Cisco Wireless LAN Controller Security Command Reference, Release 7.4

First Published: December 17, 2012

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-28149-01

CONTENTS

Preface

This preface describes the audience, organization, and conventions of the Cisco Wireless LAN Controller Command Reference Guide. It also provides information on how to obtain other documentation. This chapter includes the following sections:

Audience

This publication is for experienced network administrators who configure and maintain Cisco wireless LAN controllers and Cisco lightweight access points.

Document Organization

This document is organized into the following chapters:

Chapter	Description
Overview	Describes how to use the command-line interface (CLI) on the controller.
CLI Commands	Provides detailed information about the CLI commands for the controller.

Document Conventions

This document uses the following conventions:

Convention	Indication
bold font	Commands and keywords and user-entered text appear in **bold** font.
italic font	Document titles, new or emphasized terms, and arguments for which you supply values are in *italic* font.
[ ]	Elements in square brackets are optional.
{x | y | z }	Required alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
`courier` font	Terminal sessions and information the system displays appear in `courier` font.
<>	Nonprinting characters such as passwords are in angle brackets.
[]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

Note Means reader take note. Notes contain helpful suggestions or references to material not covered in the manual.

Tip Means the following information will help you solve a problem.

Caution Means reader be careful. In this situation, you might perform an action that could result in equipment damage or loss of data.

Warning This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. (To see translations of the warnings that appear in this publication, refer to the appendix "Translated Safety Warnings.")

Warning Title	Description
Waarschuwing	Dit waarschuwingssymbool betekent gevaar. U verkeert in een situatie die lichamelijk letsel kan veroorzaken. Voordat u aan enige apparatuur gaat werken, dient u zich bewust te zijn van de bij elektrische schakelingen betrokken risico's en dient u op de hoogte te zijn van standaard maatregelen om ongelukken te voorkomen. (Voor vertalingen van de waarschuwingen die in deze publicatie verschijnen, kunt u het aanhangsel "Translated Safety Warnings" (Vertalingen van veiligheidsvoorschriften) raadplegen.)
Varoitus	Tämä varoitusmerkki merkitsee vaaraa. Olet tilanteessa, joka voi johtaa ruumiinvammaan. Ennen kuin työskentelet minkään laitteiston parissa, ota selvää sähkökytkentöihin liittyvistä vaaroista ja tavanomaisista onnettomuuksien ehkäisykeinoista. (Tässä julkaisussa esiintyvien varoitusten käännökset löydät liitteestä "Translated Safety Warnings" (käännetyt turvallisuutta koskevat varoitukset).)
Attention	Ce symbole d'avertissement indique un danger. Vous vous trouvez dans une situation pouvant entraîner des blessures. Avant d'accéder à cet équipement, soyez conscient des dangers posés par les circuits électriques et familiarisez-vous avec les procédures courantes de prévention des accidents. Pour obtenir les traductions des mises en garde figurant dans cette publication, veuillez consulter l'annexe intitulée « Translated Safety Warnings » (Traduction des avis de sécurité).
Warnung	Dieses Warnsymbol bedeutet Gefahr. Sie befinden sich in einer Situation, die zu einer Körperverletzung führen könnte. Bevor Sie mit der Arbeit an irgendeinem Gerät beginnen, seien Sie sich der mit elektrischen Stromkreisen verbundenen Gefahren und der Standardpraktiken zur Vermeidung von Unfällen bewußt. (Übersetzungen der in dieser Veröffentlichung enthaltenen Warnhinweise finden Sie im Anhang mit dem Titel "Translated Safety Warnings" (Übersetzung der Warnhinweise).)
Avvertenza	Questo simbolo di avvertenza indica un pericolo. Si è in una situazione che può causare infortuni. Prima di lavorare su qualsiasi apparecchiatura, occorre conoscere i pericoli relativi ai circuiti elettrici ed essere al corrente delle pratiche standard per la prevenzione di incidenti. La traduzione delle avvertenze riportate in questa pubblicazione si trova nell'appendice, "Translated Safety Warnings" (Traduzione delle avvertenze di sicurezza).
Advarsel	Dette varselsymbolet betyr fare. Du befinner deg i en situasjon som kan føre til personskade. Før du utfører arbeid på utstyr, må du være oppmerksom på de faremomentene som elektriske kretser innebærer, samt gjøre deg kjent med vanlig praksis når det gjelder å unngå ulykker. (Hvis du vil se oversettelser av de advarslene som finnes i denne publikasjonen, kan du se i vedlegget "Translated Safety Warnings" [Oversatte sikkerhetsadvarsler].)
Aviso	Este símbolo de aviso indica perigo. Encontra-se numa situação que lhe poderá causar danos fisicos. Antes de começar a trabalhar com qualquer equipamento, familiarize-se com os perigos relacionados com circuitos eléctricos, e com quaisquer práticas comuns que possam prevenir possíveis acidentes. (Para ver as traduções dos avisos que constam desta publicação, consulte o apêndice "Translated Safety Warnings" - "Traduções dos Avisos de Segurança").

Warning Title	Description
¡Advertencia!	Este símbolo de aviso significa peligro. Existe riesgo para su integridad física. Antes de manipular cualquier equipo, considerar los riesgos que entraña la corriente eléctrica y familiarizarse con los procedimientos estándar de prevención de accidentes. (Para ver traducciones de las advertencias que aparecen en esta publicación, consultar el apéndice titulado "Translated Safety Warnings.")
Varning	Denna varningssymbol signalerar fara. Du befinner dig i en situation som kan leda till personskada. Innan du utför arbete på någon utrustning måste du vara medveten om farorna med elkretsar och känna till vanligt förfarande för att förebygga skador. (Se förklaringar av de varningar som förekommer i denna publikation i appendix "Translated Safety Warnings" [Översatta säkerhetsvarningar].)

Related Documentation

These documents provide complete information about the Cisco Unified Wireless Network solution:

- *Cisco Wireless LAN Controller Configuration Guide*
- *Cisco Wireless LAN Controller System Message Guide*
- *Release Notes for Cisco Wireless LAN Controllers and Lightweight Access Points*

Obtaining Documentation and Submitting a Service Request

For information about obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as an RSS feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service. Cisco currently supports RSS Version 2.0.

Overview

The Cisco Unified Wireless Network (UWN) security solution bundles potentially complicated Layer 1, Layer 2, and Layer 3 802.11 Access Point security components into a simple policy manager that customizes system-wide security policies on a per-WLAN basis. The Cisco UWN security solution provides simple,unified, and systematic security management tools.

CLI Command Keyboard Shortcuts

The table below lists the CLI keyboard shortcuts to help you enter and edit command lines on the controller.

Table 1: CLI Command Keyboard Shortcuts

Action	Description	Keyboard Shortcut
Change	The word at the cursor to lowercase.	Esc I
	The word at the cursor to uppercase.	Esc u
Delete	A character to the left of the cursor.	Ctrl-h, Delete, or Backspace
	All characters from the cursor to the beginning of the line.	Ctrl-u

Action	Description	Keyboard Shortcut
	All characters from the cursor to the end of the line.	Ctrl-k
	All characters from the cursor to the end of the word.	Esc d
	The word to the left of the cursor.	Ctrl-w or Esc Backspace
Display MORE output	Exit from MORE output.	q, Q, or Ctrl-C
	Next additional screen. The default is one screen. To display more than one screen, enter a number before pressing the Spacebar key.	Spacebar
	Next line. The default is one line. To display more than one line, enter the number before pressing the Enter key.	Enter
Enter an Enter or Return key character.		Ctrl-m
Expand the command or abbreviation.		Ctrl-t or Tab
Move the cursor	One character to the left (back).	Ctrl-b or Left Arrow
	One character to the right (forward).	Ctrl-f or Right Arrow
	One word to the left (back), to the beginning of the current or previous word.	Esc b
	One word to the right (forward), to the end of the current or next word.	Esc f
	To the beginning of the line.	Ctrl-a
	To the end of the line.	Ctrl-e
Redraw the screen at the prompt.		Ctrl-l or Ctrl-r
Return to the EXEC mode from any configuration mode		Ctrl-z
Return to the previous mode or exit from the CLI from Exec mode.		exit command
Transpose a character at the cursor with a character to the left of the cursor.		Ctrl-t

Using the Interactive Help Feature

The question mark (?) character allows you to get the following type of help about the command at the command line. The following table lists the interactive help feature list.

Table 2: Interactive Help Feature List

Command	
help	Provides a brief description of the Help feature in any command mode.
? at the command prompt	Lists all commands available for a particular command mode.
partial command?	Provides a list of commands that begin with the character string.
partial command<Tab>	Completes a partial command name.
command ?	Lists the keywords, arguments, or both associated with a command.
command keyword ?	Lists the arguments that are associated with the keyword.

Using the Help Command

Before You Begin

To look up keyboard commands, use the help command at the root level.

help

Help may be requested at any point in a command by entering a question mark '?'. If nothing matches, the help list will be empty and you must back up until entering a '?' shows the available options. Two types of help are available

1. Full help is available when you are ready to enter a command argument (for example show ?) and describes each possible argument.

2. Partial help is provided when an abbreviated argument is entered and you want to know what arguments match the input (for example show pr?).

Examples

```
> help
HELP:
Special keys:
  DEL, BS... delete previous character
  Ctrl-A  .... go to beginning of line
  Ctrl-E  .... go to end of line
  Ctrl-F  .... go forward one character
  Ctrl-B  .... go backward one character
```

```
Ctrl-D  .... delete current character
Ctrl-U, X. delete to beginning of line
Ctrl-K  .... delete to end of line
Ctrl-W  .... delete previous word
Ctrl-T  .... transpose previous character
Ctrl-P  .... go to previous line in history buffer
Ctrl-N  .... go to next line in history buffer
Ctrl-Z  .... return to root command prompt
Tab, <SPACE> command-line completion
Exit    .... go to next lower command prompt
?       .... list choices
```

Using the ? command

Before You Begin

To display all of the commands in your current level of the command tree, or to display more information about a particular command, use the ? command.

command name ?

When you enter a command information request, put a space between the **command name** and **?**.

Examples This command shows you all the commands and levels available from the root level.

```
> ?
clear          Clear selected configuration elements.
config         Configure switch options and settings.
debug          Manages system debug options.
help           Help
linktest       Perform a link test to a specified MAC address.
logout         Exit this session. Any unsaved changes are lost.
ping           Send ICMP echo packets to a specified IP address.
reset          Reset options.
save           Save switch configurations.
show           Display switch options and settings.
transfer       Transfer a file to or from the switch.
```

Using the partial? command

Before You Begin

To provide a list of commands that begin with the character string, use the partial command ?.

partial command?

There should be no space between the command and the question mark.

Examples This example shows how to provide a command that begin with the character string “ad”:

```
> controller> config>ad?
```

The command that matches with the string “ad” is as follows:

```
advanced
```

Using the partial command<tab>

Before You Begin

To completes a partial command name, use the partial command<tab> command.

partial command<tab>

There should be no space between the command and <tab>.

Examples This example shows how to complete a partial command name that begin with the character string “ad”:

```
> Controller>config>cert<tab> certificate
```

Using the command ?

Examples To list the keywords, arguments, or both associated with the command, use the command ?.

command ?

There should be space between the command and the question mark.

This example shows how to list the arguments and keyword for the command acl:

```
> Controller >config acl ?
```

Information similar to the following appears:

```
apply          Applies the ACL to the data path.
counter        Start/Stop the ACL Counters.
create         Create a new ACL.
delete         Delete an ACL.
rule           Configure rules in the ACL.
cpu            Configure the CPU Acl Information
```

command keyword ?

To list the arguments that are associated with the keyword, use the command keyword ?

command keyword ?

Usage Guidelines

There should be space between the keyword and the question mark.

Examples

This example shows how to display the arguments associated with the keyword cpu:

```
> controller>config acl cpu ?
```

Information similar to the following appears:

```
none            None - Disable the CPU ACL
<name>          <name> - Name of the CPU ACL
```

CLI Commands

The Cisco Wireless LAN solution command-line interface (CLI) enables operators to connect an ASCII console to the Cisco Wireless LAN Controller and configure the controller and its associated access points.

Show Commands

This section lists the **show** commands to display information about your security configuration settings for the controller.

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

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
h	Specifies the 802.11h network.

Command Default

None.

Examples

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.

Examples

This example shows how to display the configuration settings for the AAA authentication server database:

```
> 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 {**summary** | **detailed** *acl_name*}

Syntax Description

summary	Displays a summary of all ACLs configured on the controller.
detailed	Displays detailed information about a specific ACL.
acl_name	ACL name. The name can be up to 32 alphanumeric characters.

Command Default

None.

Examples

This example shows how to display a summary of the access control lists:

```
> show acl summary

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

This example shows how to display the detailed information of the access control lists:

```
> show acl detailed acl_name
      Source             Destination        Source Port Dest Port
I Dir IP Address/Netmask IP Address/Netmask Prot   Range    Range     DSCP 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/     6      80-80   0-65535   Any  Permit       0
                         255.255.255.0
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 acl cpu

show acl cpu

To display the access control lists (ACLs) configured on the central processing unit (CPU), use the **show acl cpu** command.

show acl cpu

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Examples

This example shows how to display the access control lists on the CPU:

```
> show acl cpu
CPU Acl Name.............................
Wireless Traffic........................... Disabled
Wired Traffic.............................. Disabled
Applied to NPU............................. No
```

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 acl

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.

Examples

This example shows how to display the EAP settings:

```
> 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.

Examples

This example shows how to display a summary of the local database configuration:

```
> 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 (blacklisted) from associating with this Cisco wireless LAN controller, use the **show exclusionlist** command.

show exclusionlist

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Usage Guidelines

This command displays all manually excluded MAC addresses.

Examples

This example shows how to display the exclusion list:

```
> 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

brief	Displays a brief summary of all active IKE SAs.
detailed	Displays a detailed summary of all active IKE SAs.
IP_or_MAC_address	IP or MAC address of active IKE SA.

Command Default

None.

Examples

This example shows how to display the active Internet Key Exchange security associations:

```
> 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*

Syntax Description

brief	Displays a brief summary of active IPsec SAs.
detailed	Displays a detailed summary of active IPsec SAs.
IP_or_MAC_address	IP address or MAC address of a device.

Command Default

None.

Examples

This example shows how to display brief information about the active Internet Protocol Security (IPsec) security associations (SAs):

```
> show IPsec brief 209.165.200.254
```

Related Commands

config radius acct ipsec authentication
config radius acct ipsec disable
config radius acct ipsec enable
config radius acct ipsec encryption
config radius auth IPsec encryption
config radius auth IPsec authentication
config radius auth IPsec disable
config radius auth IPsec encryption
config radius auth IPsec ike
config trapflags IPsec
config wlan security IPsec disable
config wlan security IPsec enable
config wlan security IPsec authentication
config wlan security IPsec encryption
config wlan security IPsec config
config wlan security IPsec ike authentication
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**}

Syntax Description

acl_name	IPv6 ACL name. The name can be up to 32 alphanumeric characters.
detailed	Displays detailed information about a specific ACL.

Command Default

None.

Examples

This example shows how to display the detailed information of the access control lists:

```
> 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
```

Related Commands

config ipv6 acl

show ipv6 summary

To display the IPv6 configuration settings, use the **show ipv6 summary** command.

show ipv6 summary

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Examples

This example shows how to display the IPv6 configuration settings:

```
> show ipv6 summary
Global Config.............................. Enabled
Reachable-lifetime value................... 300
Stale-lifetime value....................... 86400
Down-lifetime value........................ 86400
RA Throttling.............................. Enabled
RA Throttling allow at-least............... 1
RA Throttling allow at-most................ no-limit
RA Throttling max-through.................. no-limit
RA Throttling throttle-period.............. 60
RA Throttling interval-option.............. throttle
NS Mulitcast CacheMiss Forwarding.......... Disabled
```

Related Commands

show ipv6 acl

show l2tp

To display Layer 2 Tunneling Protocol (L2TP) sessions, use the **show l2tp** command.

show l2tp {**summary** | *ip_address*}

Syntax Description

summary	Displays all L2TP sessions.
ip_address	IP address.

Command Default

None.

Examples

This example shows how to display a summary of all L2TP sessions:

```
> 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*

index	LDAP server index. Valid values are from 1 to 17.

Command Default

None.

Examples

This example shows how to display the detailed LDAP server information:

```
> 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
```

Related Commands

config ldap

config ldap add

config ldap simple-bind

show ldap statistics

show ldap summary

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.

Examples

This example shows how to display the LDAP server statistics:

```
> 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.

Examples

This example shows how to display a summary of configured LDAP servers:

```
> 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.

Examples

This example shows how to display the authentication certificate information stored locally:

```
> show local-auth certificates

Certificates available for Local EAP authentication:
Certificate issuer ............................. vendor
CA certificate:
Subject: C=AU, ST=NSW, L=Sydney, O=Cisco Systems
OU=WNBU Sydney, CN=wnbu-syd-acs-a.cisco.com
Issuer: C=AU, ST=NSW, L=Sydney, O=Cisco Systems
OU=WNBU Sydney, CN=wnbu-syd-acs-a.cisco.com
Valid: 2005 Jun 15th, 04:53:49 GMT to 2008 Jun 15th, 05:03:34 GMT
Device certificate:
Subject: MAILTO=test@test.net, C=AU, ST=NSW, L=Sydney
O=Cisco Systems, OU=WNBU Sydney, CN=concannon
Issuer: C=AU, ST=NSW, L=Sydney, O=Cisco Systems
OU=WNBU Sydney, CN=wnbu-syd-acs-a.cisco.com
Valid: 2006 Aug 9th, 05:14:16 GMT to 2007 Aug 9th, 05:24:16 GMT

Certificate issuer ............................. cisco
CA certificate:
Subject: C=US, ST=California, L=San Jose, O=airespace Inc
OU=none, CN=ca, MAILTO=support@airespace.com
Issuer: C=US, ST=California, L=San Jose, O=airespace Inc
OU=none, CN=ca, MAILTO=support@airespace.com
Valid: 2003 Feb 12th, 23:38:55 GMT to 2012 Nov 11th, 23:38:55 GMT
Device certificate:
Subject: C=US, ST=California, L=San Jose, O=airespace Inc
CN=000b85335340, MAILTO=support@airespace.com
Issuer: C=US, ST=California, L=San Jose, O=airespace Inc
OU=none, CN=ca, MAILTO=support@airespace.com
Valid: 2005 Feb 22nd, 10:52:58 GMT to 2014 Nov 22nd, 10:52:58 GMT

Certificate issuer ............................. legacy
CA certificate:
Subject: C=US, ST=California, L=San Jose, O=airespace Inc
OU=none, CN=ca, MAILTO=support@airespace.com
Issuer: C=US, ST=California, L=San Jose, O=airespace Inc
OU=none, CN=ca, MAILTO=support@airespace.com
Valid: 2003 Feb 12th, 23:38:55 GMT to 2012 Nov 11th, 23:38:55 GMT
Device certificate:
Subject: C=US, ST=California, L=San Jose, O=airespace Inc
CN=000b85335340, MAILTO=support@airespace.com
Issuer: C=US, ST=California, L=San Jose, O=airespace Inc
OU=none, CN=ca, MAILTO=support@airespace.com
Valid: 2005 Feb 22nd, 10:52:58 GMT to 2014 Nov 22nd, 10:52:58 GMT
```

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.

Examples

This example shows how to display the local authentication configuration information:

```
> 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 ........................ 7b7fffffff00000000000000000000000000
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.

Examples

This example shows how to display the local authentication certificate statistics:

```
> 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.

Examples

This example shows how to display detailed statistics of network access control settings:

```
> 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.

Examples

This example shows how to display a summary information of network access control settings:

```
> 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 **show netuser** command.

show netuser {**detail** *user_name* | **guest-roles** | **summary**}

Syntax Description

detail	Displays detailed information about the specified network user.
user_name	Network user.
guest_roles	Displays configured roles for guest users.
summary	Displays a summary of all users in the local user database.

Command Default

None.

Examples

This example shows how to display a summary of all users in the local user database:

```
> show netuser summary
Maximum logins allowed for a given username ........Unlimited
```

This example shows how to display detailed information on the specified network user:

```
> show netuser detail john10
username..................................... abc
WLAN Id...................................... Any
Lifetime..................................... Permanent
Description.................................. test user
```

Related Commands

config netuser add

config netuser delete

config netuser description

config netuser guest-role apply

config netuser wlan-id

config netuser guest-roles

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.

Examples

This example shows how to display a QoS role for the guest network user:

```
> 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.

Examples This example shows how to display the network details:

```
> 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.

Examples

This example shows how to display a summary configuration:

```
> 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
Secure Web Mode RC4 Cipher Preference....... 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
oeap-600 dual-rlan-ports ................... Disable
oeap-600 local-network ..................... Enable
mDNS snooping............................... Disabled
```

```
mDNS Query Interval..................... 15 minutes
```

Related Commands

config network

show network multicast mgid summary

show network multicast mgid detail

show network

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.

Examples

This example shows how to display NTP authentication key details:

```
> show ntp-keys
Ntp Authentication Key Details...................
      Key Index
     -----------
         1
         3
```

Related Commands

config time ntp

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.

Examples

This example shows how to display active internal firewall rules:

```
> 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.

Examples

This example shows how to display parameters that apply to the Cisco wireless LAN 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 Commands

Use the **show rogue** commands to display unverified (rogue) device settings.

show rogue adhoc custom summary

To display information about custom rogue ad-hoc rogue access points, use the

show rogue adhoc custom summary

Syntax Description This command has no arguments or keywords.

Command Default None.

Examples This example shows how to display details of custom rogue ad-hoc rogue access points:

```
> 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*

Syntax Description

MAC_address	Ad-hoc rogue MAC address.

Command Default

None.

Examples

This example shows how to display detailed ad-hoc rogue MAC address information:

```
> 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
```

Related Commands

config rogue adhoc

show rogue ignore-list

show rogue rule summary

show rogue rule detailed

config rogue rule

show rogue adhoc summary

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.

Examples This example shows how to display information about friendly rogue ad-hoc rogue access points:

```
> 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.

Examples This example shows how to display details of malicious rogue ad-hoc rogue access points:

```
> 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.

Examples This example shows how to display information about unclassified rogue ad-hoc rogue access points:

```
> 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.

Examples This example shows how to display a summary of all ad-hoc rogues:

```
> 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 adhoc custom summary** command.

show rogue ap custom summary

Syntax Description This command has no arguments or keywords.

Command Default None.

Examples This example shows how to display details of custom rogue ad-hoc rogue access points:

```
> 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*

Syntax Description

ap_mac_address	Rogue access point MAC address.

Command Default

None.

Examples

This example shows how to display details of rogue access point clients:

```
> 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
```

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 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

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*

Syntax Description

ap_mac_address	Rogue access point MAC address.

Command Default

None.

Examples

This example shows how to display detailed information of a rogue access point:

```
> 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:

```
> 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 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

Syntax Description This command has no arguments or keywords.

Command Default None.

Examples This example shows how to display a summary of all rogue access points:

```
> 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
```

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.

Examples This example shows how to display a summary of all friendly rogue access points:

```
> 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.

Examples This example shows how to display a summary of all malicious rogue access points:

```
> 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.

Examples This example shows how to display a list of all unclassified rogue access points:

```
> 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
```

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 malicious summary

show rogue client detailed

show rogue client summary

show rogue ignore-list

show rogue rule detailed

show rogue rule summary

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.

Examples This example shows how to display information about rogue auto-containment:

```
> 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 *MAC_address*

Syntax Description

MAC_address	Rogue client MAC address.

Command Default

None.

Examples

This example shows how to display detailed information for a rogue client:

```
> 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
```

Related Commands

show rogue client summary

show rogue ignore-list

config rogue rule client

config rogue rule

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.

Examples This example shows how to display a list of all rogue clients:

```
> 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 19:00:08 2005
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 19:00:08 2005
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 19:00:08 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.

Examples This example shows how to display a list of all rogue access points that are configured to be ignored:

```
> 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*

Syntax Description

rule_name	Rogue rule name.

Command Default None.

Examples This example shows how to display detailed information on a specific rogue classification rule:

```
> 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.

Examples This example shows how to display a list of all rogue rules that are configured on the 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
```

This example shows how to display a list of all rogue rules that are configured on the 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 Commands

Use the **show tacacs** commands to display Terminal Access Controller Access Control System (TACACS) protocol settings and statistics.

- show tacacs acct statistics
- show tacacs athr statistics
- show tacacs auth statistics
- show tacacs summary

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.

Examples This example shows how to display detailed RFID information:

```
> 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
```

Related Commands

config tacacs acct

config tacacs athr

config tacacs auth

show tacacs summary

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.

Examples This example shows how to display TACACS server authorization statistics:

```
> 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

Syntax Description This command has no arguments or keywords.

Command Default None.

Examples This example shows how to display TACACS server authentication statistics:

```
> 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
```

Related Commands

config tacacs acct

config tacacs athr

config tacacs auth

show tacacs summary

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.

Examples This example shows how to display TACACS server summary information:

```
> show tacacs summary
Authentication Servers
Idx  Server Address    Port    State     Tout
---  ----------------  ------  --------  ----
2    10.0.0.2          6       Enabled   30
Accounting Servers
Idx  Server Address    Port    State     Tout
---  ----------------  ------  --------  ----
1    10.0.0.0          10      Enabled   2
Authorization Servers
Idx  Server Address    Port    State     Tout
---  ----------------  ------  --------  ----
3    10.0.0.3          4       Enabled   2
...
```

Related Commands

config tacacs acct

config tacacs athr

config tacacs auth

show tacacs summary

show tacacs athr statistics

show tacacs auth statistics

Show WPS Commands

Use the **show wps** commands to display Wireless Protection System (WPS) settings.

- show wps ap-authentication summary
- show wps cids-sensor
- show wps mfp
- show wps shun-list
- show wps signature detail
- show wps signature events
- show wps signature summary
- show wps summary
- show wps wips statistics
- show wps wips summary

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.

Examples This example shows how to display a summary of the Wireless Protection System (WPS) access point neighbor authentication:

```
> 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*}

Syntax Description

summary	Displays a summary of sensor settings.
detail	Displays all settings for the selected sensor.
index	IDS sensor identifier.

Command Default None.

Examples This example shows how to display all settings for the selected sensor:

```
> 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:
00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
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.

Examples

This example shows how to display a summary of the MFP configuration and status:

```
> show wps mfp summary
Global Infrastructure MFP state..................... DISABLED (*all infrastructure
settings are overridden)
Controller Time Source Valid..................... False
                                    WLAN       Infra.      Client
WLAN ID  WLAN Name                  Status     Protection  Protection
-------  -------------------------  ---------  ----------  ----------
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)
                     Infra.              Operational     --Infra. Capability--
AP Name              Validation  Radio   State           Protection  Validation
-------------------  ----------  -----   --------------  ----------  ----------
AP1252AG-EW          *Enabled    b/g     Down            Full        Full
                                 a       Down            Full        Full
```

This example shows how to display the MFP statistics:

```
> 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.

Examples This example shows how to display the IDS system sensor shun list:

```
> 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*

Syntax Description

sig-id	Signature ID of an installed signature.

Command Default None.

Examples This example shows how to display information on the attacks detected by standard signature 1:

```
> 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
```

Related Commands

config wps signature

config wps signature frequency

config wps signature mac-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

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

summary	Displays all tracking signature summary information.
standard	Displays Standard Intrusion Detection System (IDS) signature settings.
custom	Displays custom IDS signature settings.
precedenceID	Signature precedence identification value.
detailed	Displays tracking source MAC address details.

Command Default

None.

Examples

This example shows how to display the number of attacks detected by all enabled signatures:

```
> 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:

```
> 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.

Examples This example shows how to display a summary of all of the standard and custom signatures:

```
> 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.

Examples This example shows how to display WPS summary information:

```
> 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.

Examples This example shows how to display the statistics of the wIPS operation:

```
> 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.

Examples This example shows how to display a summary of the wIPS configuration:

```
> 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

Config Commands

This section lists the **config** commands to configure security settings for the controller.

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

long	Specifies the long 802.11b preamble.
short	Specifies the short 802.11b preamble.

Command Default

Short.

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.

Examples

This example shows how to change the 802.11b preamble to short:

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

Related Commands

show 802.11b

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*]

Syntax Description

mgmt	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.
aaa_server_type	(Optional) AAA authentication server type (**local**, **radius**, or **tacacs**). The **local** setting specifies the local database, the **radius** setting specifies the RADIUS server, and the **tacacs** setting specifies the TACACS+ server.

Command Default

None.

Usage Guidelines

You can enter two AAA server types as long as one of the server types is **local**. You cannot enter **radius** and **tacacs** together.

Examples

This example shows how to configure the AAA authentication search order for controller management users by the authentication server type local:

```
> config aaa auth radius local
```

Related Commands

show aaa auth

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**]

Syntax Description

radius	(Optional) Configures the order of authentication for RADIUS servers.
tacacs	(Optional) Configures the order of authentication for TACACS servers.

Command Default

None.

Examples

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

```
> config aaa auth mgmt radius
```

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

```
> 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*

Syntax Description

rule_name	ACL name that contains up to 32 alphanumeric characters.

Command Default

None.

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.

Examples

This example shows how to apply an ACL to the data path:

```
> config acl apply acl01
```

Related Commands

show acl

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

start	Enables ACL counters on your controller.
stop	Disables ACL counters on your controller.

Command Default

config acl counter stop

Usage Guidelines

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

Examples

This example shows how to enable ACL counters on your 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*

Syntax Description

rule_name	ACL name that contains up to 32 alphanumeric characters.

Command Default

None.

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.

Examples

This example shows how to create a new ACL:

```
> config acl create acl01
```

Related Commands

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

rule_name	Specifies the ACL name
wired	Specifies an ACL on wired traffic.
wireless	Specifies an ACL on wireless traffic
both	Specifies an ACL on both wired and wireless traffic.

Command Default

None.

Usage Guidelines

This command allows you to control the type of packets reaching the CPU.

Examples

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

> **config acl cpu acl01 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*

Syntax Description

rule_name	ACL name that contains up to 32 alphanumeric characters.

Command Default None.

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.

Examples This example shows how to delete an ACL named acl101 on the CPU:

```
> config acl delete acl01
```

Related Commands **show acl**

config acl rule

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

config aclrule {**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

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

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

Command Default None.

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.

Examples This example shows how to configure an ACL to permit access:

```
> 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.

Examples

This example shows how to create an authorized access point entry with a manufacturer-installed certificate on MAC address 00:0b:85:02:0d:20:

```
> 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

authorize-ap enable	Enables the authorization policy.
authorize-ap disable	Disables the AP authorization policy.
ssc enable	Allows the APs with self-signed certificates to connect.
ssc disable	Disallows the APs with self-signed certificates to connect.

Command Default

None.

Examples

This example shows how to enable an access point authorization policy:

```
> config auth-list ap-policy authorize-ap enable
```

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

```
> config auth-list ap-policy ssc disable
```

Related Commands

config auth-list delete

config auth-list add

config auth-list delete

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

config auth-list delete *AP_MAC*

Syntax Description

AP_MAC	MAC address of a Cisco lightweight access point.

Command Default

None.

Examples

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

```
> config auth-list delete 00:1f:ca:cf:b6:60
```

Related Commands

config auth-list delete

config auth-list add

config auth-list ap-policy

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

bcast-key-interval *seconds*	Specifies the EAP-broadcast key renew interval time in seconds. The range is from 120 to 86400 seconds.
eapol-key-timeout *timeout*	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.
eapol-key-retries *retries*	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.
identity-request- timeout *timeout*	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.
identity-request- retries	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.
key-index *index*	Specifies the key index (0 or 3) used for dynamic wired equivalent privacy (WEP).
max-login-ignore- identity-response	Specifies that the maximum EAP identity response login count for a user is ignored. When enabled, this command limits the number of devices that can be connected to the controller with the same username.
enable	Ignores the same username reaching the maximum EAP identity response.
disable	Checks the same username reaching the maximum EAP identity response.

request-timeout	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. The default value is 30 seconds.
request-retries	(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. The default value is 2.

Command Default

Default for **eapol-key-timeout**: 1 second.

Default for **eapol-key-retries**: 2 retries.

Examples

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

```
> config advanced eap key-index 0
```

Related Commands

show advanced eap

config advanced timers auth-timeout

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

config advanced timers auth-timeout *seconds*

Syntax Description

seconds	Authentication response timeout value in seconds between 10 and 600.

Command Default

10 seconds.

Examples

This example shows how to configure the authentication timeout to 20 seconds:

```
> config advanced timers auth-timeout 20
```

Related Commands

show advanced timers
config advanced timers ap-discovery-timeout
config advanced timers ap-heartbeat-timeout
config advanced timers ap-primary-discovery-timeout
config advanced timers ap-fast-heartbeat

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*

Syntax Description

seconds	EAP timeout value in seconds between 8 and 120.

Command Default

None.

Examples

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

```
> config advanced timers eap-timeout 10
```

Related Commands

show advanced timers

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*

Syntax Description

seconds	Advanced EAP identity request delay in number of seconds between 0 and 10.

Command Default

None.

Examples

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

```
> config advanced timers eap-identity-request-delay 8
```

Related Commands

config advanced timers auth-timeout

config advanced timers rogue-ap

show advanced timers

config cts sxp

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

config cts sxp {**enable** | **disable**}

Syntax Description

enable	Enables CTS connections on the controller.
disable	Disables CTS connections on the controller.

Command Default

None.

Examples

This example shows how to enable CTS on the controller:

```
> config cts sxp enable
```

Related Commands

config cts sxp connection

config cts sxp default password

config cts sxp retry period

config cts sxp connection

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

config cts sxp connection {**delete** | **peer**} *ip-address*

Syntax Description

delete	Deletes the CTS connection on the controller.
peer	Configures the next hop switch with which the controller is connected.
ip-address	IPv4 address of the peer.

Command Default

None.

Usage Guidelines

Default password should be configured before adding CTS connections.

Examples

This example shows how to configure a peer for a CTS connection:

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

Related Commands

config cts sxp

config cts sxp default password

config cts sxp retry period

config cts sxp default password

To configure the default password for MD5 Authentication of SXP messages, use the **config cts sxp default password** command.

config cts sxp default password *password*

Syntax Description

password	Default password for MD5 Authentication of SXP messages. The password should contain a minimum of six characters.

Command Default

None.

Examples

This example shows how to configure the default password for MD5 Authentication of SXP messages:

```
> config cts sxp default password controller
```

Related Commands

config cts sxp

config cts sxp connection

config cts sxp retry period

To configure the SXP retry period, use the **config cts sxp retry period** command.

config cts sxp retry period *time-in-seconds*

Syntax Description

time-in-seconds	Time after which a CTS connection should be again tried for after a failure to connect.

Command Default

None.

Examples

This example shows how to configure the SXP retry period as 20 seconds:

```
> config cts sxp retry period 20
```

Related Commands

config cts sxp connection

config cts sxp default password

config cts sxp

config database size

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

config database size *count*

Syntax Description

count	Database size value between 512 and 2040

Command Default None.

Usage Guidelines Use the **show database** command to display local database configuration.

Examples This example shows how to configure the size of the local database:

```
> config database size 1024
```

Related Commands **show database**

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

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

Command Default

None.

Examples

This example shows how to create a local exclusion list entry for the MAC address *xx:xx:xx:xx:xx:xx:*

```
> config exclusionlist add xx:xx:xx:xx:xx:xx lab
```

This example shows how to delete a local exclusion list entry for the MAC address *xx:xx:xx:xx:xx:xx:*

```
> 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**} *index*

Syntax Description

add	Specifies that an LDAP server is being added.
delete	Specifies that an LDAP server is being deleted.
enable	Specifies that an LDAP serve is enabled.
disable	Specifies that an LDAP server is disabled.
retransmit-timeout	Changes the default retransmit timeout for an LDAP server.
index	LDAP server index. The range is from 1 to 17.

Command Default

None.

Examples

This example shows how to enable LDAP server index 10:

```
> config ldap enable 10
```

Related Commands

config ldap add

config ldap simple-bind

show ldap summary

config ldap add

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

config lap add *index server_ip_address port user_base user_attr user_type*

Syntax Description

index	LDAP server index.
server_ip_address	IP address of the LDAP server.
port	Port number.
user_base	Distinguished name for the subtree that contains all of the users.
user_attr	Attribute that contains the username.
user_type	ObjectType that identifies the user.

Command Default

None.

Examples

This example shows how to configure a LDAP server with the index10, server IP address 209.165.201.30, port number 2:

```
> config ldap add 10 209.165.201.30 2 base_name attr_name type_name
```

Related Commands

config ldap

config ldap simple-bind

show ldap summary

config ldap simple-bind

To configure the local authentication bind method for the Lightweight Directory Access Protocol (LDAP) server, use the **config ldap simple-bind** command.

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

Syntax Description

anonymous	Allows anonymous access to the LDAP server.
index	LDAP server index.
authenticated	Specifies that a username and password be entered to secure access to the LDAP server.
username	Username for the authenticated bind method.
password	Password for the authenticated bind method.

Command Default

The default bind method is **anonymous**.

Examples

This example shows how to configure the local authentication bind method that allows anonymous access to the LDAP server:

```
> config ldap simple-bind anonymous
```

Related Commands

config ldap add

config ldap

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*

Syntax Description

timeout	Timeout measured in seconds. The range is from 1 to 3600.

Command Default

100 seconds.

Examples

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

```
> config local-auth active-timeout 500
```

Related Commands

clear stats local-auth

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

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

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

ca-issuer	(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.
cn-verify	(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.
date-valid	(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.

Examples

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

```
> config local-auth eap-profile add FAST01
```

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

```
> config local-auth eap-profile method add fast FAST01
```

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

```
> config local-auth eap-profile method fast cert-issuer cisco
```

This example shows how to specify that the incoming certificate from the client be validated against the CA certificates on the 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

anon-prov	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.
enable	(Optional) Specifies that the parameter is enabled.
disable	(Optional) Specifies that the parameter is disabled.
authority-id	Configures the authority identifier of the local EAP-FAST server.
auth_id	Authority identifier of the local EAP-FAST server (2 to 32 hexadecimal digits).
pac-ttl	Configures the number of days for the Protected Access Credentials (PAC) to remain viable (also known as the time-to-live [TTL] value).
days	Time-to-live value (TTL) value (1 to 1000 days).
server-key	Configures the server key to encrypt or decrypt PACs.
key_value	Encryption key value (2 to 32 hexadecimal digits).

Command Default

None.

Examples

This example shows how to disable the controller to allows anonymous provisioning:

```
> config local-auth method fast anon-prov disable
```

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

```
> config local-auth method fast authority-id 0125631177
```

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

```
> 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**] }

Syntax Description

local	Specifies that the local database is searched for the user credentials.
ldap	(Optional) Specifies that the Lightweight Directory Access Protocol (LDAP) database is searched for the user credentials.

Command Default

None.

Usage Guidelines

The order of the specified database parameters indicate the database search order.

Examples

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

```
> config local-auth user credentials local lda
```

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

Related Commands

clear stats local-auth

config local-auth eap-profile

config local-auth method fast

config local-auth active-timeout

debug aaa local-auth

show local-auth certificates

show local-auth config

show local-auth statistics

config ipv6 acl

To create or delete an IPv6 acl on the Cisco wireless LAN controller, use the **config ipv6 acl** command.

config ipv6 acl {**apply** *ipv6_acl_name* | **create** *ipv6_acl_name* | **delete** *ipv6_acl_name* | **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

apply	Applies an IPv6 ACL.
ipv6_acl_name	IPv6 ACL name that contains up to 32 alphanumeric characters.
create	Creates an IPv6 ACL.
delete	Deletes an IPv6 ACL.
rule	Configures the IPv6 ACL.
action	Configures whether to permit or deny access.
rule_name	ACL name that contains up to 32 alphanumeric characters.
rule_index	Rule index between 1 and 32.
permit	Permits the rule action.
deny	Denies the rule action.
add	Adds a new rule.
change	Changes a rule's index.
index	Specifies a rule index.
delete	Deletes a rule.
destination address	Configures a rule's destination IP address and netmask.
ip_address	IP address of the rule.
netmask	Netmask of the rule.
start_port	Start port number (between 0 and 65535).
end_port	End port number (between 0 and 65535).

direction	Configures a rule's direction to in, out, or any.
in	Configures a rule's direction to in.
out	Configures a rule's direction to out.
any	Configures a rule's direction to any.
dscp	Configures a rule's DSCP.
dscp	Number between 0 and 63, or **any**.
protocol	Configures a rule's DSCP.
protocol	Number between 0 and 255, or **any**.
source address	Configures a rule's source IP address and netmask.
source port range	Configures a rule's source port range.
swap	Swap's two rules' indices.
destination port range	Configure a rule's destination port range.

Command Default

None.

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.

Examples

This example shows how to configure an IPv6 ACL to permit access:

```
> config ipv6 acl rule action lab1 4 permit
```

Related Commands

show ipv6 acl

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

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

Command Default

None.

Usage Guidelines

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

Examples

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

```
> config netuser add jane able2 1 wlan_id 1 userType permanent
```

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

```
> 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*

Syntax Description

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

Command Default None.

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

Examples This example shows how to delete an existing username named able1 from the network:

```
> config netuser delete able1
Deleted user able1
```

Related Commands **show netuser**

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.

Examples

This example shows how to add a user description “HQ1 Contact” to an existing network user named able 1:

```
> 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*

Syntax Description

shared_secret	Bridging shared secret string. The string can contain up to 10 bytes.

Command Default

Enabled.

Usage Guidelines

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.

Examples

This example shows how to configure the bridging shared secret string “shhh1”:

```
> config network bridging-shared-secret shhh1
```

Related Commands

show network summary

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

enable	Allows the controller to support bypass of captive portals.
disable	Disallows the controller to support bypass of captive portals.

Command Default

None.

Examples

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

```
> 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*

Syntax Description

port	Port number. The valid range is from 0 to 65535.

Command Default

None.

Examples

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

```
> 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**}

Syntax Description

enable	Allows proxy redirect support for web authentication clients.
disable	Disallows proxy redirect support for web authentication clients.

Command Default

None.

Examples

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

```
> 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**}

Syntax Description

enable	Allows secure web (https) authentication for clients.
disable	Disallows secure web (https) authentication for clients. Enables http for Web Auth clients.

Command Default

Enabled.

Examples

This example shows how to enable the secure web (https) authentication for clients:

```
> config network web-auth secureweb enable
```

Related Commands

show network summary

config network webmode

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

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

Syntax Description

enable	Enables the web interface.
disable	Disables the web interface.

Command Default Enabled.

Examples This example shows how to disable the web interface mode:

```
> 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

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

Command Default

Disabled.

Usage Guidelines

You must reset the system for the configuration to take effect.

Examples

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

```
> config network web-auth proxy-redirect enable
```

Related Commands

show network summary

show run-config

config qos protocol-type

Configure RADIUS Account Commands

Use the **config radius acct** commands to configure RADIUS account server settings.

config radius acct

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

config radius acct {{**enable** | **disable** | **delete**} *index*} | **add** *index server_ip port* {**ascii** | **hex**} *secret*}

Syntax Description

enable	Enables a RADIUS accounting server.
disable	Disables a RADIUS accounting server.
delete	Deletes a RADIUS accounting server.
index	RADIUS server index. The controller begins the search with 1.
add	Adds a RADIUS accounting server.
server_ip	IP address of RADIUS server.
port	RADIUS server's UDP port number for the interface protocols.
ascii	Specifies the RADIUS server's secret type: **ascii**.
hex	Specifies the RADIUS server's secret type: **hex**.
secret	RADIUS server's secret.

Command Default

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

Examples

This 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*:

```
> config radius acct add 1 10.10.10.10 1813 ascii admin
```

Related Commands

show radius acct statistics

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	Enables IPsec HMAC-MD5 authentication.
hmac-sha1	Enables IPsec HMAC-SHA1 authentication.
index	RADIUS server index.

Command Default None.

Examples This example shows how to configure the IPsec hmac-md5 authentication service on the RADIUS accounting server index 1:

```
> 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*

Syntax Description

index	RADIUS server index.

Command Default

None.

Examples

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

```
> 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*

Syntax Description

index	RADIUS server index.

Command Default None.

Examples This example shows how to enable the IPsec support for RADIUS accounting server index 1:

```
> 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

3des	Enables IPsec 3DES encryption.
aes	Enables IPsec AES encryption.
des	Enables IPsec DES encryption.
index	RADIUS server index value of between 1 and 17.

Command Default

None.

Examples

This example shows how to configure the IPsec 3DES encryption for RADIUS server index value 3:

```
> config radius acct ipsec encryption 3des 3
```

Related Commands

show radius acct statistics

show radius summary

config radius acct ipsec ike

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

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

Syntax Description

dh-group	Specifies the Dixie-Hellman group.
group-1	Configures the DH Group 1 (768 bits).
group-2	Configures the DH Group 2 (1024 bits).
group-5	Configures the DH Group 5 (1024 bits).
lifetime	Configures the IKE lifetime.
seconds	IKE lifetime in seconds.
phase1	Configures the IKE phase1 node.
aggressive	Enables the aggressive mode.
main	Enables the main mode.
index	RADIUS server index.

Command Default

None.

Examples

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

```
> 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

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

Command Default

The default delimiter is a hyphen.

Examples

This 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:

```
> 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

index	RADIUS server index.
enable	Enables the server as a network user's default RADIUS server.
disable	Disables the server as a network user's default RADIUS server.

Command Default None.

Examples This example shows how to configure a default RADIUS accounting server for the network users with RADIUS server index1:

```
> 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*

Syntax Description

index	RADIUS server index.
timeout	Number of seconds (from 2 to 30) between retransmissions.

Command Default None.

Examples This example shows how to configure retransmission timeout value 5 seconds between the retransmission:

```
> config radius acct retransmit-timeout 5
```

Related Commands **show radius acct statistics**

Configure RADIUS Authentication Server Commands

Use the **config radius** auth commands to configure RADIUS authentication server settings.

config radius auth

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

config radius auth {{**enable** | **disable** | **delete**} *index* | **add** *index server_ip port* {**ascii** | **hex**} *secret*}

Syntax Description

enable	Enables a RADIUS authentication server.
disable	Disables a RADIUS authentication server.
delete	Deletes a RADIUS authentication server.
index	RADIUS server index. The controller begins the search with 1.
add	Adds a RADIUS authentication server. See the "Defaults" section.
server_ip	IP address of the RADIUS server.
port	RADIUS server's UDP port number for the interface protocols.
ascii	Specifies RADIUS server's secret type: **ascii**.
hex	Specifies RADIUS server's secret type: **hex**.
secret	RADIUS server's secret.

Command Default

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

Examples

This example shows how to configure a priority *1* RADIUS authentication server at *10.10.10.10* using port *1812* with a login password of *admin*:

```
> config radius auth add 1 10.10.10.10 1812 ascii admin
```

Related Commands

show radius auth statistics

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	Enables IPsec HMAC-MD5 authentication.
hmac-shal	Enables IPsec HMAC-SHA1 authentication.
index	RADIUS server index.

Command Default None.

Examples This example shows how to configure the IPsec hmac-md5 support for RADIUS authentication server index 1:

```
> 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

enable	Enables the IPsec support for an authentication server.
disable	Disables the IPsec support for an authentication server.
index	RADIUS server index.

Command Default

None.

Examples

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

```
> config radius auth IPsec enable 1
```

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

```
> config radius auth IPsec disable 1
```

Related Commands

show radius acct statistics

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

3des	Enables the IPsec 3DES encryption.
aes	Enables the IPsec AES encryption.
des	Enables the IPsec DES encryption.
index	RADIUS server index.

Command Default None.

Examples This example shows how to configure IPsec 3dec encryption RADIUS authentication server index 3:

```
> 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 {**dh-group** {**group-1** | **group-2** | **group-5**} | **lifetime** *seconds* | **phase1** {**aggressive** | **main**}} *index*

Syntax Description

dh-group	Configures the IKE Diffe-Hellman group.
group-1	Configures the DH Group 1 (768 bits).
group-2	Configures the DH Group 2 (1024 bits).
group-5	Configures the DH Group 2 (1024 bits).
lifetime	Configures the IKE lifetime.
seconds	Lifetime in seconds.
phase1	Configures the IKE phase1 mode.
aggressive	Enables the aggressive mode.
main	Enables the main mode.
index	RADIUS server index.

Command Default

None.

Examples

This example shows how to configure IKE lifetime of 23 seconds for RADIUS authentication server index 1:

```
> 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 index*}

Syntax Description

enable	Enables AES key wrap.
disable	Disables AES key wrap.
add	Configures AES key wrap attributes.
ascii	Configures key wrap in an ASCII format.
hex	Configures key wrap in a hexadecimal format.
kek	16-byte Key Encryption Key (KEK).
mack	20-byte Message Authentication Code Key (MACK).
index	Index of the RADIUS authentication server on which to configure the AES key wrap.

Command Default

None.

Examples

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

```
> 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

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

Command Default

The default delimiter is a hyphen.

Examples

This example shows how to specify a delimiter hyphen to be used for a RADIUS authentication server:

```
> 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

index	RADIUS server index.
enable	Enables the server as a management user's default RADIUS server.
disable	Disables the server as a management user's default RADIUS server.

Command Default

None.

Examples

This example shows how to configure a RADIUS server for management users:

```
> 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

index	RADIUS server index.
retransmit-timeout	Timeout value. The range is from 1 to 30 seconds.

Command Default None.

Examples This example shows how to configure a default RADIUS server retransmission timeout for management users:

```
> 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

index	RADIUS server index.
enable	Enables the server as a network user default RADIUS server.
disable	Disables the server as a network user default RADIUS server.

Command Default None.

Examples This example shows how to configure a default RADIUS server for network users:

```
> 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*

Syntax Description

index	RADIUS server index.
timeout	Number of seconds (from 2 to 30) between retransmissions.

Command Default

None.

Examples

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

```
> 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 wireless LAN controller, use the **config radius auth rfc3576** command.

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

Syntax Description

enable	Enables RFC-3576 support for an authentication server.
disable	Disables RFC-3576 support for an authentication server.
index	RADIUS server index.

Command Default

None.

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.

Examples

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

```
> config radius auth rfc3576 enable 2
```

Related Commands

show radius auth statistics

show radius summary

show radius rfc3576

config radius auth server-timeout

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

config radius auth server-timeout *index timeout*

Syntax Description

index	RADIUS server index.
timeout	Timeout value. The range is from 2 to 30 seconds.

Command Default

The default timeout is 2 seconds.

Examples

This example shows how to configure a server timeout value of 2 seconds for RADIUS authentication server index 10:

```
> config radius auth server-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.

Examples This example shows how to configure the controller to mark a RADIUS server as down:

```
> 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	Enables RADIUS vendor ID backward compatibility.
disable	Disables RADIUS vendor ID backward compatibility.

Command Default Enabled.

Examples This example shows how to enable the RADIUS backward compatibility settings:

```
> config radius backward compatibility disable
```

Related Commands **show radius summary**

config radius callStationIdCase

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

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

Syntax Description

legacy	Sends Call Station IDs for layer 2 auth to RADIUS in uppercase.
lower	Sends all Call Station IDs to RADIUS in lowercase.
upper	Sends all Call Station IDs to RADIUS in uppercase.

Command Default Enabled.

Examples This example shows how to send the call station ID Case (lowercase or uppercase) to use the IP address:

```
> config radius callStationIdCase lower
```

Related Commands **show radius summary**

config radius callStationIdType

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

config radius callStationIdType {**ipaddr** | **macaddr** | **ap-macaddr** | **ap-macaddr-ssid** | **ap-group-name** | **flex-group-name** | **ap-name** | **ap-name-ssid** | **ap-location**| **vlan-id**}

Syntax Description

ipaddr	Configures the Call Station ID type to use the IP address (only Layer 3).
macaddr	Configures the Call Station ID type to use the system's MAC address (Layers 2 and 3).
ap-macaddr-only	Configures the Call Station ID type to use the access point's MAC address (Layers 2 and 3).
ap-macaddr-ssid	Configures the Call Station ID type to use the access point's MAC address (Layers 2 and 3) in the format <AP MAC address>:<SSID>
ap-group-name	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.
flex-group-name	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.
ap-name	Configures the Call Station ID type to use the access point's name.
ap-name-ssid	Configures the Call Station ID type to use the access point's name in the format <AP name>:<SSID>
ap-location	Configures the Call Station ID type to use the access point's location.
vlan-id	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.

Examples

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

```
> config radius callStationIdType ipAddr
```

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

```
> config radius callStationIdType macAddr
```

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

```
> config radius callStationIdType ap-macAddr
```

Related Commands

show radius summary

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

mode	Specifies the mode.
off	Disables RADIUS server fallback.
passive	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.
active	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.
username	Specifies the username.
username	Username. The username can be up to 16 alphanumeric characters.
interval	Specifies the probe interval value.
interval	Probe interval. The range is 180 to 3600.

Command Default

The default probe interval is 300.

Examples

This example shows how to disable the RADIUS accounting server fallback behavior:

```
> config radius fallback-test mode off
```

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

```
> config radius fallback-test mode passive
```

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

```
> config radius fallback-test mode active
```

Related Commands

config advanced probe filter

config advanced probe limit

show advanced probe

show radius acct statistics

Configure Rogue Commands

Use the **configure rogue** commands to configure policy settings for unidentified (rogue) clients.

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

enable	Globally enables detection and reporting of ad-hoc rogues.
disable	Globally disables detection and reporting of ad-hoc rogues.
external	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.
rogue_MAC	MAC address of the ad-hoc rogue access point.
alert	Generates an SMNP trap upon detection of the ad-hoc rogue, and generates an immediate alert to the system administrator for further action.
all	Enables alerts for all ad-hoc rogue access points.
auto-contain	Contains all wired ad-hoc rogues detected by the controller.
monitor_ap	(Optional) IP address of the ad-hoc rogue access point.
contain	Contains the offending device so that its signals no longer interfere with authorized clients.
1234_aps	Maximum number of Cisco access points assigned to actively contain the ad-hoc rogue access point (1 through 4, inclusive).
delete	Deletes ad-hoc rogue access points.
all	Deletes all ad-hoc rogue access points.
mac-address	Deletes ad-hoc rogue access point with the specified MAC address.
mac-address	MAC address of the ad-hoc rogue access point.
classify	Configures ad-hoc rogue access point classification.
friendly state	Classifies ad-hoc rogue access points as friendly.

internal	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.
malicious state	Classifies ad-hoc rogue access points as malicious.
alert	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.
contain	Configures contain state on the rogue access point. Controller contains the offending device so that its signals no longer interfere with authorized clients.
unclassified state	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**.

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.

Examples

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

```
> config rogue adhoc enable
```

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

```
> config rogue adhoc alert all
```

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

```
> 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

friendly	Classifies a rogue access point as friendly.
state	Specifies a response to classification.
internal	Configures the controller to trust this rogue access point.
external	Configures the controller to acknowledge the presence of this access point.
ap_mac	MAC address of the rogue access point.
malicious	Classifies a rogue access point as potentially malicious.
unclassified	Classifies a rogue access point as unknown.
alert	Configures the controller to forward an immediate alert to the system administrator for further action.
contain	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.

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.

Examples

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

```
> config rogue ap classify friendly state internal 11:11:11:11:11:11
```

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

```
> config rogue ap classify malicious state alert 11:11:11:11:11:11
```

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

```
> 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

add	Adds this rogue access point from the friendly MAC address list.
delete	Deletes this rogue access point from the friendly MAC address list.
ap_mac	MAC address of the rogue access point that you want to add or delete.

Command Default

None.

Examples

This 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:

```
> config rogue ap friendly add 11:11:11:11:11:11
```

Related Commands

config rogue adhoc
config rogue ap classify
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 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

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

Command Default

None.

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.

Examples

This example shows how to enable RLDP on all access points:

```
> config rogue ap rldp enable alarm-only
```

This example shows how to enable RLDP on monitor-mode access point ap_1:

```
> config rogue ap rldp enable alarm-only ap_1
```

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

```
> config rogue ap rldp initiate 123.456.789.000
```

This example shows how to disable RLDP on all access points:

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

Command Default

None.

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.

Examples

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

```
> config rogue ap ssid auto-contain
```

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 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*

Syntax Description

seconds	Value of 240 to 3600 seconds (inclusive), with a default value of 1200 seconds.

Command Default

1200 seconds.

Examples

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

```
> config rogue ap timeout 2400
```

Related Commands

config rogue ap classify
config rogue ap friendly
config rogue ap rldp
config rogue ap ssid
config rogue rule
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 ignore-list
show rogue rule detailed
show rogue rule summary

config rogue auto-contain level

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

config rogue auto-contain level *level* [**monitor_ap_only**]

Syntax Description

level	Rogue auto-containment level in the range of 1 to 4. **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.
monitor_ap_only	(Optional) Configures auto-containment using only monitor AP mode.

Command Default

Level 1.

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 autocontainment 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- 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.

Examples

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

```
> 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**}

Syntax Description

alarm	Generates only an alarm when a rogue access point is discovered to be associated with a valid client.
auto-contain	Automatically contains a rogue access point to which a trusted client is associated.

Command Default

None.

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.

Examples

This example shows how to automatically contain a rogue access point that is associated with a valid client:

```
> config rogue ap valid-client auto-contain
```

Related Commands

config rogue ap classify
config rogue ap friendly
config rogue ap rldp
config rogue ap timeout
config rogue ap ssid
config rogue rule
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 ignore-list
show rogue rule detailed

show rogue rule summary

config rogue client

To configure rogue clients, use the **config rogue client** command.

config rogue client {**aaa** {**enable** | **disable**} | **alert** *ap_mac* | **contain** *client_mac*} *num_of_APs*

Syntax Description

aaa	Configures AAA server or local database to validate whether rogue clients are valid clients.
enable	Enables the AAA server or local database to check rogue client MAC addresses for validity.
disable	Disables the AAA server or local database to check rogue client MAC addresses for validity.
alert	Configures the controller to forward an immediate alert to the system administrator for further action.
ap_mac	Access point MAC address.
contain	Configures the controller to contain the offending device so that its signals no longer interfere with authorized clients.
client_mac	MAC address of the rogue client.
num_of_APs	Maximum number of Cisco access points to actively contain the rogue access point (1–4).

Command Default

None.

Examples

This example shows how to enable the AAA server or local database to check MAC addresses:

```
> config rogue client aaa enable
```

This example shows how to disable the AAA server or local database from checking MAC addresses:

```
> config rogue client aaa disable
```

Related Commands

config rogue rule

config trapflags rogueap

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 name ‘all’, the ‘all access points’ case takes precedence over the AP that is named ‘all’.

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

Syntax Description

enable	Enables rogue detection on this access point.
disable	Disables rogue detection on this access point.
cisco_ap	Cisco access point.
all	Specifies all access points.

Command Default

Enabled.

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.

Examples

This example shows how to enable rogue detection on the access point Cisco_AP:

```
> 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*

Syntax Description

rssi-in-dBm	Minimum RSSI value. The valid range is from –70 dBm to –128 dBm, and the default value is –128 dBm.

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.

Examples

This example shows how to configure the minimum RSSI value:

```
> config rogue detection min-rssi –80
```

Related Commands

config rogue detection

show rogue ap clients

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 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

report-interval	Specifies the interval at which rogue reports are sent.
transient-rogue-interval	Specifies the interval at which rogues are consistently scanned for by APs after the first time the rogues are scanned.
time-in-seconds	Time in seconds. The valid range is as follows: • 10 to 300 for **report-interval** • 120 to 1800 for **transient-rogue-interval**

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.

Examples

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

```
> config rogue detection monitor-ap report-interval 60
```

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

```
> 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** *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

add ap priority	Adds a rule with match any criteria and the priority that you specify.
priority	Priority of this rule within the list of rules.
classify	Specifies the classification of a rule.
custom	Classifies devices matching the rule as custom.
severity-score	Custom classification severity score of the rule. The range is from 1 to 100.
classification-name	Custom classification name. The name can be up to 32 case-sensitive, alphanumeric characters.
friendly	Classifies a rule as friendly.
malicious	Classifies a rule as malicious.
notify	Configures type of notification upon rule match.
all	Notifies the controller and a trap receiver such as Cisco Prime Infrastructure.
global	Notifies only a trap receiver such as Cisco Prime Infrastructure.
local	Notifies only the controller.
none	Notifies neither the controller nor a trap receiver such as Cisco Prime Infrastructure.
state	Configures state of the rogue access point after a rule match.
alert	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.

contain	Configures contain state on the rogue access point. Controller contains the offending device so that its signals no longer interfere with authorized clients.
external	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.
internal	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.
rule_name	Rule to which the command applies, or the name of a new rule.
condition ap	Specifies the conditions for a rule that the rogue access point must meet.
set	Adds conditions to a rule that the rogue access point must meet.
delete	Removes conditions to a rule that the rogue access point must meet.
condition_type	Type of the condition to be configured. The condition types are listed below: • client-count—Requires that a minimum number of clients be associated to the rogue access point. The valid range is 1 to 10 (inclusive). • duration—Requires that the rogue access point be detected for a minimum period of time. The valid range is 0 to 3600 seconds (inclusive). • managed-ssid—Requires that the rogue access point's SSID be known to the controller. • no-encryption—Requires that the rogue access point's advertised WLAN does not have encryption enabled. • rssi—Requires that the rogue access point have a minimum RSSI value. The range is from –95 to –50 dBm (inclusive). • ssid—Requires that the rogue access point have a specific SSID.
condition_value	Value of the condition. This value is dependent upon the condition_type. For instance, if the condition type is ssid, then the condition value is either the SSID name or all.
enable	Enables all rules or a single specific rule.
delete	Deletes all rules or a single specific rule.
disable	Deletes all rules or a single specific rule.

match	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.
all	Specifies all rules defined.
any	Specifies any rule meeting certain criteria.
priority	Changes the priority of a specific rule and shifts others in the list accordingly.

Command Default

None.

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.

Examples

This example shows how to create a rule called rule_1 with a priority of 1 and a classification as friendly:

```
> config rogue rule add ap priority 1 classify friendly rule_1
```

This example shows how to enable rule_1:

```
> config rogue rule enable rule_1
```

This example shows how to change the priority of the last command:

```
> config rogue rule priority 2 rule_1
```

This example shows how to change the classification of the last command:

```
> config rogue rule classify malicious rule_1
```

This example shows how to disable the last command:

```
> config rogue rule disable rule_1
```

This example shows how to delete SSID_2 from the user-configured SSID list in rule-5:

```
> config rogue rule condition ap delete ssid ssid_2 rule-5
```

This example shows how to create a custom rogue rule:

```
> config rogue rule classify custom 1 VeryMalicious rule6
```

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 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

Configure TACACS Commands

Use the **config tacacs** commands to configure TACACS+ settings.

config tacacs acct

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

config tacacs acct add {*server_index ip_address port type secret_key*} | **delete** *server_index* | **disable** *server_index* | **enable** *server_index* | **retransmit-timeout** {*server_index seconds*}

Syntax Description

add	Adds a new TACACS+ accounting server.
server_index	TACACS+ accounting server index (1 to 3).
ip_address	IP address for the TACACS+ accounting server.
port	Controller port used for the TACACS+ accounting server.
type	Type of secret key being used (ASCII or HEX).
secret_key	Secret key in ASCII or hexadecimal characters.
delete	Deletes a TACACS+ server.
disable	Disables a TACACS+ server.
enable	Enables a TACACS+ server.
retransmit-timeout	Changes the default retransmit timeout for the TACACS+ server.
seconds	Retransmit timeout (2 to 30 seconds).

Command Default

None.

Examples

This example shows how to add a new TACACS+ accounting server index 3 with the IP address 10.0.0.0, port number 10, and secret key 12345678 in ASCII:

```
> config tacacs acct add 1 10.0.0.0 10 ascii 12345678
```

This example shows how to change the default retransmit timeout of 30 seconds for the TACACS+ accounting server:

```
> config tacacs acct retransmit-timeout 30
```

Related Commands

show run-config

show tacacs acct statistics

show tacacs summary

config tacacs athr

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

config tacacs athr add {*server_index ip_address port type secret_key*} | **delete** *server_index* | **disable** *server_index* | **enable** *server_index* | **retransmit-timeout** {*server_index seconds*}

Syntax Description

add	Adds a new TACACS+ accounting server.
server_index	TACACS+ accounting server index (1 to 3).
ip_address	IP address for the TACACS+ accounting server.
port	Controller port used for the TACACS+ accounting server.
type	Type of secret key being used (ASCII or HEX).
secret_key	Secret key in ASCII or hexadecimal characters.
delete	Deletes a TACACS+ server.
disable	Disables a TACACS+ server.
enable	Enables a TACACS+ server.
retransmit-timeout	Changes the default retransmit timeout for the TACACS+ server.
seconds	Retransmit timeout (2 to 30 seconds).

Command Default

None.

Examples

This example shows how to add a new TACACS+ authorization server index 3 with the IP address 10.0.0.0, port number 4, and secret key 12345678 in ASCII:

```
> config tacacs athr add 3 10.0.0.0 4 ascii 12345678
```

This example shows how to change the default retransmit timeout of 30 seconds for the TACACS+ authorization server:

```
> config tacacs athr retransmit-timeout 30
```

Related Commands

show run-config

show tacacs summary

show tacacs athr statistics

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*

Syntax Description

index	TACACS+ authorization server index.
timeout	Timeout value. The range is 1 to 30 seconds.

Command Default None.

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

```
> config tacacs athr mgmt-server-timeout 1 10
```

Related Commands **config tacacs athr**

config tacacs auth

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

config tacacs auth add {*server_index ip_address port type secret_key*} | **delete** *server_index* | **disable** *server_index* | **enable** *server_index* | **retransmit-timeout** {*server_index seconds*}

Syntax Description

add	Adds a new TACACS+ accounting server.
server_index	TACACS+ accounting server index (1 to 3).
ip_address	IP address for the TACACS+ accounting server.
port	Controller port used for the TACACS+ accounting server.
type	Type of secret key being used (ASCII or HEX).
secret_key	Secret key in ASCII or hexadecimal characters.
delete	Deletes a TACACS+ server.
disable	Disables a TACACS+ server.
enable	Enables a TACACS+ server.
retransmit-timeout	Changes the default retransmit timeout for the TACACS+ server.
seconds	Retransmit timeout (2 to 30 seconds).

Command Default

None.

Examples

This example shows how to add a new TACACS+ authentication server index 2 with the IP address 10.0.0.3, port number 6, and secret key 12345678 in ASCII:

```
> config tacacs auth add 2 10.0.0.3 6 ascii 12345678
```

This example shows how to change the default retransmit timeout of 30 seconds for TACACS+ authentication server:

```
> config tacacs auth retransmit-timeout 30
```

Related Commands

show run-config

show tacacs auth statistics

show tacacs summary

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

index	TACACS+ authentication server index.
timeout	Timeout value. The range is 1 to 30 seconds.

Command Default None.

Examples This example shows how to configure a default TACACS+ authentication server timeout for management users:

```
> config tacacs auth mgmt-server-timeout 1 10
```

Related Commands **config tacacs auth**

Configure Wireless LAN Security Commands

Use the **config wlan security** commands to configure wireless LAN security settings.

config wlan security 802.1X

To change the state of 802.1X security on the wireless LAN Cisco radios, use the **config wlan security 802.1X** command.

config wlan security 802.1X {**enable** {*wlan_id* | **foreignAp**} | **disable** {*wlan_id* | **foreignAp**} | **encryption** {*wlan_id* | **foreignAp**} {**0** | **40** | **104**} | **on-macfilter-failure** {**enable** | **disable**}}

Syntax Description

enable	Enables the 802.1X settings.
wlan_id	Wireless LAN identifier between 1 and 512.
foreignAp	Specifies third-party access points.
disable	Disables the 802.1X settings.
encryption	Specifies the static WEP keys and indexes.
0	Specifies a WEP key size of 0 (no encryption) bits. The default value is 104. **Note** All keys within a wireless LAN must be the same size.
40	Specifies a WEP key size of 40 bits. The default value is 104. **Note** All keys within a wireless LAN must be the same size.
104	Specifies a WEP key size of 104 bits. The default value is 104. **Note** All keys within a wireless LAN must be the same size.
on-macfilter-failure	Configures 802.1X on MAC filter failure.
enable	Enables 802.1X authentication on MAC filter failure.
disable	Disables 802.1X authentication on MAC filter failure.

Command Default

None.

Usage Guidelines

To change the encryption level of 802.1X security on the wireless LAN Cisco radios, use the following key sizes:

- 0—no 802.1X encryption.
- 40—40/64-bit encryption.
- 104—104/128-bit encryption. (This is the default encryption setting.)

Examples This example shows how to configure 802.1X security on WLAN ID 16:

```
> config wlan security 802.1X enable 16
```

Related Commands **show wlan**

config wlan security ckip

To configure Cisco Key Integrity Protocol (CKIP) security options for the wireless LAN, use the **config wlan security ckip** command.

config wlan security ckip {**enable** | **disable**} *wlan_id* [**akm psk set-key** {**hex** | **ascii**} {**40** | **104**} **key** *key_index* *wlan_id* | **mmh-mic** {**enable** | **disable**} *wlan_id* | **kp** {**enable** | **disable**} *wlan_id*]

Syntax Description

enable	Enables CKIP security.
disable	Disables CKIP security.
wlan_id	WLAN to which you apply the command.
akm psk set-key	(Optional) Configures encryption key management for the CKIP wireless LAN.
hex	Specifies a hexadecimal encryption key.
ascii	Specifies an ASCII encryption key.
40	Sets the static encryption key length to 40 bits for the CKIP WLAN. 40-bit keys must contain 5 ASCII text characters or 10 hexadecimal characters.
104	Sets the static encryption key length to 104 bits for the CKIP WLAN. 104-bit keys must contain 13 ASCII text characters or 26 hexadecimal characters.
key	Specifies the CKIP WLAN key settings.
key_index	Configured PSK key index.
mmh-mic	(Optional) Configures multi-modular hash message integrity check (MMH MIC) validation for the CKIP wireless LAN.
kp	(Optional) Configures key-permutation for the CKIP wireless LAN.

Command Default

None.

Examples

This example shows how to configure a CKIP WLAN encryption key of 104 bits (26 hexadecimal characters) for PSK key index 2 on WLAN 03:

```
> config wlan security ckip akm psk set-key hex 104 key 2 03
```

Related Commands

config wlan ccx aironet-ie

show wlan

config wlan security cond-web-redir

To enable or disable conditional web redirect, use the **config wlan security cond-web-redir** command.

config wlan security cond-web-redir {**enable** | **disable**} *wlan_id*

Syntax Description

enable	Enables conditional web redirect.
disable	Disables conditional web redirect.
wlan_id	Wireless LAN identifier between 1 and 512.

Command Default

None.

Examples

This example shows how to enable the conditional web direct on WLAN ID 2:

```
> config wlan security cond-web-redir enable 2
```

Related Commands

show wlan

config wlan security eap-passthru

To configure the 802.1X frames pass through on to the external authenticator, use the **config wlan security eap-passthru** command.

config wlan security eap-passthru {**enable** | **disable**} *wlan_id*

Syntax Description

enable	Enables 802.1X frames pass through to external authenticator.
disable	Disables 802.1X frames pass through to external authenticator.
wlan_id	Wireless LAN identifier between 1 and 512.

Command Default None.

Examples This example shows how to enable the 802.1X frames pass through to external authenticator on WLAN ID 2:

```
> config wlan security eap-passthru enable 2
```

Related Commands **show wlan**

config wlan security ft

To configure 802.11r fast transition parameters, use the **config wlan security ft** command.

config wlan security ft {**enable** | **disable** | **reassociation-timeout** *timeout-in-seconds*} *wlan_id*

Syntax Description

enable	Enables 802.11r fast transition roaming support.
disable	Disables 802.11r fast transition roaming support.
reassociation-timeout	Configures reassociation deadline interval.
timeout-in-seconds	Reassociation timeout value in seconds. The valid range is 1 to 100 seconds.
wlan_id	Wireless LAN identifier between 1 and 512.

Command Default

None.

Usage Guidelines

Ensure that you have disabled the WLAN before you proceed.

Examples

This example shows how to enable 802.11r fast transition roaming support on WLAN 2:

```
> config wlan security ft enable 2
```

This example shows how to set the reassociation timeout value of 20 seconds for 802.11r fast transition roaming support on WLAN 2:

```
> config wlan security ft reassociation-timeout 20 2
```

Related Commands

show wlan

config wlan security ft over-the-ds

To configure 802.11r fast transition parameters over a distributed system, use the **config wlan security ft over-the-ds** command.

config wlan security ft over-the-ds {**enable** | **disable**} *wlan_id*

Syntax Description

enable	Enables 802.11r fast transition roaming support over a distributed system.
disable	Disables 802.11r fast transition roaming support over a distributed system.
wlan_id	Wireless LAN identifier between 1 and 512.

Command Default

Enabled.

Usage Guidelines

Ensure that you have disabled the WLAN before you proceed.

Ensure that 802.11r fast transition is enabled on the WLAN.

Examples

This example shows how to enable 802.11r fast transition roaming support over a distributed system on WLAN ID 2:

```
> config wlan security ft over-the-ds enable 2
```

Related Commands

show wlan

config wlan security IPsec disable

To disable IPsec security, use the **config wlan security IPsec disable** command.

config wlan security IPsec disable {*wlan_id* | **foreignAp**}

Syntax Description

wlan_id	Wireless LAN identifier between 1 and 512.
foreignAp	Specifies third-party access points.

Command Default None.

Examples This example shows how to disable the IPsec for WLAN ID 16:

```
> config wlan security IPsec disable 16
```

Related Commands **show wlan**

config wlan security IPsec enable

To enable IPsec security, use the **config wlan security IPsec enable** command.

config wlan security IPsec enable {*wlan_id* | **foreignAp**}

Syntax Description

wlan_id	Wireless LAN identifier between 1 and 512.
foreignAp	Specifies third-party access points.

Command Default None.

Examples This example shows how to enable the IPsec for WLAN ID 16:

```
> config wlan security IPsec enable 16
```

Related Commands **show wlan**

config wlan security IPsec authentication

To modify the IPsec security authentication protocol used on the wireless LAN, use the **config wlan security IPsec authentication** command.

config wlan security IPsec authentication {**hmac-md5** | **hmac-sha-1**} {*wlan_id* | **foreignAp**}

Syntax Description

hmac-md5	Specifies the IPsec HMAC-MD5 authentication protocol.
hmac-sha-1	Specifies the IPsec HMAC-SHA-1 authentication protocol.
wlan_id	Wireless LAN identifier between 1 and 512.
foreignAp	Specifies third-party access points.

Command Default

None.

Examples

This example shows how to configure the IPsec HMAC-SHA-1 security authentication parameter for WLAN ID 1:

```
> config wlan security IPsec authentication hmac-sha-1 1
```

Related Commands

show wlan

config wlan security IPsec encryption

To modify the IPsec security encryption protocol used on the wireless LAN, use the **config wlan security IPsec encryption** command.

config wlan security IPsec encryption {**3des** | **aes** | **des**} {*wlan_id* | **foreignAp**}

Syntax Description

3des	Enables IPsec 3DES encryption.
aes	Enables IPsec AES 128-bit encryption.
des	Enables IPsec DES encryption.
wlan_id	Wireless LAN identifier between 1 and 512.
foreignAp	Specifies third-party access points.

Command Default

None.

Examples

This example shows how to configure the IPsec aes encryption:

```
> config wlan security IPsec encryption aes 1
```

Related Commands

show wlan

config wlan security IPsec config

To configure the proprietary Internet Key Exchange (IKE) CFG-Mode parameters used on the wireless LAN, use the **config wlan security IPsec config** command.

config wlan security IPsec config qotd *ip_address* {*wlan_id* | **foreignAp**}

Syntax Description

qotd	Configures the quote-of-the day server IP for cfg-mode.
ip_address	Quote-of-the-day server IP for cfg-mode.
wlan_id	Wireless LAN identifier between 1 and 512.
foreignAp	Specifies third-party access points.

Command Default

None.

Usage Guidelines

IKE is used as a method of distributing the session keys (encryption and authentication), as well as providing a way for the VPN endpoints to agree on how the data should be protected. IKE keeps track of connections by assigning a bundle of Security Associations (SAs), to each connection.

Examples

This example shows how to configure the quote-of-the-day server IP 44.55.66.77 for cfg-mode for WLAN 1:

```
> config wlan security IPsec config qotd 44.55.66.77 1
```

Related Commands

show wlan

config wlan security IPsec ike authentication

To modify the IPsec Internet Key Exchange (IKE) authentication protocol used on the wireless LAN, use the **config wlan security IPsec ike authentication** command.

config wlan security IPsec ike authentication {**certificates** {*wlan_id* | **foreignAp**} | **pre-share-key** {*wlan_id* | **foreignAp**} *key* | **xauth-psk** {*wlan_id* | **foreignAp**} *key*}

Syntax Description

certificates	Enables the IKE certificate mode.
wlan_id	Wireless LAN identifier between 1 and 512.
foreignAp	Specifies third-party access points.
pre-share-key	Enables the IKE Xauth with preshared keys.
xauth-psk	Enables the IKE preshared key.
key	Key required for preshare and xauth-psk.

Command Default

None.

Examples

This example shows how to configure the IKE certification mode:

```
> config wlan security IPsec ike authentication certificates 16
```

Related Commands

show wlan

config wlan security IPsec ike dh-group

To modify the IPsec Internet Key Exchange (IKE) Diffie Hellman group used on the wireless LAN, use the **config wlan security IPsec ike dh-group** command.

config wlan security IPsec ike dh-group {*wlan_id* | **foreignAp**} {**group-1** | **group-2** | **group-5**}

Syntax Description

wlan_id	Wireless LAN identifier between 1 and 512.
foreignAp	Specifies third-party access points.
group-1	Specifies DH group 1 (768 bits).
group-2	Specifies DH group 2 (1024 bits).
group-5	Specifies DH group 5 (1536 bits).

Command Default

None.

Examples

This example shows how to configure the Diffe Hellman group parameter for group-1:

```
> config wlan security IPsec ike dh-group 1 group-1
```

Related Commands

show wlan

config wlan security IPsec ike lifetime

To modify the IPsec Internet Key Exchange (IKE) lifetime used on the wireless LAN, use the **config wlan security IPsec ike lifetime** command.

config wlan security IPsec ike lifetime {*wlan_id* | **foreignAp**} *seconds*

Syntax Description

wlan_id	Wireless LAN identifier between 1 and 512.
foreignAp	Specifies third-party access points.
seconds	IKE lifetime in seconds, between 1800 and 345600.

Command Default

None.

Examples

This example shows how to configure the IPsec IKE lifetime use on the wireless LAN:

```
> config wlan security IPsec ike lifetime 1 1900
```

Related Commands

show wlan

config wlan security IPsec ike phase1

To modify IPsec Internet Key Exchange (IKE) Phase 1 used on the wireless LAN, use the **config wlan security IPsec ike phase1** command.

config wlan security IPsec ike phase1 {**aggressive** | **main**} {*wlan_id* | **foreignAp**}

Syntax Description

aggressive	Enables the IKE aggressive mode.
main	Enables the IKE main mode.
wlan_id	Wireless LAN identifier between 1 and 512.
foreignAp	Specifies third-party access points.

Command Default

None.

Examples

This example shows how to modify IPsec IKE Phase 1:

```
> config wlan security IPsec ike phase1 aggressive 16
```

Related Commands

show wlan

config wlan security IPsec ike contivity

To modify Nortel's Contivity VPN client support on the wireless LAN, use the **config wlan security IPsec ike contivity** command.

config wlan security IPsec ike contivity {**enable** | **disable**} {*wlan_id* | **foreignAp**}

Syntax Description

enable	Enables contivity support for this WLAN.
disable	Disables contivity support for this WLAN.
wlan_id	Wireless LAN identifier between 1 and 512.
foreignAp	Specifies third-party access points.

Command Default

None.

Examples

This example shows how to modify Contivity VPN client support:

```
> config wlan security IPsec ike contivity enable 14
```

Related Commands

show wlan

config wlan security passthru

To modify the IPsec pass-through used on the wireless LAN, use the **config wlan security passthru** command.

config wlan security passthru {**enable** | **disable**} {*wlan_id* | **foreignAp**} [*ip_address*]

Syntax Description

enable	Enables IPsec pass-through.
disable	Disables IPsec pass-through.
wlan_id	Wireless LAN identifier between 1 and 512.
foreignAp	Specifies third-party access points.
ip_address	(Optional) IP address of the IPsec gateway (router) that is terminating the VPN tunnel.

Command Default

None.

Examples

This example shows how to modify IPsec pass-through used on the wireless LAN:

```
> config wlan security passthru enable 3 192.12.1.1
```

Related Commands

show wlan

config wlan security pmf

To configure 802.11w Management Frame Protection (MFP) on a WLAN, use the **config wlan security pmf** command.

config wlan security pmf {**disable** | **optional** | **required** | **association-comeback** *association-comeback_timeout* | **saquery-retrytimeout** *saquery-retry_timeout*} *wlan_id*

Syntax Description

disable	Disables 802.11w MFP protection on a WLAN.
optional	Enables 802.11w MFP protection on a WLAN.
required	Requires clients to negotiate 802.11w MFP protection on a WLAN.
association-comeback	Configures the 802.11w association comeback time.
association-comeback_timeout	Association comeback interval in seconds. Time interval that an associated client must wait before the association is tried again after it is denied with a status code 30. The status code 30 message is "Association request rejected temporarily; Try again later". The range is from 1 to 20 seconds.
saquery-retrytimeout	Configures the 802.11w Security Association (SA) query retry timeout.
saquery-retry_timeout	Time interval identified in the association response to an already associated client before the association can be tried again. This time interval checks if the client is a real client and not a rogue client during the association comeback time. If the client does not respond within this time, the client association is deleted from the controller. The range is from 100 to 500 ms.
wlan_id	Wireless LAN identifier from 1 to 512.

Command Default

Default SA query retry timeout is 200 milliseconds.

Default association comeback timeout is 1 second.

Usage Guidelines

802.11w introduces an Integrity Group Temporal Key (IGTK) that is used to protect broadcast or multicast robust management frames. IGTK is a random value, assigned by the authenticator station (controller) used to protect MAC management protocol data units (MMPDUs) from the source STA. The 802.11w IGTK key is derived using the four way handshake and is used only on WLANs that are configured with WPA or WPA2 security at Layer 2.

Examples

This example shows how to enable 802.11w MFP protection on a WLAN:

```
> config wlan security pmf optional 1
```

Examples This example shows how to configure the SA query retry timeout on a WLAN:

```
> config wlan security pmf saquery-retrytimeout 300 1
```

Related Commands

show wlan

show client detail

config wlan security wpa akm pmf

debug 11w-pmf

config wlan security splash-page-web-redir

To enable or disable splash page web redirect, use the **config wlan security splash-page-web-redir** command.

config wlan security splash-page-web-redir {**enable** | **disable**} *wlan_id*

Syntax Description

enable	Enables splash page web redirect.
disable	Disables splash page web redirect.
wlan_id	Wireless LAN identifier between 1 and 512.

Command Default Disabled.

Examples This example shows how to enable spash page web redirect:

```
> config wlan security splash-page-web-redir enable 2
```

Related Commands **show wlan**

config wlan security static-wep-key authentication

To configure static Wired Equivalent Privacy (WEP) key 802.11 authentication on a wireless LAN, use the **config wlan security static-wep-key authentication** command.

config wlan security static-wep-key authentication {**shared-key** | **open**} *wlan_id*

Syntax Description

shared-key	Enables shared key authentication.
open	Enables open system authentication.
wlan_id	Wireless LAN identifier between 1 and 512.

Command Default

None.

Examples

This example shows how to enable the static WEP shared key authentication for WLAN ID 1:

```
> config wlan security static-wep-key authentication shared-key 1
```

Related Commands

show wlan

config wlan security static-wep-key disable

To disable the use of static Wired Equivalent Privacy (WEP) keys, use the **config wlan security static-wep-key disable** command.

config wlan security static-wep-key disable *wlan_id*

Syntax Description

wlan_id	Wireless LAN identifier between 1 and 512.

Command Default

None.

Examples

This example shows how to disable the static WEP keys for WLAN ID 1:

```
> config wlan security static-wep-key disable 1
```

Related Commands

config wlan security wpa encryption

config wlan security static-wep-key enable

To enable the use of static Wired Equivalent Privacy (WEP) keys, use the **config wlan security static-wep-key enable** command.

config wlan security static-wep-key enable *wlan_id*

Syntax Description

wlan_id	Wireless LAN identifier between 1 and 512.

Command Default None.

Examples This example shows how to enable the use of static WEK keys for WLAN ID 1:

```
> config wlan security static-wep-key enable 1
```

Related Commands **config wlan security wpa encryption**

config wlan security static-wep-key encryption

To configure the static Wired Equivalent Privacy (WEP) keys and indexes, use the **config wlan security static-wep-key encryption** command.

config wlan security static-wep-key encryption *wlan_id* {**40** | **104**} {**hex** | **ascii**} *key key-index*

Syntax Description

wlan_id	Wireless LAN identifier between 1 and 512.
40	Specifies the encryption level: 40.
104	Specifies the encryption level: 104.
hex	Specifies to use hexadecimal characters to enter key.
ascii	Specifies whether to use ASCII characters to enter key.
key	WEP key in ASCII.
key-index	Key index (1 to 4).

Command Default

None.

Usage Guidelines

One unique WEP key index can be applied to each wireless LAN. Because there are only four WEP key indexes, only four wireless LANs can be configured for static WEP Layer 2 encryption.

Make sure to disable 802.1X before using this command.

Examples

This example shows how to configure the static WEP keys for WLAN ID 1 that uses hexadecimal character 0201702001 and key index 2:

```
> config wlan security static-wep-key encryption 1 40 hex 0201702001 2
```

Related Commands

show wlan

config wlan security tkip

To configure the Temporal Key Integrity Protocol (TKIP) Message Integrity Check (MIC) countermeasure hold-down timer, use the **config wlan security tkip** command.

config wlan security tkip hold-down *time wlan_id*

Syntax Description

hold-down	Configures the TKIP MIC countermeasure hold-down timer.
time	TKIP MIC countermeasure hold-down time in seconds. The range is from 0 to 60 seconds.
wlan_id	Wireless LAN identifier from 1 to 512.

Command Default

60 seconds.

Usage Guidelines

TKIP countermeasure mode can occur if the access point receives 2 MIC errors within a 60 second period. When this situation occurs, the access point deauthenticates all TKIP clients that are associated to that 802.11 radio and hold offs any clients for the countermeasure holdoff time.

Examples

This example shows how to configure the TKIP MIC countermeasure hold-down timer:

```
> config wlan security tkip
```

Related Commands

show wlan

config wlan security web-auth

To change the status of web authentication used on wireless LAN, use the **config wlan security web-auth** command.

config wlan security web-auth {{**acl** | **enable** | **disable**} {*wlan_id* | **foreignAp**} [*acl_name* | **none**]} | {**on-macfilter-failure** *wlan_id*} | {**server-precedence** *wlan_id* | **local** | **ldap** | **radius**} | {**flexacl** *wlan_id* [*ipv4_acl_name* | **none**]} | {**ipv6 acl** *wlan_id* [*ipv6_acl_name* | **none**]}

Syntax Description

acl	Configures the access control list.
enable	Enables web authentication.
disable	Disables web authentication.
wlan_id	Wireless LAN identifier between 1 and 512.
foreignAp	Specifies third-party access points.
acl_name	(Optional) ACL name (up to 32 alphanumeric characters).
none	(Optional) Specifies no ACL name.
on-macfilter-failure	Enables web authentication on MAC filter failure.
server-precendence	Configures the authentication server precedence order for Web-Auth users.
local	Specifies the server type.
ldap	Specifies the server type.
radius	Specifies the server type.
flexacl	Specifies the IPv4 ACL name. You can enter up to 32 alphanumeric characters.
ipv4_acl_name	(Optional) IPv4 ACL name. You can enter up to 32 alphanumeric characters.
ipv6_acl_name	(Optional) IPv6 ACL name. You can enter up to 32 alphanumeric characters.

Command Default

None.

Examples This example shows how to configure the security policy for WLAN ID 1 and an ACL named ACL03:

```
> config wlan security web-auth acl 1 ACL03
```

Related Commands **show wlan**

config wlan security web-passthrough acl

To add an access control list (ACL) to the wireless LAN definition, use the **config wlan security web-passthrough acl** command.

config wlan security web-passthrough acl {*wlan_id* | **foreignAp**} {*acl_name* | **none**}

Syntax Description

wlan_id	Wireless LAN identifier between 1 and 512.
foreignAp	Specifies third-party access points.
acl_name	ACL name (up to 32 alphanumeric characters).
none	Specifies that there is no ACL.

Command Default

None.

Examples

This example shows how to add an ACL to the wireless LAN definition:

```
> config wlan security web-passthrough acl 1 ACL03
```

Related Commands

show wlan

config wlan security web-passthrough disable

To disable a web captive portal with no authentication required on a wireless LAN, use the **config wlan security web-passthrough disable** command.

config wlan security web-passthrough disable {*wlan_id* | **foreignAp**}

Syntax Description

wlan_id	Wireless LAN identifier between 1 and 512.
foreignAp	Specifies third-party access points.

Command Default

None.

Examples

This example shows how to disable a web captive portal with no authentication required on wireless LAN ID 1:

```
> config wlan security web-passthrough disable 1
```

Related Commands

show wlan

config wlan security web-passthrough email-input

To configure a web captive portal using an e-mail address, use the **config wlan security web-passthrough email-input** command.

config wlan security web-passthrough email-input {**enable** | **disable**} {*wlan_id* | **foreignAp**}

Syntax Description

email-input	Configures a web captive portal using an e-mail address.
enable	Enables a web captive portal using an e-mail address.
disable	Disables a web captive portal using an e-mail address.
wlan_id	Wireless LAN identifier between 1 and 512.
foreignAp	Specifies third-party access points.

Command Default

None.

Examples

This example shows how to configure a web captive portal using an e-mail address:

```
> config wlan security web-passthrough email-input enable 1
```

Related Commands

show wlan

config wlan security web-passthrough enable

To enable a web captive portal with no authentication required on the wireless LAN, use the **config wlan security web-passthrough enable** command.

config wlan security web-passthrough enable {*wlan_id* | **foreignAp**}

Syntax Description

wlan_id	Wireless LAN identifier between 1 and 512.
foreignAp	Specifies third-party access points.

Command Default

None.

Examples

This example shows how to enable a web captive portal with no authentication required on wireless LAN ID 1:

```
> config wlan security web-passthrough enable 1
```

Related Commands

show wlan

config wlan security wpa akm 802.1x

To configure authentication key-management using 802.1X, use the **config wlan security wpa akm 802.1x** command.

config wlan security wpa akm 802.1x {**enable** | **disable**} *wlan_id*

Syntax Description

enable	Enables the 802.1X support.
disable	Disables the 802.1X support.
wlan_id	Wireless LAN identifier between 1 and 512.

Command Default

None.

Examples

This example shows how to configure authentication using 802.1X :

```
> config wlan security wpa akm 802.1x enable 1
```

Related Commands

show wlan

config wlan security wpa akm cckm

To configure authentication key-management using Cisco Centralized Key Management (CCKM), use the **config wlan security wpa akm cckm** command.

config wlan security wpa akm cckm {**enable** *wlan_id* | **disable** *wlan_id* | *timestamp-tolerance* }

Syntax Description

enable	Enables CCKM support.
disable	Disables CCKM support.
wlan_id	Wireless LAN identifier between 1 and 512.
timestamp-tolerance	CCKM IE time-stamp tolerance. The range is between 1000 to 5000 milliseconds; the default is 1000 milliseconds.

Command Default

None.

Examples

This example shows how to configure authentication key-management using CCKM:

```
> config wlan security wpa akm cckm 1500
```

Related Commands

show wlan

config wlan security wpa akm ft

To configure authentication key-management using 802.11r fast transition 802.1X, use the **config wlan security wpa akm ft** command.

config wlan security wpa akm ft [**over-the-air** | **over-the-ds** | **psk** | [**reassociation-timeout** *seconds*]] {**enable** | **disable**} *wlan_id*

Syntax Description

over-the-air	(Optional) Configures 802.11r fast transition roaming over-the-air support.
over-the-ds	(Optional) Configures 802.11r fast transition roaming DS support.
psk	(Optional) Configures 802.11r fast transition PSK support.
reassociation-timeout	(Optional) Configures the reassociation deadline interval. The valid range is between 1 to 100 seconds. The default value is 20 seconds.
seconds	Reassociation deadline interval in seconds.
enable	Enables 802.11r fast transition 802.1X support.
disable	Disables 802.11r fast transition 802.1X support.
wlan_id	Wireless LAN identifier between 1 and 512.

Command Default

None.

Examples

This example shows how to configure authentication key-management using 802.11r fast transition:

```
> config wlan security wpa akm ft reassociation-timeout 25 1
```

Related Commands

show wlan

config wlan security wpa akm pmf

To configure Authenticated Key Management (AKM) of management frames, use the **config wlan security wpa akm pmf** command.

config wlan security wpa akm pmf {**802.1x** | **psk**} {**enable** | **disable**}*wlan_id*

Syntax Description

802.1x	Configures 802.1X authentication for protection of management frames (PMF).
psk	Configures preshared keys (PSK) for PMF.
enable	Enables 802.1X authentication or PSK for PMF.
disable	Disables 802.1X authentication or PSK for PMF.
wlan_id	Wireless LAN identifier from 1 to 512.

Command Default

Disabled.

Usage Guidelines

802.11w has two new AKM suites: 00-0F-AC:5 or 00-0F-AC:6. You must enable WPA and then disable the WLAN to configure PMF on the WLAN.

Examples

This example shows how to enable 802.1X authentication for PMF in a WLAN:

```
> config wlan security wpa akm pmf 802.1x enable 1
```

Related Commands

show wlan

show client detail

config wlan security pmf

debug 11w-pmf

config wlan security wpa akm psk

To configure the Wi-Fi protected access (WPA) preshared key mode, use the **config wlan security wpa akm psk** command.

config wlan security wpa akm psk {**enable** | **disable** | **set-key** *key-format key*} *wlan_id*

Syntax Description

enable	Enables WPA-PSK.
disable	Disables WPA-PSK.
set-key	Configures a preshared key.
key-format	Specifies key format. Either ASCII or hexadecimal.
key	WPA preshared key.
wlan_id	Wireless LAN identifier between 1 and 512.

Command Default

None.

Examples

This example shows how to configure the WPA preshared key mode:

```
> config wlan security wpa akm psk disable 1
```

Related Commands

show wlan

config wlan security wpa disable

To disable WPA1, use the **config wlan security wpa disable** command.

config wlan security wpa disable *wlan_id*

Syntax Description

wlan_id	Wireless LAN identifier between 1 and 512.

Command Default None.

Examples This example shows how to disable WPA:

```
> config wlan security wpa disable 1
```

Related Commands **show wlan**

config wlan security wpa enable

To enable WPA1, use the **config wlan security wpa enable** command.

config wlan security wpa enable *wlan_id*

Syntax Description

wlan_id	Wireless LAN identifier between 1 and 512.

Command Default None.

Examples This example shows how to configure the WPA on WLAN ID 1:

```
> config wlan security wpa enable 1
```

Related Commands **show wlan**

config wlan security wpa ciphers

To configure the Wi-Fi protected authentication (WPA1) or Wi-Fi protected authentication (WPA2), use the **config wlan security wpa ciphers** command.

config wlan security wpa {**wpa1** | **wpa2**} **ciphers** {**aes** | **tkip**} {**enable** | **disable**} *wlan_id*

Syntax Description

wpa1	Configures WPA1 support.
wpa2	Configures WPA2 support.
ciphers	Configures WPA ciphers.
aes	Configures AES encryption support.
tkip	Configures TKIP encryption support.
enable	Enables WPA AES/TKIP mode.
disable	Disables WPA AES/TKIP mode.
wlan_id	Wireless LAN identifier between 1 and 512.

Command Default

None.

Usage Guidelines

If you are not specifying the WPA versions, it implies the following:

- If the cipher enabled is AES, you are configuring WPA2/AES.
- If the ciphers enabled is AES+TKIP, you are configuring WPA/TKIP, WPA2/AES,or WPA/TKIP.
- If the cipher enabled is TKIP, you are configuring WPA/TKIP or WPA2/TKIP.

Examples

This example shows how to encrypt the WPA:

```
> config wlan security wpa wpa1 ciphers aes enable 1
```

Related Commands

show wlan

config wlan security wpa gtk-random

To enable the randomization of group temporal keys (GTK) between access points and clients on a WLAN, use the **config wlan security wpa gtk-random** command.

config wlan security wpa gtk-random {**enable** | **disable**} *wlan_id*

Syntax Description

enable	Enables the randomization of GTK keys between the access point and clients.
disable	Disables the randomization of GTK keys between the access point and clients.
wlan_id	WLAN identifier between 1 and 512.

Command Default

None.

Usage Guidelines

When you enable this command, the clients in the Basic Service Set (BSS) get a unique GTK key. The clients do not receive multicast or broadcast traffic.

Examples

This example shows how to enable the GTK randomization for each client associated on a WLAN:

```
> config wlan security wpa gtk-random enable 3
```

Related Commands

show wlan

debug hotspot events

debug hotspot packets

config wlan apgroup hotspot venue

config wlan apgroup hotspot operating-class

config ap hotspot venue

config advanced hotspot

config wlan hotspot dot11u

config wlan hotspot clear-all

config wlan hotspot msap

config wlan security wpa wpa1 disable

To disable WPA1, use the **config wlan security wpa wpa1 disable** command.

config wlan security wpa wpa1 disable *wlan_id*

Syntax Description

wlan_id	Wireless LAN identifier between 1 and 512.

Command Default None.

Examples This example shows how to disable WPA1:

```
> config wlan security wpa wpa1 disable 1
```

Related Commands **show wlan**

config wlan security wpa wpa1 enable

To enable WPA1, use the **config wlan security wpa wpa1 enable** command.

config wlan security wpa wpa1 enable *wlan_id*

Syntax Description

wlan_id	Wireless LAN identifier between 1 and 512.

Command Default None.

Examples This example shows how to enable WPA1:

```
> config wlan security wpa wpa1 enable 1
```

Related Commands **show wlan**

config wlan security wpa wpa2 disable

To disable WPA2, use the **config wlan security wpa wpa2 disable** command.

config wlan security wpa wpa2 disable *wlan_id*

Syntax Description

wlan_id	Wireless LAN identifier between 1 and 512.

Command Default None.

Examples This example shows how to disable WPA2:

```
> config wlan security wpa wpa2 disable 1
```

Related Commands **show wlan**

config wlan security wpa wpa2 enable

To enable WPA2, use the **config wlan security wpa wpa2 enable** command.

config wlan security wpa wpa2 enable *wlan_id*

Syntax Description

wlan_id	Wireless LAN identifier between 1 and 512.

Command Default None.

Examples This example shows how to enable WPA2:

```
> config wlan security wpa wpa2 enable 1
```

Related Commands **show wlan**

config wlan security wpa wpa2 cache

To configure caching methods on a WLAN, use the **config wlan security wpa wpa2 cache** command.

config wlan security wpa wpa2 cache sticky {**enable** | **disable**} *wlan_id*

Syntax Description

sticky	Configures Sticky Key Caching (SKC) roaming support on the WLAN.
enable	Enables SKC roaming support on the WLAN.
disable	Disables SKC roaming support on the WLAN.
wlan_id	Wireless LAN identifier between 1 and 512.

Command Default

None.

Usage Guidelines

In SKC (Sticky Key caching) also known as PKC (Pro Active Key caching), the client stores each Pairwise Master Key (PMK) ID (PMKID) against a Pairwise Master Key Security Association (PMKSA). When a client finds an AP for which it has a PMKSA, it sends the PMKID in the association request to the AP. If the PMKSA is alive in the AP, the AP provides support for fast roaming. In SKC, full authentication is done on each new AP to which the client associates and the client must keep the PMKSA associated with all APs.

Examples

This example shows how to enable SKC roaming support on a WLAN:

```
> config wlan security wpa wpa2 cache sticky enable 1
```

Related Commands

config wlan security wpa wpa2 enable

config wlan security wpa wpa2 disable

config wlan security wpa wpa2 ciphers

show wlan

config wlan security wpa wpa2 cache sticky

To configure Sticky PMKID Caching (SKC) on a WLAN, use the **config wlan security wpa wpa2 cache sticky** command.

config wlan security wpa wpa2 cache sticky {**enable** |**disable**} *wlan_id*

Syntax Description

enable	Enables SKC on a WLAN.
disable	Disables SKC on a WLAN.
wlan_id	Wireless LAN identifier between 1 and 512 (inclusive).

Command Default

Disabled.

Usage Guidelines

Beginning in Release 7.2 and later releases, the controller supports Sticky PMKID Caching (SKC). With sticky PMKID caching, the client receives and stores a different PMKID for every AP it associates with. The APs also maintain a database of the PMKID issued to the client. In SKC also known as PKC (Pro Active Key caching), the client stores each Pairwise Master Key (PMK) ID (PMKID) against a Pairwise Master Key Security Association (PMKSA). When a client finds an AP for which it has the PMKSA, it sends the PMKID in the association request to the AP. If the PMKSA is alive in the AP, the AP provides support for fast roaming. In SKC, full authentication is done on each new AP to which the client associates and the client must keep the PMKSA associated with all APs. For SKC, PMKSA is a per AP cache that the client stores and PMKSA is precalculated based on the BSSID of the new AP.

- You cannot use SKC for large scale deployments as the controller supports SKC only up to eight APs.
- SKC does not work across controllers in a mobility group.
- SKC works only on WPA2-enabled WLANs.
- SKC works only on local mode APs.

Examples

This example shows how to enable Sticky PMKID Caching on WLAN 5:

```
> config wlan security wpa wpa2 cache sticky enable 5
```

Related Commands

config wlan security wpa wpa2 enable

config wlan security wpa wpa2 disable

config wlan security wpa wpa2 ciphers

show wlan

config wlan security wpa wpa2 ciphers

To configure WPA2 ciphers and enable or disable Advanced Encryption Standard (AES) or Temporal Key Integrity Protocol (TKIP) data encryption for WPA2, use the **config wlan security wpa wpa2 ciphers** command

config wlan security wpa wpa2 ciphers {**aes** | **tkip**} {**enable** | **disable**} *wlan_id*

Syntax Description

aes	Configures AES data encryption for WPA2.
tkip	Configures TKIP data encryption for WPA2.
enable	Enables AES or TKIP data encryption for WPA2.
disable	Disables AES or TKIP data encryption for WPA2.
wlan_id	Wireless LAN identifier between 1 and 512.

Command Default

AES.

Examples

This example shows how to enable AES data encryption for WPA2:

```
> config wlan security wpa wpa2 ciphers aes enable 1
```

Related Commands

config wlan security wpa wpa2 enable

config wlan security wpa wpa2 disable

config wlan security wpa wpa2 cache

show wlan

Configure WPS Commands

Use the **config wps** commands to configure Wireless Protection System (WPS) settings.

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

enable	(Optional) Enables WMM on the wireless LAN.
disable	(Optional) Disables WMM on the wireless LAN.
threshold	(Optional) Specifies that WMM-enabled clients are on the wireless LAN.
threshold_value	Threshold value (1 to 255).

Command Default None.

Examples

```
> 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**}

Syntax Description

enable	Enables the auto-immune feature.
disable	Disables the auto-immune feature.

Command Default

Disabled.

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.

Examples

This example shows how to configure the auto-immune mode:

```
> config wps auto-immune enable
```

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

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

Command Default

Command defaults are listed below as follows:

Port	443
Query interval	60
Certification fingerprint	00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
Query state	Disabled

Examples

This 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:

```
> 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

802.11-assoc	Specifies that the controller excludes clients on the sixth 802.11 association attempt, after five consecutive failures.
802.11-auth	Specifies that the controller excludes clients on the sixth 802.11 authentication attempt, after five consecutive failures.
802.1x-auth	Specifies that the controller excludes clients on the sixth 802.11X authentication attempt, after five consecutive failures.
ip-theft	Specifies that the control excludes clients if the IP address is already assigned to another device.
web-auth	Specifies that the controller excludes clients on the fourth web authentication attempt, after three consecutive failures.
all	Specifies that the controller excludes clients for all of the above reasons.
enable	Enables client exclusion policies.
disable	Disables client exclusion policies.

Command Default

All policies are enabled.

Examples

This example shows how to disable clients on the 802.11 association attempt after five consecutive failures:

```
> 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 {**enable** | **disable**}

Syntax Description

infrastructure	Configures the MFP infrastructure.
enable	Enables the MFP feature.
disable	Disables the MFP feature.

Command Default

None.

Examples

This example shows how to enable the infrastructure MFP:

```
> 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.

Examples This example shows how to configure the controller to synchronize with other controllers for the shun list:

```
> 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

standard	Configures a standard IDS signature.
custom	Configures a standard IDS signature.
state	Specifies the state of the IDS signature.
signature_id	Identifier for the signature to be enabled or disabled.
enable	Enables the IDS signature processing or a specific IDS signature.
disable	Disables IDS signature processing or a specific IDS signature.

Command Default

IDS signature processing is enabled by default.

Usage Guidelines

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

Examples

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

```
> config wps signature enable
```

This example shows how to disable a standard individual IDS signature:

```
> config wps signature standard state 15 disable
```

Related Commands

config wps signature frequency

config wps signature interval

config wps signature mac-frequency

config wps signature quiet-time

config wps signature reset

show wps signature events

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*

Syntax Description

signature_id	Identifier for the signature to be configured.
frequency	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.

Usage Guidelines

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

Examples

This 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:

```
> 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

signature_id	Identifier for the signature to be configured.
interval	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.

Usage Guidelines

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

Examples

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

```
> config wps signature interval 1 200
```

Related Commands

config wps signature frequency

config wps signature

config wps signature mac-frequency

config wps signature quiet-time

config wps signature reset

show wps signature events

show wps signature summary

show wps summary

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

signature_id	Identifier for the signature to be configured.
mac_frequency	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.

Usage Guidelines

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

Examples

This 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:

```
> 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

signature_id	Identifier for the signature to be configured.
quiet_time	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.

Usage Guidelines

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

Examples

This 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:

```
> config wps signature quiet-time 1 60
```

Related Commands

config wps signature

config wps signature frequency

config wps signature interval

config wps signature mac-frequency

config wps signature reset

show wps signature events

show wps signature summary

show wps summary

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**}

Syntax Description

signature_id	Identifier for the specific IDS signature to be reset.
all	Resets all IDS signatures.

Command Default

None.

Usage Guidelines

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

Examples

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

```
> 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

Clear Commands

This section lists the **clear** commands to clear existing security configurations of the controller.

clear acl counters

To clear the current counters for an access control list (ACL), use the **clear acl counters** command.

clear acl counters *acl_name*

Syntax Description

acl_name	ACL name.

Command Default None.

Usage Guidelines

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

Examples This example shows how to clear the current counters for acl1:

```
> clear acl counters acl1
```

Related Commands

config acl counter

show acl

clear radius acct statistics

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

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

Syntax Description

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

Command Default

None.

Examples

This example shows how to clear the RADIUS accounting statistics:

```
> clear radius acc statistics
```

Related Commands

show radius acct statistics

clear tacacs auth statistics

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

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

Syntax Description

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

Command Default

None.

Examples

This example shows how to clear the RADIUS authentication server statistics:

```
> 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.

Examples

This example shows how to clear the local EAP statistics:

```
> 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

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

Command Default

None.

Examples

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

> **clear stats radius auth all**

Related Commands

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

clear stats tacacs

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

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

Syntax Description

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

Command Default

None.

Examples

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

```
> clear stats tacacs acct 1
```

Related Commands

show tacacs summary

Debug Commands

This section lists the **debug** commands to manage debugging of security settings of the controller.

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

debug 11w-pmf

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

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

Syntax Description

all	Configures debug of all 802.11w messages.
keys	Configures debug of 802.11w keys.
events	Configures debug of 802.11w events.
enable	Enables the 802.1w debug.
disable	Disables the 802.1w debug.

Command Default

None.

Examples

This example shows how to enable debug of 802.11w key generation:

```
> debug 11w-pmf keys enable
```

Related Commands

show wlan

show client detail

config wlan security pmf

debug aaa

To configure AAA debug options, use the **debug aaa** command.

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

Syntax Description

all	(Optional) Specifies debugging of all AAA messages.
detail	(Optional) Specifies debugging of AAA errors.
events	(Optional) Specifies debugging of AAA events.
packet	(Optional) Specifies debugging of AAA packets.
ldap	(Optional) Specifies debugging of the AAA Lightweight Directory Access Protocol (LDAP) events.
local-auth	(Optional) Specifies debugging of the AAA local Extensible Authentication Protocol (EAP) events.
tacacs	(Optional) Specifies debugging of the AAA TACACS+ events.
enable	(Optional) Starts the debugging feature.
disable	(Optional) Stops the debugging feature.

Command Default

None.

Examples

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

```
> debug aaa ldap enable
```

Related Commands

debug aaa local-auth eap

show running-config

debug aaa local-auth

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

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

Syntax Description

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

Command Default

None.

Examples

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

```
> 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 debugging of broadcast options, use the **debug bcast** command.

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

Syntax Description

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

Command Default

None.

Examples

This example shows how to enable broadcast debug settings:

```
> debug bcast message enable
```

This example shows how to disable broadcast debug settings:

```
> debug bcast message disable
```

Related Commands

debug disable-all

show sysinfo

debug nac

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

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

Syntax Description

events	Configures debugging of NAC events.
packet	Configures debugging of NAC packets.
enable	Enables NAC debugging.
disable	Disables NAC debugging.

Command Default

None.

Examples

This example shows how to enable NAC debug settings:

```
> debug nac events enable
```

Related Commands

show nac statistics
show nac summary
config guest-lan nac
config wlan nac

debug pm

To configure 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

all disable	Disables all debugging in the policy manager module.
config	Configures debugging of the policy manager configuration.
hwcrypto	Configures debugging of hardware offload events.
ikemsg	Configures debugging of Internet Key Exchange (IKE) messages.
init	Configures debugging of policy manager initialization events.
list	Configures debugging of policy manager list mgmt.
message	Configures debugging of policy manager message queue events.
pki	Configures debugging of Public Key Infrastructure (PKI) related events.
rng	Configures debugging of random number generation.
rules	Configures debugging of Layer 3 policy events.
sa-export	Configures debugging of SA export (mobility).
sa-import	Configures debugging of SA import (mobility).
ssh-l2tp	Configures debugging of policy manager l2TP handling.
ssh-appgw	Configures debugging of application gateways.
ssh-engine	Configures debugging of the policy manager engine.
ssh-int	Configures debugging of the policy manager intercepter.
ssh-pmgr	Configures debugging of the policy manager.
ssh-ppp	Configures debugging of policy manager PPP handling.
ssh-tcp	Configures debugging of policy manager TCP handling.
enable	Enables the debugging.
disable	Disables the debugging.

Command Default None.

Examples This example shows how to configure debugging of PKI-related events:

```
> debug pm pki enable
```

Related Commands **debug disable-all**

debug web-auth

To configure debugs for web authenticated clients, use the **debug web-auth** command.

debug web-auth {**redirect**{ **enable mac** *mac_address* | **disable**} | **webportal-server** {**enable** | **disable**}}

Syntax Description

redirect	Configures debug of web authenticated and redirected clients.
enable	Enables debug of web authenticated clients.
mac	Configures the MAC address of the web authenticated client.
mac_address	MAC address of the web authenticated client.
disable	Disables debug of web authentication of clients.
webportal-server	Configures debug of portal authentication of clients.

Command Default

None.

Examples

This example shows how to enable debugging of a web authenticated and redirected client:

```
> debug web-auth redirect enable mac xx:xx:xx:xx:xx:xx
```

debug wps sig

To troubleshoot Wireless Provisioning Service (WPS) signature settings, use the **debug wps sig** command.

debug wps sig {**enable** | **disable**}

Syntax Description

enable	Enables debugging for WPS settings.
disable	Disables debugging for WPS settings.

Command Default None.

Examples This example shows how to enable WPS signature settings:

> **debug wps sig enable**

Related Commands

debug wps mfp

debug disable-all

debug wps mfp

To debug WPS Management Frame Protection (MFP) settings, use the **debug wps mfp** command.

debug wps mfp {**client** | **capwap** | **detail** | **report** | **mm**} {**enable** | **disable**}

Syntax Description

client	Configures debugging for client MFP messages.
capwap	Configures debugging for MFP messages between the controller and access points.
detail	Configures detailed debugging for MFP messages.
report	Configures debugging for MFP reporting.
mm	Configures debugging for MFP mobility (inter-controller) messages.
enable	Enables debugging for WPS MFP settings.
disable	Disables debugging for WPS MFP settings.

Command Default

None.

Examples

This example shows how to enable debugging of WPS MFP settings:

```
> debug wps mfp detail enable
```

Related Commands

debug disable-all

debug wps sig