:xx:xx	Unclassified	Alert	SSID IS HIDDEN	Open	802.11a	
149	-68 / -66					
xx:xx:xx:xx:xx:xx	Unclassified	Alert	wlan16	WEP/WPA	802.11n5G	
149	-71 / -71					
xx:xx:xx:xx:xx:xx	Unclassified	Alert	wlan15	WEP/WPA	802.11n5G	
149	-71 / -71					
xx:xx:xx:xx:xx:xx	Unclassified	Alert	wlan14	WEP/WPA	802.11n5G	
149	-71 / -71					
xx:xx:xx:xx:xx:xx	Unclassified	Alert	wlan13	WEP/WPA	802.11n5G	
149	-71 / -70					
xx:xx:xx:xx:xx:xx	Unclassified	Alert	wlan12	WEP/WPA	802.11n5G	
149	-71 / -71					

**Related Commands**

```

config rogue adhoc
config rogue ap classify
config rogue ap friendly
config rogue ap rldp
config rogue ap timeout
config rogue ap valid-client
config rogue client
config trapflags rogueap
show rogue ap clients
show rogue ap detailed
show rogue ap friendly summary
show rogue ap malicious summary

```

**show rogue ap unclassified summary**

**show rogue client detailed**

**show rogue client summary**

**show rogue ignore-list**

**show rogue rule detailed**

**show rogue rule summary**

# show rogue ap friendly summary

To display a list of the friendly rogue access points detected by the controller, use the **show rogue ap friendly summary** command.

## show rogue ap friendly summary

**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 display a summary of all friendly rogue access points:

```
(Cisco Controller) > show rogue ap friendly summary
Number of APs..... 1
MAC Address      State      # APs  # Clients Last Heard
-----
XX:XX:XX:XX:XX:XX Internal    1     0  Tue Nov 27 13:52:04 2007
```

## Related Commands

- config rogue adhoc
- config rogue ap classify
- config rogue ap friendly
- config rogue ap rldp
- config rogue ap timeout
- config rogue ap valid-client
- config rogue client
- config trapflags rogueap
- show rogue ap clients
- show rogue ap detailed
- show rogue ap summary
- show rogue ap malicious summary
- show rogue ap unclassified summary
- show rogue client detailed
- show rogue client summary
- show rogue ignore-list

**show rogue rule detailed**

**show rogue rule summary**

## show rogue ap malicious summary

To display a list of the malicious rogue access points detected by the controller, use the **show rogue ap malicious summary** command.

**show rogue ap malicious summary**

**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 display a summary of all malicious rogue access points:

```
(Cisco Controller) > show rogue ap malicious summary
Number of APs..... 2
MAC Address      State      # APs  # Clients Last Heard
-----
XX:XX:XX:XX:XX:XX Alert          1    0 Tue Nov 27 13:52:04 2007
XX:XX:XX:XX:XX:XX Alert          1    0 Tue Nov 27 13:52:04 2007
```

### Related Commands

- config rogue adhoc**
- config rogue ap classify**
- config rogue ap friendly**
- config rogue ap rldp**
- config rogue ap timeout**
- config rogue ap valid-client**
- config rogue client**
- config trapflags rogueap**
- show rogue ap clients**
- show rogue ap detailed**
- show rogue ap summary**
- show rogue ap friendly summary**
- show rogue ap unclassified summary**
- show rogue client detailed**
- show rogue client summary**

**show rogue ignore-list**  
**show rogue rule detailed**  
**show rogue rule summary**

## show rogue ap unclassified summary

To display a list of the unclassified rogue access points detected by the controller, use the **show rogue ap unclassified summary** command.

### show rogue ap unclassified summary

**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 display a list of all unclassified rogue access points:

```
(Cisco Controller) > show rogue ap unclassified summary
Number of APs..... 164
MAC Address      State # APs # Clients Last Heard
-----
XX:XX:XX:XX:XX:XX Alert 1      0    Fri Nov 30 11:12:52 2007
XX:XX:XX:XX:XX:XX Alert 1      0    Fri Nov 30 11:29:01 2007
XX:XX:XX:XX:XX:XX Alert 1      0    Fri Nov 30 11:26:23 2007
XX:XX:XX:XX:XX:XX Alert 1      0    Fri Nov 30 11:26:23 2007
```

# show rogue auto-contain

To display information about rogue auto-containment, use the **show rogue auto-contain** command.

**show rogue auto-contain**

---

**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 display information about rogue auto-containment:

```
(Cisco Controller) > show rogue auto-contain
Containment Level..... 3
monitor_ap_only..... false
```

---

**Related Commands**

- config rogue adhoc**
- config rogue auto-contain level**

## show rogue client detailed

To display details of a rogue client detected by a Cisco wireless LAN controller, use the **show rogue client detailed** command.

**show rogue client detailed** *Rogue\_AP MAC\_address*

<b>Syntax Description</b>	<i>Rogue_AP</i>	Rogue AP address.
	<i>MAC_address</i>	Rogue client MAC address.
<b>Command Default</b>	None	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.
	8.1	The <i>Rogue_AP</i> parameter to the <b>show rogue client detailed</b> command is added.

The following example shows how to display detailed information for a rogue client:

```
(Cisco Controller) > show rogue client detailed xx:xx:xx:xx:xx:xx
Rogue BSSID..... 00:0b:85:23:ea:d1
State..... Alert
First Time Rogue was Reported..... Mon Dec 3 21:50:36 2007
Last Time Rogue was Reported..... Mon Dec 3 21:50:36 2007
Rogue Client IP address..... Not known
Reported By
AP 1
MAC Address..... 00:15:c7:82:b6:b0
Name..... AP0016.47b2.31ea
Radio Type..... 802.11a
RSSI..... -71 dBm
SNR..... 23 dB
Channel..... 149
Last reported by this AP..... Mon Dec 3 21:50:36 2007
```

<b>Related Commands</b>	<b>show rogue client summary</b>
	<b>show rogue ignore-list</b>
	<b>config rogue rule client</b>
	<b>config rogue rule</b>

# show rogue client summary

To display a summary of the rogue clients detected by the Cisco wireless LAN controller, use the **show rogue client summary** command.

## show rogue client summary

**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 display a list of all rogue clients:

```
(Cisco Controller) > show rogue client summary
Validate rogue clients against AAA..... Disabled
Total Rogue Clients supported..... 2500
Total Rogue Clients present..... 3
MAC Address          State          # APs Last Heard
-----
xx:xx:xx:xx:xx:xx  Alert          1    Thu Aug  4 19:00:08 2005
xx:xx:xx:xx:xx:xx  Alert          1    Thu Aug  4 19:09:11 2005
xx:xx:xx:xx:xx:xx  Alert          1    Thu Aug  4 19:03:11 2005
xx:xx:xx:xx:xx:xx  Alert          1    Thu Aug  4 19:03:11 2005
xx:xx:xx:xx:xx:xx  Alert          1    Thu Aug  4 19:09:11 2005
xx:xx:xx:xx:xx:xx  Alert          1    Thu Aug  4 18:57:08 2005
xx:xx:xx:xx:xx:xx  Alert          1    Thu Aug  4 19:12:08 2005
```

**Related Commands**

- show rogue client detailed
- show rogue ignore-list
- config rogue client
- config rogue rule

## show rogue ignore-list

To display a list of rogue access points that are configured to be ignored, use the **show rogue ignore-list** command.

**show rogue ignore-list**

---

**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 display a list of all rogue access points that are configured to be ignored.

```
(Cisco Controller) > show rogue ignore-list
```

```
MAC Address
-----
xx:xx:xx:xx:xx:xx
```

---

**Related Commands**

- config rogue adhoc
- config rogue ap classify
- config rogue ap friendly
- config rogue ap rldp
- config rogue ap ssid
- config rogue ap timeout
- config rogue ap valid-client
- config rogue rule
- config trapflags rogueap
- show rogue client detailed
- show rogue ignore-list
- show rogue rule summary
- show rogue client summary
- show rogue ap unclassified summary
- show rogue ap malicious summary
- show rogue ap friendly summary

**config rogue client**  
**show rogue ap summary**  
**show rogue ap clients**  
**show rogue ap detailed**  
**config rogue rule**

# show rogue rule detailed

To display detailed information for a specific rogue classification rule, use the **show rogue rule detailed** command.

**show rogue rule detailed** *rule\_name*

<b>Syntax Description</b>	<i>rule_name</i>	Rogue rule name.
<b>Command Default</b>	None	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display detailed information on a specific rogue classification rule:

```
(Cisco Controller) > show rogue rule detailed Rule2
Priority..... 2
Rule Name..... Rule2
State..... Enabled
Type..... Malicious
Severity Score..... 1
Class Name..... Very_Malicious
Notify..... All
State ..... Contain
Match Operation..... Any
Hit Count..... 352
Total Conditions..... 2
Condition 1
  type..... Client-count
  value..... 10
Condition 2
  type..... Duration
  value (seconds)..... 2000
Condition 3
  type..... Managed-ssid
  value..... Enabled
Condition 4
  type..... No-encryption
  value..... Enabled
Condition 5
  type..... Rssi
  value (dBm)..... -50
Condition 6
  type..... Ssid
  SSID Count..... 1
  SSID 1..... test
```

**Related Commands**

- config rogue rule**
- show rogue ignore-list**

**show rogue rule summary**

## show rogue rule summary

To display the rogue classification rules that are configured on the controller, use the **show rogue rule summary** command.

### show rogue rule summary

**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 display a list of all rogue rules that are configured on the controller:

```
(Cisco Controller) > show rogue rule summary
Priority Rule Name           State   Type           Match Hit Count
-----
1       mtest                   Enabled Malicious      All    0
2       asdfasdf                 Enabled Malicious      All    0
```

The following example shows how to display a list of all rogue rules that are configured on the controller:

```
(Cisco Controller) > show rogue rule summary
Priority Rule Name           Rule state Class Type  Notify
State   Match Hit Count
-----
1       rule2                   Enabled  Friendly Global
Alert   All    234
2       rule1                   Enabled  Custom  Global
Alert   All    0
```

**Related Commands**

- config rogue rule
- show rogue ignore-list
- show rogue rule detailed

## show tacacs acct statistics

To display detailed radio frequency identification (RFID) information for a specified tag, use the **show tacacs acct statistics** command.

### show tacacs acct 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 display detailed RFID information:

```
(Cisco Controller) > show tacacs acct statistics
Accounting Servers:
Server Index..... 1
Server Address..... 10.0.0.0
Msg Round Trip Time..... 0 (1/100 second)
First Requests..... 1
Retry Requests..... 0
Accounting Response..... 0
Accounting Request Success..... 0
Accounting Request Failure..... 0
Malformed Msgs..... 0
Bad Authenticator Msgs..... 0
Pending Requests..... -1
Timeout Requests..... 1
Unknowntype Msgs..... 0
Other Drops..... 0
```

## show tacacs athr statistics

To display TACACS+ server authorization statistics, use the **show tacacs athr statistics** command.

### show tacacs athr 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 display TACACS server authorization statistics:

```
(Cisco Controller) > show tacacs athr statistics
Authorization Servers:
Server Index..... 3
Server Address..... 10.0.0.3
Msg Round Trip Time..... 0 (1/100 second)
First Requests..... 0
Retry Requests..... 0
Received Responses..... 0
Authorization Success..... 0
Authorization Failure..... 0
Challenge Responses..... 0
Malformed Msgs..... 0
Bad Authenticator Msgs..... 0
Pending Requests..... 0
Timeout Requests..... 0
Unknowntype Msgs..... 0
Other Drops..... 0
```

**Related Commands**

- config tacacs acct**
- config tacacs athr**
- config tacacs auth**
- show tacacs auth statistics**
- show tacacs summary**

## show tacacs auth statistics

To display TACACS+ server authentication statistics, use the **show tacacs auth statistics** command.

### show tacacs auth statistics

<b>Syntax Description</b>	This command has no arguments or keywords.
---------------------------	--

<b>Command Default</b>	None
------------------------	------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display TACACS server authentication statistics:

```
(Cisco Controller) > show tacacs auth statistics
Authentication Servers:
Server Index..... 2
Server Address..... 10.0.0.2
Msg Round Trip Time..... 0 (msec)
First Requests..... 0
Retry Requests..... 0
Accept Responses..... 0
Reject Responses..... 0
Error Responses..... 0
Restart Responses..... 0
Follow Responses..... 0
GetData Responses..... 0
Encrypt no secret Responses..... 0
Challenge Responses..... 0
Malformed Msgs..... 0
Bad Authenticator Msgs..... 0
Pending Requests..... 0
Timeout Requests..... 0
Unknowntype Msgs..... 0
Other Drops..... 0
```

# show tacacs summary

To display TACACS+ server summary information, use the **show tacacs summary** command.

## show tacacs summary

**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 display TACACS server summary information:

```
(Cisco Controller) > show tacacs summary
Authentication Servers
Idx  Server Address      Port   State   Tout
---  -
2    10.0.0.1             49    Enabled 30
Accounting Servers
Idx  Server Address      Port   State   Tout
---  -
1    10.0.0.0             49    Enabled  5
Authorization Servers
Idx  Server Address      Port   State   Tout
---  -
3    10.0.0.3             49    Enabled  5
Idx  Server Address      Port   State   Tout
---  -
4    2001:9:6:40::623    49    Enabled  5
...
```

**Related Commands**

- config tacacs acct**
- config tacacs athr**
- config tacacs auth**
- show tacacs summary**
- show tacacs athr statistics**
- show tacacs auth statistics**

# show wps ap-authentication summary

To display the access point neighbor authentication configuration on the controller, use the **show wps ap-authentication summary** command.

## show wps ap-authentication summary

**Syntax Description** This command has no arguments or keywords.

**Command Default** None

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display a summary of the Wireless Protection System (WPS) access point neighbor authentication:

```
(Cisco Controller) > show wps ap-authentication summary
AP neighbor authentication is <disabled>.
Authentication alarm threshold is 1.
RF-Network Name: <B1>
```

**Related Commands** **config wps ap-authentication**

## show wps cids-sensor

To display Intrusion Detection System (IDS) sensor summary information or detailed information on a specified Wireless Protection System (WPS) IDS sensor, use the **show wps cids-sensor** command.

**show wps cids-sensor** { **summary** | **detail** *index* }

<b>Syntax Description</b>	<b>summary</b>	Displays a summary of sensor settings.
	<b>detail</b>	Displays all settings for the selected sensor.
	<i>index</i>	IDS sensor identifier.
<b>Command Default</b>	None	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display all settings for the selected sensor:

```
(Cisco Controller) > show wps cids-sensor detail1
IP Address..... 10.0.0.51
Port..... 443
Query Interval..... 60
Username..... Sensor_user1
Cert Fingerprint..... SHA1:
00:00:00:00:00:00:00:00:
00:00:00:00:00:00:00:00:00:00:00
Query State..... Disabled
Last Query Result..... Unknown
Number of Queries Sent..... 0
```

**Related Commands**    **config wps ap-authentication**

# show wps mfp

To display Management Frame Protection (MFP) information, use the **show wps mfp** command.

**show wps mfp** {summary | statistics}

Syntax Description	summary	Displays the MFP configuration and status.
	statistics	Displays MFP 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 display a summary of the MFP configuration and status:

```
(Cisco Controller) > show wps mfp summary
Global Infrastructure MFP state..... DISABLED (*all infrastructure
settings are overridden)
Controller Time Source Valid..... False

WLAN ID  WLAN Name                WLAN      Infra.    Client
-----  -
1         homeap                          Disabled  *Enabled  Optional but inactive
(WPA2 not configured)
2         7921                            Enabled   *Enabled  Optional but inactive
(WPA2 not configured)
3         open1                           Enabled   *Enabled  Optional but inactive
(WPA2 not configured)
4         7920                            Enabled   *Enabled  Optional but inactive
(WPA2 not configured)

AP Name      Infra.      Operational  --Infra. Capability--
Validation  Radio      State         Protection  Validation
-----
AP1252AG-EW  *Enabled   b/g          Down        Full        Full
              a          Down        Full        Full
```

The following example shows how to display the MFP statistics:

```
(Cisco Controller) > show wps mfp statistics
BSSID      Radio Validator AP      Last Source Addr  Found  Error Type
Count      Frame Types
-----
no errors
```

**Related Commands**    **config wps mfp**

# show wps shun-list

To display the Intrusion Detection System (IDS) sensor shun list, use the **show wps shun-list** command.

**show wps shun-list**

---

**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 display the IDS system sensor shun list:

```
(Cisco Controller) > show wps shun-list
```

---

**Related Commands** **config wps shun-list re-sync**

# show wps signature detail

To display installed signatures, use the **show wps signature detail** command.

**show wps signature detail** *sig-id*

<b>Syntax Description</b>	<i>sig-id</i>	Signature ID of an installed signature.
<b>Command Default</b>	None	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.6	This command was introduced in a release earlier than Release 7.6.

This example shows how to display information on the attacks detected by standard signature 1:

```
(Cisco Controller) > show wps signature detail 1
Signature-ID..... 1
Precedence..... 1
Signature Name..... Bcast deauth
Type..... standard
FrameType..... management
State..... enabled
Action..... report
Tracking..... per Signature and Mac
Signature Frequency..... 500 pkts/interval
Signature Mac Frequency..... 300 pkts/interval
Interval..... 10 sec
Quiet Time..... 300 sec
Description..... Broadcast Deauthentication Frame
Patterns:
    0 (Header):0x0:0x0
    4 (Header):0x0:0x0
```

<b>Related Commands</b>	<b>config wps signature</b> <b>config wps signature frequency</b> <b>config wps signature mac-frequency</b> <b>config wps signature interval</b> <b>config wps signature quiet-time</b> <b>config wps signature reset</b> <b>show wps signature events</b> <b>show wps signature summary</b> <b>show wps summary</b>
-------------------------	--

## show wps signature events

To display more information about the attacks detected by a particular standard or custom signature, use the **show wps signature events** command.

**show wps signature events** {summary | {standard | custom} *precedenceID* {summary | detailed}

Syntax Description		
<b>summary</b>		Displays all tracking signature summary information.
<b>standard</b>		Displays Standard Intrusion Detection System (IDS) signature settings.
<b>custom</b>		Displays custom IDS signature settings.
<i>precedenceID</i>		Signature precedence identification value.
<b>detailed</b>		Displays tracking source MAC address details.

**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 display the number of attacks detected by all enabled signatures:

```
(Cisco Controller) > show wps signature events summary
Precedence  Signature Name      Type      # Events
-----
1           Bcast deauth                Standard   2
2           NULL probe resp 1          Standard   1
```

This example shows how to display a summary of information on the attacks detected by standard signature 1:

```
(Cisco Controller) > show wps signature events standard 1 summary
Precedence..... 1
Signature Name..... Bcast deauth
Type..... Standard
Number of active events..... 2
Source MAC Addr   Track Method   Frequency # APs Last Heard
-----
00:a0:f8:58:60:dd Per Signature  50           1   Wed Oct 25 15:03:05
2006
00:a0:f8:58:60:dd Per Mac       30           1   Wed Oct 25 15:02:53
2006
```

---

**Related Commands**

**config wps signature frequency**  
**config wps signature mac-frequency**  
**config wps signature interval**  
**config wps signature quiet-time**  
**config wps signature reset**  
**config wps signature**  
**show wps signature summary**  
**show wps summary**

## show wps signature summary

To see individual summaries of all of the standard and custom signatures installed on the controller, use the **show wps signature summary** command.

### show wps signature summary

**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 display a summary of all of the standard and custom signatures:

```
(Cisco Controller) > show wps signature summary
Signature-ID..... 1
Precedence..... 1
Signature Name..... Bcast deauth
Type..... standard
FrameType..... management
State..... enabled
Action..... report
Tracking..... per Signature and Mac
Signature Frequency..... 50 pkts/interval
Signature Mac Frequency..... 30 pkts/interval
Interval..... 1 sec
Quiet Time..... 300 sec
Description..... Broadcast
Deauthentication Frame
Patterns:
          0 (Header) :0x00c0:0x00ff
          4 (Header) :0x01:0x01
...
```

**Related Commands**

- config wps signature frequency**
- config wps signature interval**
- config wps signature quiet-time**
- config wps signature reset**
- show wps signature events**
- show wps summary**
- config wps signature mac-frequency**

**config wps signature**

## show wps summary

To display Wireless Protection System (WPS) summary information, use the **show wps summary** command.

### show wps summary

**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 display WPS summary information:

```
(Cisco Controller) > show wps summary
Auto-Immune
  Auto-Immune..... Disabled
Client Exclusion Policy
  Excessive 802.11-association failures..... Enabled
  Excessive 802.11-authentication failures..... Enabled
  Excessive 802.1x-authentication..... Enabled
  IP-theft..... Enabled
  Excessive Web authentication failure..... Enabled
Trusted AP Policy
  Management Frame Protection..... Disabled
  Mis-configured AP Action..... Alarm Only
    Enforced encryption policy..... none
    Enforced preamble policy..... none
    Enforced radio type policy..... none
  Validate SSID..... Disabled
  Alert if Trusted AP is missing..... Disabled
  Trusted AP timeout..... 120
Untrusted AP Policy
  Rogue Location Discovery Protocol..... Disabled
  RLDP Action..... Alarm Only
Rogue APs
  Rogues AP advertising my SSID..... Alarm Only
  Detect and report Ad-Hoc Networks..... Enabled
Rogue Clients
  Validate rogue clients against AAA..... Enabled
  Detect trusted clients on rogue APs..... Alarm Only
  Rogue AP timeout..... 1300
Signature Policy
  Signature Processing..... Enabled
...
```

---

**Related Commands**

**config wps signature frequency**  
**config wps signature interval**  
**config wps signature quiet-time**  
**config wps signature reset**  
**show wps signature events**  
**show wps signature mac-frequency**  
**show wps summary**  
**config wps signature**  
**config wps signature interval**

## show wps wips statistics

To display the current state of the Cisco Wireless Intrusion Prevention System (wIPS) operation on the controller, use the **show wps wips statistics** command.

### show wps wips 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 display the statistics of the wIPS operation:

```
(Cisco Controller) > show wps wips statistics
Policy Assignment Requests..... 1
Policy Assignment Responses..... 1
Policy Update Requests..... 0
Policy Update Responses..... 0
Policy Delete Requests..... 0
Policy Delete Responses..... 0
Alarm Updates..... 13572
Device Updates..... 8376
Device Update Requests..... 0
Device Update Responses..... 0
Forensic Updates..... 1001
Invalid WIPS Payloads..... 0
Invalid Messages Received..... 0
NMSP Transmitted Packets..... 22950
NMSP Transmit Packets Dropped..... 0
NMSP Largest Packet..... 1377
```

**Related Commands**

- config 802.11 enable**
- config ap mode**
- config ap monitor-mode**
- show ap config**
- show ap monitor-mode summary**
- show wps wips summary**

# show wps wips summary

To display the adaptive Cisco Wireless Intrusion Prevention System (wIPS) configuration that the Wireless Control System (WCS) forwards to the controller, use the **show wps wips summary** command.

## show wps wips summary

**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 display a summary of the wIPS configuration:

```
(Cisco Controller) > show wps wips summary
Policy Name..... Default
Policy Version..... 3
```

**Related Commands**

- config 802.11 enable**
- config ap mode**
- config ap monitor-mode**
- show ap config**
- show ap monitor-mode summary**
- show wps wips statistics**

show wps wips summary