

AOS-CX 10.14 Security Guide

8100, 8360 Switch Series



a Hewlett Packard
Enterprise company

Copyright Information

© Copyright 2024 Hewlett Packard Enterprise Development LP.

This product includes code licensed under certain open source licenses which require source compliance. The corresponding source for these components is available upon request. This offer is valid to anyone in receipt of this information and shall expire three years following the date of the final distribution of this product version by Hewlett Packard Enterprise Company. To obtain such source code, please check if the code is available in the HPE Software Center at <https://myenterpriselicense.hpe.com/cwp-ui/software> but, if not, send a written request for specific software version and product for which you want the open source code. Along with the request, please send a check or money order in the amount of US \$10.00 to:

Hewlett Packard Enterprise Company
Attn: General Counsel
WW Corporate Headquarters
1701 E Mossy Oaks Rd Spring, TX 77389
United States of America.

Notices

The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

Confidential computer software. Valid license from Hewlett Packard Enterprise required for possession, use, or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Links to third-party websites take you outside the Hewlett Packard Enterprise website. Hewlett Packard Enterprise has no control over and is not responsible for information outside the Hewlett Packard Enterprise website.

Contents	3
About this document	15
Applicable products	15
Latest version available online	15
Command syntax notation conventions	15
About the examples	16
Identifying switch ports and interfaces	16
About security	18
About Authentication, Authorization, and Accounting (AAA)	18
Managing users and groups	19
Default user admin	19
Example of first login with password setting	19
Built-in user groups and their privileges	19
User-defined user groups	20
User name requirements	20
Password requirements	21
Per-user management interface enablement	21
Local per-user management interface enablement	21
Remote (TACACS+ or RADIUS) per-user management interface enablement	22
User and user group management tasks	23
Resetting the switch admin password using the Service OS console	24
Resetting the admin password by reverting the switch to factory defaults	25
User and group commands	26
password complexity	26
service export-password	30
show password-complexity	31
show user-group	31
show user-list	32
show user-list management-interface	34
show user information	35
user	36
user-group	39
user management-interface	43
user password	44
SSH server	47
SSH defaults	47
SSH server tasks	47
SSH server commands	48
show ssh host-key	48
show ssh server	49
show ssh server sessions	53
ssh ciphers	54

ssh host-key	55
ssh host-key-algorithms	56
ssh key-exchange-algorithms	57
ssh known-host remove	59
ssh macs	59
ssh maximum-auth-attempts	60
ssh public-key-algorithms	61
ssh server allow-list	62
ssh server port	64
ssh server vrf	65
SSH client	66
SSH client commands	66
ssh (client login)	66
Local AAA	68
Local AAA defaults and limits	68
Supported platforms and standards	68
Scale	68
Local authentication	69
Password-based local authentication	69
SSH public key-based local authentication	69
Local authentication tasks	69
Local authorization	71
Local authorization tasks	71
Local accounting	72
Local accounting tasks	72
Local AAA commands	73
aaa accounting all-mgmt	73
aaa authentication console-login-attempts	74
aaa authentication limit-login-attempts	76
aaa authentication login	77
aaa authentication minimum-password-length	78
aaa authorization commands (local)	79
show aaa accounting	81
show aaa authentication	82
show aaa authorization	83
show authentication locked-out-users	85
show ssh authentication-method	85
show user	86
ssh password-authentication	87
ssh public-key-authentication	88
user authorized-key	88
Remote AAA with TACACS+	91
Parameters for TACACS+ server	91
Default server groups	92
Supported platforms and standards	92
About global versus per-TACACS+ server passkeys (shared secrets)	93
Remote AAA TACACS+ server configuration requirements	93
User role assignment using TACACS+ attributes	94
TACACS+ server redundancy and access sequence	94
Single source IP address for consistent source identification to AAA servers	94
TACACS+ general tasks	95
TACACS+ authentication	95

About authentication fail-through	96
TACACS+ authentication tasks	96
TACACS+ authorization	97
Using local authorization as fallback from TACACS+ authorization	97
About authentication fail-through and authorization	97
TACACS+ authorization tasks	97
TACACS+ accounting	98
Sample accounting information on a TACACS+ server	98
Sample REST accounting information on a TACACS+ server	100
TACACS+ accounting tasks	100
Example: Configuring the switch for Remote AAA with TACACS+	101

Remote AAA with RADIUS 105

Parameters for RADIUS server	105
Default server groups	106
Supported platforms and standards	107
About global versus per-RADIUS server passkeys (shared secrets)	107
Remote AAA RADIUS server configuration requirements	108
User role assignment using RADIUS attributes	108
RADIUS server redundancy and access sequence	109
Configuration task list	109
Single source IP address for consistent source identification to AAA servers	110
RADIUS general tasks	111
Per-port RADIUS server group configuration	112
RADIUS authentication	112
About authentication fail-through	112
RADIUS authentication tasks	113
Two-factor authentication	114
Configuring two-factor authentication (for local users)	114
Configuring two-factor authentication with SSH (for remote-only users)	115
Configuring two-factor authentication with HTTPS server and REST (for remote-only users)	118
Two-factor authentication commands	121
aaa authorization radius	121
https-server authentication certificate	122
ssh certificate-as-authorized-key	123
ssh two-factor-authentication	124
RADIUS accounting	125
Sample general accounting information	126
RADIUS accounting tasks	127
Example: Configuring the switch for Remote AAA with RADIUS	128

Remote AAA (TACACS+, RADIUS) commands 132

aaa accounting allow-fail-through	132
aaa accounting all-mgmt	132
aaa authentication allow-fail-through	135
aaa authentication login	136
aaa authorization allow-fail-through	138
aaa authorization commands	140
aaa group server	143
radius-server auth-type	144
radius-server host	145
radius-server host secure ipsec	148
radius-server host tls port-access	153
radius-server host tls tracking-method	154
radius-server key	155

radius-server retries	156
radius-server status-server interval	157
radius-server timeout	158
radius-server tracking	159
server	161
show aaa accounting	162
show aaa authentication	164
show aaa authorization	167
show aaa server-groups	169
show accounting log	171
show radius-server	174
show radius-server secure ipsec	179
show radius-server authentication statistics	180
show radius-server authentication statistics host	181
show tacacs-server	182
show tacacs-server statistics	185
show tech aaa	186
tacacs-server auth-type	192
tacacs-server host	192
tacacs-server key	195
tacacs-server timeout	196
tacacs-server tracking	196
RADIUS dynamic authorization	199
Requirements and tips	199
RADIUS dynamic authorization commands	199
radius dyn-authorization enable	199
radius dyn-authorization client	200
radius dyn-authorization client tls (RadSec)	202
radius dyn-authorization port	204
show radius dyn-authorization	204
show radius dyn-authorization client	206
IP Flow Information Export	208
Traffic Insight	209
Protocol and feature details	209
Supported Platforms	209
Caveats for Traffic Insight	209
Configuring Traffic Insight	210
Traffic Insight Configuration	210
Traffic insight commands	211
diag-dump traffic-insight basic	211
show capacities traffic-insight	212
show debug buffer module trafficinsight	212
show events traffic-insightd	213
show running-config traffic-insight	214
show tech traffic-insight	215
show traffic-insight monitor-type	215
traffic insight	216
Client Insight	219
Supported Platforms	220
Prerequisites	220
Points to Note	220
Limitations	220

Feature Interoperability	221
Troubleshooting Client Insight	221
Client Insight Commands	221
client-insight enable	221
client-insight on-boarding event logs	222
diag-dump client-insight basic	223
show capacities client-insight-client-limit	225
show capacities-status client-insight-client-limit	226
show events -c client-insight	226
show tech client-insight	229

PKI 234

PKI concepts	234
Digital certificate	234
Certificate authority	234
Root certificate	235
Leaf certificate	235
Intermediate certificate	235
Trust anchor	235
OCSP	235
PKI on the switch	235
Trust anchor profiles	235
Leaf certificates	236
Mandatory matching of peer device hostname	236
PKI EST	236
EST usage overview	236
Prerequisites for using EST for certificate enrollment	237
EST profile configuration	237
Certificate enrollment	237
Certificate re-enrollment	238
Checking EST profile and certificate configuration	238
EST best practices	238
Example using EST for certificate enrollment	239
Example including the use of an intermediate certificate	246
Installing a self-signed leaf certificate (created inside the switch)	248
Installing a self-signed leaf certificate (created outside the switch)	249
Installing a certificate of a root CA	250
Installing a downloadable user role certificate	251
Installing a CA-signed leaf certificate (initiated in the switch)	253
Installing a CA-signed leaf certificate (created outside the switch)	254
PKI commands	255
crypto pki application	256
crypto pki certificate	257
crypto pki ta-profile	258
enroll self-signed	259
enroll terminal	259
import (CA-signed leaf certificate)	260
import (self-signed leaf certificate)	262
key-type	264
ocsp disable-nonce	265
ocsp enforcement-level	266
ocsp url	267
ocsp vrf	268
revocation-check ocsp	269
show crypto pki application	269
show crypto pki certificate	270

show crypto pki ta-profile	272
ta-certificate	274
subject	275
PKI EST commands	276
arbitrary-label	277
arbitrary-label-enrollment	278
arbitrary-label-reenrollment	279
crypto pki est-profile	280
enroll est-profile	281
reenrollment-lead-time	282
retry-count	283
retry-interval	283
show crypto pki est-profile	284
url	285
username	286
vrf	288

MACsec **290**

MACsec in AOS-CX	290
MACsec use cases	291
MACsec configuration (using 802.1X EAP TLS)	293
Configure the authenticator	293
Configure the supplicant	294
MACsec configuration (using pre-shared keys)	295
MACsec limitations	296
MACsec WAN extension	297
WAN MACsec on a LAG interface	297
Replay protection with WAN MACsec	297
MACsec WAN extension configuration	297
MACsec WAN extension use cases	298
Debugging and troubleshooting	301
MACsec best practices	303
Switch-to-Host MACsec Limitations	303
MACsec troubleshooting	304
MACsec commands	304
apply macsec policy	304
bypass	306
cipher-suite	307
clear macsec statistics	308
clear tag mode	309
confidentiality	310
include-sci-tag	311
macsec policy	312
macsec selftest	313
replay-protection	314
secure-mode	315
show macsec policy	316
show macsec selftest	317
show macsec statistics	318
show macsec status	321
MKA commands (MACsec)	323
apply mka policy	323
clear mka statistics	324
data-delay-protection	325
eapol-destination-mac	326
eapol-dot1q-tagged	327

eapol-eth-type	328
key-server-priority	329
mka policy	330
pre-shared-key	331
show mka policy	332
show mka statistics	333
show mka status	334
transmit-interval	335
Port access	337
Port access 802.1X authentication	337
Port access MAC authentication	338
How MAC authentication works	339
How RADIUS server is used in MAC authentication	339
Supported platforms and standards	340
Scale	340
Supported RFCs and standards	340
Port access configuration task list	340
Port access 802.1X and MAC authentication configuration example	340
Use cases	342
Use case 1: Faster onboarding of MAC authentication clients using concurrent onboarding	342
Use case 2: PXE clients that download the supplicant	343
Port access 802.1X authentication commands	343
aaa authentication port-access dot1x authenticator	343
aaa authentication port-access dot1x authenticator auth-method	344
aaa authentication port-access dot1x authenticator cached-reauth	345
aaa authentication port-access dot1x authenticator cached-reauth-period	345
aaa authentication port-access dot1x authenticator discovery-period	346
aaa authentication port-access dot1x authenticator eap-tls-fragment	347
aaa authentication port-access dot1x authenticator eapol-timeout	348
aaa authentication port-access dot1x authenticator initial-auth-response-timeout	349
aaa authentication port-access dot1x authenticator macsec	350
aaa authentication port-access dot1x authenticator max-eapol-requests	351
aaa authentication port-access dot1x authenticator mka cak-length	351
aaa authentication port-access dot1x authenticator max-retries	352
aaa authentication port-access dot1x authenticator quiet-period	353
aaa authentication port-access dot1x authenticator radius server-group	354
aaa authentication port-access dot1x authenticator reauth	355
aaa authentication port-access dot1x authenticator reauth-period	356
clear dot1x authenticator statistics interface	357
show aaa authentication port-access dot1x authenticator interface client-status	357
show aaa authentication port-access dot1x authenticator interface port-statistics	359
Port access MAC authentication commands	360
aaa authentication port-access allow-lldp-auth [mac {source-mac chassis-mac}]	361
aaa authentication port-access mac-auth	362
aaa authentication port-access mac-auth addr-format	363
aaa authentication port-access mac-auth auth-method	363
aaa authentication port-access mac-auth cached-reauth	364
aaa authentication port-access mac-auth cached-reauth-period	365
aaa authentication port-access mac-auth password	366
aaa authentication port-access mac-auth quiet-period	367
aaa authentication port-access mac-auth radius server-group	367
aaa authentication port-access mac-auth reauth	369
aaa authentication port-access mac-auth reauth-period	369
clear mac-auth statistics	370

show aaa authentication port-access mac-auth interface client-status	371
show aaa authentication port-access mac-auth interface port-statistics	373
Port access general commands	374
aaa authentication port-access allow-ldp-auth	374
aaa authentication port-access allow-cdp-auth	376
aaa authentication port-access auth-mode	376
aaa authentication port-access auth-precedence	378
aaa authentication port-access auth-priority	379
aaa authentication port-access auth-role	380
aaa authentication port-access client-auto-log-off final-authentication-failure	381
aaa authentication port-access client-limit	382
aaa authentication port-access client-limit multi-domain	382
aaa authentication port-access radius-override	383
port-access allow-flood-traffic	384
port-access auto-vlan	385
port-access client-move	386
port-access event-log client	387
port-access fallback-role	388
port-access log-off client	389
port-access onboarding-method precedence	390
port-access onboarding-method concurrent	391
port-access reauthenticate interface	392
show aaa authentication port-access interface client-status	393
show port-access clients	394
show port-access clients detail	400
show port-access clients onboarding-method	408
show port-access interface	409
Port access debugging and troubleshooting	411
Radius server reachability debugging and troubleshooting	411
Port access MAC authentication debugging and troubleshooting	412
Using show commands	412
Using debug commands	413
Port access 802.1X authentication debugging and troubleshooting	414
Using show commands	414
Using other commands	417
Port access FAQ	417
References	418
Multidomain authentication	418
Multidomain authentication requirements	418
Scenarios with Aruba-Port-Auth-Mode and Aruba-Device-Traffic-Class VSAs	419
Scenarios with device-traffic-class configuration in role	419
Port access security violation	420
Port access security violation commands	420
port-access security violation action	420
port-access security violation action shutdown auto-recovery	421
port-access security violation action shutdown recovery-timer	422
show interface	423
show port-access aaa violation interface	424
show port-access port-security violation client-limit-exceeded interface	425
Port access policy	426
Classes and actions supported by port access policies	426
RADIUS policies	427
Filter-ID	427
NAS-Filter-Rule	427
Aruba-NAS-Filter-Rule	428
Limitations	429

Port access policy commands	429
port-access policy	429
port-access policy copy	433
port-access policy resequence	434
port-access policy reset	435
clear port-access policy hitcounts	437
show port-access policy	439
show port-access policy hitcounts	441
Port access role	442
Operational notes	443
Downloadable user roles	444
Mixed roles	444
Important points to note	444
Limitations	445
Supported RADIUS attributes in mixed roles	445
Cached-critical role	445
Cached-critical role tasks	446
Restrictions	448
Troubleshooting	448
Special roles	449
Critical role	449
Reject role	449
Pre-authentication role	449
Auth-role	450
Fallback role	450
Port access role commands	451
associate macsec-policy	451
associate policy	452
auth-mode	453
cached-reauth-period	454
client-inactivity timeout	455
device-traffic-class	455
description	456
mtu	457
poe-priority	457
port-access role	458
reauth-period	459
session timeout	460
show aaa authentication port-access interface client-status	460
show port-access role	461
stp-admin-edge-port	464
trust-mode	464
vlan	465
Port access cached-critical role commands	467
aaa authentication port-access cached-critical-role (global)	467
aaa authentication port-access cached-critical-role (per interface)	469
port-access clear cached-client	470
show port-access cached-clients	471
show port-access cached-critical-role info	473
Port access VLAN groups	474
VLAN grouping limitations	474
VLAN group load balancing	475
Port access VLAN group commands	476
associate-vlan	476
port-access vlan-group	477
show running-config port-access vlan-group	477

Port access 802.1X supplicant authentication	479
Feature details	479
Sub-features	480
Supported platforms	481
802.1X supplicant policy configuration and considerations	481
Recommended configuration	482
Port access 802.1X supplicant commands	482
aaa authentication port-access dot1x supplicant(global)	482
aaa authentication port-access dot1x supplicant(port)	483
associate policy	484
canned-eap-success	485
clear dot1x supplicant statistics	486
discovery-timeout	487
eap-identity	488
eapol-force-multicast	490
eapol-method	491
eapol-protocol-version	492
eapol-source-mac	493
eapol-timeout	494
enable	495
enable	496
fail-mode	497
held-period	498
macsec	499
macsec-policy	500
max-retries	501
mka cak-length	502
policy (supplicant)	503
port-access dot1x supplicant restart	504
show aaa authentication port-access dot1x supplicant policy	505
show aaa authentication port-access dot1x supplicant statistics	507
show aaa authentication port-access dot1x supplicant status	509
start-mode	511
Troubleshooting	512
Prerequisites	512
Packet capture	513
FAQ	514
Configurable RADIUS attributes (port access)	515
Configurable RADIUS attribute commands	515
aaa radius-attribute group	515
nas-id request-type	516
nas-id value	517
nas-ip-addr request-type authentication	518
nas-ip-addr service-type user-management	519
tunnel-private-group-id request-type	520
tunnel-private-group-id value	521
Supported RADIUS attributes	523
Attributes supported in 802.1X authentication	523
Attributes supported in MAC authentication	523
Attributes supported in dynamic authorization	524
Session authorization attributes supported in 802.1X and MAC authentication, and CoA	524
Standard session attributes supported	525
Vendor-Specific Attributes supported in session authorization	525
Description of VSAs	525

Attributes supported in RADIUS network accounting	527
Attributes supported in RADIUS server tracking	527
Port security	528
Port-security sticky MAC	528
Basic operation	528
Default port security operation	529
Intruder protection	529
General operation for port security	529
Blocking unauthorized traffic	529
Trunk group exclusion	530
Port security commands	530
port-access port-security	530
port-access port-security client-limit	531
port-access port-security mac-address	532
show port-access port-security interface client-status	533
show port-access port-security interface port-statistics	534
sticky-learn enable	535
sticky-learn mac	536
show port-access security violation sticky-mac-client-move interface	537
Fault Monitor	539
Fault monitoring conditions	539
Excessive broadcasts	539
Excessive multicasts	539
Excessive link flaps	539
Excessive oversize packets	539
Excessive jabbers	539
Excessive fragments	539
Excessive CRC errors	540
Excessive TX drops	540
Fault monitor commands	540
(Fault enabling/disabling)	540
action	541
apply fault-monitor profile	544
fault-monitor profile	544
show fault-monitor profile	545
show interface fault-monitor profile	547
show interface fault-monitor status	548
show running-config	549
threshold	550
vsx-sync (fault monitor)	552
Group based policy (GBP)	553
Limitations and considerations	553
GBP scenarios	554
Group Policy ID-based segmentation in the wired network	554
Group Policy ID-based segmentation between wired and wireless clients	556
Group Policy ID-based segmentation for multicast traffic	557
Multicast traffic limitations	558
GBP limitations	559
Group based policy commands	559
apply gbp role-access-list	559
gbp enable	559
gbp role	560
gbp role infra	562

gbp role-access-list	563
class gbp-ip	564
class gbp-ipv6	567
class gbp-mac	570
port-access gbp	572
port-access role associate gbp	574
clear port-access gbp hitcounts	575
show gbp role-mapping	575
show class	576
show port-access gbp	577
show port-access gbp hitcounts	578
Configuring enhanced security	580
Configuring enhanced security	580
Configuring remote logging using SSH reverse tunnel	581
CLI user session management commands	582
cli-session	582
Auditors and auditing tasks	585
Auditing tasks (CLI)	585
Auditing tasks (Web UI)	585
REST requests and accounting logs	586
Support and Other Resources	587
Accessing HPE Aruba Networking Support	587
Accessing Updates	588
Warranty Information	588
Regulatory Information	588
Documentation Feedback	588

This document describes features of the AOS-CX network operating system. It is intended for administrators responsible for installing, configuring, and managing Aruba switches on a network.

Applicable products

This document applies to the following products:

- HPE Aruba Networking 8100 Switch Series (R9W94A, R9W95A, R9W96A, R9W97A)
- HPE Aruba Networking 8360 Switch Series (JL700A, JL701A, JL702A, JL703A, JL706A, JL707A, JL708A, JL709A, JL710A, JL711A, JL700C, JL701C, JL702C, JL703C, JL706C, JL707C, JL708C, JL709C, JL710C, JL711C, JL704C, JL705C, JL719C, JL718C, JL717C, JL720C, JL722C, JL721C)

Latest version available online

Updates to this document can occur after initial publication. For the latest versions of product documentation, see the links provided in [Support and Other Resources](#).

Command syntax notation conventions

Convention	Usage
<code>example-text</code>	Identifies commands and their options and operands, code examples, filenames, pathnames, and output displayed in a command window. Items that appear like the example text in the previous column are to be entered exactly as shown and are required unless enclosed in brackets ([]).
example-text	In code and screen examples, indicates text entered by a user.
Any of the following: ■ <code><example-text></code> ■ <code><example-text></code> ■ <i>example-text</i> ■ <i>example-text</i>	Identifies a placeholder—such as a parameter or a variable—that you must substitute with an actual value in a command or in code: ■ For output formats where italic text cannot be displayed, variables are enclosed in angle brackets (<code>< ></code>). Substitute the text—including the enclosing angle brackets—with an actual value. ■ For output formats where italic text can be displayed, variables might or might not be enclosed in angle brackets. Substitute the text including the enclosing angle brackets, if any, with an actual value.
	Vertical bar. A logical OR that separates multiple items from which you can choose only one. Any spaces that are on either side of the vertical bar are included for readability and are not a required part of the command syntax.

Convention	Usage
{ }	Braces. Indicates that at least one of the enclosed items is required.
[]	Brackets. Indicates that the enclosed item or items are optional.
... or ...	Ellipsis: ■ In code and screen examples, a vertical or horizontal ellipsis indicates an omission of information. ■ In syntax using brackets and braces, an ellipsis indicates items that can be repeated. When an item followed by ellipses is enclosed in brackets, zero or more items can be specified.

About the examples

Examples in this document are representative and might not match your particular switch or environment.

The slot and port numbers in this document are for illustration only and might be unavailable on your switch.

Understanding the CLI prompts

When illustrating the prompts in the command line interface (CLI), this document uses the generic term **switch**, instead of the host name of the switch. For example:

```
switch>
```

The CLI prompt indicates the current command context. For example:

```
switch>
```

Indicates the operator command context.

```
switch#
```

Indicates the manager command context.

switch(CONTEXT-NAME)#

Indicates the configuration context for a feature. For example:

```
switch(config-if) #
```

Identifies the **interface** context.

Variable information in CLI prompts

In certain configuration contexts, the prompt may include variable information. For example, when in the VLAN configuration context, a VLAN number appears in the prompt:

```
switch(config-vlan-100) #
```

When referring to this context, this document uses the syntax:

```
switch(config-vlan-<VLAN-ID>) #
```

Where <VLAN-ID> is a variable representing the VLAN number.

Identifying switch ports and interfaces

Physical ports on the switch and their corresponding logical software interfaces are identified using the format:

```
member/slot/port
```

On the 83xx, 9300, and 10000 Switch Series

- *member*: Always 1. VSF is not supported on this switch.
- *slot*: Always 1. This is not a modular switch, so there are no slots.
- *port*: Physical number of a port on the switch.

For example, the logical interface **1/1/4** in software is associated with physical port 4 on the switch.



If using breakout cables, the port designation changes to x:y, where x is the physical port and y is the lane when split to 4 x 10G or 4 x 25G. For example, the logical interface 1/1/4:2 in software is associated with lane 2 on physical port 4 in slot 1 on member 1.

This AOS-CX Switch provides the following security features:

- Local user and group management.
- Authentication, Authorization, and Accounting (AAA), either local (password or SSH public key-based), or remote password-based TACACS+ or RADIUS.
- SSH server. SSH is a cryptographic protocol that encrypts all communication between devices.
- Ability to use enhanced security as described in [Configuring enhanced security](#).
- Making sensitive switch configuration information available for secure export/import between switches. For information, see `service export-password`.

About Authentication, Authorization, and Accounting (AAA)

- **Authentication:** identifies users, validates their credentials, and grants switch access.
- **Authorization:** controls authenticated users command execution and switch interaction privileges.
- **Accounting:** collects and manages user session activity logs for auditing and reporting purposes.

Local AAA on your Aruba switch provides:

- Authentication using local password or SSH public key.
- Authorization using role-based access control (RBAC), and optionally, using user-defined local user groups with command authorization rules defined per group.
- Accounting of user activity on the switch using accounting logs.

Remote AAA provides the following for your Aruba switch:

- Authentication using remote AAA servers with either TACACS+ or RADIUS.
- Authorization using remote AAA servers with TACACS+ fine-grained command authorization. Local RBAC or local rule-based authorization is also possible.
- Transmission of locally collected accounting information to remote TACACS+ and RADIUS servers.



TACACS+ (Terminal Access Controller Access-Control System Plus) and RADIUS (Remote Authentication Dial-In User Service) server software is readily available as either open source or from various vendors.



For switches that support multiple management modules such as the Aruba 8400, all AAA functionality discussed only applies to the active management module. See also *AAA on switches with multiple management modules* in the *High Availability Guide*.

Default user admin

A factory-default switch comes with a single user named **admin**.

The **admin** user:

- Has an empty password. Press **Enter** in response to the **admin** password prompt. At initial boot, you are prompted to define a password for the **admin** user. Although empty (blank) passwords are allowed, it is recommended that you use strong passwords for all production switches.
- Is a member of the **administrators** group.
- Cannot be removed from the switch.



The switch **admin** user is distinct from the Service OS **admin** user. The Service OS acts as the **bootloader** and recovery operating system. The Service OS has its own CLI.

Example of first login with password setting

```
switch login: admin
Password:

Please configure the 'admin' user account password.
Enter new password: *****
Confirm new password: *****
switch#
```

Built-in user groups and their privileges

The switch provides the following built-in user groups with corresponding roles. Each of these roles comes with a set of privileges.

Group/Role	Privileges
administrators	Administrators have full privileges, including: ▪ Full CLI access. ▪ Performing firmware upgrades. ▪ Viewing switch configuration information, including sensitive information such as passwords which are displayed as ciphertext. ▪ Performing switch configuration. ▪ Adding/removing user accounts. ▪ Configuring users accounts, including passwords. Once set, a password cannot be deleted or set to empty.

Group/Role	Privileges
	REST API: All methods (GET, PUT, POST, DELETE) and switch resources are available. The privilege level for administrators is 15.
operators	Operators have no switch configuration privileges. Operators are restricted to: - Basic display-only CLI access. - Viewing of nonsensitive switch configuration information. - REST API: Other than the \login and \logout resources, only the GET method is available. The privilege level for operators is 1.
auditors	Auditors are restricted to functions related to auditing only: - CLI: Access to commands in the auditor context (auditor>) only. - Web UI: Access to the System > Log page only. - REST API: POST method available for the \login and \logout resources. GET method available for the following resources only: - Audit log: /logs/audit - Event log: /logs/event The privilege level for auditors is 19.

User-defined user groups

The switch enables you to create up to 29 user-defined local user groups, for the purpose of configuring local authorization. Each of the 29 user-defined groups support up to 1024 CLI command authorization rules that define what CLI commands can be executed by members of the group.

The local user groups with their command execution rules are useful for the following:

- Providing authorization for use with RADIUS servers.
- Providing fallback authorization for use with TACACS+ servers.
- Providing authorization when neither RADIUS or TACACS+ servers are used.

User name requirements

Specifies the user name. Requirements:

- Must start with a lowercase letter.
- Can contain numbers and lowercase letters.
- Can include only these three special characters: hyphens (-), dots (.), and underscores (_).
- Can have a maximum of 32 characters.
- Cannot be empty.
- Cannot contain uppercase letters.
- Cannot be: `admin`, `root`, or `remote_user`.
- Cannot be Linux reserved names such as:
 - `daemon`, `bin`, `sys`, `sync`, `proxy`, `www-data`, `backup`, `list`, `irc`, `gnats`, `nobody`, `systemd-bus-proxy`, `sshd`, `messagebus`, `rpc`, `systemd-journal-gateway`, `systemd-journal-remote`, `systemd-journal-`

upload, systemd-timesync, systemd-coredump, systemd-resolve, rpcuser, vagrant, opsd, rdanet, _lldpd, rdaadmin, rdaweb, docker_container, tss.

Password requirements

Passwords must:

- Contain only ASCII characters from hexadecimal 21 to hexadecimal 7E [\x21-\x7E] (decimal 33 to 126). Spaces are not allowed. When the password is entered directly without prompting, the "?" symbol (hexadecimal 3F [\x3F] (decimal 63)) is not permitted.
- Contain at most 32 characters.
- Contain at least the number of characters configured (optionally) for minimum-password-length.



Although empty passwords are supported, it is recommended that you use strong passwords for all production switches.



Only an administrator can change the password of a user assigned to the `operators` role.

Per-user management interface enablement

By default, switch users are enabled for accessing the switch through all these available management interfaces: **ssh**, **telnet**, **https-server**, **console**.

Optionally, one or more of the management interfaces can be disabled for specific users.

User accounts can be local or managed on remote TACACS+ or RADIUS servers.

Local per-user management interface enablement

Local per-user management interface enablement is performed with CLI command **user management-interface**. CLI command **show user-list management-interface** is available for showing the current configuration.

Example of disabling the SSH management interface for local user **admin1**:

```
switch(config)# no user admin1 management-interface ssh
switch(config)# show user-list management-interface
USER                               ENABLED MANAGEMENT INTERFACE(S)
-----
admin                               ssh,telnet,https-server,console
admin1                             telnet,https-server,console
```

Example of disabling the telnet management interface for local user **admin1**:

```
switch(config)# no user admin1 management-interface telnet
switch(config)# show user-list management-interface
USER                               ENABLED MANAGEMENT INTERFACE(S)
-----
admin                               ssh,telnet,https-server,console
```

```
admin1                                https-server,console
```

Example of re-enabling the SSH management interface for local user **admin1**:

```
switch(config)# user admin1 management-interface ssh
switch(config)# show user-list management-interface
USER                                ENABLED MANAGEMENT INTERFACE(S)
-----
admin                               ssh,telnet,https-server,console
admin1                              ssh,https-server,console
```

Remote (TACACS+ or RADIUS) per-user management interface enablement

For remote TACACS+ and RADIUS servers, per-user management interface enablement is performed by configuring the Aruba VSA **Aruba-User-Mgmt-Interface**.

On the TACACS+ or RADIUS server, the Aruba VSA **Aruba-User-Mgmt-Interface** must be set to a comma-separated list of management interface names for which login is permitted by the associated user. Management interfaces omitted from the list are disabled for the associated user. A maximum of four management interface names are allowed, with each management interface name given once.

Permitted management interface names (always lowercase) are as follows:

- **ssh**
- **telnet**
- **https-server**
- **console**

The VSA has a maximum length of 32 characters. The VSA is ignored by the switch if longer than 32 characters.

When a user login fails because of an attempt to use a management interface that is not allowed, an event log is available indicating the enabled management interfaces as received in the TACACS+ or RADIUS VSA.

When using a RADIUS server other than ClearPass Policy Manager (CPPM), before setting the **Aruba-User-Mgmt-Interface** VSA, you must first define the VSA on the RADIUS server in file **/usr/share/freeradius/dictionary.aruba** as follows:

```
ATTRIBUTE  Aruba-User-Mgmt-Interface  69  string
```

Example RADIUS server VSA value that enables the two named management interfaces (**ssh**, **telnet**) while disabling the two unnamed management interfaces (**https-server**, **console**):

```
Aruba-User-Mgmt-Interface = "ssh,telnet"
```

Example RADIUS server VSA value that enables all four management interfaces:

```
Aruba-User-Mgmt-Interface = "ssh,telnet,https-server,console"
```

Example TACACS+ server configuration for user **admin1** with a VSA that enables management interfaces **ssh** and **console**:

```
key = test
group = admin {
    default service = permit
    service = exec {
        priv-lvl = 15
        Aruba-User-Mgmt-Interface = ssh,console
    }
}
user = admin1 {
    member = admin
    pap = cleartext testing
}
```

User and user group management tasks

User and user group management common tasks are as follows:

Task	Command or procedure	Example
Creating a user	user	user jamie group administrators password
Changing a user password	user password	user jamie password
Removing a user	user	no user jamie
Setting a user account password	user password	user admin password
Resetting the admin password using the Service OS	(procedure)	
Resetting the admin password by reverting the switch to factory defaults	(procedure)	erase startup-config boot system
Showing a list of all users	show user-list	show user-list
Showing information for the logged-in user	show user information	show user information
Creating a user group	user-group	user-group admuser2
Adding command authorization rules to a user group	permit or deny (within user-group)	10 deny cli command "show aaa .*" 20 permit cli command "show .*"
Adding comments to rules in a user group	comment (within user-group)	10 comment Deny all show aaa commands. 20 comment Permit all other show commands.

Task	Command or procedure	Example
Resequencing rules in a user group	resequence (within user-group)	resequence 100 20
Showing a list of all user groups	show user-group	show user-group

Resetting the switch admin password using the Service OS console

Perform this task only when the switch (Product OS) `admin` user password has been forgotten.

Prerequisites

- You are connected to the switch through the console port.
- You know the Service OS password (if configured).



If you forget the Service OS password, the only recourse is to zeroize the switch, reverting it to factory defaults. For more information, see *Zeroization* in the *Diagnostics and Supportability Guide*.

Procedure

1. Reboot the switch.
2. At the boot prompt, select **0. Service OS Console**.

```
0. Service OS Console
1. Primary Software Image [XL.01.01.0001]
2. Secondary Software Image [XL.01.01.0002]
```

3. At the **Switch Login** prompt, enter **admin** and press **Enter**. If prompted for a Service OS password, enter it and press **Enter**.

```
Switch login: admin
Password: *****
Hewlett Packard Enterprise
SVOS>
```

4. At the `svos>` prompt, enter `password` and press **Enter**.
5. Enter the new switch (Product OS) password at both password prompts.

```
SVOS> password
Enter password: *****
Confirm password: *****
```



```
SVOS>
```

1. Enter `boot` and press `Enter`.

```
SVOS> boot

ServiceOS Information:
  Version: **.10.06.0001
  Build Date: 2020-12-01 14:52:31 PDT
  Build ID: ServiceOS:**.01.01.0001:461519208911:20180301452
  SHA: 46151920891195cdb2267ea6889a3c6cbc3d4193

Boot Profiles:
0. Service OS Console
1. Primary Software Image [**.10.06.0001]
2. Secondary Software Image [**.10.06.0001]

Select profile(primary):
```

2. To boot with the primary switch image press `1` and then `Enter`. To boot with the secondary switch image, press `2` and then `Enter`. If you make no selection for approximately 10 seconds, the switch boots the default image. The default is shown in parentheses to the right of `Select profile`, for example: `Select profile(primary):.`
3. Once in AOS-CX, save the configuration to make the `admin` login user account password setting persistent.

Resetting the admin password by reverting the switch to factory defaults



This task erases all switch configuration, reverting the switch to its factory default state. Consider using other less-impacting techniques for admin password reset. For example, another administrator user can reset the admin user password to a known value. See also [Resetting the switch admin password using the Service OS console](#).

Prerequisites

If wanted, you have saved a copy of the switch configuration.

Procedure

1. At the manager command prompt, enter **`erase startup-config`**.

```
switch# erase startup-config
```

2. Enter **`boot system`**, responding **`n`** to the **Do you want to save the current configuration** prompt and then responding **`y`** to the **Continue** prompt.

```
switch# boot system
Do you want to save the current configuration (y/n)? n

This will reboot the entire switch and render it unavailable
until the process is complete.
Continue (y/n)? y
The system is going down for reboot.
```

3. At the login prompt, enter **admin** and press **Enter**. The admin password remains empty until it is set.

User and group commands

password complexity

```
password complexity
no password complexity
```

Description

Enters the password-complexity context (shown in the switch prompt as **config-pwd-cplx**) for the purpose of enabling and configuring password complexity. Password complexity enhances security by enforcing specific password complexity requirements. Password complexity is disabled by default and must be enabled by execution of the **enable** command.

Enabling or changing password complexity settings effects password creation or password change after the password complexity feature is enabled or changed. All existing passwords will continue to function as currently configured. When existing passwords are changed they will have to comply with whatever password complexity settings are enabled at the time of the change.

The **no** form of this command reverts all settings to their default values and disables password complexity enforcement.



To ensure that enhanced security is maintained, it is recommended that you do not set any values to less than their defaults.



Password complexity applies only to local authentication. For remote authentication, you may choose to set up an equivalent of password complexity according to whatever is supported on your particular TACACS+ or RADIUS server.

Subcommands

These subcommands are available within the password complexity context (shown in the switch prompt as **config-pwd-cplx**).

enable

Enables password complexity enforcement. The enforcement only applies to passwords created after this enabling. Existing passwords are not checked against password complexity.

disable

Disables password complexity enforcement.

[no] history-count <COUNT>

Specifies the number of previous passwords checked to prevent excessive reuse. Not applicable when adding new users. The **no** form of this subcommand resets the value to its default. Default: 5. Range: 1 to 5.



Previous passwords checked includes passwords used prior to enabling the password complexity feature.

[no] minimum-length **<LENGTH>**

Specifies the minimum password length. The no form of this subcommand resets the value to its default. Default: 8. Range: 1 to 32.

[no] position-changes **<POSITIONS>**

Specifies the minimum number of characters that must change in the new password compared to the previous password. Not applicable if no previous password exists, including when adding new users. The no form of this subcommand resets the value to its default. Default: 8. Range: 1 to 32.

The number of password position changes is based on the number of simple character insertions, deletions, or replacements. For example:

Old password: abCD4\$ New password: abCD\$ Position changes=1 ("4" deleted) Old password: abCD4\$ New password: abCDEF4\$ Position changes=2 ("EF" inserted) Old password: abCD4\$ New password: ebCD4\$ Position changes=2 ("a" replaced with "e," "1" added) Old password: abCD4\$ New password: abC\$# Position changes=3 ("D4" deleted, "#" added)

[no] lowercase-count **<COUNT>**

Specifies the minimum lowercase character count for new passwords. The no form of this subcommand resets the value to its default. Default: 1. Range: 0 to 32.

[no] uppercase-count **<COUNT>**

Specifies the minimum uppercase character count for new passwords. The no form of this subcommand resets the value to its default. Default: 1. Range: 0 to 32.

[no] numeric-count **<COUNT>**

Specifies the minimum numeric digit count for new passwords. The no form of this subcommand resets the value to its default. Default: 1. Range: 0 to 32.

[no] special-char-count **<COUNT>**

Specifies the minimum special character count for new passwords. The no form of this subcommand resets the value to its default. Default: 1. Range: 0 to 32.

[no] adjacent-char-type-count

Specifies the maximum number of adjacent characters from a character set allowed in a password. The different character sets are:

- Numbers
- Lowercase alphabets
- Uppercase alphabets
- Special characters

The number of adjacent characters from the character set in the password has to be less than or equal to the configured value. When set to 0, adjacent character type length check requirement is disabled. The no form of this subcommand resets the value to its default. Default: 0. Range: 0-31.

list

List the subcommands available within the password complexity context.

exit

Exits the password complexity context.

end

Exits the password complexity context and then the config context.

Usage

- Password complexity is only for use with plaintext passwords. With password complexity enabled, existing ciphertext passwords will continue working until a password is changed. All new passwords must be entered in plaintext form and be compliant with your password complexity configuration.

- The effective minimum password length may be larger than the configured **minimum-length** value.

The effective minimum password length is calculated as follows:

`LARGEST-of:(minimum-length, position-changes, (SUM-of:lowercase-count+uppercase-count+numeric-count+special-char-count))`

For example, with **minimum-length=8**, and **position-changes=10** (and the sum of the other four count settings ≤ 9), the **effective minimum-length is 10** (because **position-changes** is largest). Similarly, with a **minimum-length=12**, **position-changes=8**, **lowercase-count=8**, **uppercase-count=4**, **numeric-count=1**, **special-char-count=1**, the **effective minimum-length is 14** ($8+4+1+1=14$) (because sum off the four counts is largest).

Examples

Configuring password complexity settings with an effective minimum length of 10 (because **position-changes** is 10):

```
switch(config)# password complexity
switch(config-pwd-cplx)# history-count 3
switch(config-pwd-cplx)# minimum-length 8
switch(config-pwd-cplx)# position-changes 10
switch(config-pwd-cplx)# lowercase-count 2
switch(config-pwd-cplx)# uppercase-count 2
switch(config-pwd-cplx)# numeric-count 2
switch(config-pwd-cplx)# special-char-count 2
switch(config-pwd-cplx)# adjacent-char-type-count 3
switch(config-pwd-cplx)# enable
switch# exit
```

Configuring password complexity settings with an effective minimum length of 14 (because the sum of the four count items is 14):

```
switch(config)# password complexity
switch(config-pwd-cplx)# history-count 4
switch(config-pwd-cplx)# minimum-length 12
switch(config-pwd-cplx)# position-changes 8
switch(config-pwd-cplx)# lowercase-count 8
switch(config-pwd-cplx)# uppercase-count 4
switch(config-pwd-cplx)# numeric-count 1
switch(config-pwd-cplx)# special-char-count 1
switch(config-pwd-cplx)# adjacent-char-type-count 3
switch(config-pwd-cplx)# enable
switch# exit
```

Enabling password complexity (with default settings) and changing a user (admin1) password successfully but failing to change another user (admin2) password due to not meeting complexity requirements:

```
switch(config)# password complexity
switch(config-pwd-cplx)# enable
switch(config-pwd-cplx)# exit
switch(config)#
switch(config)# user admin1 password
Changing password for user admin1
Enter old password:*****
Enter new password:*****
Confirm new password:*****
switch(config)#
```

```

switch(config)# user admin2 password
Changing password for user admin2
Enter old password:*****
Enter new password:*****
Confirm new password:*****
User password not changed.
The new password does not meet one or more of the following complexity
requirements:
Minimum length           : 8
Position changes        : 8
Numeric count           : 1
Lowercase count         : 1
Uppercase count         : 1
Special character count : 1
Adjacent character type count: 3

```

With password complexity already enabled, attempting to change an existing user password but failing because the new password is identical to a recently used one (**history-count**).

```

switch(config)# user admin1 password
Changing password for user admin1
Enter old password:*****
Enter new password:*****
Confirm new password:*****
User password not changed.
The new password is the same as a recently used password.

```

With password complexity already enabled, creating a new admin user (admin3) with a plaintext password that meets complexity requirements.

```

switch(config)# user admin3 group administrators password
Adding user admin3
Enter password:*****
Confirm password:*****

```

With password complexity already enabled, attempting to create a new admin user (admin4) with a ciphertext password but failing because ciphertext passwords are not supported with password complexity enabled.

```

switch(config)# user admin4 group administrators password ciphertext AQBapPd...==
Ciphertext passwords cannot be used when password complexity is enabled.
switch(config)#

```

Command History

Release	Modification
10.11.1010	adjacent-char-type-count subcommand added.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

service export-password

```
service export-password
no service export-password
```

Description

Configures a nondefault export password. The export password is used to transform critical security parameters (such as password hashes) into ciphertext suitable for exporting and showing by commands such as **show running-config**. This transformation enables safe switch configuration import and export.

The **no** form of this command reverts the export password to its factory default.



All factory-default switches have identical default export passwords. For security, it is recommended that you set the same nondefault export password on every switch in a group that will exchange configuration information. Only switches with identical export passwords can exchange configuration information.

Usage

Prompts you twice for the new export password.

The export password must:

- Contain only ASCII characters from hexadecimal 21 to hexadecimal 7E [$\backslash$ x21- $\backslash$ x7E] (decimal 33 to 126). Spaces are not allowed.
- Contain at most 32 characters.
- Not be blank.

Examples

Configuring a new export password:

```
switch(config)# service export-password
Enter password:*****
Confirm password:*****
```

Reverting the export password to its factory default:

```
switch(config)# no service export-password
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

show password-complexity

show password-complexity

Description

Shows user-configured or default password complexity checking criteria.

Examples

Showing the current password complexity checking criteria:

```
switch(config)# show password-complexity

Global password complexity checking criteria:
  Password complexity           : Enabled
  Previous passwords to check   : 3
  Minimum password length      : 12
  Minimum position changes     : 10
  Maximum adjacent characters count : 3
  Password composition
    Minimum lowercase characters : 3
    Minimum uppercase characters : 1
    Minimum special characters   : 1
    Minimum numeric characters   : 3
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Manager (#)	Administrators or local user group members with execution rights for this command.

show user-group

show user-group [<GROUP-NAME>] [vsx-peer]

Description

Shows user group information for the built-in groups plus any user-defined local user groups. When entered without <GROUP-NAME>, summary information is shown for all groups.

Parameter	Description
<GROUP-NAME>	Narrows the show command output to that of the specified group, and for local user groups, adds the User Group Rules list.
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Examples

Show the list of all user groups, including built-in groups and local user groups.

```
switch# show user-group
GROUP NAME      GROUP TYPE      INCLUDED GROUP  NUMBER OF RULES
-----
administrators  built-in        n/a             n/a
admuser1        configuration    --             5
admuser2        configuration    admuser1        2
auditors        built-in        n/a             n/a
operators       built-in        n/a             n/a
```

Show detailed information for local user group **admuser2**.

```
switch(config-usr-grp-admuser2)# show user-group admuser2
User Group Summary
=====
Name           : admuser2
Type           : configuration
Included Group : admuser1
Number of Rules : 2
User Group Rules
=====
SEQUENCE NUM  ACTION      COMMAND      COMMENT
-----
10            deny        show aaa .*   Deny all show aaa commands.
20            permit      show .*       Permit all other show
commands.
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Manager (#)	Administrators or local user group members with execution rights for this command.

show user-list


```
show user-list [vsx-peer]
```

Description

Shows all configured users and their corresponding group names.

Parameter	Description
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Examples

Show the user list from a switch with only the admin user defined.

```
switch# show user-list

USER                               GROUP
-----
admin                             administrators
```

Show the user list after adding a user to the operators built-in group.

```
switch# show user-list

USER                               GROUP
-----
admin                             administrators
oper1                             operators
```

Show the user list after adding a user to the auditors built-in group.

```
switch# show user-list

USER                               GROUP
-----
admin                             administrators
oper1                             operators
audit1                            auditors
```

Show the user list after adding a total of three users to two user-defined user groups.

```
switch# show user-list

USER                               GROUP
-----
admin                             administrators
oper1                             operators
audit1                            auditors
adm1a                             admuser1
admin2-a                          admuser2
admin2-b                          admuser2
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Manager (#)	Administrators or local user group members with execution rights for this command.

show user-list management-interface

show user-list management-interface [vsx-peer]

Description

Shows a list of local users and the enabled management interfaces for each user.

Parameter	Description
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Examples

Disabling SSH and https-server for user **admin1**, disabling Telnet for **admin2**, then showing the configuration:

```
switch(config)# no user admin1 management-interface ssh
switch(config)# no user admin1 management-interface https-server
switch(config)# no user admin2 management-interface telnet
switch(config)# show user-list management-interface
USER                               ENABLED MANAGEMENT INTERFACE(S)
-----
admin                               ssh,telnet,https-server,console
admin1                             telnet,console
admin2                             ssh, https-server, console
```

Re-enabling https-server for user **admin1**, re-enabling Telnet for **admin2**, then showing the configuration:

```
switch(config)# user admin1 management-interface https-server
switch(config)# user admin2 management-interface telnet
switch(config)# show user-list management-interface
USER                               ENABLED MANAGEMENT INTERFACE(S)
-----
admin                               ssh,telnet,https-server,console
admin1                             telnet,https-server,console
admin2                             telnet,https-server,console
```

Command History

Release	Modification
10.11	Command introduced

Command Information

Platforms	Command context	Authority
All platforms	Manager (#)	Administrators or local user group members with execution rights for this command.

show user information

show user information

Description

Shows the following information for the logged-in user:

- User name.
- User authentication type: **local**, **RADIUS**, or **TACACS+**.
- User group: **administrators**, **operators**, or **<GROUP-NAME>**. This field is not applicable for remote authenticated users who are mapped to administrators or operators based on their privilege level.
- User privilege level: For the built-in user groups and RADIUS or TACACS+, the role privilege level value is shown. For user-defined user groups, **N/A** is shown.
- User login session: **ssh**, **telnet**, **https-server**, or **console**.

Examples

Showing information for the **admin** user:

```
switch# show user information
Username           : admin
Authentication type : Local
User group         : administrators
User privilege level : 15
User login session  : console
```

Showing information for a member of the user-defined local user group **admuser2**:

```
switch# show user information
Username           : admin2-b
Authentication type : Local
User group         : admuser2
User privilege level : N/A
User login session  : telnet
```

Showing information for a member of **operators**:

```
switch# show user information
Username           : operator
Authentication type : Local
User group         : operators
```

```
User privilege level : 1
User login session   : https-server
```

Showing information for remote RADIUS user **rad_user1** mapped to local user group **administrators**:

```
switch# show user information
Username           : rad_user1
Authentication type : RADIUS
User group         : administrators
User privilege level : 15
User login session  : telnet
```

Showing information for remote RADIUS user **rad_user2** mapped to local user group **operators**:

```
switch# show user information
Username           : rad_user2
Authentication type : RADIUS
User group         : operators
User privilege level : 1
User login session  : console
```

Showing information for remote TACACS+ **tac_user1** logged in with **priv-lvl** 15 (mapped to user group **administrators**):

```
switch# show user information
Username           : tac_user1
Authentication type : TACACS+
User group         : administrators
User privilege level : 15
User login session  : ssh
```

Command History

Release	Modification
10.11	Command now includes User login session information in its output
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

user

```
user <USERNAME> group {administrators | operators | auditors | <USER-GROUP>}
    password [ciphertext <CIPHERTEXT-PASSWORD> | plaintext <PLAINTEXT-PASSWORD>]
no user <USERNAME>
```

Description

Creates a user and adds the user to one of the user groups. Users are given the privileges of their group. For the three built-in user groups (**administrators**, **operators**, **auditors**), the privileges are fixed. For user-defined local user groups, the privileges are defined by the CLI command authorization rules of the group.

When entered without either optional **ciphertext** or **plaintext** parameters, the cleartext password is prompted for twice, with the characters entered masked with "*" symbols.

The **no** form of this command removes a user account from the switch. The administrator cannot delete the user account from which they are logged in. The **admin** user cannot be deleted.

Parameter	Description
<code><USERNAME></code>	Specifies the user name. Requirements: - Must start with a lowercase or uppercase letter. - Can contain numbers, lowercase, and uppercase letters. - Can include only these three special characters: hyphens (-), dots (.), and underscores (_). - Can have a maximum of 32 characters. - Cannot be empty. - Cannot be: <code>admin</code>, <code>root</code>, or <code>remote_user</code>. - Cannot be Linux reserved names such as: <code>daemon</code>, <code>bin</code>, <code>sys</code>, <code>sync</code>, <code>proxy</code>, <code>www-data</code>, <code>backup</code>, <code>list</code>, <code>irc</code>, <code>gnats</code>, <code>nobody</code>, <code>systemd-bus-proxy</code>, <code>sshd</code>, <code>messagebus</code>, <code>rpc</code>, <code>systemd-journal-gateway</code>, <code>systemd-journal-remote</code>, <code>systemd-journal-upload</code>, <code>systemd-timesync</code>, <code>systemd-coredump</code>, <code>systemd-resolve</code>, <code>rpcuser</code>, <code>vagrant</code>, <code>opds</code>, <code>rdanet</code>, <code>_lldpd</code>, <code>rdaadmin</code>, <code>rdaweb</code>, <code>docker_container</code>, <code>tss</code>. NOTE: Usernames containing the same consecutive letters with varying capitalization, such as <code>Admin</code>, <code>ADMIN</code>, and <code>aDmin</code>, will each be treated as different customer-configured user accounts.
<code>group</code>	Selects the local user group to which the new user will be assigned.
<code>administrators operators auditors</code>	Selects one of three built-in local user groups.
<code><USER-GROUP></code>	Specifies an existing user-defined local user group.
<code>ciphertext <CIPHERTEXT-PASSWORD></code>	Specifies a ciphertext password. No password prompts are provided and the ciphertext password is validated before the configuration is applied for the user. The variable <code><CIPHERTEXT-PASSWORD></code> is Base64 and is typically copied from another switch using the <code>show running-config</code> command output and then pasted into this command. NOTE: The administrator cannot construct ciphertext passwords themselves. The ciphertext is only created by an AOS-CX switch. The ciphertext is created by setting a password for a user with the <code>user</code> command. The ciphertext is available for copying from the <code>show</code>

Parameter	Description
	<code>running-config</code> output and pasting into the configuration on any other AOS-CX switch. The target switch must have the same export password (default or otherwise) as the source switch.
<code>plaintext <PLAINTEXT-PASSWORD></code>	Specifies the password without prompting. The password is visible as cleartext when entered but is encrypted thereafter. Command history does show the password as cleartext.

Usage

- Up to 63 local users can be added, for a total of 64 users including the default user **admin**. A user can belong to only one group.
- The switch ships with the **admin** user account and three built-in local user groups: **administrators**, **operators**, and **auditors**. The **admin** account belongs to the **administrators** group. The Service OS also includes the administrator user **admin**. The two admin users are entirely distinct.
- When a local user account is removed, the user loses all active login/SSH sessions. Any calls on the existing REST session with that local user account fail with a permissions issue as soon as the user is deleted. Soon afterwards, the existing REST sessions with the deleted local user account become invalidated. If a user is viewing the GUI while their account is deleted, the user is redirected to the login page within 60 seconds. The home directory associated with the user is also removed from the switch.
- Cleartext passwords (whether entered with prompting or entered directly) must:
 - Contain only ASCII characters from hexadecimal 21 to hexadecimal 7E [`\x21-\x7E`] (decimal 33 to 126). Spaces are not allowed. When the password is entered directly without prompting, the "?" symbol (hexadecimal 3F [`\x3F`] (decimal 63)) is not permitted.
 - Contain at most 32 characters.
 - Contain at least the number of characters configured (optionally) for `minimum-password-length`.



Although empty passwords are supported, it is recommended that you use strong passwords for all production switches.



Only an administrator can change the password of a user assigned to the `operators` role.

Although usernames with uppercase letters appear in the show-running configuration, users will not have login access if the username was configured and downgraded to a version without uppercase support.

Examples

Creating local user **jamie** in the **administrators** group with a prompted password:

```
switch(config)# user jamie group administrators password
Adding user jamie
```

```
Enter password:*****
Confirm password:*****
```

Creating user **chris** in the existing user-defined local user group **admuser2** with a cleartext password, using direct entry without prompting:

```
switch(config)# user chris group admuser2 password plaintext passWORDxJ|989
```

Creating user **alex** in the **operators** group with a ciphertext password (the ciphertext shown is a placeholder that must be replaced with actual ciphertext):

```
switch(config)# user alex group operators password ciphertext NDcDI2...8igJfA=
```

Removing user **jamie**:

```
switch(config)# no user jamie
User jamie's home directory and active sessions will be deleted.
Do you want to continue [y/n]?y
```

Using uppercase letters within username:

```
switch(config)# user TestUser1 group administrators password plaintext testuser1
switch(config)#
```

Command History

Release	Modification
10.13	Added support for use of uppercase letters within username.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

user-group

```
user-group <GROUP-NAME>
no user-group <GROUP-NAME>
```

Description

If **<GROUP-NAME>** does not exist, this command creates a local user group and then enters its context. If **<GROUP-NAME>** exists, this command enters the context for the specified **<GROUP-NAME>**. Within

the **<GROUP-NAME>** context, several subcommands are available for working with rules that specify what CLI commands are permitted or denied for all members of the local group.

In addition to the three built-in user groups **administrators**, **operators**, and **auditors**, up to 29 user-defined local user groups can be defined. All users can be members of only one of the up to 32 groups. The **no** form of this command deletes the specified user group. All members of the deleted group lose all command authorization privilege.

Parameter	Description
<code><GROUP-NAME></code>	Specify a user group name up to 32 characters long. A new group is created if the specified group does not exist and then the group context is entered. If the group name exists, its context is entered.



Do not causally delete user-defined local user groups without understanding the implications. Although user-defined local user groups can be deleted with the respective members losing all privileges, the three built-in groups `administrators`, `operators`, and `auditors` are always available and their privileges are unchangeable.

Subcommands

These subcommands are available within the user-defined local user group context (shown in the switch prompt as **config-usr-grp-<GROUP-NAME>**).

```
[<SEQ-NUM>] {permit | deny} cli command "<REGEX>"  
no <SEQ-NUM>
```

Defines a CLI command privilege **permit** or **deny** rule. There is an implicit **"deny .*"** rule at the end of every user-defined group rule list. Members of a user-defined group without any **permit** rules have no CLI command privileges.

The **no** form of this subcommand deletes the specified (by sequence number) rule from the group.



Rule evaluation proceeds from lowest to highest sequence number until the first successful match, resulting in either CLI command permission or denial. Rule evaluation ceases upon first match. Therefore, rules for related CLI commands must be defined in most restrictive to least restrictive order.

`<SEQ-NUM>`

Specifies the CLI command rule sequence number. When omitted, a sequence number that is 10 greater the highest existing sequence number is auto-assigned. When no rules exist, the first auto-assigned sequence number is 10.

{permit | deny}

Sets the rule type as either **permit** or **deny**. Rule order is important. For example, these two related rules together authorize all **show** commands except for the **show aaa** commands.

```
switch(config-usr-grp-admuser2)#10 deny cli command "show aaa .*"
switch(config-usr-grp-admuser2)#20 permit cli command "show .*"

```

To achieve the wanted effect in this example, the **deny** rule must precede the **permit** rule. These two rules together achieve the following:

- All **show aaa** commands match on rule 10, triggering command denial, and the immediate cessation of further rule evaluation. Matching on rule 20 is never attempted.

- All other **show** commands (excluding **show aaa** commands) match on rule 20 and are therefore permitted.

<REGEX>

Specifies the CLI command matching criteria of the rule. The criteria can be expressed as **".*"** which matches all commands. Otherwise, the criteria is expressed as a POSIX-compliant regular expression (regex) string starting with an exact match command token (for example **show**) followed by a regex representing command arguments. The first word must be a string that contains only alphanumeric or hyphen characters.

For example, to allow all commands starting with the word **interface**, the regex must be **"interface .*"** or just **"interface"**. Using **"interface.*"** (without the space) is not supported. For example, **"show .*"** matches every **show** command. Consult the Extended regular expression information available at: https://pubs.opengroup.org/onlinepubs/9699919799/basedefs/V1_chap09.html#tag_09_04.

Sample matching criteria	Sample matched CLI command or specifier	Matches
show .*	show accounting log	All show commands
bgp .*	bgp router-id 1.1.1.1	All bgp commands
interface .*	interface 1/1/1	All interface specifiers
vlan (3 4)	vlan 3	VLAN 3 or 4
vlan [1-9]	vlan 5	A single VLAN in the range 1 to 9
vlan ([1-9] 1[0-9])	vlan 19	A single VLAN in the range 1 to 19

```
[<SEQ-NUM>] comment <TEXT-STRING>
no <SEQ-NUM> comment
```

Adds a comment to an existing rule. The no form of this subcommand removes an existing comment.

```
switch(config-usr-grp-admuser2)# 10 comment Deny all show aaa commands.
switch(config-usr-grp-admuser2)# 20 comment Permit all other show commands.
switch(config-usr-grp-admuser2)#
switch(config-usr-grp-admuser2)# show running-config current-context
user-group admuser2
  10 comment Deny all show aaa commands.
  10 deny cli command "show aaa .*"
  20 comment Permit all other show commands.
  20 permit cli command "show .*"

```

```
include <GROUP-NAME> [no] include <GROUP-NAME>
```

Include all rules from the specified user-defined **<GROUP-NAME>**. Only one group can be included in the definition of another group. The content of the included group is effectively placed at the top of the rules list in the current group. If the specified **<GROUP-NAME>** does not exist, it is created.

The no form of this subcommand removes the specified included group from the current group. The specified included group must exist and must be included in the current group or else an error message is shown.

The name of the included group is shown at the top of the **show user-group** command for the group with the **include**.

In this example, group **admuser1** is included in group **admuser2**. So the **admuser1** rules are evaluated first and then the rules in the **admuser2** group are only evaluated if no CLI command match occurs for the rules in group **admuser1**.

```
switch(config-usr-grp-admuser2)# include admuser1
switch(config-usr-grp-admuser2)# show user-group admuser2
User Group Summary
=====
Name           : admuser2
Type           : configuration
Included Group : admuser1
Number of Rules : 2
User Group Rules
=====
SEQUENCE NUM  ACTION      COMMAND      COMMENT
-----
10            deny        show aaa .*   Deny all show aaa commands.
20            permit     show .*       Permit all other show
commands.
```

`resequence [<STARTING-SEQ-NUM> <INCREMENT>]`

Resequences the CLI command authorization rules. When entered without the optional parameters the rules are resequenced with a **<STARTING-SEQ-NUM>** of 10 and an **<INCREMENT>** of 10.

<STARTING-SEQ-NUM>

Specifies the starting sequence number.

<INCREMENT>

Specifies the sequence number increment.

Resequencing the rules to start at 100 with an increment of 20:

```
switch(config-usr-grp-admuser2)# resequence 100 20
switch(config-usr-grp-admuser2)# show running-config current-context
user-group admuser2
  100 comment Deny all show aaa commands.
  100 deny cli command "show aaa .*"
  120 comment Permit all other show commands.
  120 permit cli command "show .*"
```

Resequencing the rules to the default of starting at 10 with an increment of 10:

```
switch(config-usr-grp-admuser2)# resequence
switch(config-usr-grp-admuser2)# show running-config current-context
user-group admuser2
  10 comment Deny all show aaa commands.
  10 deny cli command "show aaa .*"
  20 comment Permit all other show commands.
  20 permit cli command "show .*"
```

`show running-config current-context`

Shows all the commands used to configure the rules in the current group context.

```
switch(config-usr-grp-admuser2)# show running-config current-context
user-group admuser2
  10 comment Deny all show aaa commands.
  10 deny cli command "show aaa .*"
```

```
20 comment Permit all other show commands.
20 permit cli command "show *.*"
```

list

List the subcommands available within the user-defined group context.

exit

Exits the user-defined group context.

end

Exits the user-defined group context and then the config context.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

user management-interface

```
user <USERNAME> management-interface <MGMT-INTERFACE>
no user <USERNAME> management-interface <MGMT-INTERFACE>
```

Description

Enables a management interface for the specified local user. By default, all management interfaces are enabled for all local users.

The **no** form of this command disables the selected management interface for the specified local user.

Parameter	Description
<USERNAME>	Specifies the name of an existing local user.
<MGMT-INTERFACE>	Selects one of the management interfaces: ssh , telnet , https-server , console . Note that https-server corresponds to the Web UI and REST.

Examples

Enabling the SSH management interface for local user **admin1**:

```
switch(config)# user admin1 management-interface ssh
```

Disabling the SSH management interface for local user **admin1**:

```
switch(config)# no user admin1 management-interface ssh
```

Enabling the telnet management interface for local user **admin1**:

```
switch(config)# user admin1 management-interface telnet
```

Disabling the telnet management interface for local user **admin1**:

```
switch(config)# no user admin1 management-interface telnet
```

Enabling the https-server (Web UI) management interface for local user **admin1**:

```
switch(config)# user admin1 management-interface https-server
```

Disabling the https-server (Web UI) management interface for local user **admin1**:

```
switch(config)# no user admin1 management-interface https-server
```

Enabling the console management interface for local user **admin1**:

```
switch(config)# user admin1 management-interface console
```

Disabling the console management interface for local user **admin1**:

```
switch(config)# no user admin1 management-interface console
```

Command History

Release	Modification
10.11	Command introduced

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

user password

```
user <USERNAME> password [ciphertext <CIPHERTEXT-PASSWORD> | plaintext <PLAINTEXT-PASSWORD>]
```

Description

Changes a password for an account or enables the password for the admin account. When entered without either optional **ciphertext** or **plaintext** parameters, the cleartext password is prompted for twice, with the characters entered masked with "*" symbols.

Parameter	Description
<code><USERNAME></code>	Specifies the corresponding user name for the password you want to change.
<code>ciphertext <CIPHERTEXT-PASSWORD></code>	Specifies a ciphertext password. No password prompts are provided and the ciphertext password is validated before the configuration is applied for the user. The variable <code><CIPHERTEXT-PASSWORD></code> is Base64 and is typically copied from another switch using the <code>show running-config</code> command output and then pasted into this command. NOTE: The administrator cannot construct ciphertext passwords themselves. The ciphertext is only created by an AOS-CX switch. The ciphertext is created by setting a password for a user with the <code>user</code> command. The ciphertext is available for copying from the <code>show running-config</code> output and pasting into the configuration on any other AOS-CX switch. The target switch must have the same export password (default or otherwise) as the source switch.
<code>plaintext <PLAINTEXT-PASSWORD></code>	Specifies the password without prompting. The password is visible as cleartext when entered but is encrypted thereafter. Command history does show the password as cleartext.

Usage

The admin account is available on the switch without a password by default.

Cleartext passwords (whether entered with prompting or entered directly) must:

- Contain only ASCII characters from hexadecimal 21 to hexadecimal 7E [`\x21-\x7E`] (decimal 33 to 126). Spaces are not allowed. When the password is entered directly without prompting, the "?" symbol (hexadecimal 3F [`\x3F`] (decimal 63)) is not permitted.
- Contain at most 32 characters.
- Contain at least the number of characters configured (optionally) for `minimum-password-length`.



Although empty passwords are supported, it is recommended that you use strong passwords for all production switches.



Only an administrator can change the password of a user assigned to the `operators` role.

Although usernames with uppercase letters appear in the show-running configuration, users will not have login access if the username was configured and downgraded to a version without uppercase support.

Examples

Enabling (or changing) a cleartext password for **admin**:

```
switch(config)# user admin password
Changing password for user admin
```

```
Enter password:*****
Confirm password:*****
```

Changing the cleartext password for user **chris**, using direct entry without prompting:

```
switch(config)# user chris password plaintext PASSwordZQ#@67
```

Changing the ciphertext password for user **alex** (the ciphertext shown is a placeholder that must be replaced with actual ciphertext):

```
switch(config)# user alex password ciphertext XqYJ36...W83D4Y=
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

SSH (Secure Shell) is a cryptographic protocol that encrypts all communication between devices. Each switch VRF includes an SSH server. The SSH server on the **mgmt** VRF is enabled by default in software version 10.02 and higher, and disabled in version 10.01 and lower. Only the SSH servers included in the switch are supported.

The SSH server provides SSH client to switch communications, enabling SSH clients (at least SSH v2.0) to connect to the switch for the purpose of managing it. The SSH server interfaces with the authentication service that provides local and/or remote AAA.



The SSH server will perform a rekey operation for all open SSH sessions at every hour or after 1 GB of data transferred, whichever occurs first. The rekey is performed to address a common security concern that encryption/decryption keys not be used for long periods of time. This limits the amount of data exposed in the unfortunate case where a key is exposed or refactored.



SSH public key authentication is separate from SSH server. Look for information on *SSH public key* under [Local authentication](#).

SSH defaults

Setting	Default value
Maximum SSH password retries	3 password retries.
Password-based (with SSH client) authentication	Enabled.
SSH password-based login grace period timeout	120 seconds.
SSH public key authentication	Enabled.
SSH idle session timeout	60 seconds.

SSH server tasks

SSH server tasks are as follows:

Task	Command name	Example
Enabling the SSH server	<code>ssh server vrf</code>	<code>ssh server vrf default</code>
Disabling the SSH server	<code>no ssh server vrf</code>	<code>no ssh server vrf default</code>
Generating an SSH host-key pair	<code>ssh host-key</code>	<code>ssh host-key rsa bits 2048</code>
Clearing the list of trusted SSH servers for your user account	<code>ssh known-host remove</code>	<code>ssh known-host remove 1.1.1.1</code>
Configuring SSH to use a set of ciphers	<code>ssh ciphers</code>	<code>ssh ciphers chacha20-poly1305@openssh.com aes256-ctr aes256-cbc</code>
Configuring SSH to use a set of host key algorithms	<code>ssh host-key-algorithms</code>	<code>ssh host-key-algorithms ssh-rsa ssh-ed25519 ecdsa-sha2-nistp521</code>
Configuring SSH to use a set of MACs	<code>ssh macs</code>	<code>ssh macs hmac-sha2-256 hmac-sha2-512</code>
Configuring SSH to use a set of key exchange algorithms	<code>ssh key-exchange-algorithms</code>	<code>ssh key-exchange-algorithms ecdh-sha2-nistp256</code>
Configuring SSH to use a set of public key algorithms	<code>ssh public-key-algorithms</code>	<code>ssh public-key-algorithms x509v3-ssh-rsa ssh-rsa rsa-sha2-256</code>
Configuring SSH idle session timeout	<code>cli-session</code>	<code>switch(config)# cli-session</code> <code>switch(config-cli-session)# timeout 20</code>
Showing the SSH server configuration	<code>show ssh server</code>	<code>show ssh server all-vrfs</code>
Showing the active SSH sessions	<code>show ssh server sessions</code>	<code>show ssh server sessions all-vrfs</code>
Showing the SSH server host keys	<code>show ssh host-key</code>	<code>show ssh host-key ecdsa</code>

SSH server commands

show ssh host-key

```
show ssh host-key [ecdsa | ed25519 | rsa]
```

Description

Shows the public host keys for the SSH server. If the key type is not provided, all available host-keys are shown.

Parameter	Description
ecdsa	Selects the ECDSA host-key pair.
ed25519	Selects the ED25519 host-key pair.
rsa	Selects the RSA host-key pair.

Examples

Showing the ECDSA public host-key:

```
switch# show ssh host-key ecdsa

Key Type : ECDSA      Curve : ecdsa-sha2-nistp256

ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAhtuv5rABBBGs
...
O4mjVFGMVkZ87RWkyrxeQa2fAGZZEp1902K33/k3q17fA4EivRzC75YvjDu8=
```

Showing all public host keys:

```
switch# show ssh host-key
Key Type : ECDSA      Curve : ecdsa-sha2-nistp256
ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAhtuv5rABBBGs
...
O4mjVFGMVkZ87RWkyrxeQa2fAGZZEp1902K33/k3q17fA4EivRzC75YvjDu8=

Key Type : ED25519
ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIGb6910Jwoe8Hkl9K5YhqijrWI3yovNbiJVq6tw4WjJr4

Key Type : RSA        Key Size : 2048
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQDdVCXlW43h4n1bwg9jI6DSBMngymCdPD0JUG42Sn9IS
...
nGSXtrNy6OmlFDJTAy+zz5Kd8d21ZLuhf07IHNgF3pff65Xc8qNJBv
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Manager (#)	Administrators or local user group members with execution rights for this command.

show ssh server

```
show ssh server [vrf <VRF-NAME> | all-vrfs] [vsx-peer]
```

Description

Shows the SSH server configuration for the specified VRF. Administrators can show the server configuration of all VRFs by using the **all-vrfs** parameter. If no VRF name is provided in this command, the command shows the SSH server configuration on the default VRF.

Parameter	Description
vrf <VRF-NAME>	Specifies the VRF name.
all-vrfs	Selects all VRFs.
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Examples

Showing the SSH server configuration on the default VRF:

```
switch# show ssh server

SSH server configuration on VRF default :

IP Version           : IPv4 and IPv6           SSH Version          : 2.0
TCP Port             : 22                      Grace Timeout (sec)  : 120
Max Auth Attempts    : 6
Allow-list           : disabled

Ciphers:
chacha20-poly1305@openssh.com, aes128-ctr, aes192-cbc,
aes128-cbc, aes192-ctr, aes256-gcm@openssh.com,
aes128-gcm@openssh.com, aes256-ctr, aes256-cbc

Host Key Algorithms:
ecdsa-sha2-nistp256, ecdsa-sha2-nistp384, ecdsa-sha2-nistp521,
ssh-ed25519, rsa-sha2-256, rsa-sha2-512, ssh-rsa

Key Exchange Algorithms:
curve25519-sha256, curve25519-sha256@libssh.org,
ecdh-sha2-nistp256,ecdh-sha2-nistp384, ecdh-sha2-nistp521,
diffie-hellman-group-exchange-sha256,diffie-hellman-group16-sha512,
diffie-hellman-group18-sha512,diffie-hellman-group14-sha256,
diffie-hellman-group14-sha1

MACs:
hmac-sha1-etm@openssh.com, umac-64@openssh.com,
umac-128@openssh.com, hmac-sha2-256,hmac-sha2-512,hmac-sha1

Public Key Algorithms:
rsa-sha2-256, rsa-sha2-512ssh-rsa, ecdsa-sha2-nistp256,
ecdsa-sha2-nistp384, ecdsa-sha2-nistp521, ssh-ed25519,
x509v3-rsa2048-sha256, x509v3-ssh-rsa, x509v3-sign-rsa,
x509v3-ecdsa-sha2-nistp256, x509v3-ecdsa-sha2-nistp384,
x509v3-ecdsa-sha2-nistp521
```

Showing the SSH server configuration on the management VRF:

```
switch# show ssh server vrf mgmt

SSH server configuration on VRF mgmt :

IP Version           : IPv4 and IPv6      SSH Version          : 2.0
TCP Port             : 22                  Grace Timeout (sec)  : 120
Max Auth Attempts    : 6

Ciphers:
chacha20-poly1305@openssh.com, aes128-ctr, aes192-cbc,
aes128-cbc, aes192-ctr, aes256-gcm@openssh.com,
aes128-gcm@openssh.com, aes256-ctr, aes256-cbc

Host Key Algorithms:
ecdsa-sha2-nistp256, ecdsa-sha2-nistp384, ecdsa-sha2-nistp521,
ssh-ed25519, rsa-sha2-256, rsa-sha2-512, ssh-rsa

Key Exchange Algorithms:
curve25519-sha256, curve25519-sha256@libssh.org,
ecdh-sha2-nistp256, ecdh-sha2-nistp384, ecdh-sha2-nistp521,
diffie-hellman-group-exchange-sha256, diffie-hellman-group16-sha512,
diffie-hellman-group18-sha512, diffie-hellman-group14-sha256,
diffie-hellman-group14-sha1

MACs:
hmac-sha1-etm@openssh.com, umac-64@openssh.com,
umac-128@openssh.com, hmac-sha2-256, hmac-sha2-512, hmac-sha1

Public Key Algorithms:
rsa-sha2-256, rsa-sha2-512, ssh-rsa, ecdsa-sha2-nistp256,
ecdsa-sha2-nistp384, ecdsa-sha2-nistp521, ssh-ed25519,
x509v3-rsa2048-sha256, x509v3-ssh-rsa, x509v3-sign-rsa,
x509v3-ecdsa-sha2-nistp256, x509v3-ecdsa-sha2-nistp384,
```

Showing the SSH server configuration for all VRFs:

```
switch# show ssh server all-vrfs

SSH server configuration on VRF default :

IP Version           : IPv4 and IPv6      SSH Version          : 2.0
TCP Port             : 22                  Grace Timeout (sec)  : 120
Max Auth Attempts    : 6

Ciphers:
chacha20-poly1305@openssh.com, aes128-ctr, aes192-cbc,
aes128-cbc, aes192-ctr, aes256-gcm@openssh.com,
aes128-gcm@openssh.com, aes256-ctr, aes256-cbc

Host Key Algorithms:
ecdsa-sha2-nistp256, ecdsa-sha2-nistp384, ecdsa-sha2-nistp521,
ssh-ed25519, rsa-sha2-256, rsa-sha2-512, ssh-rsa

Key Exchange Algorithms:
curve25519-sha256, curve25519-sha256@libssh.org,
ecdh-sha2-nistp256, ecdh-sha2-nistp384, ecdh-sha2-nistp521,
diffie-hellman-group-exchange-sha256, diffie-hellman-group16-sha512,
diffie-hellman-group18-sha512, diffie-hellman-group14-sha256,
```

MACs:
hmac-sha1-etm@openssh.com, umac-64@openssh.com,
umac-128@openssh.com, hmac-sha2-256, hmac-sha2-512, hmac-sha1

Public Key Algorithms:
rsa-sha2-256, rsa-sha2-512ssh-rsa, ecdsa-sha2-nistp256,
ecdsa-sha2-nistp384, ecdsa-sha2-nistp521, ssh-ed25519,
x509v3-rsa2048-sha256, x509v3-ssh-rsa, x509v3-sign-rsa,
x509v3-ecdsa-sha2-nistp256, x509v3-ecdsa-sha2-nistp384,
x509v3-ecdsa-sha2-nistp521

SSH server configuration on VRF mgmt :

IP Version	: IPv4 and IPv6	SSH Version	: 2.0
TCP Port	: 22	Grace Timeout (sec)	: 120
Max Auth Attempts	: 6		

Ciphers:
chacha20-poly1305@openssh.com, aes128-ctr, aes192-cbc,
aes128-cbc, aes192-ctr, aes256-gcm@openssh.com,
aes128-gcm@openssh.com, aes256-ctr, aes256-cbc

Host Key Algorithms:
ecdsa-sha2-nistp256, ecdsa-sha2-nistp384, ecdsa-sha2-nistp521,
ssh-ed25519, rsa-sha2-256, rsa-sha2-512, ssh-rsa

Key Exchange Algorithms:
curve25519-sha256, curve25519-sha256@libssh.org,
ecdh-sha2-nistp256, ecdh-sha2-nistp384, ecdh-sha2-nistp521,
diffie-hellman-group-exchange-sha256, diffie-hellman-group16-sha512,
diffie-hellman-group18-sha512, diffie-hellman-group14-sha256,
diffie-hellman-group14-sha1

MACs:
hmac-sha1-etm@openssh.com, umac-64@openssh.com,
umac-128@openssh.com, hmac-sha2-256, hmac-sha2-512, hmac-sha1

Public Key Algorithms:
rsa-sha2-256, rsa-sha2-512ssh-rsa, ecdsa-sha2-nistp256,
ecdsa-sha2-nistp384, ecdsa-sha2-nistp521, ssh-ed25519,
x509v3-rsa2048-sha256, x509v3-ssh-rsa, x509v3-sign-rsa,
x509v3-ecdsa-sha2-nistp256, x509v3-ecdsa-sha2-nistp384,

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ssh server sessions

```
show ssh server sessions [vrf <VRF-NAME> | all-vrfs] [vsx-peer]
```

Description

Shows the active SSH sessions on a specified VRF or on all VRFs. If no VRF is specified, the active sessions on the **default** VRF are shown.

Parameter	Description
vrf <VRF-NAME>	Specifies the VRF name.
all-vrfs	Selects all VRFs.
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Usage

If you provide the command with a VRF name, the command shows the active SSH session for the specified VRF. Any user can show sessions of all VRFs by using the **all-vrfs** parameter. The maximum number of sessions per VRF is five. The maximum SSH idle session timeout is 60 seconds.

Examples

Showing the active SSH sessions on the default VRF:

```
switch# show ssh server sessions

SSH sessions on VRF default
IPv4 SSH Sessions
  Server IP      : 10.1.1.1
  Client IP      : 10.1.1.2
  Client Port    : 58835

IPv6 SSH Sessions
  Server IP      : FF01:0:0:0:0:0:FB
  Client IP      : FF01:0:0:0:0:0:FC
  Client Port    : 58836
```

Showing the SSH server configuration for all VRFs:

```
switch# show ssh server sessions all-vrf

SSH sessions on VRF mgmt
IPv4 SSH Sessions
  Server IP      : 10.1.1.1
  Client IP      : 10.1.1.2
  Client Port    : 58835

IPv6 SSH Sessions
  Server IP      : FF01:0:0:0:0:0:FB
  Client IP      : FF01:0:0:0:0:0:FC
  Client Port    : 58836
```

```

SSH sessions on VRF default
IPv4 SSH Sessions
  Server IP      : 20.1.1.1
  Client IP     : 20.1.1.2
  Client Port   : 58837

IPv6 SSH Sessions
  Server IP      : FF01:0:0:0:0:0:0:FD
  Client IP     : FF01:0:0:0:0:0:0:FE
  Client Port   : 58838

```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Administrators or local user group members with execution rights for this command.

ssh ciphers

```

ssh ciphers <CIPHERS-LIST>
no ssh ciphers

```

Description

Configures SSH to use a set of ciphers in the specified priority order. Ciphers in SSH are used for privacy of data being transported over the connection. The first cipher type entered in the CLI is considered a first priority. Each option is an algorithm that is used to encrypt the link and each name indicates the algorithm and cryptographic parameters that are used. Only ciphers that are entered by the user are configured.

The **no** form of this command removes the configuration of ciphers and reverts SSH to use the default set of ciphers.

Parameter	Description
<CIPHERS-LIST>	Valid ciphers: ■ aes128-cbc ■ aes192-cbc ■ aes256-cbc ■ aes128-ctr ■ aes192-ctr ■ aes256-ctr ■ aes128-gcm@openssh.com ■ aes256-gcm@openssh.com ■ chacha20-poly1305@openssh.com

Parameter	Description
	Default set of ciphers in priority order (highest at top): ▪ chacha20-1305@openssh.com ▪ aes128-ctr ▪ aes192-ctr ▪ aes256-ctr ▪ aes128-gcm@openssh.com ▪ aes256-gcUm@openssh.com

Examples

Configuring SSH to use only specified ciphers in the priority order:

```
switch(config)# ssh ciphers chacha20-poly1305@openssh.com aes256-ctr aes256-cbc
```

Reverting SSH to use the default set of ciphers:

```
switch(config)# no ssh ciphers
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

ssh host-key

```
ssh host-key {ecdsa [ecdsa-sha2-nistp256 | ecdsa-sha2-nistp384 | ecdsa-sha2-nistp521] |
ed25519 | rsa [bits {2048 | 4096}] }
```

Description

Generates an SSH host-key pair.

Parameter	Description
ecdsa	Selects the ECDSA host-key pair type as ecdsa-sha2-nistp256 (the default), ecdsa-sha2-nistp384 , or ecdsa-sha2-nistp521 .
ed25519	Selects the ED25519 host-key pair.
rsa	Selects the RSA host-key pair. Optionally, the key bit length is selected with either bits 2048 (the default) or bits 4096 .

Usage

When an SSH server is enabled on a VRF for the first time, host-keys are generated.

If the host-key of the given type exists, a warning message is displayed with a request to overwrite the previous host-key with the new key.

Examples

Overwriting an old ECDSA host-key with a new ecdsa-sha2-nistp384 host-key:

```
switch(config)# ssh host-key ecdsa ecdsa-sha2-nistp384  
ecdsa host-key will be overwritten.  
Do you want to continue (y/n)?
```

Overwriting an old RSA host-key with a new RSA host-key with 2048 bits:

```
switch(config)# ssh host-key rsa bits 2048  
rsa host-key will be overwritten.  
Do you want to continue (y/n)?
```

Overwriting an ECDSA host-key with an ED25519 host-key pair:

```
switch(config)# ssh host-key ed25519  
ed25519 host-key will be overwritten.  
Do you want to continue (y/n)?
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

ssh host-key-algorithms

```
ssh host-key-algorithms <HOST-KEY-ALGORITHMS-LIST>  
no ssh host-key-algorithms
```

Description

Configures SSH to use a set of host key algorithms in the specified priority order. Host key algorithms specify which host key types are allowed to be used for the SSH connection. The first host key entered in the CLI is considered a first priority. Each option represents a type of key that can be used. Host keys are used to verify the host that you are connecting to. This configuration allows you to control which host key types are presented to incoming clients, or which host key types to receive first from hosts. Only the host key algorithms that are specified by the user are configured.

The **no** form of this command removes the configuration of host key algorithms and reverts SSH to use the default set of algorithms.

Parameter	Description
<code><HOST-KEY-ALGORITHMS-LIST></code>	Default set of public key algorithms in priority order (highest at top), comprised of all possible valid algorithms: ▪ ecdsa-sha2-nistp256 ▪ ecdsa-sha2-nistp384 ▪ ecdsa-sha2-nistp521 ▪ ssh-ed25519 ▪ rsa-sha2-256 ▪ rsa-sha2-512 ▪ ssh-rsa

Examples

Configuring SSH to use only specified host key algorithms:

```
switch(config)# ssh host-key-algorithms ssh-rsa ssh-ed25519 ecdsa-sha2-nistp521
```

Reverting SSH to use the default set of host key algorithms:

```
switch(config)# no host-key-algorithms
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	<code>config</code>	Administrators or local user group members with execution rights for this command.

ssh key-exchange-algorithms

```
ssh key-exchange-algorithms <KEY-EXCHANGE-ALGORITHMS-LIST>
no ssh key-exchange-algorithms
```

Description

Configures SSH to use a set of key exchange algorithm types in the specified priority order. The first key exchange type entered in the CLI is considered a first priority. Key exchange algorithms are used to exchange a shared session key with a peer securely. Each option represents an algorithm that is used to distribute a shared key in a way that prevents outside interference, manipulation, or recovery. Only the key exchange algorithms that are specified by the user are configured.

The **no** form of this command removes the configuration of key exchange algorithms and reverts SSH to use the default set of algorithms.

Parameter	Description
<code><KEY-EXCHANGE-ALGORITHMS-LIST></code>	Valid key exchange algorithms: ▪ <code>curve25519-sha256</code> ▪ <code>curve25519-sha256@libssh.org</code> ▪ <code>diffie-hellman-group-exchange-sha1</code> ▪ <code>diffie-hellman-group-exchange-sha256</code> ▪ <code>diffie-hellman-group14-sha1</code> ▪ <code>diffie-hellman-group14-sha256</code> ▪ <code>diffie-hellman-group16-sha512</code> ▪ <code>diffie-hellman-group18-sha512</code> ▪ <code>ecdh-sha2-nistp256</code> ▪ <code>ecdh-sha2-nistp384</code> ▪ <code>ecdh-sha2-nistp521</code> Default set of key exchange algorithms in priority order (highest at top): ▪ <code>curve25519-sha256</code> ▪ <code>curve25519-sha256@libssh.org</code> ▪ <code>ecdh-sha2-nistp256</code> ▪ <code>ecdh-sha2-nistp384</code> ▪ <code>ecdh-sha2-nistp521</code> ▪ <code>diffie-hellman-group-exchange-sha256</code> ▪ <code>diffie-hellman-group16-sha512</code> ▪ <code>diffie-hellman-group18-sha512</code> ▪ <code>diffie-hellman-group14-sha256</code> ▪ <code>diffie-hellman-group-exchange-sha1</code>

Examples

Configuring SSH to use a set of specified key exchange algorithms:

```
switch(config)# ssh key-exchange-algorithms ecdh-sha2-nistp256 curve25519-sha256
diffie-hellman-group-exchange-sha256
```

Reverting SSH to use the default set of key-exchange-algorithms:

```
switch(config)# no key-exchange-algorithms
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	<code>config</code>	Administrators or local user group members with execution rights for this command.

ssh known-host remove

```
ssh known-host remove {all | {<IPv4-ADDRESS> | <HOSTNAME> | <IPv6-ADDRESS>} }
```

Description

Clears the list of trusted SSH servers for your user account. When you download or upload a file to or from a server using SFTP, you establish a trusted SSH relationship with that server. Each user account maintains its own set of SSH server host-keys for every server to which the user previously connected.

Parameter	Description
all	Clears the trusted servers list.
<IPv4-ADDRESS>	Specifies the IPv4 address of the remote device.
<HOSTNAME>	Specifies the host name of the remote device. Range: up to 255 characters.
<IPv6-ADDRESS>	Specifies the IPv6 address of the remote device.

Examples

Clearing the trusted server list:

```
switch(config)# ssh known-host remove all
```

Removing a specified server from the trusted server list:

```
switch(config)# ssh known-host remove 1.1.1.1
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

ssh macs

```
ssh macs <MACS-LIST>  
no ssh macs
```

Description

Configures SSH to use a set of message authentication codes (MACs) in the specified priority order. The first MAC entered in the CLI is considered a first priority. MACs maintain the integrity of each message

sent across an SSH connection. Each option represents an algorithm that can be used to provide integrity between peers. Only the MAC types that are specified by the user are configured.

The **no** form of this command removes the configuration of MACs and reverts SSH to use the default set of MACs.

Parameter	Description
<code><MACS-LIST></code>	Valid MACs: ▪ hmac-sha1 ▪ hmac-sha1-96 ▪ hmac-sha1-etm@openssh.com ▪ hmac-sha2-256 ▪ hmac-sha2-512 ▪ hmac-sha2-256-etm@openssh.com ▪ hmac-sha2-512-etm@openssh.com Default set of MACs in priority order (highest at top): ▪ hmac-sha2-256-etm@openssh.com ▪ hmac-sha2-512-etm@openssh.com ▪ hmac-sha1-etm@openssh.com ▪ hmac-sha2-256 ▪ hmac-sha2-512 ▪ hmac-sha1

Examples

Configuring SSH to use a set of specified MACs:

```
switch(config)# ssh macs hmac-sha2-256 hmac-sha2-512
```

Reverting SSH to use the default set of MACs:

```
switch(config)# no ssh macs
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

ssh maximum-auth-attempts

```
ssh maximum-auth-attempts <ATTEMPTS>  
no maximum-auth-attempts
```

Description

Sets the SSH maximum number of authentication attempts.

The **no** form of the command resets the maximum to its default of 6.

Parameter	Description
<code><ATTEMPTS></code>	Specifies the maximum number of SSH authentication attempts. Range: 1 to 10. Default: 6.

Examples

Setting the maximum number of authentication attempts:

```
switch(config)# ssh maximum-auth-attempts 3
```

Resetting the maximum number of authentication attempts to its default of 6:

```
switch(config)# no maximum-auth-attempts
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

ssh public-key-algorithms

```
ssh public-key-algorithms <PUBLIC-KEY-ALGORITHMS-LIST>  
no ssh public-key-algorithms
```

Description

Configures SSH to use a set of public key algorithms in the specified priority order. The first public key type entered in the CLI is considered a first priority. Public key algorithms specify which public key types can be used for public key authentication in SSH. Each option represents a public key type that the SSH server can accept or that the SSH client can present to a server. Only the public key algorithms that are chosen by the user are configured.

The **no** form of this command removes the configuration of public key algorithms and reverts SSH to use the default set.

Parameter	Description
<code><PUBLIC-KEY-ALGORITHMS-LIST></code>	Default set of public key algorithms in priority order (highest at

Parameter	Description
	top), comprised of all possible valid algorithms: ▪ rsa-sha2-256 ▪ rsa-sha2-512 ▪ ssh-rsa ▪ ecdsa-sha2-nistp256 ▪ ecdsa-sha2-nistp384 ▪ ecdsa-sha2-nistp521 ▪ ssh-ed25519 ▪ x509v3-rsa2048-sha256 ▪ x509v3-ssh-rsa ▪ x509v3-sign-rsa ▪ x509v3-ecdsa-sha2-nistp256 ▪ x509v3-ecdsa-sha2-nistp384 ▪ x509v3-ecdsa-sha2-nistp521

Examples

Configuring SSH to use a set of specified public key algorithms:

```
switch(config)# ssh public-key-algorithms x509v3-ssh-rsa ssh-rsa rsa-sha2-256
```

Reverting SSH to use the default set of public key algorithms:

```
switch(config)# no ssh public-key-algorithms
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

ssh server allow-list

```
ssh server allow-list
  ip <ipv4-addr>[mask]
  ipv6 <ipv6-addr>[mask]
  enable
  no
```

Description

Configure a list of addresses that will be the only hosts allowed to connect to the SSH servers running on all VRFs of the switch. By default, the allow-list is disabled and any host is allowed to connect given

the correct authentication criteria. When the allow-list is enabled, only the hosts that fall under one of the entries may connect with the correct authentication criteria, all other hosts will be denied to attempt authentication.

Parameter	Description
<code>ip <ipv4-addr>[mask]</code>	An allowed host IP address and (optional) subnet in any of the following formats: ▪ A.B.C.D: An allowed IPv4 address ▪ A.B.C.D/M: An allowed IPv4 subnet with prefix length ▪ A.B.C.D W.X.Y.Z: An allowed IPv4 address with network mask ▪ A.B.C.D/W.X.Y.Z: An allowed IPv4 address with network mask
<code>ipv6 <iv6p-addr>[mask]</code>	An allowed host IPv6 address and (optional) subnet in any of the following formats: ▪ X:X::X:X: An allowed IPv6 address ▪ X:X::X:X/M: An allowed IPv6 subnet
<code>enable</code>	Enable the allow-list.
<code>no ...</code>	Negate a command or set its default.

Usage

The allow-list can contain up to 20 entries of IPv4 or IPv6 addresses, including entire subnets. The order in which the entries are added to the list does not matter. The configuration will only take effect once the allow-list is enabled by issuing the **enable** command in the the `config-ssh-al` (**ssh server allow-list**) context.

When the allow-list is enabled, SSH servers on all VRFs will restart and all active SSH sessions will be terminated. The enabled allow-list may be modified to remove existing entries or add new entries, and each of those modifications will trigger an SSH server restart for all VRFs and will terminate all active SSH sessions, which may include the current user if they are connected via SSH. If you disable the allow-list before making changes and enabling the allow-list again once the changes are made, any host will be allowed to connect during the modification period before the allow-list is re-enabled. When the allow-list is disabled, the SSH servers on all VRFs will restart and active SSH sessions will persist.



Every SSH allow-list ends with an implicit **deny all** rule. When you add entries to an allow list, take care to avoid blocking connectivity to the SSH server. If an SSH allow-list is enabled with no entries configured, the **deny all** functionality will block all addresses, and the SSH server will be unusable.

Examples

Configuring and enabling an SSH server allow list

```
switch(config)# ssh server allow-list
switch(config-ssh-al)# 1.1.1.1
switch(config-ssh-al)# enable
Active SSH sessions will be terminated.
Do you want to continue (y/n)?
```

Command History

Release	Modification
10.12	Command introduced

Command Information

Platforms	Command context	Authority
All platforms	config and config-ssh-al contexts	Administrators or local user group members with execution rights for this command.

ssh server port

```
ssh server port <PORT-NUMBER>
no ssh server port [<PORT-NUMBER>]
```

Description

Configures SSH server to listen on a particular TCP port number. The default value is 22. This port will be used for all VRFs that have SSH server enabled.



Configuring the TCP port number restarts the SSH server and terminates all active SSH sessions. It may take a few seconds for the SSH sessions to reach the running state on some VRFs.

The **no** form of the command resets the TCP port number to the default, 22.

Parameter	Description
<PORT-NUMBER>	Specifies the TCP port number. Range: 1 to 65535. Default: 22.

Examples

Configuring TCP port number 19222:

```
switch(config)# ssh server port 19222
```

Resetting the TCP port number to the default, 22:

```
switch(config)# no ssh server port
```

Command History

Release	Modification
10.11.1000	Command introduced

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

ssh server vrf

```
ssh server vrf <VRF-NAME>
no ssh server vrf <VRF-NAME>
```

Description

Enables the SSH server on the specified VRF. SSH is disabled by default and will not be operational till the admin password is set on the switch. Note that the admin password is considered set even if it is configured to be empty.

The **no** form of the command disables the SSH server on the specified VRF. If no VRF is specified, by default the SSH server will be enabled on the **default** or **mgmt** VRF, depending on the switch model.

Parameter	Description
vrf <VRF-NAME>	Specifies the VRF name.

Examples

Enabling the SSH server on the management VRF:

```
switch(config)# ssh server vrf mgmt
```

Disabling the SSH server on the management VRF:

```
switch(config)# no ssh server vrf mgmt
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

The switch provides an SSH client that enables the switch to log in to an SSH server such as another switch, typically for command execution purposes. The SSH client provides secure encrypted communications between the switch and the SSH server over any network.

SSH client commands

ssh (client login)

```
ssh [<USERNAME>@] {<IPv4> | <HOSTNAME>} [vrf <VRF-NAME>] [port <PORT-NUMBER>]
```

Description

Establishes a client session with an SSH server which is typically another switch.

username, vrf and port number are optional parameters. If a source ip address or source interface is configured for the ssh client protocol, the configuration values are used for establishing the client session with the SSH server.



The source interface can be configured using the IP source interface configuration commands described in the Fundamentals Guide.

Parameter	Description
<USERNAME>	Specifies the username that the client uses to log in to an SSH server. When omitted, the username of the current session is used.
<IPv4>	Specifies the SSH server to which the SSH client will connect as an IPv4 address.
<HOSTNAME>	Specifies the SSH server to which the SSH client will connect as a host name.
vrf <VRF-NAME>	Specifies the VRF to be used for the SSH client session. When omitted, the default VRF named <code>default</code> is used.
port <PORT-NUMBER>	Specifies the SSH server TCP port number. When omitted, the default TCP port 22 is used.

Examples

Establishing an SSH client session (using the management VRF) with an SSH server:

```
switch# ssh admin@10.0.11.180 vrf mgmt
```

Establishing an SSH client session (using the default VRF and a specific port) with an SSH server:

```
switch# ssh admin@10.0.11.175 port 223
```

Configuring a test user on switch 1 and then connecting to switch 1 from switch 2 using the SSH client on the mgmt VRF:

```
** Configuring a test user on switch 1 **
switch(config)# user-group test
switch(config-usr-grp-test)# permit cli command ".*"
switch(config)# exit
switch(config)# user test-user group test password plaintext tst#9J

** On switch 2, connecting to switch 1 using the SSH client **
switch# ssh test-user@10.0.11.177 vrf mgmt
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Manager (#)	Administrators or local user group members with execution rights for this command.

Local AAA on your Aruba CX switch provides:

- Authentication using local password or SSH public key.
- Authorization using local role-based access control (RBAC). Optional per-command authorization is possible through configuration of user-defined local user groups, with command authorization rules applied to respective group members.
- Accounting of user activity on the switch using accounting logs.



For switches that support multiple management modules such as the Aruba 8400, all AAA functionality discussed only applies to the active management module. See also *AAA on switches with multiple management modules* in the *High Availability Guide*.

Local AAA defaults and limits

Setting	Default value / limit
Local authentication	Enabled by default for all connection types: console, SSH, and REST.
Local role-based access control (RBAC) authorization	Enabled by default for all connection types: console, SSH, and REST.
Local accounting	Enabled.
Maximum number of local users	64 users, including the default <code>admin</code> user.
Maximum number of user-defined local user groups	32 groups, including the three built-in groups <code>administrators</code> , <code>operators</code> , <code>auditors</code> .
Password for default admin account	The password is empty by default.
SSH public key authentication	Enabled.

Supported platforms and standards

Local AAA is supported on the 4100i, 6000, 6100, 6200, 6300, 6400, 8320, 8325, 8360, 8400, 9300, and 10000 Switch Series.

Scale

Setting	Default value / limit
Local authentication	Enabled by default for all connection types: console, SSH, and REST.
Local role-based access control (RBAC) authorization	Enabled by default for all connection types: console, SSH, and REST.
Local accounting	Enabled.
Maximum number of local users	64 users, including the default admin user.
Maximum number of user-defined local user groups	32 groups, including the three built-in groups administrators , operators , auditors .
Password for default admin account	The password is empty by default.
SSH public key authentication	Enabled.

Local authentication

Authentication identifies users, validates their credentials, and grants switch access. Local authentication is either password-based or SSH public key-based.

Password-based local authentication

- Validates users with local user name and password credentials
- Is supported on all interfaces/channels (SSH, WebUI, Console, REST)
- Is enabled by default but can be superseded by remote authentication or with SSH client using SSH public key authentication

SSH public key-based local authentication

- Validates users identified with SSH public keys stored in the local user database
- Is supported on the SSH interface/channel with SSH client
- Takes precedence over password-based authentication whether local or remote
- Is enabled by default (also requires key configuration to work)

Local authentication tasks

The local authentication (local password and SSH public key) tasks are as follows:

Task	Command	Example
Enable authentication as local for the specified connection types	<pre>aaa authentication login</pre>	Enable local authentication for the default and console connection types: <pre>aaa authentication login default local aaa authentication login console local</pre>

Task	Command	Example
Show authentication configuration	show aaa authentication	show aaa authentication
Enable password-based authentication on minimum password length checking	aaa authentication minimum-password-length	aaa authentication minimum-password-length 12
Disable password-based authentication on minimum password length checking	aaa authentication minimum-password-length	no aaa authentication minimum-password-length
Enable local password-based authentication on login attempt limiting	aaa authentication limit-login-attempts	aaa authentication limit-login-attempts 4 lockout-time 20
Disable local password-based authentication on login attempt limiting	aaa authentication limit-login-attempts	no aaa authentication limit-login-attempts
Enable local password-based authentication for use with SSH clients (enabled by default)	ssh password-authentication	ssh password-authentication
Disable local password-based authentication for use with SSH clients	ssh password-authentication	no ssh password-authentication
Enable SSH	ssh public-	ssh public-key-authentication

Task	Command	Example
public key authentication (enabled by default)	key-authentication	
Disable SSH public key authentication	ssh public-key-authentication	no ssh public-key-authentication
Show state of local password-based (for SSH) and SSH public key authentication	show ssh authentication-method	show ssh authentication-method
Copying the client SSH public key into the key list	user authorized-key	user admin authorized-key ecdsa-sha2-nistp256 E2VjZH...QUiCAk= root@switch
Removing SSH public keys from the key list	user authorized-key	no user admin authorized-key 2
Showing the SSH client public key list	show user	show user admin authorized-key

Local authorization

Authorization controls authenticated users command execution and switch interaction privileges. Local authorization uses role-based access control (RBAC) to provide role-based privilege levels plus optional user-defined local user groups with command execution rules. Authorization occurs only after successful authentication.

- **Administrators** have full command execution and switch interaction privilege.
- **Operators** are limited to the use of several nonsensitive `show` commands.
- **Auditors** are limited to a few auditing-related commands.

Optional per-command authorization is available through configuration of user-defined local user groups with command authorization rules applied to respective group members. see [User-defined user groups](#) .

Local authorization tasks

The local authorization tasks are as follows:

Task	Command name	Example
Enable authorization as local RBAC for the specified connection types	aaa authorization commands	Enable local authorization for the default and console connection types: aaa authorization commands default local aaa authorization commands console local
Show authorization configuration	show aaa authorization	show aaa authorization

Local accounting

Local accounting is always active. It cannot be turned off.

This accounting information is captured and made available locally (using **show accounting log**) and, if desired, for sending to remote AAA servers:

- Exec Accounting: user login/logout events.
- Command accounting: commands executed by users.
- System accounting: remote accounting On/Off events.
- CLI show commands.
- Interactions on the non-CLI interfaces: REST and WebUI.

The following is not captured or made available as accounting information:

- CLI commands that reboot the switch.
- Interactions in the bash shell.



See also the **show accounting log** command.

Local accounting tasks

The local accounting tasks are as follows:

Task	Command name	Example
Enable accounting as local for the specified connection types	aaa accounting all-mgmt	Enable local accounting for the default and console connection types: aaa accounting all-mgmt default start-stop local aaa accounting all-mgmt console start-stop local
Show accounting configuration	show aaa accounting	show aaa accounting
Show local accounting log contents	show accounting log	show accounting log last 10

aaa accounting all-mgmt

```
aaa accounting all-mgmt <CONNECTION-TYPE> start-stop {local | group <GROUP-LIST>}  
no aaa accounting all-mgmt <CONNECTION-TYPE>
```

Description

Defines accounting as being local (with the name **local**) (the default). Or defines a sequence of remote AAA server groups to be accessed for accounting purposes.

For remote accounting, the information is sent to the first reachable remote server that was configured with this command for remote accounting. If no remote server is reachable, local accounting remains available. Each available connection type (channel) can be configured individually as either local or using remote AAA server groups. All server groups named in your command, must exist. This command can be issued multiple times, once for each connection type. Local is always available for any connection type not configured for remote accounting.



The system accounting log is not associated with any connection type (channel) and is therefore sent to the accounting method configured on the default connection type (channel) only.

The **no** form of this command removes for the specified connection type, any defined remote AAA server group accounting sequence. Local accounting is available for connection types without a configured remote AAA server group list (whether default or for the specific connection type).

Parameter	Description
<CONNECTION-TYPE>	One of these connection types (channels): default Defines a list of accounting server groups to be used for the default connection type. This configuration applies to all other connection types (console, https-server, ssh) that are not explicitly configured with this command. For example, if you do not use aaa accounting all-mgmt console... to define the console accounting list, then this default configuration is used for console. console Defines a list of accounting server groups to be used for the console connection type. https-server Defines a list of accounting server groups to be used for the https-server (REST, Web UI) connection type. ssh Defines a list of accounting server groups to be used for the ssh connection type.
start-stop	Selects accounting information capture at both the beginning and

Parameter	Description
	end of a process.
local	Selects local-only accounting when used without the group parameter.
group <GROUP-LIST>	Specifies the list of remote AAA server group names. Each name can be specified one time. Predefined remote AAA group names tacacs and radius are available. Although not a group name, predefined name local is available. User-defined TACACS+ and RADIUS server group names may also be used. The remote AAA server groups are accessed in the order that the group names are listed in this command. Within each group, the servers are accessed in the order in which the servers were added to the group. Server groups are defined using command aaa group server and servers are added to a server group with the command server. If the AAA server(s) in the group are not reachable, or the if there is a key mismatch error between the server and the switch, the next accounting method is attempted.

Usage

Local accounting is always active. It cannot be turned off.

Examples

Setting local accounting for the default connection type:

```
switch(config)# aaa accounting all-mgmt default start-stop local
```

Setting local accounting for the console connection type:

```
switch(config)# aaa accounting all-mgmt console start-stop local
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

aaa authentication console-login-attempts

```
aaa authentication console-login-attempts <ATTEMPTS> console-lockout-time <LOCKOUT-TIME>
no aaa authentication console-login-attempts
```

Description

For the console interface (channel) only, enables console login attempt limiting. If the number of failed console login attempts equals the configured threshold, the user is locked out for the configured duration.

The **no** form of this command disables console login attempt limits.



Important: If you enable the lockout using this command and also enable the SSH, REST, and Telnet lockout using command **aaa authentication limit-login-attempts**, and then enter too many consecutive wrong passwords, you may become locked out, and will have to wait for the configured lockout time to elapse before logging in on any interface.



This console login attempt limiting feature is only available when not using remote authentication through AAA servers (TACACS+ or RADIUS) on any interface. Remote authentication through AAA servers (TACACS+ or RADIUS) is not possible when limit login attempts is configured on any interface.

Parameter	Description
<ATTEMPTS>	Specifies the threshold of failed console login attempts that triggers user lockout. Range: 1 to 10. For example, if <ATTEMPTS> is set to 1 , a single failed login attempt triggers immediate user lockout.
<LOCKOUT-TIME>	Specifies the amount of time a user is locked out. Range: 1 to 3600 seconds.

Examples

Enabling console login attempt failure limiting with a 60 second lockout being triggered upon the third consecutive login attempt failure.

```
switch(config)# aaa authentication console-login-attempts 3 console-lockout-time 60
```

Disabling console login attempt failure limiting:

```
switch(config)# no aaa authentication console-login-attempts
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

aaa authentication limit-login-attempts

aaa authentication limit-login-attempts <ATTEMPTS> logout-time <LOCKOUT-TIME>
no aaa authentication limit-login-attempts <ATTEMPTS> logout-time <LOCKOUT-TIME>

Description

For the SSH, REST, and Telnet interface (channel), enables local login attempt limiting. If the number of failed local login attempts equals the configured threshold, the user is locked out for the configured duration.

The **no** form of this command disables local login attempt limits.



Important: If you enable the lockout using this command and also enable the console lockout using command **aaa authentication console-login-attempts**, and then enter too many consecutive wrong passwords, you may become locked out, and will have to wait for the configured lockout time to elapse before logging in on any interface.



This local login attempt limiting feature is only available when not using remote authentication through AAA servers (TACACS+ or RADIUS) on any interface. Remote authentication through AAA servers (TACACS+ or RADIUS) is not possible when limit login attempts is configured on any interface.

Parameter	Description
<ATTEMPTS>	Specifies the threshold of failed local login attempts that triggers user lockout. Range: 1 to 10. For example, if <ATTEMPTS> is set to 1 , a single failed login attempt triggers immediate user lockout.
<LOCKOUT-TIME>	Specifies the amount of time a user is locked out. Range: 1 to 3600 seconds.

Examples

Enabling local login attempt failure limiting with a 20 second lockout being triggered upon the fourth consecutive login attempt failure.

```
switch(config)# aaa authentication limit-login-attempts 4 logout-time 20
```

Disabling login attempt failure limiting:

```
switch(config)# no aaa authentication limit-login-attempts
```

Command History

Release	Modification
10.11	Added Telnet support on the 10000, 9300, 83xx, 6100, 6000 and 4100i Switch Series.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

aaa authentication login

```
aaa authentication login <CONNECTION-TYPE> {local | group <GROUP-LIST>}
no aaa authentication login <CONNECTION-TYPE> {local | group <GROUP-LIST>}
```

Description

Defines authentication as being local (with the name **local**) (the default). Or defines a sequence of remote AAA server groups to be accessed for authentication purposes. Each available connection type (channel) can be configured individually as either local or using remote AAA server groups. All server groups named in your command, must exist. This command can be issued multiple times, once for each connection type. Local is always available for any connection type not configured for remote AAA authentication.

The **no** form of this command removes for the specified connection type, any defined remote AAA server group authentication sequence. Local authentication is available for connection types without a configured remote AAA server group list (whether default or for the specific connection type).

Parameter	Description
<CONNECTION-TYPE>	One of these connection types (channels): default Defines a list of accounting server groups to be used for the default connection type. This configuration applies to all other connection types (console, https-server, ssh) that are not explicitly configured with this command. For example, if you do not use <code>aaa accounting all-mgmt console...</code> to define the console accounting list, then this default configuration is used for console. console Defines a list of accounting server groups to be used for the console connection type. https-server Defines a list of accounting server groups to be used for the https-server (REST, Web UI) connection type. ssh Defines a list of accounting server groups to be used for the ssh connection type.
local	Selects local-only accounting when used without the group parameter.
group <GROUP-LIST>	Specifies the list of remote AAA server group names. Each name can be specified one time. Predefined remote AAA group names tacacs and radius are available. Although not a group name, predefined name local is available. User-defined TACACS+ and RADIUS server group names may also be used. The remote AAA server groups are accessed in the order that the group names are listed in this command. Within each group, the servers are accessed in the order in which the servers were added

Parameter	Description
	to the group. Server groups are defined using command aaa group server and servers are added to a server group with the command server . If no AAA server(s) in the group are reachable, or if there is a key mismatch error between the server and the switch, the next authentication method is attempted.

Examples

Setting local authentication for the default connection type:

```
switch(config)# aaa authentication login default local
```

Setting local authentication for the console connection type:

```
switch(config)# aaa authentication login console local
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

aaa authentication minimum-password-length

```
aaa authentication minimum-password-length <LENGTH>
no aaa authentication minimum-password-length <LENGTH>
```

Description

Enables minimum password length checking. Existing passwords shorter than the minimum length are unaffected. Length checking does not apply to ciphertext passwords. Length checking applies both to local and remote authentication.

The **no** form of this command disables minimum password length checking.

Parameter	Description
<LENGTH>	Specifies the minimum password length. Range: 1 to 32.

Examples

Enabling password length checking, with a minimum length of 12.

```
switch(config)# aaa authentication minimum-password-length 12
```

Disabling minimum password length checking:

```
switch(config)# no aaa authentication minimum-password-length
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

aaa authorization commands (local)

```
aaa authorization commands <CONNECTION-TYPE> {local | none}
no aaa authorization commands <CONNECTION-TYPE> {local | none}
aaa authorization commands <CONNECTION-TYPE> group <GROUP-LIST>
no aaa authorization commands <CONNECTION-TYPE> group <GROUP-LIST>
```

Description

Defines authorization as being basic local RBAC (specified as **none**), or as full-fledged local RBAC specified as **local** (the default), or as remote TACACS+ (specified with `group <GROUP-LIST>`). Each available connection type (channel) can be configured individually. All server groups named in the command, must exist. This command can be issued multiple times, once for each connection type.

The **no** form of this command unconfigures authorization for the specified connection type, reverting to the default of **local**.



Although only TACACS+ servers are supported for remote authorization, local authorization (basic or full-fledged) can be used with remote RADIUS authentication. If your switch uses command authorization, best practices is to configure [authorization fail-through](#) before configuring authentication fail-through. If not, the switch may fall into an unusable state where authorization will fail for all commands.

Parameter	Description
<CONNECTION-TYPE>	One of these connection types (channels): default Selects the default connection type for configuration. This configuration applies to all other connection types (console , ssh) that are not explicitly configured with this command. For example, if you do not use aaa authentication commands console... to define the console authorization list, then this

Parameter	Description
	default configuration is used for console. <code>console</code> Selects the console connection type for configuration. <code>ssh</code> Selects the ssh connection type for configuration.
<code>local</code>	When used alone without <code>group <GROUP-LIST></code>, selects local authorization which can be used to provide authorization for a purely local setup without any remote AAA servers and also for when RADIUS is used for remote Authentication and Accounting but Authorization is local. When used after <code>group</code>, provides for fallback (to full-fledged local authorization) when every server in every specified TACACS+ server group cannot be reached. NOTE: If any TACACS+ server in the specified groups is reachable, but the command fails to be authorized by that server, the command is rejected and local authorization is never attempted. Local authorization is only attempted if every TACACS+ server cannot be reached.
<code>none</code>	When used alone without <code>group <GROUP-LIST></code>, selects basic local RBAC authorization, for use with the built-in user groups (administrators, operators, auditors). When used after <code>group</code>, provides for fallback (to basic local RBAC authorization) when every server in every specified TACACS+ server group cannot be reached. NOTE: With none, for users belonging to user-defined user groups, all commands can be executed regardless of what authorization rules are defined in such groups. For per-command local authorization, use local instead.
<code>group <GROUP-LIST></code>	Specifies the list of remote AAA server group names. Predefined remote AAA group name tacacs is available. User-defined TACACS+ server group names may also be used. The remote AAA server groups are accessed in the order that the group names are listed in this command. Within each group, the servers are accessed in the order in which the servers were added to the group. Server groups are defined using command aaa server group and servers are added to a server group using command server. It is recommended to always include either the special name local or none as the last name in the group list. If both local or none are omitted, and no remote AAA server is reachable (or the first reachable server cannot authorize the command), command execution for the current user will not be possible. If no AAA server(s) in the group are reachable, or if there is a key mismatch error between the server and the switch, the next authorization method is attempted.

Examples

Setting the authorization for default to **local**:

```
switch(config)# aaa authorization commands default local
```

Setting the authorization for the SSH interface to **none**:


```
switch(config)# aaa authorization commands ssh none
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

show aaa accounting

```
show aaa accounting [vsx-peer]
```

Description

Shows the accounting configuration per connection type (channel).

Parameter	Description
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Example

Configuring and then showing local accounting for the default and console connection types:

```
switch(config)# aaa accounting all default start-stop local
switch(config)# aaa accounting all console start-stop local
switch(config)# exit
switch# show aaa accounting
AAA Accounting:
  Accounting Type           : all
  Accounting Mode           : start-stop
```

Accounting for default channel:

```
-----
GROUP NAME                | GROUP PRIORITY
-----
local                      | 0
-----
```

Accounting for console channel:

```
-----
GROUP NAME                | GROUP PRIORITY
-----
```

```
local | 0
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show aaa authentication

```
show aaa authentication [vsx-peer]
```

Description

Shows the authentication configuration per connection type (channel).

Parameter	Description
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Example

Configuring and then showing local authentication for the default and console connection types (channels):

```
switch(config)# aaa authentication login default local
switch(config)# aaa authentication login console local
switch(config)# exit
switch# show aaa authentication
```

```
AAA Authentication:
  Fail-through           : Disabled
  Limit Login Attempts   : Not set
  Lockout Time           : 300
  Minimum Password Length: Not set
```

```
Authentication for default channel:
```

```
-----
GROUP NAME | GROUP PRIORITY
-----
```

```
local | 0
-----
```

```
Authentication for console channel:
```

```
-----  
GROUP NAME | GROUP PRIORITY  
-----  
local | 0  
-----
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show aaa authorization

```
show aaa authorization [vsx-peer]
```

Description

Shows the authorization configuration per connection type (channel).

Parameter	Description
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Example

Configuring and then showing full-fledged local RBAC authorization for the default and console connection types (channels):

```
switch(config)# aaa authorization commands default none  
switch(config)#  
switch(config)# aaa authorization commands console none  
switch(config)# exit  
switch#  
switch# show aaa authorization  
Authorization for default channel:  
-----  
GROUP NAME | GROUP PRIORITY  
-----  
none | 0  
-----
```

Authorization for console channel:

```
-----  
GROUP NAME | GROUP PRIORITY  
-----  
none | 0  
-----
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show authentication locked-out-users

show authentication locked-out-users

Description

Shows a list of users currently locked out due to excessive failed login attempts. This applies to console, REST, SSH, WebUI, and telnet logins.

Example

Showing locked-out users.

```
switch# show authentication locked-out-users
USER                                GROUP
-----
admin                               administrators
admin-1                             administrators
```

Command History

Release	Modification
10.11	The output of this command now also includes information for users locked out due to excessive REST login attempts.
10.09	Command introduced.

Command Information

Platforms	Command context	Authority
All platforms	Manager (#)	Administrators or local user group members with execution rights for this command.

show ssh authentication-method

show ssh authentication-method

Description

Shows the status of the SSH public key method and the local password-based (through SSH client) authentication method.

Example

Showing the authentication methods.

```
switch# show ssh authentication-method
SSH publickey authentication : Enabled
SSH password authentication  : Enabled
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show user

show user <USERNAME> authorized-key

Description

Shows the SSH client public key list for a specified user.

Parameter	Description
<USERNAME>	Specifies the username for which you want to show the SSH client public key list.

Usage

Any user can show their own public key list; however, administrators can also show a public key list of other users.

Examples

Showing a client public key:

```
switch# show user admin authorized-key

1. Key Type : RSA      Key size : 2048
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQDMtyMBmmAaF6r1zxf3DZNHSYVHBjhlbBlyAIqQ8DSHK
...
U+aE14UW/ifiukmK67sIHwK+FhhRYwPztQc5pjyOPk128a4pgKQaHCcOF169Z admin@switch
```

Showing two client public keys:

```
switch# show user admin authorized-key
1. Key Type : ECDSA    Curve : nistp256
ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBEqEFevZ0
...
176V+D0svdCJ9Wo32zqI9OeAdTJw/eZYp5qknhNgS81HjAI6J/4/kAqdZAjbqQUiCAk= admin@switch

2. Key Type : RSA      Key size : 2048
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQDXQHrqV7+/GcMdOhr//IRjJkX7TQKupW89j80bL7xq8
...
j8qKuHWSN0/h/HxjzQJuYDVmZN5vG3DhpXbBZU1ZNnchVod13QLCesqA3VLKN admin@switch
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

ssh password-authentication

`ssh password-authentication`

`no ssh password-authentication`

Description

Enables the password-based authentication method for use with SSH clients.

The **no** form of this command disables the password-based authentication method for use with SSH clients.

Usage

The switch ships with password-based authentication (for SSH clients) enabled. The maximum number of password retries is three.

Examples

Enabling password authentication for use with SSH clients:

```
switch(config)# ssh password-authentication
```

Disabling password authentication for use with SSH clients:

```
switch(config)# no ssh password-authentication
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	<code>config</code>	Administrators or local user group members with execution rights for this command.

ssh public-key-authentication

```
ssh public-key-authentication
no ssh public-key-authentication
```

Description

Enables the SSH public key authentication method. The switch ships with SSH public key authentication enabled.

The **no** form of this command disables the SSH public key authentication method.



Although SSH public key authentication is enabled by default, it cannot be used until SSH public keys are added with the **user authorized-key** command.

Examples

Enabling SSH public key authentication:

```
switch(config)# ssh public-key-authentication
```

Disabling SSH public key authentication:

```
switch(config)# no ssh public-key-authentication
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

user authorized-key

```
user <USERNAME> authorized-key <PUBKEY>
no user <USERNAME> authorized-key [<KEYNUM>]
```

Description

Copies an SSH client public key into the key list. If the key list and the public key do not exist, it creates a list with the public key. If the SSH client public key exists, the command appends the new key to the existing list. The client public key list holds a maximum of 32 client keys.

The **no** form of the command removes either one or all SSH public keys from the key list.

Parameter	Description
<USERNAME>	Specifies the name of the user.
<PUBKEY>	Specifies the SSH client public key to be copied into the key list.
<KEYNUM>	Specifies the key number. The range is 1 to 32. Use the show user <USERNAME> authorized-key command to find the key number associated with the key.

Usage

Each key on the key list has a key identifier. The **show user <USERNAME> authorized-key** command displays the key identifier associated with the key.

Administrators can add and remove the public keys of themselves and other users. Operators can add and remove only their own public keys. If the public key authentication method is enabled, the client public key present is used by the SSH server to authenticate the client. The authentication method reverts to the password authentication method and prompts for a client password when one of the following occurs:

- The client public keys are not present.
- The server does not have the keys enabled.
- The public key method is disabled.

You can either remove all keys or a specific key. Each key on the key list has a key identifier. If you provide the key identifier in this command, the command removes the corresponding key from the list. If you provide no key identifier, the command removes all keys from the key list.

Examples

Adding a public key:

```
switch(config)#user admin authorized-key ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBEqEFevZ0l76V+D0svdCJ9Wo32zqI9OeAIdTJwT/eZYp50qkAnhZNgS81HBjAI6QJ/4/kAyqdZ9oAjbicQUiCAk= root@switch
```

Removing all SSH public keys from the list:

```
switch(config)# no user admin authorized-key
```

Removing the specified SSH public key from the list:

```
switch(config)# no user admin authorized-key 2
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

Remote AAA with TACACS+ provides the following for your Aruba CX switch:

- Authentication using remote TACACS+ AAA servers.
- Authorization using remote TACACS+ AAA servers, providing fine-grained command authorization. Optional user-defined local user groups with configured command authorization rules can be used to provide authorization fallback protection for when TACACS+ servers become temporarily unavailable.
- Transmission of locally collected accounting information to remote TACACS+ servers.



For switches that support multiple management modules such as the Aruba 8400, all AAA functionality discussed only applies to the active management module. See also *AAA on switches with multiple management modules* in the *High Availability Guide*.

Parameters for TACACS+ server

When creating a TACACS+ server for AAA, you must configure the following parameters using the `tacacs-server host` command:

Parameter	Description
<code>{<FQDN> <IPV4> <IPV6>}</code>	Specifies the TACACS+ server as: ▪ <code><FQDN></code>: a fully qualified domain name. ▪ <code><IPV4></code>: an IPv4 address. ▪ <code><IPV6></code>: an IPv6 address.
<code>key [plaintext <PASSKEY> ciphertext <PASSKEY>]</code>	Selects either a plaintext or an encrypted local shared-secret passkey for the server. As per RFC 2865, shared-secret can be a mix of alphanumeric and special characters. Plaintext passkeys are between 1 and 32 alphanumeric and special characters. NOTE: When <code>key</code> is entered without either sub-parameter, plaintext passkey prompting occurs upon pressing Enter. Enter must be pressed immediately after the <code>key</code> parameter without entering other parameters. The entered passkey characters are masked with asterisks. When <code>key</code> is omitted, the server uses the global passkey. This command requires either the global or local passkey to be set; otherwise the server will not be contacted. The command <code>tacacs-server key</code> is available for setting the global passkey.
<code>timeout <TIMEOUT-SECONDS></code>	Specifies the timeout. Range: 1 to 60 seconds. Default : 5 seconds.
<code>port <PORT-NUMBER></code>	Specifies the TCP authentication port number. Range: 1 to 65535. Default: 49.

Parameter	Description
<code>auth-type {pap chap}</code>	Selects either the PAP (the default) or CHAP authentication types. If this parameter is not specified, the TACACS+ global default is used.
<code>tracking {enable disable}</code>	Enables or disables server tracking for the RADIUS server. Tracked servers are probed at the start of each server tracking interval to check if they are reachable. Use command tacacs-server tracking to configure TACACS+ server tracking globally.
<code>vrf <VRF-NAME></code>	Specifies the VRF name to be used for communicating with the server. If no VRF name is provided, the default VRF named <code>default</code> is used.

Default server groups

The switch always has these four default groups:

- `tacacs`: for remote AAA, always contains every configured TACACS+ server.
- `radius`: for remote AAA, always contains every configured RADIUS server.
- `local`: for local authentication.
- `none`: for local (RBAC) authorization.

User-defined AAA servers are always added to the matching default group, either **tacacs** or **radius**. A maximum of 28 user-defined groups can be created.



- On the 4100i, 6000, 6100, 6200, 6300, 6400, 8100, 8325, 8360, and 10000 Switch Series, a RADIUS server can be associated with a maximum of four different user-defined server groups.
- On the 8320, 8400, and 9300 Switch Series, a RADIUS server can be associated with only one user-defined server group.

The order in which servers are added to a group is important. The server added first is accessed first, and if necessary, the second server is accessed second, and so on.

Supported platforms and standards

Remote AAA with TACACS+ is supported on the 4100i, 6000, 6100, 6200, 6300, 6400, 8100, 8320, 8325, 8360, 8400, 9300, and 10000 Switch Series.



TACACS VxLAN overlay (IPv4 and IPv6) is supported on the following platforms only: 6300, 6400, 8100, and 8360.
TACACS Static VxLAN underlay (IPv4) is supported on the 6200 platform.

Setting	Default value / limit
Authentication of REST sessions with TACACS+	Disabled

Setting	Default value / limit
Maximum number of TACACS+ servers in an AAA group	16
Maximum number of TACACS+ servers that can be configured	16
Maximum number of user-defined AAA server groups that can be configured	28
TACACS+ authentication	Disabled
TACACS+ authentication global timeout	5 seconds
TACACS+ authentication passkey (shared secret)	None
TACACS+ authentication tcp-port	49
TACACS+ global authentication protocol	PAP
TACACS+ server tracking default interval	300 seconds
TACACS+ server access through the default VRF	default*

*The default value is **default**, unless another VRF is specified during the server configuration.

About global versus per-TACACS+ server passkeys (shared secrets)

To communicate with a TACACS+ AAA server, the switch must have a passkey (shared secret) configured that matches what is configured on the server. Use one of these commands to achieve the desired configuration:

- For a global passkey common to every TACACS+ server, use **tacacs-server key**.
- For a per-TACACS+ server passkey, use **tacacs-server host** with the **key** parameter.



If both passkeys are configured on the switch, the per-TACACS+ server passkey is used.

Remote AAA TACACS+ server configuration requirements

The user-supplied TACACS+ server must:

- Have an IPv4/IPv6 address or fully qualified domain name (FQDN) that is visible to the switch.
- Have a passkey (shared secret) that matches what is configured on the switch.
- Provide username and password definitions for every switch user. Remote users do not require definition on the switch.
- Configure user role assignment using TACACS+ attributes.
- Have any needed command authorization configured to control what commands (per user or user role) will be executable on the switch.



Consult your TACACS+ server documentation for installation and general configuration details.



If SSH public key authentication is used, the key information is stored locally on the switch, making username and password definition on the TACACS+ server unnecessary.

User role assignment using TACACS+ attributes

User role assignment is configured on the TACACS+ server using VSAs (vendor-specific attributes) and TACACS+ specified attributes.

TACACS+ servers can return multiple attribute value pairs (AVPs) in response to an authentication request. The attributes are processed in this order of precedence to determine the user role assigned:

- If the **Aruba-Admin-Role** VSA is present, map the user to the matching corresponding local user-group name.
 - Else if the **priv-lvl** TACACS+ specified attribute is present, extract the privilege level (1, 15, or 19) and map the user to the local user-group corresponding to this privilege level (**1=operators**, **15=administrators**, **19=auditors**). Privilege levels 2 to 14 may also be used with matching local user groups named 2 to 14.
 - Otherwise, the user role cannot be determined, and authentication fails.

Aruba-Admin-Role	priv-lvl	User role assigned
<GROUP-NAME>	Do not care	Matching local user <GROUP-NAME>
Not present	1	Operators
Not present	15	Administrators
Not present	19	Auditors
Not present	2 to 14	Matching local user groups named 2 to 14
Not present	Not present	None (not authenticated)

TACACS+ server redundancy and access sequence

To prevent authentication and authorization interruption, it is common practice to configure more than one TACACS+ server. When identifying TACACS+ servers to the switch, server group order (and server order within the group), determines server access order.



When defining the server access sequence for authentication with **aaa authentication login default**, there is an implied `local` included as the last item in the list. If no TACACS+ server can be reached, local authentication will be attempted.



When defining the server access sequence for authorization with **aaa authorization commands**, it is recommended to always include either `local` or `none` as the last item in the list.

Single source IP address for consistent source identification to AAA servers



If applicable to your installation, it is recommended that you perform the optional configuration mentioned in this section.

If your topology allows the AAA server to be reached through multiple paths, the server interprets the incoming packets to be from different switches even though they are all coming from the same switch. Having a switch associated with multiple IP addresses makes it more difficult to interpret system logs and accounting data.

To ensure that all traffic sent from the switch to the AAA server uses the same source IP address, use **ip source-interface** or **ipv6 source-interface**. These two commands plus the related commands **show ip source-interface** and **show ipv6 source-interface** are described under *Layer 2/3 Interface commands* in the *Command-Line Interface Guide*.

TACACS+ general tasks

General TACACS+ tasks, not specific to authentication, authorization, or accounting, are as follows:

Task	Command name	Example
Configuring a TACACS+ server	<code>tacacs-server host</code>	<code>tacacs-server host 1.1.1.1 vrf default</code> <code>no tacacs-server host 1.1.1.1 vrf default</code>
Showing global and TACACS+ server configurations	<code>show tacacs-server</code>	<code>show tacacs-server detail</code>
Configuring a TACACS+ server group	<code>aaa group server</code>	<code>aaa group server tacacs sgl</code> <code>no aaa group server tacacs sgl</code>
Showing server groups	<code>show aaa server-groups</code>	<code>show aaa server-groups</code>
Adding a TACACS server to a server-group	<code>server</code>	<code>aaa group server tacacs sgl</code> <code>server 1.1.1.2 port 32 vrf default</code>
Deleting a TACACS server from a server-group	<code>server</code>	<code>aaa group server tacacs sgl</code> <code>no server 1.1.1.2 port 32 vrf default</code>
Configuring a TACACS+ global passkey	<code>tacacs-server key</code>	<code>tacacs-server key plaintext mypasskey123</code>
Configuring PAP or CHAP for TACACS+	<code>tacacs-server auth-type</code>	<code>tacacs-server auth-type chap</code> <code>no tacacs-server auth-type</code>
Configuring the TACACS+ global timeout	<code>tacacs-server timeout</code>	<code>tacacs-server timeout 20</code> <code>no tacacs-server timeout</code>

TACACS+ authentication

TACACS+ authentication occurs as follows:

- User credentials are sent from the switch to TACACS+ server using the PAP or CHAP authentication protocol.
- If a user is authenticated, their role is communicated to the switch as Administrator, Operator, or Auditor.
- An unknown user or a user who entered an invalid password is identified as such to the switch, which then rejects user login.

About authentication fail-through

Normally, authentication is performed by the first AAA server reached. A rarely needed feature named "Authentication fail-through" is available. If authentication fail-through is enabled and authentication fails on the first reachable AAA server, authentication is attempted on the second AAA server, and so on, until successful authentication or the server list is exhausted.

Enabling Authentication fail-through is typically unnecessary because the user credential databases should be consistent across all AAA servers. Authentication fail-through might be helpful if your AAA user credential databases are not quickly synchronized across all AAA servers.



[Authentication fail-through](#), [authorization fail-through](#), and [accounting fail-through](#) must each be configured separately.

TACACS+ authentication tasks

The TACACS+ authentication-related tasks are as follows:

Task	Command name	Example
Configuring the authentication sequence for the default connection type	aaa authentication login	aaa authentication login default group tg1 tg2 tacacs local
Configuring the authentication sequence for the console connection type	aaa authentication login	aaa authentication login console group tg2 tg3 tacacs local
Configuring the authentication sequence for the ssh connection type	aaa authentication login	aaa authentication login ssh group tg2 tacacs local
Removing remote AAA for the default connection type	aaa authentication login	no aaa authentication login default

Task	Command name	Example
Configuring authentication fail-through	aaa authentication allow-fail-through	aaa authentication allow-fail-through no aaa authentication allow-fail-through
Showing the authentication sequence	show aaa authentication	show aaa authentication

TACACS+ authorization

Upon successful user authentication, the user is assigned their role by the TACACS+ server. See also [User role assignment using TACACS+ attributes](#).

TACACS+ authorization provides command filtering to allow/disallow individual command or command set execution. Each command is sent to the TACACS+ server for approval, and the switch then allows/disallows command execution according to the server response.



TACACS+ authorization applies only to the CLI interface.

Using local authorization as fallback from TACACS+ authorization

Local authorization can be used for the situation in which communication is lost with all TACACS+ servers after a successful authentication. Users that are members of the built-in local user groups (**administrators**, **operators**, or **auditors**) are authorized according to the fixed roles and privilege levels of those groups. Optionally, local user-defined user groups can be configured with specific command execution rules per group. Users that are members of such groups, are authorized according to the command execution rules of the group to which they belong. For configuring local user groups, see **user-group**.

About authentication fail-through and authorization



Rare potential out-of-synchronization situation when using authentication fail-through: Successful authentication on one server can be followed by authorization denial on another. The user is known on the server doing the authentication but unknown on the server attempting the authorization. This situation typically arises only during brief periods in which user credential databases are not synchronized across all TACACS+ servers. See also TACACS+ server authorization considerations in [aaa authorization commands](#).

TACACS+ authorization tasks

The TACACS+ authorization-related tasks are as follows:

Task	Command name	Example
Configuring	aaa	aaa authorization commands default group tgl tacacs local

Task	Command name	Example
the authorization sequence for the default connection type	authorization commands	
Configuring the authorization sequence for the console connection type	aaa authorization commands	aaa authorization commands console group tg1 tg2 tacacs none
Removing remote AAA for the default connection type	aaa authorization commands	no aaa authorization commands default
Showing the TACACS+ authorization sequence	show aaa authorization	show aaa authorization

TACACS+ accounting

This accounting information is captured and made available for sending to remote accounting servers:

- Exec Accounting: user login/logout events.
- Command accounting: commands executed by users.
- System accounting: remote accounting On/Off events.
- CLI show commands.
- Interactions on the non-CLI interfaces: REST and WebUI.

The following is not captured or made available as accounting information:

- CLI commands that reboot the switch.
- Interactions in the bash shell.



Local accounting (always enabled) must be functioning properly for remote Accounting to work.



The accounting information is sent to the first reachable remote TACACS+ AAA server (configured for remote accounting). If no remote TACACS+ server is reachable, local accounting remains available.

Sample accounting information on a TACACS+ server

```

Mon May 9 17:52:32 10.10.11.1 UNKNOWN tty 0.0.0.0 start task_id=1525899775430
timezone=UTC start_time=1525913552.428 service=system event=sys_acct
reason="System-accounting-ON" result=success
Mon May 9 17:52:48 10.10.11.1 admin tty 192.168.1.20 start task_id=1525899775431
timezone=UTC start_time=1525913567.611 service=shell priv_lvl=15 result=success
Mon May 9 17:52:48 10.10.11.1 admin tty 192.168.1.20 stop task_id=1525899775432
timezone=UTC stop_time=1525913567.614 service=shell priv_lvl=15 cmd="enable"
result=success
Mon May 9 17:52:51 10.10.11.1 admin tty 192.168.1.20 stop task_id=1525899775433
timezone=UTC stop_time=1525913570.851 service=shell priv_lvl=15
cmd="configure" result=success
Mon May 9 17:52:53 10.10.11.1 admin tty 192.168.1.20 stop task_id=1525899775434
timezone=UTC stop_time=1525913573.427 service=shell priv_lvl=15 cmd="interface
1/1/3" result=success
Mon May 9 17:52:54 10.10.11.1 admin tty 192.168.1.20 stop task_id=1525899775435
timezone=UTC stop_time=1525913574.447 service=shell priv_lvl=15 cmd="no
shutdown" result=success
Mon May 9 17:52:58 10.10.11.1 admin tty 192.168.1.20 stop task_id=1525899775436
timezone=UTC stop_time=1525913578.131 service=shell priv_lvl=15 cmd="ip
address 10.10.13.1/24" result=success
Mon May 9 17:52:59 10.10.11.1 admin tty 192.168.1.20 stop task_id=1525899775437
timezone=UTC stop_time=1525913579.468 service=shell priv_lvl=15 cmd="exit"
result=success
Mon May 9 17:53:10 10.10.11.1 admin tty 192.168.1.20 stop task_id=1525899775442
timezone=UTC stop_time=1525913590.204 service=shell priv_lvl=15 cmd="exit"
result=success
Mon May 9 17:53:10 10.10.11.1 admin tty 192.168.1.20 stop task_id=1525899775431
timezone=UTC stop_time=1525913590.205 service=shell priv_lvl=15 result=success
Mon May 9 17:53:44 10.10.11.1 UNKNOWN tty 0.0.0.0 stop task_id=1525899775430
timezone=UTC stop_time=1525913624.473 service=system event=sys_acct
reason="System-accounting-OFF" result=successMon May 9 17:52:32 10.10.11.1
UNKNOWN tty 0.0.0.0 start task_id=1525899775430 timezone=UTC start_
time=1525913552.428 service=system event=sys_acct reason="System-accounting-ON"
result=success
Mon May 9 17:52:48 10.10.11.1 admin tty 192.168.1.20 start task_id=1525899775431
timezone=UTC start_time=1525913567.611 service=shell priv_lvl=15 result=success
Mon May 9 17:52:48 10.10.11.1 admin tty 192.168.1.20 stop task_id=1525899775432
timezone=UTC stop_time=1525913567.614 service=shell priv_lvl=15 cmd="enable"
result=success
Mon May 9 17:52:51 10.10.11.1 admin tty 192.168.1.20 stop task_id=1525899775433
timezone=UTC stop_time=1525913570.851 service=shell priv_lvl=15
cmd="configure" result=success
Mon May 9 17:52:53 10.10.11.1 admin tty 192.168.1.20 stop task_id=1525899775434
timezone=UTC stop_time=1525913573.427 service=shell priv_lvl=15 cmd="interface
1/1/3" result=success
Mon May 9 17:52:54 10.10.11.1 admin tty 192.168.1.20 stop task_id=1525899775435
timezone=UTC stop_time=1525913574.447 service=shell priv_lvl=15 cmd="no
shutdown" result=success
Mon May 9 17:52:58 10.10.11.1 admin tty 192.168.1.20 stop task_id=1525899775436
timezone=UTC stop_time=1525913578.131 service=shell priv_lvl=15 cmd="ip
address 10.10.13.1/24" result=success
Mon May 9 17:52:59 10.10.11.1 admin tty 192.168.1.20 stop task_id=1525899775437
timezone=UTC stop_time=1525913579.468 service=shell priv_lvl=15 cmd="exit"
result=success
Mon May 9 17:53:10 10.10.11.1 admin tty 192.168.1.20 stop task_id=1525899775442
timezone=UTC stop_time=1525913590.204 service=shell priv_lvl=15 cmd="exit"
result=success
Mon May 9 17:53:10 10.10.11.1 admin tty 192.168.1.20 stop task_id=1525899775431
timezone=UTC stop_time=1525913590.205 service=shell priv_lvl=15 result=success
Mon May 9 17:53:44 10.10.11.1 UNKNOWN tty 0.0.0.0 stop task_id=1525899775430
timezone=UTC stop_time=1525913624.473 service=system event=sys_acct
reason="System-accounting-OFF" result=success

```



This sample is representative and not from any particular TACACS+ server implementation.

Sample REST accounting information on a TACACS+ server

```
Oct 30 16:31:56 10.10.10.1 admin tty 127.0.0.1 start task_id=1540942055868
timezone=UTC start_time=1540942316.36 service=https-server priv_lvl=15
cmd="http-method=POST http-uri=/rest/v1/login" result=success
```



This sample is representative and not from any particular TACACS+ server implementation.

TACACS+ accounting tasks

The TACACS+ accounting-related tasks are as follows:

Task	Command name	Example
Configuring the accounting sequence for the default connection type	aaa accounting all-mgmt	aaa accounting all-mgmt default start-stop group tg1 tg2 tacacs local
Configuring the accounting sequence for the console connection type	aaa accounting all-mgmt	aaa accounting all-mgmt console start-stop group tg2 tg3 tacacs local
Configuring the accounting sequence for the ssh connection type	aaa accounting all-mgmt	aaa accounting all-mgmt ssh start-stop group tg2 tacacs local
Removing remote AAA for the default connection type	aaa accounting all-mgmt	no aaa accounting all-mgmt default start-stop
Showing the accounting configuration	show aaa accounting	show aaa accounting

Example: Configuring the switch for Remote AAA with TACACS+

Prerequisites

- TACACS+ servers configured in general according to the information in [Remote AAA TACACS+ server configuration requirements](#). The exact settings appropriate to your environment will vary.
- Logged in to the switch with Administrator privilege and in the **config** context.

Procedure

1. Configure the global TACACS+ passkey (shared secret) as "xjKW74932qX3j_\$"

```
switch(config)# tacacs-server key plaintext xjKW74932qX3j_$
switch(config)#
```

2. Add these configuration details for two remote TACACS+ servers:

- Server 1 with IPv4 address 10.0.0.2, on the management interface (belonging to VRF "mgmt"), using the default PAP protocol.
- Server 2 with IPv4 address 4.0.0.2, on the data interface (belonging to VRF "default"), using the CHAP protocol.

```
switch(config)# tacacs-server host 10.0.0.2 vrf mgmt
switch(config)# tacacs-server host 4.0.0.2 auth-type chap
switch(config)#
```

3. Create a TACACS+ group named **tac_grp1**, assign TACACS+ server 10.0.0.2 to the group, show the group information.



The default TACACS+ group named `tacacs` includes every TACACS+ server regardless of whether any TACACS+ servers are also assigned to a user-defined TACACS+ group.

```
switch(config)# aaa group server tacacs tac_grp1
switch(config-sg)# server 10.0.0.2 vrf mgmt
switch(config-sg)# exit
switch(config)#
switch(config)# do show aaa server-groups tacacs

***** AAA Mechanism TACACS+ *****

-----
GROUP NAME          | SERVER NAME          | PORT | VRF      | PRIORITY
-----
tac_grp1            | 10.0.0.2             | 49   | mgmt     | 1
-----
tacacs (default)    | 10.0.0.2             | 49   | mgmt     | 1
tacacs (default)    | 4.0.0.2              | 49   | default  | 2
-----
switch(config)#
```

4. Define the authentication sequence list so that the new TACACS+ group is first, the default TACACS+ group is second, and local is third. Show the authentication sequence.

```

switch(config)# aaa authentication login default group tac_grp1 tacacs local
switch(config)#
switch(config)# do show aaa authentication
AAA Authentication:
  Fail-through           : Disabled
  Limit Login Attempts   : Not set
  Lockout Time           : 300
  Minimum Password Length : Not set

Default Authentication for All Channels:
-----
GROUP NAME                | GROUP PRIORITY
-----
tac_grp1                  | 0
tacacs                    | 1
local                     | 2
-----
switch(config)#

```

5. Define the authorization sequence list with two TACACS+ server groups plus local RBAC. Show the authorization sequence.

```

switch(config)# aaa authorization commands default group tac_grp1 tacacs local
switch(config)#
switch(config)# do show aaa authorization

Default command Authorization for All Channels:
-----
GROUP NAME                | GROUP PRIORITY
-----
tac_grp1                  | 0
tacacs                    | 1
local                     | 2
-----
switch(config)#

```

6. Define the accounting sequence list with two TACACS+ server groups. Show the accounting sequence.

```

switch(config)# aaa accounting all default start-stop group tac_grp1 tacacs
switch(config)#
switch(config)# do show aaa accounting
AAA Accounting:
  Accounting Type         : all
  Accounting Mode         : start-stop

Default Accounting for All Channels:
-----
GROUP NAME                | GROUP PRIORITY
-----

```

```

-----
tac_grp1                      | 0
tacas                        | 1
-----
-----

```

```

switch(config)# aaa accounting all default start-stop group tac_grp1 tacacs
switch(config)#
switch(config)# do show aaa accounting
AAA Accounting:
  Accounting Type              : all
  Accounting Mode              : start-stop

Default Accounting for All Channels:
-----
-----
GROUP NAME                      | GROUP PRIORITY
-----
-----
tac_grp1                      | 0
tacas                        | 1
-----
-----

```

```

switch(config)# aaa accounting all default start-stop group tac_grp1 tacacs
switch(config)#
switch(config)# do show aaa accounting
AAA Accounting:
  Accounting Type              : all
  Accounting Mode              : start-stop

Default Accounting for All Channels:
-----
-----
GROUP NAME                      | GROUP PRIORITY
-----
-----
tac_grp1                      | 0
tacas                        | 1
-----
-----

```

```

switch(config)# aaa accounting all default start-stop group tac_grp1 tacacs
switch(config)#
switch(config)# do show aaa accounting
AAA Accounting:
  Accounting Type              : all
  Accounting Mode              : start-stop

Default Accounting for All Channels:
-----
-----
GROUP NAME                      | GROUP PRIORITY
-----
-----
tac_grp1                      | 0
tacas                        | 1
-----
-----

```

Remote AAA with RADIUS is supported on the 4100i, 6000, 6100, 6200, 6300, 6400, 8320, 8325, 8360, 8400, 9300, and 10000 Switch Series.

Remote AAA with RADIUS provides the following for your Aruba CX switch:

- Authentication using remote RADIUS AAA servers. For added security, two-factor authentication may be used. In two-factor authentication, X.509 certificate-based authentication is combined with RADIUS authentication.
- Command authorization is not supported by RADIUS servers, however, user-defined local user groups can be configured with command-authorization rules, providing locally configured per-command authorization for members of such groups. See [User-defined user groups](#).

In the switch default state (without user-defined local groups), basic role-based authorization is available with the three built-in roles (**administrators**, **operators**, **auditors**).

- Transmission of locally collected accounting information to remote RADIUS servers.

AOS-CX supports IPv4 and IPv6 Radius over the VXLAN overlay network without additional configuration from the user.

Parameters for RADIUS server

When creating a RADIUS server for AAA, you must configure the following parameters using the [radius-server host](#) command:

Parameter	Description
{<FQDN> <IPv4> <IPv6>}	Specifies the RADIUS server as: ■ <FQDN>: a fully qualified domain name. ■ <IPv4>: an IPv4 address. ■ <IPv6>: an IPv6 address.
key [plaintext <PASSKEY> ciphertext <PASSKEY>]	Selects either a plaintext or an encrypted local shared-secret passkey for the server. As per RFC 2865, shared-secret can be a mix of alphanumeric and special characters. Plaintext passkeys are between 1 and 32 alphanumeric and special characters. NOTE: When <code>key</code> is entered without either sub-parameter, plaintext passkey prompting occurs upon pressing Enter. Enter must be pressed immediately after the <code>key</code> parameter without entering other parameters. The entered passkey characters are masked with asterisks. When <code>key</code> is omitted, the server uses the global passkey. This command requires either the global or local passkey to be set; otherwise the server will not be contacted. Command <code>radius-server key</code> is available for setting the global passkey.

Parameter	Description
<code>timeout <TIMEOUT-SECONDS></code>	Specifies the timeout. Range: 1 to 60 seconds. If a timeout is not specified, the value from the global timeout for RADIUS is used.
<code>port <PORT-NUMBER></code>	Specifies the authentication port number. Range: 1 to 65535. Default: 1812.
<code>auth-type {pap chap}</code>	Selects either the PAP (the default) or CHAP authentication types. If this parameter is not specified, the RADIUS global default is used.
<code>acct-port <ACCT-PORT></code>	Specifies the UDP accounting port number. Range: 1 to 65535. Default: 1813.
<code>retries <RETRY-COUNT></code>	Specifies the number of retry attempts for contacting the specified RADIUS server. Range is 0 to 5 attempts. If no retry value is provided, the default value of 1 is used.
<code>tracking {enable disable}</code>	Enables or disables server tracking for the RADIUS server. Tracked servers are probed at the start of each server tracking interval to check if they are reachable. Use command radius-server tracking to configure RADIUS server tracking globally. NOTE: Server tracking uses authentication request and response packets to determine server reachability status. The server tracking user name and password are used to form the request packet which is sent to the server with tracking enabled. Upon receiving a response to the request packet, the server is considered to be reachable.
<code>tracking-mode {any dead-only}</code>	Configures tracking mode for the RADIUS server that has tracking enabled with the server. The tracking mode is used to monitor the status of RADIUS server reachability. The default tracking mode is any. ▪ any: Track the RADIUS server irrespective of its server reachability. ▪ dead-only: Track the RADIUS server only when the server is marked as unreachable.
<code>vrf <VRF-NAME></code>	Specifies the VRF name to be used for communicating with the server. If no VRF name is provided, the default VRF named default is used.

Default server groups

The switch always has these four default groups:

- **tacacs:** for remote AAA, always contains every configured TACACS+ server.
- **radius:** for remote AAA, always contains every configured RADIUS server.
- **local:** for local authentication.
- **none:** for local (RBAC) authorization.

User-defined AAA servers are always added to the matching default group, either **tacacs** or **radius**. A maximum of 28 user-defined groups can be created.



- On the 4100i, 6000, 6100, 6200, 6300, 6400, 8100, 8325, 8360, and 10000 Switch Series, a RADIUS server can be associated with a maximum of four different user-defined server groups.
- On the 8320, 8400, and 9300 Switch Series, a RADIUS server can be associated with only one user-defined server group.

The order in which servers are added to a group is important. The server added first is accessed first, and if necessary, the second server is accessed second, and so on.

Supported platforms and standards

Remote AAA with RADIUS is supported on the 4100i, 6000, 6100, 6200, 6300, 6400, 8320, 8325, 8360, 8400, 9300, and 10000 Switch Series.

Setting	Default value / limit
Maximum number of RADIUS servers in a AAA group	16
Maximum number of RADIUS servers that can be configured	16
Maximum number of user-defined AAA server groups that can be configured	28
RADIUS authentication	Disabled
RADIUS authentication global timeout	5 seconds
RADIUS authentication passkey (shared secret)	None
RADIUS authentication udp-port	1812
RADIUS global authentication protocol	PAP
RADIUS global retries	1 retry
RADIUS server tracking default interval	300 seconds
RADIUS server access through the default VRF	default*

*The default value is **default**, unless another VRF is specified during the server configuration.

About global versus per-RADIUS server passkeys (shared secrets)

To communicate with a RADIUS AAA server, the switch must have a passkey (shared secret) configured that matches what is configured on the server. Use one of these commands to achieve the desired

configuration:

- For a global passkey common to every RADIUS server, use **radius-server key**.
- For a per-RADIUS server passkey, use **radius-server host** with the **key** parameter.



If both passkeys are configured on the switch, the per-RADIUS server passkey is used.

Remote AAA RADIUS server configuration requirements

The user-supplied RADIUS server must:

- Have an IPv4/IPv6 address or fully qualified domain name (FQDN) that is visible to the switch.
- Have a passkey (shared secret) that matches what is configured on the switch.
- Provide username and password definitions for every switch user. Remote users do not require definition on the switch.
- Configure user role assignment using RADIUS attributes.

If SSH public key authentication is used, the key information is stored locally on the switch, making username and password definition on the RADIUS server unnecessary.

One of the RADIUS attributes **User-Group**, **Privilege-Level** or **Service-Type** is mandatory in an Access-Accept message for the switch to authenticate the client.

AOS-CX supports the following AV pairs -



- Aruba-Admin-Role VSA (user-groups configured on the switch)
- Aruba-Priv-Admin-User VSA (built-in user groups)
- Service-Type.

If the privilege level of the user is not among the fully defined privilege levels then the user is denied access.



Consult your RADIUS server documentation for installation and general configuration details.

User role assignment using RADIUS attributes

User role assignment is configured on the RADIUS server using VSAs (vendor-specific attributes).

RADIUS servers can return multiple attribute value pairs (AVPs) in response to an authentication request. The attributes are processed in this order of precedence to determine the user role assigned:

- If the **Aruba-Admin-Role** VSA is present, map the user to the matching local user-group name.
- Else, if the **Aruba-Priv-Admin-User** VSA is present, extract the privilege level (1, 15, or 19) and map the user to the local user-group corresponding to this privilege level (**1=operators**, **15=administrators**, **19=auditors**). Privilege levels 2 to 14 may also be used with matching local user groups named 2 to 14.
- Else, If Service-Type AVP is present, map **Administrative-User(6)** to **administrators** and map **NAS-Prompt-User(7)** to **operators**.
- Otherwise, the user role cannot be determined, and the authentication fails.

Aruba-Admin-Role	Aruba-Priv-Admin-User	service-type	User role assigned
<GROUP-NAME>	Do not care	Do not care	Matching local user <GROUP-NAME>
Not present	privilege level =1	Do not care	Operators
Not present	privilege level =15	Do not care	Administrators
Not present	privilege level =19	Do not care	Auditors
Not present	privilege level =2 to 14	Do not care	Matching local user groups named 2 to 14
Not present	Not present	Administrative-User (6)	Administrators
Not present	Not present	NAS-Prompt-User (7)	Operators
Not present	Not present	Not present (or = any other value)	None (not authenticated)



The `Service-Type` attribute is retained only for backward compatibility. It is recommended that you instead use the **Aruba-Admin-Role** or **Aruba-Priv-Admin-User** VSA.

RADIUS server redundancy and access sequence

To prevent authentication interruption, it is common practice to configure more than one RADIUS server. When identifying RADIUS servers to the switch, server group order (and server order within the group), determines server access order.



When defining the server access sequence for authentication with `aaa authentication login default`, there is an implied `local` included as the last item in the list. If no RADIUS server can be reached, local authentication will be attempted.

Configuration task list

Steps	Example	Comments
Step 1: Configure the UBT mode	Local VLAN (Reserved VLAN) mode : <pre>ubt-client-vlan 4000</pre> VLAN extend mode: <pre>ubt-mode vlan-extend</pre>	In the local VLAN mode, the UBT client VLAN on the switch will be a reserved UBT VLAN. The default UBT mode is Local VLAN. For the

Steps	Example	Comments
		Local VLAN mode, UBT client VLAN needs to be configured.
Step 2: Configure the source IP address	<pre> interface vlan 10 no shutdown ip address 192.168.10.1/24 ip source-interface ubt interface vlan10 </pre>	UBT source IP address can be a loopback interface, ROP, or SVI.
Step 3: Configure the UBT zones	<pre> ubt zone zone1 vrf default primary-controller ip 192.168.10.8 backup-controller ip 192.168.10.18 enable </pre>	
Step 4: Configure the UBT client role	VLAN extend mode configuration: <pre> port-access role ubt-switch-role gateway-zone zone zone1 gateway-role ubt- controller-role vlan access 20 </pre> Local VLAN mode configuration: <pre> port-access role ubt-switch-role gateway-zone zone zone1 gateway-role ubt- controller-role </pre>	UBT supports both LUR and DUR roles for the UBT client. In the case of LUR, the UBT client role needs to be configured on the switch. In case of DUR, UBT client role needs to be configured on the CPPM server. NOTE: In the case of Local VLAN UBT mode, UBT client primary/switch role VLAN configuration is not needed.
Step 5: Configure the secondary role on the gateway	<pre> user-role ubt-controller-role access-list session allowall access-list session v6-allowall vlan 20 </pre>	VLAN 20 is the secondary role VLAN on the controller for the UBT client.

Single source IP address for consistent source identification to AAA servers



If applicable to your installation, it is recommended that you perform the optional configuration mentioned in this section.

If your topology allows the AAA server to be reached through multiple paths, the server interprets the incoming packets to be from different switches even though they are all coming from the same switch. Having a switch associated with multiple IP addresses makes it more difficult to interpret system logs and accounting data.

To ensure that all traffic sent from the switch to the AAA server uses the same source IP address, use **ip source-interface** or **ipv6 source-interface**. These two commands plus the related commands **show ip source-interface** and **show ipv6 source-interface** are described under *Layer 2/3 Interface commands* in the *Command-Line Interface Guide*.

RADIUS general tasks

General RADIUS tasks, not specific to authentication, are as follows:

Task	Command name	Example
Configuring a RADIUS server	<code>radius-server host</code>	<code>radius-server host 1.1.1.1 vrf default</code> <code>no radius-server host 1.1.1.1 vrf default</code>
Showing global and RADIUS server configurations	<code>show radius-server</code>	<code>show radius-server detail</code>
Configuring a RADIUS server group	<code>aaa group server</code>	<code>aaa group server radius sg3</code> <code>no aaa group server radius sg3</code>
Showing server groups	<code>show aaa server-groups</code>	<code>show aaa server-groups</code>
Adding a RADIUS server to a server-group	<code>server</code>	<code>aaa group server radius sg3</code> <code>server 1.1.1.4 port 32 vrf default</code>
Deleting a RADIUS server from a server-group	<code>server</code>	<code>aaa group server tacacs sg3</code> <code>no server 1.1.1.4 port 32 vrf default</code>
Configuring a RADIUS global passkey	<code>radius-server key</code>	<code>radius-server key plaintext mypasskey123</code>
Configuring PAP or CHAP for RADIUS	<code>radius-server auth-type</code>	<code>radius-server auth-type chap</code> <code>no radius-server auth-type</code>
Configuring the RADIUS global timeout	<code>radius-server timeout</code>	<code>radius-server timeout 15</code> <code>no radius-server timeout</code>
Configuring the RADIUS global retries	<code>radius-server retries</code>	<code>radius-server retries 3</code> <code>no radius-server retries</code>
Overriding the global retries for a RADIUS server	<code>radius-server host</code>	<code>radius-server host 1.1.1.1 retries 2</code>

Per-port RADIUS server group configuration

RADIUS server groups can be configured for MAC and 802.1X authentication mechanisms on a port. This port-specific server group configuration overrides any global server group configured for the authentication mechanisms.

In the absence of a port-specific configuration, clients authenticated on a port will be associated with the globally configured RADIUS server group. When a RADIUS server group is configured on a port, any existing clients already authenticated on that port, using the previous group, will be associated with the new port-specific server group during the subsequent reauthentication cycle.



- On the 4100i, 6000, 6100, 6200, 6300, 6400, 8100, 8325, 8360, and 10000 Switch Series, a RADIUS server can be associated with a maximum of four different user-defined RADIUS server groups.
- On the 8320, 8400, and 9300 Switch Series, a RADIUS server can be associated with only one user-defined server group.

Different NAS-IDs can be sent to the same RADIUS server as a RADIUS server can be associated with four user-defined server groups.



- For more details on NAS-IDs configuration, refer to [Configurable RADIUS attributes \(port access\)](#).
- Dynamic authentication is not affected by this port configuration, because only the authentication server will be determined by this configuration. Any COA or disconnect requests from any of the reachable server will be successful.

To configure per-port or global RADIUS server groups for MAC and 802.1X authentication mechanisms, see:

- [aaa authentication port-access dot1x authenticator radius server-group](#)
- [aaa authentication port-access mac-auth radius server-group](#)

RADIUS authentication

RADIUS authentication occurs as follows:

- User credentials are sent from the switch to RADIUS server using the PAP or CHAP authentication protocol.
- If a user is authenticated, their role is communicated to the switch as Administrator, Operator, or Auditor.
- An unknown user or a user who entered an invalid password is identified as such to the switch, which then rejects user login.

About authentication fail-through

Normally, authentication is performed by the first AAA server reached. A rarely needed feature named "Authentication fail-through" is available. If authentication fail-through is enabled and authentication fails on the first reachable AAA server, authentication is attempted on the second AAA server, and so on, until successful authentication or the server list is exhausted.

Enabling Authentication fail-through is typically unnecessary because the user credential databases should be consistent across all AAA servers. Authentication fail-through might be helpful if your AAA user credential databases are not quickly synchronized across all AAA servers.



[Authentication fail-through](#), [authorization fail-through](#), and [accounting fail-through](#) must each be configured separately.

RADIUS authentication tasks

The RADIUS authentication-related tasks are as follows:

Task	Command name	Example
Configuring the authentication sequence for the default connection type	<code>aaa authentication login</code>	<code>aaa authentication login default group rg1 rg2 radius local</code>
Configuring the authentication sequence for the https-server connection type	<code>aaa authentication login</code>	<code>aaa authentication login https-server group rg1 radius local</code>
Removing remote AAA for the default connection type	<code>aaa authentication login</code>	<code>no aaa authentication login default</code>
Configuring authentication fail-through	<code>aaa authentication allow-fail-through</code>	<code>aaa authentication allow-fail-through</code> <code>no aaa authentication allow-fail-through</code>
Configuring authorization fail-through	<code>aaa authorization allow-fail-through</code>	<code>aaa authorization allow-fail-through</code> <code>no aaa authorization allow-fail-through</code>
Configuring accounting fail-through	<code>aaa accounting allow-fail-through</code>	<code>aaa accounting allow-fail-through</code> <code>no aaa accounting allow-fail-through</code>
Showing the authentication sequence	<code>show aaa authentication</code>	<code>show aaa authentication</code>

Two-factor authentication

Two-factor authentication is available for added security. In two-factor authentication, X.509 certificate-based authentication is combined with RADIUS authentication.

Two-factor authentication can be performed with local or remote (on RADIUS server) users.

Configuring two-factor authentication (for local users)

Two-factor authentication is available for added security. In two-factor authentication, X.509 certificate-based authentication is combined with RADIUS authentication. When a user establishes an SSH connection to the switch, two factor-authentication occurs as follows:

- The username in the user's X.509 certificate is validated against the local user accounts on the switch.
- The username and password are validated against the accounts on the RADIUS server and the configured trust anchors.

Prerequisites

- The switch SSH server is enabled.
- Your switch management computer, though its SSH client, is connected to the switch.
- A remote RADIUS server is available to authenticate switch users and is configured on the switch.
- Every user that will use two-factor authentication is configured both on the RADIUS server and locally on the switch using identical usernames. Users are added locally on the switch with the **user** command. These usernames must precisely match the usernames identified by the X.509 user certificates.
- The X.509 CA certificate is both installed on your switch management computer and is also visible to your computer's SSH client. The X.509 CA certificate is the root of trust for the client certificate being used.
- One X.509 certificate per user is available on your switch management computer and is visible to your computer's SSH client. The usernames identified by these user certificates must be the same as the usernames already defined on the RADIUS server and locally on the switch.

Procedure

1. Create a TA profile with the command **crypto pki ta-profile**. This command switches to the TA configuration context. The TA profile is where the switch stores the root certificate of the CA that is used to validate the certificates of clients communicating with the SSH server.
2. Although optional, it is recommended that you enable certificate revocation checking with the command **revocation-check oosp**.
3. Import the root certificate of the CA with the command **ta-certificate**.
4. Exit the TA configuration context with the command **exit**.
5. For each user that will be using two-factor authentication, import the public key from the individual X.509 user certificate with the command **user <USERNAME> authorized-key <PUBKEY>**. Each user identified by <USERNAME> must exist locally on the switch and on the RADIUS authentication server.
6. Enable two-factor authentication with the command `ssh two-factor-authentication`.

Example

This example shows the above steps being executed:

```
--- step 1 ---
switch(config)# crypto pki ta-profile root-cert

--- step 2 ---
switch(config-ta-root-cert)# revocation-check oosp

--- step 3 ---
switch(config-ta-root-cert)# ta-certificateta-certificate
Paste the certificate in PEM format below, then hit enter and ctrl-D:
switch(config-ta-cert)# -----BEGIN CERTIFICATE-----
switch(config-ta-cert)# MIIDuTCCAqECCQCuoxeJ2ZNYcjANBgqhkiG9w0BAQsFADCBq
...
switch(config-ta-cert)# 3LvMLZcssSe5J2Ca2XIhfdme8UaNZ7syGYoCD/TMsAW0nG7yY
switch(config-ta-cert)# -----END CERTIFICATE-----
switch(config-ta-cert)#
The certificate you are importing has the following attributes:
Issuer: C=US, ST=CA, L=Rocklin, O=Company, OU=Site,
        CN=site.com/emailAddress=test.ca@site.com
Subject: C=US, ST=CA, L=Rocklin, O=Company, OU=Site,
         CN=8400/emailAddress=test.ca@site.com
Serial Number: 12121221634631568498 (0xae51217d5945772)

Do you want to accept this certificate (y/n)? y
TA certificate accepted.

--- step 4 ---
switch(config-ta-root-cert)# exit
switch(config)#

--- step 5 ---
switch(config)# user admin authorized-key ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAQAC6krLTTrFTnzg3YjLiZKTZEYnh4cUiuOK+cjduxFnZUa
...
iAfcGvqvWtWWBS0Wd011DeEZnKn008uEKeTEcAjfrnRHeOk2QJmw== "sv1@site.net"
switch(config)#

--- step 6 ---
switch(config)# ssh two-factor-authentication
```

Configuring two-factor authentication with SSH (for remote-only users)

Two-factor authentication is available for added security. In two-factor authentication, X.509 certificate-based authentication is combined with RADIUS authorization.

In circumstances where it is desirable to have no local users, when a user establishes an SSH connection to the switch, two factor-authentication occurs as follows:

- The certificate is validated by the switch using the set of customer-configured trusted TA profiles. If validated, the switch then sends a RADIUS Authorize-Only request to the RADIUS server using the username found in the certificate. The username is chosen from either the certificate UserPrincipalName (UPN) or CommonName (CN).
- A password is not required at time of authentication.

Prerequisites

- The switch SSH server is enabled.
- The remote RADIUS server providing authentication supports the "authorize-only" Service-Type. This includes RADIUS servers such as Aruba's ClearPass Policy Manager, Windows 2019 NPS, or FreeRADIUS.
- The RADIUS server is configured using a TLS (RadSec) connection. This requires the provisioning of a RadSec tunnel between the Switch and a RadSec proxy server, which then forwards the request to the RADIUS server. For information, see *Secure RADIUS (RadSec)* in the Security Guide for your switch.
- An appropriate set of Certificate Authority (CA) and leaf certificates for mutual TLS communication has been created for the switch-to-RADIUS server connection.
- Your switch management computer, through its SSH client, is connected to the switch. Typical supported clients are VanDyke SecureCRT and Pragma Fortress SSH Client Suite.
- Your SSH client is configured to get the username from the certificate.
- For the user being authenticated, an X.509 certificate is installed on your switch management computer and is visible to your computer SSH client. The username identified in the certificate matches a username already defined on the remote RADIUS server.

Procedure

1. Create a TA profile with the command **crypto pki ta-profile**. This command switches to the TA configuration context. The TA profile is where the switch stores the root certificate of the CA that is used to validate the certificates of clients communicating with the SSH server.
2. Although optional, it is recommended that you enable certificate revocation checking with the command **revocation-check ocsp**.
3. Import the root certificate of the CA with the command **ta-certificate**.
4. Exit the TA configuration context with the command **exit**.
5. Repeat steps 1 to 4 for the root certificate authority used for the RADIUS server.
6. Create a leaf certificate profile for the RADIUS client certificate, using the command **crypto pki certificate**. This command switches to the certificate configuration context.
7. Import the leaf certificate with the command **import terminal ta-profile**. Paste the leaf certificate in PEM format, followed by the corresponding private key.
8. Set the certificate for usage with RADIUS communication. Do this with the command **crypto pki application radsec-client certificate**.
9. Configure SSH to enforce the requirement to have the username defined in the X.509 certificate, within any of these two certificate fields: UserPrincipalName (UPN) or Common Name (CN). Do this with command **ssh certificate-as-authorized-key**.
10. Enable two-factor authentication with authorization performed by the RADIUS server. Do this with command **ssh two-factor-authentication authorization radius**.
11. Add the radius server connection to the switch. Do this with the command **radius-server host tls**.
12. Enable authorization by any RADIUS server (in default group **radius**) configured for Authorize-Only with command **aaa authorization radius ssh group radius**. Note also that user-defined RADIUS groups can be used in addition to or instead of the default RADIUS group.

Example

This example shows the above steps being executed:

```
--- step 1 ---
switch(config)# crypto pki ta-profile root-cert

--- step 2 ---
switch(config-ta-root-cert)# revocation-check ocsf

--- steps 3, 4 ---
switch(config-ta-root-cert)# ta-certificate
Paste the certificate in PEM format below, then hit enter and ctrl-D:
switch(config-ta-cert)# -----BEGIN CERTIFICATE-----
switch(config-ta-cert)# MIIDuTCCAqECCQCuoxeJ2ZNYcjANBgkqhkiG9w0BAQsFADCBq
...
switch(config-ta-cert)# 3LvMLZcssSe5J2Ca2XIhfDme8UaNZ7syGYoCD/TMsAW0nG7yY
switch(config-ta-cert)# -----END CERTIFICATE-----
switch(config-ta-cert)#
The certificate you are importing has the following attributes:
Issuer: C=XX, ST=XX, L=Xxxx, O=Company, OU=Site,
       CN=9999/emailAddress=test.ca@site.com
Subject: C=XX, ST=XX, L=Xxxx, O=Company, OU=Site,
        CN=9999/emailAddress=test.ca@site.com
Serial Number: 99999999999999999999 (0xffffffffffffffff)

Do you want to accept this certificate (y/n)? y
TA certificate accepted.
switch(config-ta-root-cert)# exit

--- step 5 ---
switch(config)# crypto pki ta-profile radius-root-cert
switch(config-ta-root-cert)# ta-certificate
Paste the certificate in PEM format below, then hit enter and ctrl-D:
switch(config-ta-cert)# -----BEGIN CERTIFICATE-----
switch(config-ta-cert)# MIIDuTCCAqECCQCuoxeJ2ZNYcjANBgkqhkiG9w0BAQsFADCBq
...
switch(config-ta-cert)# 3LvMLZcssSe5J2Ca2XIhfDme8UaNZ7syGYoCD/TMsAW0nG7yY
switch(config-ta-cert)# -----END CERTIFICATE-----
switch(config-ta-cert)#
The certificate you are importing has the following attributes:
Issuer: C=XX, ST=XX, L=Xxxx, O=Company, OU=Site,
       CN=9999/emailAddress=test.ca@site.com Subject: C=XX, ST=XX, L=Xxxx, O=Company,
       OU=Site,
       CN=9999/emailAddress=test.ca@site.com
Serial Number: 99999999999999999999 (0xffffffffffffffff)

Do you want to accept this certificate (y/n)? y
TA certificate accepted.
switch(config-ta-radius-root-cert)# exit

--- step 6 ---
switch(config)# crypto pki certificate radius-client-cert

--- step 7 ---
switch(config-cert-radius-client-cert)# import terminal ta-profile radius-root-
cert
Paste the certificate in PEM format below, then hit enter and ctrl-D:
switch(config-cert-import)# -----BEGIN CERTIFICATE-----
switch(config-cert-import)# MIIDuTCCAqECCQCuoxeJ2ZNYcjANBgkqhkiG9w0BAQsFADCBq
...
switch(config-cert-import)# 3LvMLZcssSe5J2Ca2XIhfDme8UaNZ7syGYoCD/TMsAW0nG7yY
switch(config-cert-import)# -----END CERTIFICATE-----
```

```

switch(config-cert-import)#
Leaf certificate is validated with radius-root-cert and imported successfully.
Certificate is installed and ready to use.
switch(config-cert-radius-client-cert)#
Paste the certificate in PEM format below, then hit enter and ctrl-D:
switch(config-cert-import)# -----BEGIN CERTIFICATE-----
switch(config-cert-import)# MIIDuTCCAqECCQCuoxeJ2ZNYcjANBgkqhkiG9w0BAQsFADCBq
...
switch(config-cert-import)# 3LvMLZcssSe5J2Ca2XIhfDme8UaNZ7syGYoCD/TMsAW0nG7yY
switch(config-cert-import)# -----END CERTIFICATE-----
switch(config-cert-import)#
Leaf certificate is validated with radius-root-cert and imported successfully.
Certificate is installed and ready to use.
switch(config-cert-radius-client-cert)# exit

--- step 8 ---
switch(config)# crypto pki application radsec-client certificate radius-client-
cert

--- step 9 ---
switch(config)# ssh certificate-as-authorized-key

--- step 10 ---
switch(config)# ssh two-factor-authentication authorization radius

--- step 11 ---
switch(config)# radius-server host 999.99.9.9 tls

--- step 12 ---
switch(config)# aaa authorization radius ssh group radius
All commands will fail if none of the radsec servers in the group list are
reachable.
Continue (y/n)?

```

Configuring two-factor authentication with HTTPS server and REST (for remote-only users)

Two-factor authentication is available for added security. In two-factor authentication, X.509 certificate-based authentication is combined with RADIUS authorization.

In circumstances where it is desirable to have no local users, when a user establishes an HTTPS connection to the switch, two factor-authentication occurs as follows:

- The certificate is validated by the switch using the set of customer-configured trusted TA profiles. If validated, the switch then sends a RADIUS Authorize-Only request to the RADIUS server using the username found in the certificate. The username is chosen from either the certificate User Principal Name (UPN) or Common Name (CN).
- A password is not required at time of authentication.

Prerequisites

- The switch HTTPS REST server is enabled in the desired VRF.
- The remote RADIUS server providing authentication supports the "authorize-only" Service-Type. This includes RADIUS servers such as Aruba's ClearPass Policy Manager, Windows 2019 NPS, or FreeRADIUS.

- The RADIUS server is configured using a TLS (RadSec) connection. This requires the provisioning of a RadSec tunnel between the Switch and a RadSec proxy server, which then forwards the request to the RADIUS server. For information, see *Secure RADIUS (RadSec)* in the Security Guide for your switch.
- An appropriate set of Certificate Authority (CA) and leaf certificates for mutual TLS communication has been created for the switch-to-RADIUS server connection.
- Your switch management computer has access to the REST API using an appropriate HTTPS client. This can be done with a web browser, using the WebUI, or other HTTP request tools such as Postman. Usage of Firefox is not recommended, as it requires additional configuration to work with this feature.
- For the user being authenticated, an X.509 certificate is installed on your switch management computer and loaded to your preferred HTTPS client. The username identified in the certificate (whether in the User Principal Name (UPN) or Common Name (CN) fields) matches a username already defined on the remote RADIUS server.

Procedure

1. Create a TA profile with the command **crypto pki ta-profile**. This command switches to the TA configuration context. The TA profile is where the switch stores the root certificate of the CA that is used to validate the certificates of clients logging in to the HTTPS REST server.
2. Although optional, it is recommended that you enable certificate revocation checking with the command **revocation-check ocsp**.
3. Import the root certificate of the CA with the command **ta-certificate**.
4. Exit the TA configuration context with the command **exit**.
5. Repeat steps 1 to 4 for the root certificate authority used for the RADIUS server.
6. Create a leaf certificate profile for the RADIUS client certificate, using the command **crypto pki certificate**. This command switches to the certificate configuration context.
7. Import the leaf certificate with the command **import terminal ta-profile**. Paste the leaf certificate in PEM format, followed by the corresponding private key.
8. Set the certificate for usage with RADIUS communication. Do this with the command **crypto pki application radsec-client certificate**.
9. Enable certificate authentication for the HTTPS server. Configure it with authorization performed by the RADIUS server and enforce the requirement to have the username defined in the X.509 certificate, within any of these two certificate fields: User Principal Name (UPN) or Common Name (CN). Do this with command **https-server authentication certificate authorization radius**.
10. Respond with **y** (yes) to the prompt indicating that HTTP authentication with certificate will be enabled and that password authentication will be disabled .
11. Add the radius server connection to the switch. Do this with the command **radius-server host tls**.
12. Enable authorization by any RADIUS server (in default group **radius**) configured for Authorize-Only with command **aaa authorization radius ssh group radius**. Note also that user-defined RADIUS groups can be used in addition to or instead of the default RADIUS group.
13. At this point you can send a POST request to the **/certificate_login** endpoint in the REST API, including the corresponding user certificate. Alternatively you can access the login page of the WebUI, where a login button is presented. Upon pressing the login button, the browser prompts you to select a certificate.

Example

This example shows the above steps being executed:

```

--- step 1 ---
switch(config)# crypto pki ta-profile https-root-cert

--- step 2 ---
switch(config-ta-root-cert)# revocation-check ocsp

--- steps 3, 4 ---
switch(config-ta-root-cert)# ta-certificate
Paste the certificate in PEM format below, then hit enter and ctrl-D:
switch(config-ta-cert)# -----BEGIN CERTIFICATE-----
switch(config-ta-cert)# MIIDuTCCAqECCQCuoxeJ2ZNYcjANBgkqhkiG9w0BAQsFADCBq
...
switch(config-ta-cert)# 3LvMLZcssSe5J2Ca2XIhfDme8UaNZ7syGYoCD/TMsAW0nG7yY
switch(config-ta-cert)# -----END CERTIFICATE-----
switch(config-ta-cert)#
The certificate you are importing has the following attributes:
Issuer: C=XX, ST=XX, L=Xxxx, O=Company, OU=Site,
CN=9999/emailAddress=test.ca@site.com Subject: C=XX, ST=XX, L=Xxxx, O=Company,
OU=Site,
CN=9999/emailAddress=test.ca@site.com
Serial Number: 99999999999999999999 (0xffffffffffffffff)

Do you want to accept this certificate (y/n)? y
TA certificate accepted.
switch(config-ta-root-cert)# exit

--- step 5 ---
switch(config)# crypto pki ta-profile radius-root-cert
switch(config-ta-root-cert)# ta-certificate
Paste the certificate in PEM format below, then hit enter and ctrl-D:
switch(config-ta-cert)# -----BEGIN CERTIFICATE-----
switch(config-ta-cert)# MIIDuTCCAqECCQCuoxeJ2ZNYcjANBgkqhkiG9w0BAQsFADCBq
...
switch(config-ta-cert)# 3LvMLZcssSe5J2Ca2XIhfDme8UaNZ7syGYoCD/TMsAW0nG7yY
switch(config-ta-cert)# -----END CERTIFICATE-----
switch(config-ta-cert)#
The certificate you are importing has the following attributes:
Issuer: C=XX, ST=XX, L=Xxxx, O=Company, OU=Site,
CN=9999/emailAddress=test.ca@site.com Subject: C=XX, ST=XX, L=Xxxx, O=Company,
OU=Site,
CN=9999/emailAddress=test.ca@site.com
Serial Number: 99999999999999999999 (0xffffffffffffffff)

Do you want to accept this certificate (y/n)? y
TA certificate accepted.
switch(config-ta-radius-root-cert)# exit

--- step 6 ---
switch(config)#
switch(config)# crypto pki certificate radius-client-cert

--- step 7 ---
switch(config-cert-radius-client-cert)# import terminal ta-profile radius-root-
cert
Paste the certificate in PEM format below, then hit enter and ctrl-D:
switch(config-cert-import)# -----BEGIN CERTIFICATE-----
switch(config-cert-import)# MIIDuTCCAqECCQCuoxeJ2ZNYcjANBgkqhkiG9w0BAQsFADCBq
...
switch(config-cert-import)# 3LvMLZcssSe5J2Ca2XIhfDme8UaNZ7syGYoCD/TMsAW0nG7yY
switch(config-cert-import)# -----END CERTIFICATE-----
switch(config-cert-import)#
Leaf certificate is validated with radius-root-cert and imported successfully.

```



```

Certificate is installed and ready to use.
switch(config-cert-radius-client-cert)# exit

--- step 8 ---
switch(config)# crypto pki application radsec-client certificate radius-client-
cert

--- steps 9, 10 ---
switch(config)# https-server authentication certificate authorization radius
username common_name
This will enable HTTPS authentication with certificate and disable password
authentication
Continue (y/n)? y

--- step 11 ---
switch(config)# radius-server host 999.99.9.9 tls

--- step 12 ---
switch(config)# aaa authorization radius ssh group radius
All commands will fail if none of the radsec servers in the group list are
reachable.
Continue (y/n)? y

```

Two-factor authentication commands

aaa authorization radius

```

aaa authorization radius {ssh | https-server} group <GROUP-LIST>
no aaa authorization radius {ssh | https-server} group <GROUP-LIST>

```

Description

Enables RADIUS authorize-only for use with two-factor authentication. By default RADIUS authenticates and authorizes a client that is configured for AAA based access. This command causes the RADIUS server to instead be used only for authorization and not for authentication.

Authorization requests are sent over TLS and therefore RADIUS authorize-only requires a RadSec RADIUS server.



If command authorization is also configured it is given priority over RADIUS authorize-only and therefore command authorization is done on the basis of command authorization configuration and not the user role and privilege level assigned by the RADIUS server.

The **no** form of this command disables RADIUS authorize-only, causing RADIUS to be again used for both authentication and authorization.

Parameter	Description
ssh	Selects the SSH authorization list.
https-server	Selects the HTTPS server authorization list.
group <GROUP-LIST>	Specifies the list of remote RADIUS server group names. Each name can be specified one time. Predefined remote RADIUS group name radius is available. The remote RADIUS server groups are accessed in the order that the group names are listed in this command. Within each group,

Parameter	Description
	the servers are accessed in the order in which the servers were added to the group. Server groups are defined using command aaa group server and servers are added to a server group with the command server .

Examples

Enabling RADIUS authorize only for SSH with the default RADIUS group:

```
switch(config)# aaa authorization radius ssh group radius
All commands will fail if none of the radsec servers in the group list are
reachable.
Continue (y/n)? y
```

Disabling RADIUS authorize only for SSH with the default RADIUS group, causing RADIUS to be again used for both authentication and authorization:

```
switch(config)# no aaa authorization radius ssh group radius
```

Enabling RADIUS authorize only for HTTPS server with the default RADIUS group:

```
switch(config)# aaa authorization radius https-server group radius
All commands will fail if none of the radsec servers in the group list are
reachable.
Continue (y/n)? y
```

Disabling RADIUS authorize only for HTTPS server with the default RADIUS group, causing RADIUS to be again used for both authentication and authorization:

```
switch(config)# no aaa authorization radius https-server group radius
```

Release	Modification
10.11	Command introduced

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

https-server authentication certificate

```
https-server authentication certificate [authorization radius] [username {<CERT-FIELD>}]
```

Description

Enables certificate-based authentication where the HTTPS server uses an X.509 certificate for authentication and a RADIUS server for authorization.

Enabling password authentication is the only way of disabling certificate authentication.

Parameter	Description
<code>authorization radius</code>	Specifies that after certificate authentication succeeds, instead of prompting for a password, the HTTPS server checks the RADIUS server only for authorization. A local user is not required. By default, the username found in the certificate field UserPrincipalName (UPN) is used for authorization on the RADIUS server. When this parameter is omitted, authorization radius is still the assumed active setting.
<code><CERT-FIELD></code>	Selects which certificate username field is to be used for authorization. - Specify user_principal_name to use the certificate UserPrincipalName (UPN) field. This is the default. - Specify common_name to use the certificate CommonName (CN) field. When this parameter is omitted, user_principal_name is assumed.

Examples

Enabling HTTPS server authentication with authorization on a RADIUS server with the username in certificate field UserPrincipalName (UPN):

```
switch(config)# https-server authentication certificate authorization radius
```

Enabling HTTPS server authentication with authorization on a RADIUS server with the username in certificate field UserPrincipalName (UPN) (**authorization radius** is still implied even though not specified):

```
switch(config)# https-server authentication certificate
```

Enabling HTTPS server authentication with authorization on a RADIUS server with the username in certificate field CommonName (CN):

```
switch(config)# https-server authentication certificate authorization radius  
username common_name
```

Command History

Release	Modification
10.11	Command introduced

Command Information

Platforms	Command context	Authority
All platforms	<code>config</code>	Administrators or local user group members with execution rights for this command.

ssh certificate-as-authorized-key

```
ssh certificate-as-authorized-key
no ssh certificate-as-authorized-key
```

Description

Enables SSH enforcement that the username must be present in the certificate that is being used for authorization. This configuration alters how certificate-based authentication maps to a user account. When this is enabled, SSH will not require local user association with an authorized-key and instead enforces that the username used to log in is present within the certificate.

The SSH server will check for the username in certificate fields **Common Name** or **User Principle Name** for a match. If a certificate is not used for authentication then this configuration has no effect on SSH authentication.

The **no** form of this command disables the SSH enforcement of username in the certificate.

Examples

Enabling SSH enforcement of username in the certificate:

```
switch(config)# ssh certificate-as-authorized-key
```

Disabling SSH enforcement of username in the certificate:

```
switch(config)# no ssh certificate-as-authorized-key
```

Command History

Release	Modification
10.11	Command introduced

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

ssh two-factor-authentication

```
ssh two-factor-authentication [authorization radius]
no ssh two-factor-authentication [authorization radius]
```

Description

Enables the selected SSH Two Factor authentication method. Two-factor authentication uses an X.509 certificate and possibly a password. First the X.509 certificate presented by the user is authenticated. Then, if successful, (when the **authorization-radius** parameter is not specified) the (locally-defined) user is prompted for a password. When the **authorization radius** parameter is specified, instead of prompting for a password, SSH checks only for authorization with the remote RADIUS server. A local user is not required.

The **no** form of the command disables SSH two-factor authentication.

Parameter	Description
authorization radius	Specifies that after certificate authentication succeeds, SSH checks the RADIUS server only for authorization.

Examples

Enabling two-factor authentication for local user with password prompting:

```
switch(config)# ssh two-factor-authentication
```

Disabling two-factor authentication for local user with password prompting:

```
switch(config)# no ssh two-factor-authentication
```

Enabling two-factor authentication for remote-only RADIUS-defined users without password prompting:

```
switch(config)# ssh two-factor-authentication authorization radius
```

Disabling two-factor authentication for remote-only RADIUS-defined users without password prompting: :

```
switch(config)# no ssh two-factor-authentication authorization radius
```

Command History

Release	Modification
10.11	Added the authorization radius parameter
10.10	Command introduced

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

RADIUS accounting

This accounting information is captured and made available for sending to remote accounting servers:

- Port access accounting
- Exec Accounting: user login/logout events
- Command accounting: commands executed by users. The Vendor-Specific Attribute (VSA) **Aruba_Command_String** with a value of 46 is available.
- System accounting: remote accounting On/Off events.

- CLI show commands.
- Interactions on the non-CLI interfaces: REST and WebUI.



With RADIUS, command accounting logs a maximum of 247 characters per command entered by the user.

The following is not captured or made available as accounting information:

- CLI commands that reboot the switch.
- Interactions in the bash shell.



Local accounting (always enabled) must be functioning properly for remote Accounting to work.



The accounting information is sent to the first reachable remote RADIUS AAA server (configured for remote accounting). If no remote RADIUS server is reachable, local accounting remains available.

Sample general accounting information

```
~~~~~ EXEC ~~~~~~

Mon Jul 16 16:25:27 2018
  User-Name = "admin"
  NAS-Identifier = "switchx"
  NAS-Port = 331
  NAS-Port-Type = Virtual
  Acct-Status-Type = Start
  Acct-Session-Id = "1531769192494"
  Acct-Authentic = Local
  Calling-Station-Id = "0.0.0.0"
  Event-Timestamp = "Jul 16 2018 16:25:22 PDT"
  Acct-Delay-Time = 0
  NAS-IP-Address = 10.10.10.1
  Acct-Unique-Session-Id = "b83e29f4140c17b1"
  Timestamp = 1531783527

~~~ EXEC stop ~~~

Mon Jul 16 16:26:42 2018
  User-Name = "admin"
  NAS-Identifier = "switchx"
  NAS-Port = 331
  NAS-Port-Type = Virtual
  Acct-Status-Type = Stop
  Acct-Session-Id = "1531769192494"
  Acct-Authentic = Local
  Calling-Station-Id = "0.0.0.0"
  Event-Timestamp = "Jul 16 2018 16:26:37 PDT"
  Acct-Delay-Time = 0
  Acct-Session-Time = 75
  NAS-IP-Address = 10.10.10.1
  Acct-Unique-Session-Id = "b83e29f4140c17b1"
  Timestamp = 1531783602

~~~~~ CMD ACCOUNTING ~~~~~~

Mon Jul 16 16:26:42 2018
  User-Name = "admin"
```

```
NAS-Identifier = "switchx"
NAS-Port = 331
NAS-Port-Type = Virtual
Acct-Status-Type = Stop
Acct-Session-Id = "1531769192496"
Acct-Authentic = Local
Aruba-Command-String = "exit"
Calling-Station-Id = "0.0.0.0"
Event-Timestamp = "Jul 16 2018 16:26:37 PDT"
Acct-Delay-Time = 0
NAS-IP-Address = 10.10.10.1
Acct-Unique-Session-Id = "280710992629128c"
Timestamp = 1531783602
```

~~~~~ SYSTEM ACCOUNTING ~~~~~

```
Mon Jul 16 17:13:02 2018
  User-Name = "UNKNOWN"
  NAS-Identifier = "UNKNOWN"
  NAS-Port = 331
  NAS-Port-Type = Virtual
  Acct-Status-Type = Accounting-On
  Acct-Session-Id = "1531769192506"
  Acct-Authentic = Local
  Calling-Station-Id = "0.0.0.0"
  Event-Timestamp = "Jul 16 2018 17:12:56 PDT"
  Acct-Delay-Time = 0
  NAS-IP-Address = 10.10.10.1
  Acct-Unique-Session-Id = "b478e6402c86933e"
  Timestamp = 1531786382
```

```
Mon Jul 16 17:12:55 2018
  User-Name = "UNKNOWN"
  NAS-Identifier = "UNKNOWN"
  NAS-Port = 331
  NAS-Port-Type = Virtual
  Acct-Status-Type = Accounting-Off
  Acct-Session-Id = "1531769192491"
  Acct-Authentic = Local
  Calling-Station-Id = "0.0.0.0"
  Event-Timestamp = "Jul 16 2018 17:12:49 PDT"
  Acct-Delay-Time = 0
  NAS-IP-Address = 10.10.10.1
  Acct-Unique-Session-Id = "93da1f094121f2ee"
  Timestamp = 1531786375
```

~~~~~



This sample is representative and not from any particular RADIUS server implementation.

RADIUS accounting tasks

The RADIUS accounting-related tasks are as follows:

Task	Command name	Example
Configuring the accounting sequence for the default connection type	aaa accounting all-mgmt	aaa accounting all-mgmt default start-stop group rg1 rg2 radius local
Configuring the accounting sequence for the https-server connection type	aaa accounting all-mgmt	aaa accounting all-mgmt https-server start-stop group rg1 radius local
Removing remote AAA for the default connection type	aaa accounting all-mgmt	no aaa accounting all-mgmt default start-stop
Showing the accounting configuration	show aaa accounting	show aaa accounting

Example: Configuring the switch for Remote AAA with RADIUS

Prerequisites

- RADIUS servers configured in general according to the information in [Remote AAA RADIUS server configuration requirements](#). The exact settings appropriate to your environment will vary.
- Logged in to the switch with Administrator privilege and in the **config** context.

Procedure

1. Configure the global RADIUS passkey (shared secret) as "xjKW74932qX3j_\$"

```
switch(config)# radius-server key plaintext xjKW74932qX3j_$
switch(config)#
```

2. Add these configuration details for two remote RADIUS servers.
 - Server 1 with IPv4 address 10.0.0.2, on the management interface (belonging to VRF "mgmt"), using the default PAP protocol.
 - Server 2 with IPv4 address 4.0.0.2, on the data interface (belonging to VRF "default"), using the CHAP protocol.


```
switch(config)# radius-server host 10.0.0.2 vrf mgmt
switch(config)# radius-server host 4.0.0.2 auth-type chap
switch(config)#
```

3. Create a RADIUS group named `rad_grp1`, assign RADIUS server 10.0.0.2 to the group, show the group information.



The default RADIUS group named `radius` includes every RADIUS server regardless of whether any RADIUS servers are also assigned to a user-defined RADIUS group.

```
switch(config)# aaa group server radius rad_grp1
switch(config-sg)# server 10.0.0.2 vrf mgmt
switch(config-sg)# exit
switch(config)#
switch(config)# do show aaa server-groups radius

***** AAA Mechanism RADIUS *****
-----
GROUP NAME          | SERVER NAME          | PORT | VRF    | PRIORITY
-----
rad_grp1            | 10.0.0.2             | 1812 | mgmt   | 1
-----
radius (default)    | 10.0.0.2             | 1812 | mgmt   | 1
radius (default)    | 4.0.0.2              | 1812 | default| 2
-----
switch(config)#
```

```
switch(config)# aaa group server radius rad_grp1
switch(config-sg)# server 10.0.0.2 vrf mgmt
switch(config-sg)# exit
switch(config)#
switch(config)# do show aaa server-groups radius

***** AAA Mechanism RADIUS *****
-----
GROUP NAME          | SERVER NAME          | PORT | VRF    | PRIORITY
-----
rad_grp1            | 10.0.0.2             | 1812 | mgmt   | 1
-----
radius (default)    | 10.0.0.2             | 1812 | mgmt   | 1
radius (default)    | 4.0.0.2              | 1812 | default| 2
-----
switch(config)#
```

4. Define the authentication sequence list so that the new RADIUS group is first, the default RADIUS group is second, and local is third. Show the authentication sequence.

```
switch(config)# aaa authentication login default group rad_grp1 radius local
switch(config)#
switch(config)# do show aaa authentication
AAA Authentication:
  Fail-through           : Disabled
  Limit Login Attempts   : Not set
  Lockout Time           : 300
```

```
Minimum Password Length           : Not set
```

```
Default Authentication for All Channels:
```

```
-----  
---  
GROUP NAME                        | GROUP PRIORITY  
-----  
---  
rad_grpl                          | 0  
radius                            | 1  
local                             | 2  
-----  
---  
switch(config)#
```

5. Define the accounting sequence list with two RADIUS server groups. Show the accounting sequence.

```
switch(config)# aaa accounting all default start-stop group rad_grpl radius  
switch(config)#  
switch(config)# do show aaa accounting  
AAA Accounting:  
  Accounting Type                  : all  
  Accounting Mode                  : start-stop  
  
Default Accounting for All Channels:  
-----  
--  
GROUP NAME                        | GROUP PRIORITY  
-----  
--  
rad_grpl                          | 0  
radius                            | 1  
-----  
--
```

```
switch(config)# aaa accounting all default start-stop group rad_grpl radius  
switch(config)#  
switch(config)# do show aaa accounting  
AAA Accounting:  
  Accounting Type                  : all  
  Accounting Mode                  : start-stop  
  
Default Accounting for All Channels:  
-----  
--  
GROUP NAME                        | GROUP PRIORITY  
-----  
--  
rad_grpl                          | 0  
radius                            | 1  
-----  
--
```

```
switch(config)# aaa accounting all default start-stop group rad_grpl radius  
switch(config)#  
switch(config)# do show aaa accounting
```

```
AAA Accounting:
  Accounting Type           : all
  Accounting Mode           : start-stop
```

```
Default Accounting for All Channels:
```

```
-----
--
GROUP NAME                | GROUP PRIORITY
-----
--
rad_grp1                  | 0
radius                    | 1
-----
--
```

aaa accounting allow-fail-through

```
aaa accounting allow-fail-through  
no aaa accounting allow-fail-through
```

Description

Enables accounting fail-through. When this option is enabled, the next server or accounting method is attempted after an accounting failure.

The **no** form of this command disables accounting fail-through. The system only attempts to reach the next server or accounting method if there is an accounting failure due to an unreachable TACACS+ or RADIUS server or a shared key mismatch error between the switch and the server.

Example

Enabling accounting fail-through:

```
switch(config)# aaa accounting allow-fail-through
```

Command History

Release	Modification
10.12.1000	Command introduced.

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

aaa accounting all-mgmt

```
aaa accounting all-mgmt <CONNECTION-TYPE> start-stop {local | group <GROUP-LIST>}  
no aaa accounting all-mgmt <CONNECTION-TYPE> start-stop {local | group <GROUP-LIST>}
```

Description

Defines accounting as being local (with the name **local**) (the default). Or defines a sequence of remote AAA server groups to be accessed for accounting purposes.

For remote accounting, the information is sent to the first reachable remote server that was configured with this command for remote accounting. If no remote server is reachable, local accounting remains available. Each available connection type (channel) can be configured individually as either local or using remote AAA server groups. All server groups named in your command, must exist. This command can be issued multiple times, once for each connection type. Local is always available for any connection type not configured for remote accounting.



The system accounting log is not associated with any connection type (channel) and is therefore sent to the accounting method configured on the default connection type (channel) only.

The **no** form of this command removes for the specified connection type, any defined remote AAA server group accounting sequence. Local accounting is available for connection types without a configured remote AAA server group list (whether default or for the specific connection type).

Parameter	Description
<code><CONNECTION-TYPE></code>	One of these connection types (channels): default Defines a list of accounting server groups to be used for the default connection type. This configuration applies to all other connection types (console, ssh, https-server, telnet) that are not explicitly configured with this command. For example, if you do not use aaa accounting all-mgmt console... to define the console accounting list, then this default configuration is used for console. console Defines a list of accounting server groups to be used for the console connection type. ssh Defines a list of accounting server groups to be used for the ssh connection type. https-server Defines a list of accounting server groups to be used for the https-server (REST, Web UI) connection type. telnet Defines a list of accounting server groups to be used for the telnet connection type.
<code>start-stop</code>	Selects accounting information capture at both the beginning and end of a process.
<code>local</code>	Selects local-only accounting when used without the group parameter.
<code>group <GROUP-LIST></code>	Specifies the list of remote AAA server group names. Each name can be specified one time. Predefined remote AAA group names tacacs and radius are available. Although not a group name, predefined name local is available. User-defined TACACS+ and RADIUS server group names may also be used. The remote AAA server groups are accessed in the order that the group names are listed in this command. Within each group, the servers are accessed in the order in which the servers were added to the group. Server groups are defined using command aaa group server and servers are added to a server group with the command server. If the remote server(s) in the group is unreachable or if there is a

Parameter	Description
	key mismatch error between the switch and the AAA Server, then the next accounting method is attempted.

Usage

Local accounting is always active. It cannot be turned off.

Examples

Defining the default accounting sequence based on two user-defined TACACS+ server groups, then the default TACACS+ server group, and finally (if needed), local accounting.

```
switch(config)# aaa accounting all-mgmt default start-stop group tg1 tg2 tacacs
local
```

Defining the console accounting sequence based on two user-defined TACACS+ server groups, then the default TACACS+ server group, and finally (if needed), local accounting.

```
switch(config)# aaa accounting all-mgmt console start-stop group tg2 tg3 tacacs
local
```

Defining the ssh accounting sequence based on one user-defined TACACS+ server group and then the default TACACS+ server group.

```
switch(config)# aaa accounting all-mgmt ssh start-stop group tg2 tacacs
```

Defining the Telnet accounting sequence based on one user-defined TACACS+ server group and then the default TACACS+ server groups.

```
switch(config)# aaa accounting all-mgmt telnet start-stop group tg1 tacacs
```

Defining the default accounting sequence based on two user-defined RADIUS server groups, then the default RADIUS server group, and finally (if needed), local accounting.

```
switch(config)# aaa accounting all-mgmt default start-stop group rg1 rg2 radius
local
```

Defining the https-server accounting sequence based on one user-defined RADIUS server group and then the default RADIUS server group.

```
switch(config)# aaa accounting all-mgmt https-server start-stop group rg1 radius
```

Setting local accounting for the default connection type:

```
switch(config)# aaa accounting all-mgmt default start-stop local
```

Command History

Release	Modification
10.11	Added the telnet parameter for all other platforms.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

aaa authentication allow-fail-through

```
aaa authentication allow-fail-through
no aaa authentication allow-fail-through
```

Description

Enables authentication fail-through. If this feature is enabled, the next server or authentication method is tried after an authentication failure.

The **no** form of this command disables authentication fail-through. The system only attempts to reach the next server or authentication method if there is an accounting failure due to an unreachable TACACS+/RADIUS server or a shared key mismatch error between the switch and the server.



If your switch uses command authorization, best practices is to configure [authorization fail-through](#) before configuring authentication fail-through. If not, the switch may fall into an unusable state where authorization will fail for all commands.

Example

Enabling authentication fail-through:

```
switch(config)# aaa authentication allow-fail-through
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

aaa authentication login

```
aaa authentication login <CONNECTION-TYPE> {local | group <GROUP-LIST>}  
no aaa authentication login <CONNECTION-TYPE> {local | group <GROUP-LIST>}
```

Description

Defines authentication as being local (with the name **local**) (the default). Or defines a sequence of remote AAA server groups to be accessed for authentication purposes. Each available connection type (channel) can be configured individually as either local or using remote AAA server groups. All server groups named in your command, must exist. This command can be issued multiple times, once for each connection type. Local is always available for any connection type not configured for remote AAA authentication.



If you do not want local authentication to occur in cases where all AAA servers contacted reject the user's credentials, do not enable authentication fail-through (command **aaa authentication allow-fail-through**).

The **no** form of this command removes for the specified connection type, any defined remote AAA server group authentication sequence. Local authentication is available for connection types without a configured remote AAA server group list (whether default or for the specific connection type).

Parameter	Description
<CONNECTION-TYPE>	One of these connection types (channels): default Defines a list of AAA server groups to be used for the default connection type. This configuration applies to all other connection types (console, ssh, https-server, telnet) that are not explicitly configured with this command. For example, if you do not use aaa accounting all-mgmt console... to define the console accounting list, then this default configuration is used for console. console Defines a list of AAA server groups to be used for the console connection type. ssh Defines a list of AAA server groups to be used for the ssh connection type. https-server Defines a list of AAA server groups to be used for the https-server (REST, Web UI) connection type. telnet Defines a list of AAA server groups to be used for the telnet connection type.
local	Selects local-only authentication when used without the group parameter.
group <GROUP-LIST>	Specifies the list of remote AAA server group names. Each name can be specified one time. Predefined remote AAA group names tacacs and radius are available. Although not a group name, predefined name local is available. User-defined TACACS+ and RADIUS server group names may also be used. The remote AAA server groups are accessed in the order that the group names are listed in this command. Within each group, the

Parameter	Description
	servers are accessed in the order in which the servers were added to the group. Server groups are defined using command aaa group server and servers are added to a server group with the command server . If the remote server(s) in the group is unreachable or if there is a key mismatch error between switch and the AAA Server, then the next authentication method is attempted.

Examples

Defining the default authentication sequence based on two user-defined TACACS+ server groups, then the default TACACS+ server group, and finally (if needed), local authentication.

```
switch(config)# aaa authentication login default group tg1 tg2 tacacs local
```

Defining the default authentication sequence based on two user-defined TACACS+ server groups, then the default TACACS+ server group, and finally (if needed), local authentication.

```
switch(config)# aaa authentication login console group tg2 tg3 tacacs local
```

Defining the ssh authentication sequence based on one user-defined TACACS+ server group and then the default TACACS+ server group.

```
switch(config)# aaa authentication login ssh group tg2 tacacs
```

Defining the Telnet authentication sequence with two user-defined TACACS+ server groups, the default TACACS+ server group, and finally (if needed), local authentication.

```
switch(config)# switch(config)# aaa authentication login telnet group tg1 tg2
tacacs local
```

Defining the default authentication sequence based on two user-defined RADIUS server groups, then the default RADIUS server group, and finally (if needed), local authentication.

```
switch(config)# aaa authentication login default group rg1 rg2 radius local
```

Defining the https-server authentication sequence based on one user-defined RADIUS server group and then the default RADIUS server group.

```
switch(config)# aaa authentication login https-server group rg1 radius
```

Setting local authentication for the default connection type:

```
switch(config)# aaa authentication login default local
```

Command History

Release	Modification
10.11	Added the telnet parameter on 10000, 9300, 83xx, 6100, 6000 and 4100i Switch Series.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

aaa authorization allow-fail-through

```
aaa authorization allow-fail-through
no aaa authorization allow-fail-through
```

Description

Enables authorization fail-through. When this option is enabled, the next server or authorization method is attempted after an authorization failure.

The **no** form of this command disables authorization fail-through. The system only attempts to reach the next server or authorization method if there is an authorization failure due to an unreachable TACACS+ server or a shared key mismatch error between the switch and the server.



If your switch uses command authorization, best practices is to configure [authorization fail-through](#) before configuring authentication fail-through. If not, the switch may fall into an unusable state where authorization will fail for all commands.

Example

Enabling authorization fail-through:

```
switch(config)# aaa authorization allow-fail-through
```

The following configurations use authorization fail-through in different scenarios.

Example configuration one:

```
aaa authentication allow-fail-through
aaa authorization allow-fail-through
aaa group server tacacs CPPM-TACACS
server 172.16.1.12
aaa authentication login ssh group CPPM-TACACS local
aaa authorization commands ssh group CPPM-TACACS local
```

Example configuration one does not support authentication via the TACACS+ server for a locally configured user. If the user is configured locally and that user does not have a profile present in the TACACS+ server, authentication fails with TACACS+, but the user is authenticated successfully with local

authentication. Similarly, if authorization is rejected, the user is authorized locally with a fail-through configuration.

Example configuration two:

```
aaa group server tacacs CPPM-TACACS
server 172.16.1.12
aaa authentication allow-fail-through
aaa authorization allow-fail-through
aaa authentication login ssh group CPPM-TACACS local
aaa authorization commands ssh group local CPPM-TACACS
```

With configuration two, if a user's profile is configured only in the TACACS+ server, user authorization is rejected locally and is authorized with TACACS using the fail-through configuration. When authentication fail-through is configured, if the first authentication method fails, authentication is attempted using the next server or authentication method. The authorization fail-through is based on the authorization sequence, and is independent of the authentication method of the user.

Example configuration three:

```
aaa group server tacacs CPPM-TACACS
server 172.16.1.12
aaa group server tacacs TACACS
server 192.168.10.15
aaa authentication allow-fail-through
aaa authorization allow-fail-through
aaa authentication login ssh group CPPM-TACACS local
aaa authorization commands ssh group TACACS local
```

Example configuration four:

```
aaa group server radius RAD-GRP
server 172.16.1.12
aaa group server tacacs TACACS
server 192.168.10.15
aaa authentication allow-fail-through
aaa authorization allow-fail-through
aaa authentication login ssh group RAD-GRP local
aaa authorization commands ssh group TACACS local
```

With configurations three and four, the **CPPM-TACACS** or **RAD-GRP** groups reject authentication requests for locally configured users, and the users are authenticated locally with fail-through. Authorization is attempted with the TACACS group in these configurations, and if this authorization attempt fails, the user will be authorized locally due to the fail-through configuration.



When authorization is rejected by multiple servers/server groups due to the fail-through configuration, a delay may be seen while executing commands.

Command History

Release	Modification
10.12.1000	Command introduced.

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

aaa authorization commands

```
aaa authorization commands <CONNECTION-TYPE> {local | none}
no aaa authorization commands <CONNECTION-TYPE> {local | none}
aaa authorization commands <CONNECTION-TYPE> group <GROUP-LIST>
no aaa authorization commands <CONNECTION-TYPE> group <GROUP-LIST>
```

Description

Defines authorization as being basic local RBAC (specified as **none**), or as full-fledged local RBAC specified as **local** (the default), or as remote TACACS+ (specified with group <GROUP-LIST>). Each available connection type (channel) can be configured individually. All server groups named in the command, must exist. This command can be issued multiple times, once for each connection type.

The **no** form of this command unconfigures authorization for the specified connection type, reverting to the default of **local**.



Although only TACACS+ servers are supported for remote authorization, local authorization (basic or full-fledged) can be used with remote RADIUS authentication. If your switch uses command authorization, best practices is to configure [authorization fail-through](#) before configuring authentication fail-through. If not, the switch may fall into an unusable state where authorization will fail for all commands.

Parameter	Description
<CONNECTION-TYPE>	One of these connection types (channels): default Selects the default connection type for configuration. This configuration applies to all other connection types (console , ssh , telnet) that are not explicitly configured with this command. For example, if you do not use aaa authorization commands console... to define the console authorization list, then this default configuration is used for console. console Selects the console connection type for configuration. ssh Selects the ssh connection type for configuration. telnet Selects the telnet connection type for configuration.
local	When used alone without group <GROUP-LIST>, selects local authorization which can be used to provide authorization for a purely local setup without any remote AAA servers and also for when RADIUS is used for remote Authentication and Accounting but Authorization is local. When used after group , provides for fallback (to full-fledged local authorization) when every server in every specified TACACS+ server group cannot be reached.

Parameter	Description
	NOTE: If any TACACS+ server in the specified groups is reachable, but the command fails to be authorized by that server, the command is rejected and local authorization is never attempted. Local authorization is only attempted if every TACACS+ server cannot be reached.
none	When used alone without group <code><GROUP-LIST></code>, selects basic local RBAC authorization, for use with the built-in user groups (administrators, operators, auditors). When used after group, provides for fallback (to basic local RBAC authorization) when every server in every specified TACACS+ server group cannot be reached. NOTE: With none, for users belonging to user-defined user groups, all commands can be executed regardless of what authorization rules are defined in such groups. For per-command local authorization, use local instead.
group <code><GROUP-LIST></code>	Specifies the list of remote AAA server group names. Predefined remote AAA group name tacacs is available. User-defined TACACS+ server group names may also be used. The remote AAA server groups are accessed in the order that the group names are listed in this command. Within each group, the servers are accessed in the order in which the servers were added to the group. Server groups are defined using command aaa server group and servers are added to a server group using command server. It is recommended to always include either the special name local or none as the last name in the group list. If both local and none are omitted, and no remote AAA server is reachable (or the first reachable server cannot authorize the command), command execution for the current user will not be possible. If the AAA server(s) in the group are not reachable, or if there is a key mismatch error between the server and the switch, the next authorization method is attempted.

Usage

TACACS+ server authorization considerations



Use caution when configuring authorization, as it has no fail through. If the switch is not configured properly, the switch might get into an unusable state in which all command execution is prohibited.

To prevent authorization difficulties:

- Make sure that all listed TACACS+ servers can authorize users for command execution.
- Make sure that credential database changes are promptly synchronized across all TACACS+ servers.
- Make sure either **local** or **none** is included as the last name in the group list. If both **local** and **none** are omitted, and no remote TACACS+ server is reachable (or the first reachable server cannot authorize), authorization will not be possible.
- Although not recommended, if you choose to omit both **local** and **none** from the list, and are manipulating configuration files, special caution is necessary. If the source configuration includes TACACS+ authorization and you are copying configuration from an existing switch into the running configuration of a new switch, and you have not yet configured the interface or routing information

to reach the TACACS+ server, the switch will enter an unusable state, requiring hard reboot.

To avoid getting into this situation that can occur when **local** and **none** have been omitted, do either of the following:

- In the configuration source, delete or comment-out the line configuring remote authorization. Then, after the configuration copy and paste, manually configure authorization.
- Move the line configuring the authorization to the end of the source configuration before copying and pasting.

Examples

Defining the default authorization sequence based on a user-defined TACACS+ server group, then the default TACACS+ server group, and finally (as a precaution), **local** authorization:

```
switch(config)# aaa authorization commands default group tg1 tacacs local  
All commands will fail if none of the servers in the group list are reachable.  
Continue (y/n)? y
```

Defining the Telnet authorization sequence based on a user-defined TACACS+ server group, then the default TACACS+ server group, and finally (as a precaution), **local** authorization:

```
switch(config)# aaa authorization commands telnet group tg1 tacacs local  
All commands will fail if none of the servers in the group list are reachable.  
Continue (y/n)? y
```

Defining the console authorization sequence based on two user-defined TACACS+ server groups, and finally (as a precaution), **local** authorization:

```
switch(config)# aaa authorization commands console group tg1 tg2 local  
All commands will fail if none of the servers in the group list are reachable.  
Continue (y/n)? y
```

Setting the authorization for default to **local**:

```
switch(config)# aaa authorization commands default local
```

Setting the authorization for the SSH interface to **none**:

```
switch(config)# aaa authorization commands ssh none
```

Command History

Release	Modification
10.11	Added the telnet parameter on the 10000, 9300, 83xx, 6100, 6000 and 4100i Switch Series.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

aaa group server

```
aaa group server {tacacs | radius} <SERVER-GROUP-NAME>
no aaa group server {tacacs | radius} <SERVER-GROUP-NAME>
```

Description

Creates an AAA server group that is either empty or contains preconfigured RADIUS/TACACS+ servers. You can create a maximum of 28 server groups.

The **no** form of this command deletes a server group. Only a preconfigured user-defined RADIUS/TACACS+ server group can be deleted. RADIUS or TACACS+ servers that were in a deleted server group remain a part of their default server group. The default server group for TACACS+ servers is **tacacs**. The default server group for RADIUS servers is **radius**.

Parameter	Description
server {tacacs radius}	Select either tacacs or radius for the server type.
<SERVER-GROUP-NAME>	Specifies the name of the server group to be created. The name of the server group can have a maximum of 32 characters.

Examples

Creating TACACS+ server group sg1:

```
switch(config)# aaa group server tacacs sg1
```

Creating RADIUS server group sg3:

```
switch(config)# aaa group server radius sg3
```

Deleting TACACS+ server group sg1:

```
switch(config)# no aaa group server tacacs sg1
```

Deleting RADIUS server group sg3:

```
switch(config)# no aaa group server radius sg3
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

radius-server auth-type

```
radius-server auth-type {pap | chap}
no radius-server auth-type {pap | chap}
```

Description

Enables the CHAP or PAP authentication protocol, which is used for communication with the RADIUS servers, at the global level. You can override this command with a fine-grained per server **auth-type** configuration.

The **no** form of this command resets the global authentication mechanism for RADIUS to PAP or CHAP. PAP is the default authentication mechanism for RADIUS.

Parameter	Description
auth-type {pap chap}	Selects either the PAP or CHAP authentication protocol.

Examples

Authenticating CHAP:

```
switch(config)# radius-server auth-type chap
```

Authenticating PAP:

```
switch(config)# radius-server auth-type pap
```

Removing CHAP authentication:

```
switch(config)# no radius-server auth-type chap
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

radius-server host

```
radius-server host {<FQDN> | <IPv4> | <IPv6>}  
    [key [plaintext <PASSKEY> | ciphertext <PASSKEY>]]  
    [timeout <TIMEOUT-SECONDS>] [port <PORT-NUMBER>]  
    [auth-type {pap | chap}] [acct-port <ACCT-PORT>] [retries <RETRY-COUNT>]  
    [tracking {enable | disable}] [tracking-mode {any | dead-only}][vrf <VRF-NAME>]  
no radius-server host {<FQDN> | <IPv4> | <IPv6>}  
    [key [plaintext <PASSKEY> | ciphertext <PASSKEY>]]  
    [timeout <TIMEOUT-SECONDS>] [port <PORT-NUMBER>]  
    [auth-type {pap | chap}] [acct-port <ACCT-PORT>] [retries <RETRY-COUNT>]  
    [tracking {enable | disable}] [tracking-mode {any | dead-only}][vrf <VRF-NAME>]
```

Description

Adds a RADIUS server. By default, the RADIUS server is associated with the server group named **radius**. The **no** form of this command removes a previously added RADIUS server.



For enhanced security with IPsec, the alternative command **radius-server host secure ipsec** is available. The standard non-IPsec **radius-server host** command does not modify any existing IPsec configuration. If IPsec is already configured for the RADIUS server, then IPsec will remain enabled for the server.

Parameter	Description
{<FQDN> <IPv4> <IPv6>}	Specifies the RADIUS server as: ▪ <FQDN>: a fully qualified domain name. ▪ <IPv4>: an IPv4 address. ▪ <IPv6>: an IPv6 address.
key [plaintext <PASSKEY> ciphertext <PASSKEY>]	Selects either a plaintext or an encrypted local shared-secret passkey for the server. As per RFC 2865, shared-secret can be a mix of alphanumeric and special characters. Plaintext passkeys are between 1 and 32 alphanumeric and special characters. NOTE: When key is entered without either sub-parameter, plaintext passkey prompting occurs upon pressing Enter. Enter must be pressed immediately after the key parameter without entering other parameters. The entered passkey characters are masked with asterisks. When key is omitted, the server uses the global passkey. This command requires either the global or local passkey to be set; otherwise the server will not be contacted. Command radius-server key is available for setting the global passkey.
timeout <TIMEOUT-SECONDS>	Specifies the timeout. Range: 1 to 60 seconds. If a timeout is not specified, the value from the global timeout for RADIUS is used.
port <PORT-NUMBER>	Specifies the authentication port number. Range: 1 to 65535. Default: 1812.
auth-type {pap chap}	Selects either the PAP (the default) or CHAP authentication types. If this parameter is not specified, the RADIUS global default is used.
acct-port <ACCT-PORT>	Specifies the UDP accounting port number. Range: 1 to 65535. Default: 1813.

Parameter	Description
<code>retries <RETRY-COUNT></code>	Specifies the number of retry attempts for contacting the specified RADIUS server. Range is 0 to 5 attempts. If no retry value is provided, the default value of 1 is used.
<code>tracking {enable disable}</code>	Enables or disables server tracking for the RADIUS server. Tracked servers are probed at the start of each server tracking interval to check if they are reachable. Use command radius-server tracking to configure RADIUS server tracking globally. NOTE: Server tracking uses authentication request and response packets to determine server reachability status. The server tracking user name and password are used to form the request packet which is sent to the server with tracking enabled. Upon receiving a response to the request packet, the server is considered to be reachable.
<code>tracking-mode {any dead-only}</code>	Configures tracking mode for the RADIUS server that has tracking enabled with the server. The tracking mode is used to monitor the status of RADIUS server reachability. The default tracking mode is any. any Track the RADIUS server irrespective of its server reachability. dead-only Track the RADIUS server only when the server is marked as unreachable.
<code>vrf <VRF-NAME></code>	Specifies the VRF name to be used for communicating with the server. If no VRF name is provided, the default VRF named default is used.

Usage

If the fully qualified domain name is provided for the RADIUS server, a DNS server must be configured and accessible through the same VRF which is configured for the RADIUS server. This configuration is required for the resolution of the RADIUS server hostname to its IP address. If a DNS server is not available for this VRF, the RADIUS servers reachable through this VRF must be configured by means of their IP addresses only.

Examples

Adding a RADIUS server with an IPv4 address and a prompted passkey:

```
switch(config)# radius-server host 1.1.1.5 key
Enter the RADIUS server key: *****
Re-Enter the RADIUS server key: *****
```

Deleting a RADIUS server with an IPv4 address and a prompted passkey:

```
switch(config)# no radius-server host 1.1.1.5 key
Enter the RADIUS server key: *****
Re-Enter the RADIUS server key: *****
```

Adding a RADIUS server with an IPv4 address and a named VRF:

```
switch(config)# radius-server host 1.1.1.1 vrf mgmt
```

Deleting a RADIUS server with an IPv4 address and a named VRF:

```
switch(config)# no radius-server host 1.1.1.1 vrf mgmt
```

Adding a RADIUS server with an IPv4 address, a port, and a named VRF:

```
switch(config)# radius-server host 1.1.1.2 port 32 vrf mgmt
```

Deleting a RADIUS server with an IPv4 address, a port, and a named VRF:

```
switch(config)# no radius-server host 1.1.1.2 port 32 vrf mgmt
```

Adding a RADIUS server with an IPv6 address:

```
switch(config)# radius-server host 2001:0db8:85a3:0000:0000:8a2e:0370:7334
```

Deleting a RADIUS server with an IPv6 address:

```
switch(config)# no radius-server host 2001:0db8:85a3:0000:0000:8a2e:0370:7334
```

Adding a RADIUS server with tracking enabled and tracking mode is set to dead-only:

```
switch(config)# radius-server host 1.1.1.1 tracking enable tracking-mode dead-only
```

Deleting a RADIUS server with tracking enabled and tracking mode is set to dead-only:

```
switch(config)# no radius-server host 1.1.1.1 tracking enable tracking-mode dead-only
```

Adding a RADIUS server with tracking disabled:

```
switch(config)# radius-server host 1.1.1.1 tracking disable
```

Deleting a RADIUS server with tracking disabled:

```
switch(config)# no radius-server host 1.1.1.1 tracking disable
```

Deleting a RADIUS server with an IPv4 address and specified VRF:

```
switch(config)# no radius-server host 1.1.1.1 vrf mgmt
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

radius-server host secure ipsec

Syntax for a RADIUS server that uses IPsec for authentication:

```
radius-server host {<FQDN> | <IPV4> | <IPV6>}
[key [plaintext <PASSKEY> | ciphertext <PASSKEY>]]
[timeout <TIMEOUT-SECONDS>] [port <PORT-NUMBER>]
[auth-type {pap | chap}] [acct-port <ACCT-PORT>] [retries <RETRY-COUNT>]
[tracking {enable | disable}] [tracking-mode {any | dead-only}] [vrf <VRF-NAME>]
secure ipsec authentication spi <SPI-INDEX> <AUTH-TYPE> <AUTH-KEY-TYPE> [<AUTH-KEY>]
no radius-server host {<FQDN> | <IPV4> | <IPV6>}
[key [plaintext <PASSKEY> | ciphertext <PASSKEY>]]
[timeout <TIMEOUT-SECONDS>] [port <PORT-NUMBER>]
[auth-type {pap | chap}] [acct-port <ACCT-PORT>] [retries <RETRY-COUNT>]
[tracking {enable | disable}] [tracking-mode {any | dead-only}] [vrf <VRF-NAME>]
secure ipsec authentication spi <SPI-INDEX><AUTH-TYPE><AUTH-KEY-TYPE> [<AUTH-KEY>]
```

Syntax for a RADIUS server that uses IPsec for both authentication and encryption:

```
radius-server host {<FQDN> | <IPV4> | <IPV6>}
[key [plaintext <PASSKEY> | ciphertext <PASSKEY>]]
[timeout <TIMEOUT-SECONDS>] [port <PORT-NUMBER>]
[auth-type {pap | chap}] [acct-port <ACCT-PORT>] [retries <RETRY-COUNT>]
[tracking {enable | disable}] [tracking-mode {any | dead-only}] [vrf <VRF-NAME>]
secure ipsec encryption spi <SPI-INDEX> <AUTH-TYPE> <AUTH-KEY-TYPE>
[<AUTH-KEY>] <ENCRYPT-TYPE> <ENCRYPT-KEY-TYPE> [<ENCRYPT-KEY>]
no radius-server host {<FQDN> | <IPV4> | <IPV6>}
[key [plaintext <PASSKEY> | ciphertext <PASSKEY>]]
[timeout <TIMEOUT-SECONDS>] [port <PORT-NUMBER>]
[auth-type {pap | chap}] [acct-port <ACCT-PORT>] [retries <RETRY-COUNT>]
[tracking {enable | disable}] [tracking-mode {any | dead-only}] [vrf <VRF-NAME>]
secure ipsec encryption spi <SPI-INDEX><AUTH-TYPE><AUTH-KEY-TYPE>
[<AUTH-KEY>] <ENCRYPT-TYPE><ENCRYPT-KEY-TYPE> [<ENCRYPT-KEY>]
```

Description

Adds a RADIUS server that uses IPsec for enhanced security (authentication and possibly encryption). By default, the RADIUS server is associated with the server group named **radius**.

The **no** form of this command removes a previously added RADIUS (with IPsec) server.



Unless enhanced security with IPsec is required, use the **radius-server host** command instead.

Parameter	Description
{<FQDN> <IPv4> <IPv6>}	Specifies the RADIUS server as: ▪ <FQDN>: a fully qualified domain name. ▪ <IPv4>: an IPv4 address. ▪ <IPv6>: an IPv6 address.
key [plaintext <PASSKEY> ciphertext <PASSKEY>]	Selects either a plaintext or an encrypted local shared-secret passkey for the server. As per RFC 2865, shared-secret can be a mix of alphanumeric and special characters. Plaintext passkeys are between 1 and 32 alphanumeric and special characters. NOTE: When key is entered without either sub-parameter, plaintext passkey prompting occurs upon pressing Enter. Enter must be pressed immediately after the key parameter without entering other parameters. The entered passkey characters are masked with asterisks. When key is omitted, the server uses the global passkey. This command requires either the global or local passkey to be set; otherwise the server will not be contacted. Command radius-server key is available for setting the global passkey.
timeout <TIMEOUT-SECONDS>	Specifies the timeout. Range: 1 to 60 seconds. If a timeout is not specified, the value from the global timeout for RADIUS is used.
port <PORT-NUMBER>	Specifies the authentication port number. Range: 1 to 65535. Default: 1812.
auth-type {pap chap}	Selects either the PAP (the default) or CHAP authentication types. If this parameter is not specified, the RADIUS global default is used.
acct-port <ACCT-PORT>	Specifies the UDP accounting port number. Range: 1 to 65535. Default: 1813.
retries <RETRY-COUNT>	Specifies the number of retry attempts for contacting the specified RADIUS server. Range is 0 to 5 attempts. If no retry value is provided, the default value of 1 is used.
tracking {enable disable}	Enables or disables server tracking for the RADIUS server. Tracked servers are probed at the start of each server tracking interval to check if they are reachable. Use command radius-server tracking to configure RADIUS server tracking globally. NOTE: Server tracking uses authentication request and response packets to determine server reachability status. The server tracking user name and password are used to form the request packet which is sent to the server with tracking enabled. Upon receiving a response to the request packet, the server is considered to be reachable.
tracking-mode {any dead-only}	Configures tracking mode for the RADIUS server that has tracking enabled with the server. The tracking mode is used to monitor the status of RADIUS server reachability. The default tracking mode is any . any Track the RADIUS server irrespective of its server reachability.

Parameter	Description
	dead-only Track the RADIUS server only when the server is marked as unreachable.
vrf <VRF-NAME>	Specifies the VRF name to be used for communicating with the server. If no VRF name is provided, the default VRF named default is used.
spi <SPI-INDEX>	Specifies the Security Parameters Index. The SPI is an identification tag carried in the IPsec AH header. The SPI must be unique on the switch. Range: 256 to 4294967295.
<AUTH-TYPE>	Specifies the authentication algorithm: md5 , sha1 , or sha256 .
<AUTH-KEY-TYPE>	Specifies the authentication key type: plaintext , hex-string , or ciphertext .
[<AUTH-KEY>]	Specifies the authentication key. For <AUTH-TYPE> of ciphertext , this is the ciphertext string. For <AUTH-TYPE> of plaintext or hex-string : ▪ md5 (plaintext): 1 to 16 characters, (hex-string): 2 to 32 hexadecimal digits. ▪ sha1 (plaintext): 1 to 20 characters, (hex-string): 2 to 40 hexadecimal digits. ▪ sha256 (plaintext): 1 to 32 characters, (hex-string): 2 to 64 hexadecimal digits. NOTE: When <AUTH-KEY-TYPE> is not followed by <AUTH-KEY>, plaintext authentication key prompting occurs upon pressing Enter. Enter must be pressed immediately after the <AUTH-KEY-TYPE> parameter without entering other parameters. The entered authentication key characters are masked with asterisks.
<ENCRYPT-TYPE>	Specifies the encryption algorithm: 3des , aes , des , or null .
<ENCRYPT-KEY-TYPE>	Specifies the encryption key type: plaintext , hex-string , or ciphertext .
[<ENCRYPT-KEY>]	Specifies the encryption key. For <ENCRYPT-TYPE> of ciphertext , this is the ciphertext string. For <ENCRYPT-TYPE> of plaintext or hex-string : ▪ 3des (plaintext): 24 characters, (hex-string): 48 hexadecimal digits. ▪ aes (plaintext): 16, 24, or 32 characters, (hex-string): 32, 48, or 64 hexadecimal digits. ▪ des (plaintext): 8 characters, (hex-string): 16 hexadecimal digits. NOTE: When <ENCRYPT-KEY-TYPE> is not followed by <ENCRYPT-KEY>, plaintext encryption key prompting occurs upon pressing Enter. Enter must be pressed immediately after the <ENCRYPT-KEY-TYPE> parameter without entering other parameters. The entered encryption key characters are masked with asterisks.

Usage

If the fully qualified domain name is provided for the RADIUS server host, a DNS server must be configured and accessible through the same VRF as mentioned for the server host. This configuration is required for the resolution of the RADIUS server hostname to its IP address. If a DNS server is not available for this VRF, the RADIUS servers reachable through this VRF must be configured by means of their IP addresses only.

Examples

Adding a RADIUS server with an IPv4 address, a plaintext passkey, and IPsec authentication (md5 plaintext).

```
switch(config)# radius-server host 1.1.1.1 key plaintext 98ab vrf mgmt secure
ipsec authentication spi 261 md5 plaintext 1abc
```

Deleting a RADIUS server with an IPv4 address, a plaintext passkey, and IPsec authentication (md5 plaintext).

```
switch(config)# no radius-server host 1.1.1.1 key plaintext 98ab vrf mgmt secure
ipsec authentication spi 261 md5 plaintext 1abc
```

Adding a RADIUS server with an IPv4 address and a prompted IPsec authentication (md5) plaintext authentication key.

```
switch(config)# radius-server host 1.1.1.1 secure ipsec authentication spi 261
md5
Enter the IPsec authentication key: *****
Re-Enter the IPsec authentication key: *****
```

Deleting a RADIUS server with an IPv4 address and a prompted IPsec authentication (md5) plaintext authentication key.

```
switch(config)# no radius-server host 1.1.1.1 secure ipsec authentication spi 261
md5
Enter the IPsec authentication key: *****
Re-Enter the IPsec authentication key: *****
```

Adding a RADIUS server with an IPv4 address, IPsec authentication (MD5 plaintext), and IPsec encryption (AES plaintext):

```
switch(config)# radius-server host 1.1.1.2 vrf mgmt secure
ipsec encryption spi 262 md5 plaintext 9xyz aes plaintext 1234567890abcdef
```

Deleting a RADIUS server with an IPv4 address, IPsec authentication (MD5 plaintext), and IPsec encryption (AES plaintext):

```
switch(config)# no radius-server host 1.1.1.2 vrf mgmt secure
ipsec encryption spi 262 md5 plaintext 9xyz aes plaintext 1234567890abcdef
```

Adding a RADIUS server by providing an IPv4 address and IPsec MD5 authentication type, and then responding to prompts for the keys and encryption type:

```
switch(config)# radius-server host 1.1.1.6 secure ipsec encryption spi 262 md5
Enter the IPsec authentication key: *****
Re-Enter the IPsec authentication key: *****

Enter the IPsec encryption type (3des/aes/des/null)? aes

Enter the IPsec encryption key: *****
Re-Enter the IPsec encryption key: *****
```

Deleting a RADIUS server by providing an IPv4 address and IPsec MD5 authentication type, and then responding to prompts for the keys and encryption type:

```
switch(config)# no radius-server host 1.1.1.6 secure ipsec encryption spi 262 md5
Enter the IPsec authentication key: *****
Re-Enter the IPsec authentication key: *****

Enter the IPsec encryption type (3des/aes/des/null)? aes

Enter the IPsec encryption key: *****
Re-Enter the IPsec encryption key: *****
```

Adding a RADIUS server with an IPv4 address, tracking enabled, tracking mode, IPsec authentication (MD5 plaintext), IPsec encryption (AES plaintext) is set to dead-only:

```
switch(config)# radius-server host 1.1.1.1 tracking enable tracking-mode dead-only
vrf mgmt secure ipsec encryption spi 262 md5 plaintext 9xyz
aes plaintext 1234567890abcdef
```

Deleting a RADIUS server with an IPv4 address, tracking enabled, tracking mode, IPsec authentication (MD5 plaintext), IPsec encryption (AES plaintext) is set to dead-only:

```
switch(config)# no radius-server host 1.1.1.1 tracking enable tracking-mode dead-only
vrf mgmt secure ipsec encryption spi 262 md5 plaintext 9xyz
aes plaintext 1234567890abcdef
```

Removing a RADIUS server:

```
switch(config)# no radius-server host 1.1.1.1 vrf mgmt
```

Removing the ipsec configuration from a RADIUS server:

```
switch(config)# no radius-server host 1.1.1.2 vrf mgmt secure ipsec encryption
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

radius-server host tls port-access

```
radius-server host {<FQDN> | <IPv4> | <IPv6>} tls port-access {status-server | keep-alive}
no radius-server host {<FQDN> | <IPv4> | <IPv6>} tls port-access {status-server | keep-alive}
```

Description

Configures the type of messages to be sent inside RadSec sessions for port access authentication. Default message type for port access authentication sessions is `status-server`.

The **no** form of this command removes the message type configured for port access authentication sessions and sets the default, **status-server**.

Parameter	Description
{<FQDN> <IPv4> <IPv6>}	Specifies the RADIUS server as: ▪ <FQDN>: a fully qualified domain name. ▪ <IPv4>: an IPv4 address. ▪ <IPv6>: an IPv6 address.
port-access {status-server keep-alive}	Specifies the message type to be used for port access authentication in RadSec sessions. Following message types are supported: ▪ status-server: Sets status server message type for authentication. ▪ keep-alive: Sets keep-alive message type for authentication. NOTE: Keep-alive as tracking method and for port access sessions is recommended in networks where a RadSec server is connected to more number of RadSec clients. The server requires additional resources to process status-server and access-request messages when compared to keep-alive messages. This is because status-server and access-request messages are RADIUS protocol packets. However, keep-alive packets are TCP control packets that does not require any additional resources for processing by the RadSec server.

Examples

Configuring the **keep-alive** messages for port access authentication in RadSec session on host **1.1.1.1**:

```
switch(config)# radius-server host 1.1.1.1 tls port-access keep-alive
```

Deleting the message type configured on host **1.1.1.1** for port access authentication session and setting the method to the default, **status-server**:

```
switch(config)# no radius-server host 1.1.1.1 tls port-access status-server
```

Command History

Release	Modification
10.10	Command introduced

Command Information

Platforms	Command context	Authority
8100 8360	config	Administrators or local user group members with execution rights for this command.

radius-server host tls tracking-method

```
radius-server host {<FQDN> | <IPv4> | <IPv6>} tls tracking-method {status-server | keep-alive | access-request}
no radius-server host {<FQDN> | <IPv4> | <IPv6>} tls tracking-method {status-server | keep-alive | access-request}
```

Description

Configures the tracking method to be used for RADIUS server tracking. RADIUS server tracking must be configured for enabling the tracking method. Default tracking method is **access-request**.

The **no** form of this command sets the tracking method to the default option, **access-request**.

Parameter	Description
{<FQDN> <IPv4> <IPv6>}	Specifies the RADIUS server as: ▪ <FQDN>: a fully qualified domain name. ▪ <IPv4>: an IPv4 address. ▪ <IPv6>: an IPv6 address.
tracking-method {status-server keep-alive access-request}	Specifies the tracking method for RadSec tracking. Following methods are supported: ▪ status-server: Status server responses are used to update the reachability status of the RadSec server. ▪ keep-alive: Server socket status is verified to update the reachability status of the RadSec server. NOTE: keep-alive as tracking method and for port access sessions is recommended in networks where a RadSec server is connected to more number of RadSec clients. The server requires additional resources to process status-server and access-request messages when compared to keep-alive messages. This is because status-server and access-request messages are RADIUS protocol packets. However, keep-alive packets are TCP control packets that does not require any additional resources for processing by the RadSec server.

Parameter	Description
	▪ access-request: Access response messages are used to update the reachability status of the RadSec server.

Usage

- If the network has a RADIUS proxy, then it is recommended to use the **access-request** tracking method to track the RadSec server.
- If **keep-alive** is the tracking method, then make sure to check whether the server has the capability to treat the **keep-alive** messages sent in RadSec sessions as valid RadSec messages to keep the session active.

Examples

Configuring the RADIUS server tracking method on host **1.1.1.1**:

```
switch(config)# radius-server host 1.1.1.1 tls tracking-method status-server
```

Deleting the RADIUS server tracking method on host **1.1.1.1** and setting the method to the default, **access-request**:

```
switch(config)# no radius-server host 1.1.1.1 tls tracking-method access-request
```

Command History

Release	Modification
10.10	Command introduced

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

radius-server key

```
radius-server key [plaintext <GLOBAL-PASSKEY> | ciphertext <GLOBAL-PASSKEY>]
no radius-server key [plaintext <GLOBAL-PASSKEY> | ciphertext <GLOBAL-PASSKEY>]
```

Description

Creates or modifies a RADIUS global passkey. The RADIUS global passkey is used as a shared-secret for encrypting the communication between all RADIUS servers and the switch. The RADIUS global passkey is required for authentication unless local passkeys have been set. By default, the RADIUS global passkey is empty. If the administrator has not set this key, the switch will not be able to perform RADIUS authentication. The switch will instead rely on the authentication mechanism configured with **aaa authentication login**.



When this command is entered without parameters, plaintext passkey prompting occurs upon pressing Enter. The entered passkey characters are masked with asterisks.

The **no** form of the command removes the global passkey.

Parameter	Description
plaintext <GLOBAL-PASSKEY>	Specifies the RADIUS global passkey in plaintext format with a length of 1 to 31 characters. As per RFC 2865, a shared-secret can be a mix of alphanumeric and special characters.
ciphertext <GLOBAL-PASSKEY>	Specifies the RADIUS global passkey in encrypted format.

Examples

Adding the global passkey:

```
switch(config)# radius-server key plaintext mypasskey123
```

Adding the global passkey with prompting:

```
switch(config)# radius-server key
Enter the RADIUS server key: *****
Re-Enter the RADIUS server key: *****
```

Removing the global passkey:

```
switch(config)# no radius-server key
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

radius-server retries

```
radius-server retries <0-5>
no radius-server retries <0-5>
```

Description

Sets at the global level the number of retries the switch makes before concluding that the RADIUS server is unreachable.

You can override this setting with a fine-grained per RADIUS server retries configuration.

The **no** form of this command resets the RADIUS global retries to the default retries value of 1.

Parameter	Description
<code>retries <0-5></code>	Specifies the number of retry attempts for contacting RADIUS servers. Range is 0 to 5 retries.

Example

```
switch(config)# radius-server retries 3
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

radius-server status-server interval

```
radius-server status-server interval <10-86400>  
no radius-server status-server interval <10-86400>
```

Description

Configures the time interval in seconds to send the status server requests to the RADIUS server.

The **no** form of this command configures the default time interval, **300** seconds.

Parameter	Description
<code><10-86400></code>	Specifies the status server time interval in seconds. Default: 300 .

Examples

Configuring the status server time interval of 200 seconds:

```
switch(config)# radius-server status-server interval 200
```

Resetting the status server time interval to the default, 300 seconds:

```
switch(config)# no radius-server status-server interval 200
```

Command History

Release	Modification
10.10	Command introduced

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

radius-server timeout

```
radius-server timeout [<1-60>]  
no radius-server timeout [<1-60>]
```

Description

Specifies the number of seconds to wait for a response from the RADIUS server before trying the next RADIUS server. If a value is not specified, a default value of 5 seconds is used. You can override this value with a fine-grained per server timeout configured for individual servers.

The **no** form of this command resets the RADIUS global authentication timeout to the default of 5 seconds.

Parameter	Description
timeout <1-60>	Specifies the timeout interval of 1 to 60 seconds. Default: 5 seconds.

Examples

Setting the RADIUS server timeout:

```
switch(config)# radius-server timeout 10
```

Resetting the timeout for the RADIUS server to the default:

```
switch(config)# no radius-server timeout
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

radius-server tracking

```
radius-server tracking interval <INTERVAL>
no radius-server tracking interval
```

```
radius-server tracking retries <RETRIES>
no radius-server tracking retries
```

```
radius-server tracking user-name <NAME>
    [password [plaintext <PASSWORD> | ciphertext <PASSWORD>]]
no radius-server tracking user-name <NAME>
    [password [plaintext <PASSWORD> | ciphertext <PASSWORD>]]
```

Description

Configures RADIUS server tracking settings globally for all configured RADIUS servers that have tracking enabled with the **radius-server host** command on individual servers.

The **no** form of the command removes the specified configuration, reverting it to its default. The **no** form with **user-name** also clears the password (resets it to empty).

Parameter	Description
<code>interval <INTERVAL></code>	Specifies the time interval, in seconds, to wait before checking the server reachability status. Default: 300. Range 60 to 84600.
<code>retries <RETRIES></code>	Specifies the number of server retries. Default: Global RADIUS retries. Range: 0 to 5.
<code>user-name <NAME></code> <code> [password [plaintext <PASSWORD> </code> <code> ciphertext <PASSWORD>]]</code>	Specifies the user name (and optionally a password) to be used for server checking. The default user name is radius-tracking-user with an empty password. The password is optional and may be entered as plaintext or pasted in as ciphertext. The plaintext password is visible as cleartext when entered but is encrypted thereafter. Command history does show the password as cleartext. NOTE: When password is entered without a following sub-parameter, plaintext password prompting occurs upon pressing Enter. The entered password characters are masked with asterisks. NOTE: The user does not have to be configured on the server. Server tracking can still be performed with a user which is not configured on the server because authentication failure on the server achieves confirmation that the server is reachable. NOTE: Server tracking uses authentication request and response packets to determine server reachability status.

Parameter	Description
	The server tracking user name and password are used to form the request packet which is sent to the server with tracking enabled. Upon receiving a response to the request packet, the server is considered to be reachable.

Examples

Configuring a tracking interval of 120 seconds:

```
switch(config)# radius-server tracking interval 120
```

Reverting the tracking interval to its default of 300 seconds:

```
switch(config)# no radius-server tracking interval
```

Configuring three retries:

```
switch(config)# radius-server tracking retries 3
```

Configuring user **radius-tracker** with a plaintext password.

```
switch(config)# radius-server tracking user-name radius-tracker
password plaintext track$1
```

Configuring user **radius-tracker** with a prompted plaintext password.

```
switch(config)# radius-server tracking user-name radius-tracker password
Enter the RADIUS server tracking password: *****
Re-Enter the RADIUS server tracking password: *****
```

Reverting the tracking user name to its default of **radius-tracking-user**:

```
switch(config)# no radius-server tracking user-name
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

server

```
server {<FQDN> | <IPv4> | <IPv6>} [port <PORT-NUMBER>] [vrf <VRF-NAME>]  
no server {<FQDN> | <IPv4> | <IPv6>} [port <PORT-NUMBER>] [vrf <VRF-NAME>]
```

Description

Adds a TACACS+ or RADIUS server to a server group. Only the configured TACACS+ or RADIUS servers are allowed to be added within the server group. If the same server name exists with multiple ports or multiple VRFs, specify the server name, port, and VRF when adding the server to the server-group.

The **no** form of this command removes a TACACS+/RADIUS server from a server-group.



On the 4100i, 6000, 6100, 6200, 6300, 6400, 8100, 8325, 8360, and 10000 Switch Series, a RADIUS server can be associated with a maximum of four different user-defined server groups.

On the 8320, 8400, and 9300 Switch Series, a RADIUS server can be associated with only one user-defined server group.

Parameter	Description
{<FQDN> <IPv4> <IPv6>}	Specifies the RADIUS server as: ▪ <FQDN>: a fully qualified domain name. ▪ <IPv4>: an IPv4 address. ▪ <IPv6>: an IPv6 address.
port <PORT-NUMBER>	Specifies the authentication port number. Range: 1 to 65535. Default TACACS+ (TCP): 49, RADIUS (UDP): 1812. If a port number is not provided, the system searches the TACACS+/RADIUS server by host name and sets the default authentication port. Group server priority is assigned based on the sequence in which the servers are added.
vrf <VRF-NAME>	Specifies the VRF name to be used for communicating with the server. If no VRF name is provided, the default VRF named default is used.

Examples

Adding a server to TACACS+ server group sg1 by providing an IPv4 address, port number, and VRF name:

```
switch(config)# aaa group server tacacs sg1  
switch(config-sg)# server 1.1.1.2 port 32 vrf default
```

Adding a server to TACACS+ server group sg2 by providing an IPv6 address and default VRF:

```
switch(config)# aaa group server tacacs sg2  
switch(config-sg)# server 2001:0db8:85a3:0000:0000:8a2e:0370:7334 vrf default
```

Adding a server to RADIUS server group sg3 by providing an IPv4 address, port number, and VRF name:

```
switch(config)# aaa group server radius sg3
switch(config-sg)# server 1.1.1.5 port 12 vrf default
```

Adding a server to RADIUS server group sg4 by providing an IPv6 address and default VRF:

```
switch(config)# aaa group server radius sg4
switch(config-sg)# server 2001:0db8:85a3:0000:0000:8a2e:0371:7334 vrf default
```

Adding a server to RADIUS server group sg4 by providing an IPv4 address, port number, and VRF name:

```
switch(config)# aaa group server radius sg4
switch(config-sg)# server 1.1.1.6 port 32 vrf vrf_red
```

Specifying an IPv4 address when removing a TACACS+ server from server group sg1:

```
switch(config)# aaa group server tacacs sg1
switch(config-sg)# no server 1.1.1.2 port 12 vrf default
```

Specifying an IPv6 address when removing a TACACS+ server from server group sg2 with the default VRF:

```
switch(config)# aaa group server tacacs sg2
switch(config-sg)# no server 2001:0db8:85a3:0000:0000:8a2e:0370:7334 vrf default
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-sg	Administrators or local user group members with execution rights for this command.

show aaa accounting

```
show aaa accounting [vsx-peer]
```

Description

Shows the accounting configuration per connection type (channel).

Parameter	Description
vsx-peer	Shows the output from the VSX peer switch. If the switches do not

Parameter	Description
	have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Examples

Configuring and then showing the accounting sequence for TACACS+ groups and local:

```
(config)# aaa accounting all-mgmt default start-stop group sgl tacacs radius
(config)# aaa accounting all-mgmt console start-stop local
(config)# aaa accounting all-mgmt ssh start-stop group radius tacacs local
(config)# aaa accounting all-mgmt https-server start-stop group sgl tacacs
(config)# aaa accounting all-mgmt telnet start-stop group radius tacacs local
(config)# show aaa accounting
```

AAA Accounting:

```
Accounting Type           : all
Accounting Mode           : start-stop
Accounting Failthrough    : Enabled
```

Accounting for https-server channel:

```
-----
GROUP NAME                | GROUP PRIORITY
-----
sgl                        | 0
tacacs                    | 1
-----
```

Accounting for console channel:

```
-----
GROUP NAME                | GROUP PRIORITY
-----
local                     | 0
-----
```

Accounting for default channel:

```
-----
GROUP NAME                | GROUP PRIORITY
-----
sgl                        | 0
tacacs                    | 1
radius                    | 2
-----
```

Accounting for ssh channel:

```
-----
GROUP NAME                | GROUP PRIORITY
-----
radius                    | 0
tacacs                    | 1
local                     | 2
-----
```

Accounting for telnet channel:

```
-----
GROUP NAME                | GROUP PRIORITY
-----
radius                    | 0
tacacs                    | 1
local                     | 2
-----
```

Configuring and then showing the accounting sequence for RADIUS groups and local:

```

switch(config)# aaa accounting all default start-stop group rg1 rg2 radius local
switch(config)# aaa accounting all console start-stop group rg4 radius local
switch(config)# exit
switch# show aaa accounting
AAA Accounting:
Accounting Type                : all
Accounting Mode                : start-stop
Accounting Failthrough         : Enabled
Accounting for default channel:
-----
GROUP NAME                     | GROUP PRIORITY
-----
rg1                            | 0
rg2                            | 1
radius                         | 2
local                          | 3
-----
Accounting for console channel:
-----
GROUP NAME                     | GROUP PRIORITY
-----
tg4                            | 0
radius                         | 1
local                          | 2
-----

```

Configuring and then showing only local accounting for default:

```

switch(config)# aaa accounting all default start-stop local
switch(config)# exit
switch# show aaa accounting
AAA Accounting:
Accounting Type                : all
Accounting Mode                : start-stop
Accounting for default channel:
-----
GROUP NAME                     | GROUP PRIORITY
-----
local                          | 0
-----

```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show aaa authentication

```
show aaa authentication [vsx-peer]
```

Description

Shows the authentication configuration per connection type (channel).

Parameter	Description
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Example

Configuring TACACS+ authentication sequences and then showing the configuration per connection type (channel):

```
switch(config)# aaa authentication login default group sg1 sg2 sg3 sg4 tacacs local
switch(config)# aaa authentication login ssh group sg1 sg2
switch(config)# aaa authentication login console group sg4 tacacs local
switch(config)# aaa authentication login https-server local group tacacs sg3
switch(config)# aaa authentication login telnet group sg1 sg2
switch(config)# exit
```

```
switch# show aaa authentication
```

```
AAA Authentication:
```

```
Fail-through           : Enabled
Limit Login Attempts   : Not set
Lockout Time           : 300
Minimum Password Length : Not set
```

```
Authentication for ssh channel:
```

```
-----
GROUP NAME                | GROUP PRIORITY
-----
sg1                        | 0
sg2                        | 1
-----
```

```
Authentication for https-server channel:
```

```
-----
GROUP NAME                | GROUP PRIORITY
-----
local                     | 0
tacacs                    | 1
sg3                        | 2
-----
```

```
Authentication for console channel:
```

```
-----
GROUP NAME                | GROUP PRIORITY
-----
sg4                       | 0
tacacs                    | 1
local                     | 2
-----
```

```
Authentication for default channel:
```

GROUP NAME	GROUP PRIORITY
sg1	0
sg2	1
sg3	2
sg4	3
tacacs	4
local	5

Authentication for telnet channel:

GROUP NAME	GROUP PRIORITY
sg1	0
sg2	1

Configuring RADIUS authentication sequences and then showing the configuration per connection type (channel):

```
switch(config)# aaa authentication login default group rg1 rg2 rg3 rg4 radius local
switch(config)# aaa authentication login console group rg4 radius local
switch(config)# exit
switch# show aaa authentication
AAA Authentication:
  Fail-through           : Enabled
  Limit Login Attempts   : Not set
  Lockout Time           : 300
  Minimum Password Length : Not set
```

Authentication for default channel:

GROUP NAME	GROUP PRIORITY
rg1	0
rg2	1
rg3	2
rg4	3
radius	4
local	5

Authentication for console channel:

GROUP NAME	GROUP PRIORITY
rg4	0
radius	1
local	2

Configuring only default authentication and then showing the default connection type (channel):

```
switch(config)# aaa authentication login default local
switch(config)# exit
switch# show aaa authentication

AAA Authentication:
```

```

Fail-through           : Disabled
Limit Login Attempts   : Not set
Lockout Time           : 300
Minimum Password Length : Not set

```

Authentication for default channel:

```

-----
GROUP NAME                | GROUP PRIORITY
-----
local                     | 0
-----

```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show aaa authorization

show aaa authorization [vsx-peer]

Description

Shows the authorization configuration per connection type (channel).

Parameter	Description
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Example

Configuring and then showing the authorization sequence for default and console connection types (channels):

```

(config)# aaa authorization commands default group sg1 tacacs local
All commands will fail if none of the servers in the group list are reachable.
Continue (y/n)? y
(config)# aaa authorization commands ssh group sg2
All commands will fail if none of the servers in the group list are reachable.
Continue (y/n)? y
(config)# aaa authorization commands telnet group sg2
All commands will fail if none of the servers in the group list are reachable.

```

```

Continue (y/n)? y
(config)# aaa authorization commands console group sg1 local
All commands will fail if none of the servers in the group list are reachable.
Continue (y/n)? y
(config)# aaa authorization radius ssh group sg1
All commands will fail if none of the radsec servers in the group list are
reachable.
Continue (y/n)? y
(config)# aaa authorization radius https-server group sg2
All commands will fail if none of the radsec servers in the group list are
reachable.
Continue (y/n)? y

```

```

(config)# show aaa authorization

```

```

***** Command authorization *****

```

```

Authorization for console channel:

```

```

-----
GROUP NAME | GROUP PRIORITY
-----
sg1 | 0
local | 1
-----

```

```

Authorization for default channel:

```

```

-----
GROUP NAME | GROUP PRIORITY
-----
sg1 | 0
tacacs | 1
local | 2
-----

```

```

Authorization for ssh channel:

```

```

-----
GROUP NAME | GROUP PRIORITY
-----
sg2 | 0
-----

```

```

Authorization for telnet channel:

```

```

-----
GROUP NAME | GROUP PRIORITY
-----
sg2 | 0
-----

```

```

***** User authorization through radius *****

```

```

Authorization for ssh channel:

```

```

-----
GROUP NAME | GROUP PRIORITY
-----
sg1 | 0
-----

```

```

Authorization for https-server channel:

```

```

-----
GROUP NAME | GROUP PRIORITY
-----
sg2 | 0
-----

```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show aaa server-groups

```
show aaa server-groups [tacacs | radius] [vsx-peer]
```

Description

Shows TACACS+ and RADIUS AAA server group information for all server types or for the specified server type.

Parameter	Description
tacacs	Narrows the command output to only TACACS+ servers.
radius	Narrows the command output to only RADIUS servers.
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Example

Showing all AAA server group information:

```
switch# show aaa server-groups

***** AAA Mechanism TACACS+ *****
-----
GROUP NAME          | SERVER NAME                               | PORT | VRF      | PRIORITY
-----
sg2                  | 2001:0db8:85a3:0000:0000:8a2e:          | 49   | default  | 1
                    | 0370:7334                               |
sg1                  | 1.1.1.2                                 | 12   | mgmt     | 1
-----
tacacs (default)    | FQDN.com                               | 32   | mgmt     | 1
tacacs (default)    | 1.1.1.1                                 | 49   | mgmt     | 2
tacacs (default)    | 1.1.1.2                                 | 12   | mgmt     | 3
tacacs (default)    | abc.com                                | 32   | vrf_red  | 4
tacacs (default)    | 2001:0db8:85a3:0000:0000:8a2e:          | 49   | default  | 5
                    | 0370:7334                               |
tacacs (default)    | 1.1.1.3                                 | 32   | vrf_blue | 6
-----
***** AAA Mechanism RADIUS *****
```

GROUP NAME	SERVER NAME	PORT	VRF	PRIORITY
sg4	2001:0db8:85a3:0000:0000:8a2e:0370:7334	1812	default	1
sg3	1.1.1.5	12	mgmt	1
radius (default)	1.1.1.4	1812	mgmt	1
radius (default)	1.1.1.5	12	mgmt	2
radius (default)	abc1.com	32	mgmt	3
radius (default)	2001:0db8:85a3:0000:0000:8a2e:0370:7334	1812	default	4
radius (default)	1.1.1.6	32	vrf_red	5
radius (default)	1.1.1.7	32	vrf_blue	6

Showing TACACS+ server group information:

```
switch# show aaa server-groups tacacs
```

***** AAA Mechanism TACACS+ *****

GROUP NAME	SERVER NAME	PORT	VRF	PRIORITY
sg2	2001:0db8:85a3:0000:0000:8a2e:0370:7334	49	default	1
sg1	1.1.1.2	12	mgmt	1
tacacs (default)	FQDN.com	32	mgmt	1
tacacs (default)	1.1.1.1	49	mgmt	2
tacacs (default)	1.1.1.2	12	mgmt	3
tacacs (default)	abc.com	32	vrf_red	4
tacacs (default)	2001:0db8:85a3:0000:0000:8a2e:0370:7334	49	default	5
tacacs (default)	1.1.1.3	32	vrf_blue	6

Showing RADIUS server group information:

```
switch# show aaa server-groups radius
```

***** AAA Mechanism RADIUS *****

GROUP NAME	SERVER NAME	PORT	VRF	PRIORITY
sg4	2001:0db8:85a3:0000:0000:8a2e:0370:7334	1812	default	1
sg3	1.1.1.5	12	mgmt	1
radius (default)	1.1.1.4	1812	mgmt	1
radius (default)	1.1.1.5	12	mgmt	2
radius (default)	abc1.com	32	mgmt	3
radius (default)	2001:0db8:85a3:0000:0000:8a2e:0370:7334	1812	default	4
radius (default)	1.1.1.6	32	vrf_red	5

```
radius (default) | 1.1.1.7 | 32 | vrf_blue | 6
-----
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show accounting log

```
show accounting log [last <QTY-TO-SHOW> | all]
```

Description

Entered without optional parameters, this command shows all accounting log records for the current boot. Sensitive information is masked from the log, by being represented as asterisks.



This **show accounting log** command replaces the **show audit-log** command that is supported only in 10.00 releases.

Parameter	Description
last <QTY-TO-SHOW>	Specifies how many most-recent accounting log records to show for the current boot. Range: 1 to 1000.
all	Selects for showing, all accounting records from the current boot and the previous boot.

Usage

The log message starts with the record type, which is specific to AOS-CX. Values are the following:

USER_START

Record of a user login action.

USER_END

Record of a user logout action.

USYS_CONFIG

Record of a command executed by the user.

The three types of accounting log information are identified by the **msg=** element starting with the **rec=** item as follows:

- Exec is identified with: **msg='rec=ACCT_EXEC**
- Command is identified with: **msg='rec=ACCT_CMD**

- System is identified with: **msg='rec=ACCT_SYSTEM**

The user group is indicated by **priv-lvl**, which is specific to AOS-CX. Values are the following:

Privilege level	User group
1	operators
15	administrators
19	auditors

The value of **service** indicates which user interface was used:

`service=shell`

Indicates that the log entry is a result of a CLI command.

`service=https-server`

Indicates that the log entry is a result of a REST API request or a Web UI action.

The string value of **data** identifies the CLI command or REST API request that was executed.

These elements are shown in context under *Examples*.

Examples

Showing the accounting log for the previous and current boot. Line breaks have been added for readability.

```
switch# show accounting log all

-----
Local accounting logs from previous boot
-----
----
type=DAEMON_START msg=audit(Nov 05 2018 23:00:58.607:9057) :
auditd start, ver=2.4.3 format=raw kernel=4.9.119-yocto-standard res=success
----
type=USER_START msg=audit(Nov 05 2018 23:06:42.398:42) :
msg='rec=ACCT_EXEC op=start session=CONSOLE timezone=UTC user=user1 priv-lvl=15
auth-method=LOCAL auth-type=LOCAL service=shell isconfig=no
hostname=8xxx addr=0.0.0.0 res=success'
----
type=USYS_CONFIG msg=audit(Nov 05 2018 23:06:42.399:43) :
msg='rec=ACCT_CMD op=stop session=CONSOLE timezone=UTC user=user1 priv-lvl=15
auth-method=LOCAL auth-type=LOCAL service=shell isconfig=no
data="enable" hostname=8xxx addr=0.0.0.0 res=success'
----
type=USYS_CONFIG msg=audit(Nov 05 2018 23:08:24.693:51) :
msg='rec=ACCT_CMD op=stop session=CONSOLE timezone=UTC user=user1 priv-lvl=1
auth-method=LOCAL auth-type=LOCAL service=shell isconfig=no
data="configure terminal" hostname=8xxx addr=0.0.0.0 res=success'
----
type=USYS_CONFIG msg=audit(Nov 05 2018 23:08:39.108:52) :
msg='rec=ACCT_CMD op=stop session=CONSOLE timezone=UTC user=user1 priv-lvl=15
auth-method=LOCAL auth-type=LOCAL service=shell isconfig=yes
data="https-server rest access-mode read-write"
hostname=8xxx addr=0.0.0.0 res=success'
----
type=USER_START msg=audit(Nov 05 2018 23:10:57.238:58) :
```

```

msg='rec=ACCT_EXEC op=start session=REST timezone=UTC user=admin priv-lvl=15
auth-method=LOCAL auth-type=LOCAL service=https-server
data="http-method=POST http-uri=/rest/v1/login"
hostname=8xxx addr=127.0.0.1 res=success'
----
type=USYS_CONFIG msg=audit(Nov 05 2018 23:15:11.958:75) :
msg='rec=ACCT_CMD op=stop session=CONSOLE timezone=UTC user=user1 priv-lvl=15
auth-method=LOCAL auth-type=LOCAL service=shell isconfig=yes
data="tacacs-server host 2.2.2.2" hostname=8xxx addr=0.0.0.0 res=success'
----
type=USYS_CONFIG msg=audit(Nov 05 2018 23:15:37.090:76) :
msg='rec=ACCT_CMD op=stop session=REST timezone=UTC user=admin priv-lvl=15
auth-method=LOCAL auth-type=LOCAL service=https-server
data="http-method=GET http-uri=/rest/v1/system/vrfs/mgmt/tacacs_servers"
hostname=8xxx addr=127.0.0.1 res=success'
----
type=USER_END msg=audit(Nov 05 2018 23:26:59.207:90) :
msg='rec=ACCT_EXEC op=stop session=REST timezone=UTC user=admin priv-lvl=15
auth-method=LOCAL auth-type=LOCAL service=https-server
data="http-method=POST http-uri=/rest/v1/logout"
hostname=8xxx addr=127.0.0.1 res=success'
----
type=USER_END msg=audit(Nov 05 2018 23:27:49.164:93) :
msg='rec=ACCT_EXEC op=stop session=CONSOLE timezone=UTC user=user1 priv-lvl=15
auth-method=LOCAL auth-type=LOCAL service=shell isconfig=no
hostname=8xxx addr=0.0.0.0 res=success'

-----
Local accounting logs from current boot
-----
----
type=DAEMON_START msg=audit(Nov 05 2018 23:32:05.642:626) :
auditd start, ver=2.4.3 format=raw kernel=4.9.119-yocto-standard res=success
----
type=USER_START msg=audit(Nov 05 2018 23:35:52.915:11) :
msg='rec=ACCT_EXEC op=start session=CONSOLE timezone=UTC user=admin priv-lvl=15
auth-method=LOCAL auth-type=LOCAL service=shell isconfig=no
hostname=8xxx addr=0.0.0.0 res=success'
----
type=USYS_CONFIG msg=audit(Nov 05 2018 23:35:52.917:12) :
msg='rec=ACCT_CMD op=stop session=CONSOLE timezone=UTC user=admin priv-lvl=15
auth-method=LOCAL auth-type=LOCAL service=shell isconfig=no data="enable"
hostname=8xxx addr=0.0.0.0 res=success'

```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Manager (#) or Auditor (auditor)	Auditors or Administrators or local user group members with execution rights for this command. Auditors can execute this command from the auditor context (auditor>) only.

show radius-server

show radius-server [detail] [vsx-peer]

Description

Shows configured RADIUS servers information.

Parameter	Description
detail	Selects additional RADIUS server details and global parameters for showing.
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Usage

- When the **show radius-server** command shows **None** for the shared-secret, the passkey is missing.
- The **Tracking-Last-Attempted** and **Next-Tracking-Request** fields are applicable only when the RADIUS server tracking method is **access-request**.
- The **TLS Connection Status** section of the output of the **show radius-server detail** command displays the connection status of the TLS connection created for port-access (network client) authentication. If no port-access related configuration is present, the TLS Connection Status field displays a status of **N/A**.

Examples

Showing a summary of the global RADIUS configuration:

```
switch# show radius-server
***** Global RADIUS Configuration *****

Shared-Secret:<password>
Timeout: 60
Auth-Type: pap
Retries: 5
Tracking Time Interval (seconds): 60
Tracking Retries: 5
Tracking User-name: radius-tracking-user
Tracking Password: None
Number of Servers: 1
```

```
-----
SERVER NAME                               | PORT | VRF
-----
20.1.1.129                               | 1812 | default
1.1.1.4                                   | 1812 | default
1.1.1.5                                   | 12   | default
abc1.com                                 | 32   | default
2001:0db8:85a3:0000:0000:8a2e:0371:7334 | 1812 | default
-----
```

Showing a summary of a RADIUS server when the status server time interval is configured:

```
switch# show radius-server
Unreachable servers are preceded by *
***** Global RADIUS Configuration *****
```

```
Shared-Secret: None
Timeout: 5
Auth-Type: pap
Retries: 1
TLS Timeout: 5
Tracking Time Interval (seconds): 300
Tracking Retries: 1
Tracking User-name: radius-tracking-user
Tracking Password: None
Status-Server Time Interval (seconds): 400
Number of Servers: 2
```

SERVER NAME	TLS	PORT	VRF
1.1.1.1	Yes	2083	default
2.2.2.2		1812	default

Showing details of a global RADIUS configuration:

```
switch# show radius-server detail
***** Global RADIUS Configuration *****
```

```
Shared-Secret: ***
Timeout: 5
Auth-Type: pap
Retries: 5
Tracking Time Interval (seconds): 60
Tracking Retries: 5
Tracking User-name: radius-tracking-user
Tracking Password: None
Number of Servers: 1
```

```
***** RADIUS Server Information *****
```

```
Server-Name      : 20.1.1.129
Auth-Port        : 1812
Accounting-Port  : 1813
VRF              : default
Shared-Secret    : None
Timeout          : 60
Retries          : 5
Auth-Type        : pap
Server-Group:Priority : radius:1
Tracking         : disabled
Tracking-Mode     : any
Reachability-Status : N/A
ClearPass-Username : 
ClearPass-Password : None
```

Showing details of a RADIUS server when the per-server shared key and the global RADIUS shared key are not set:

```
switch# show radius-server detail
***** Global RADIUS Configuration *****
```

```

Shared-Secret: None
Timeout: 5
Auth-Type: pap
Retries: 1
Number of Servers: 1

***** RADIUS Server Information *****
Server-Name           : 1.1.1.1
Auth-Port             : 2083
VRF                   : default
Shared-Secret (default) : None
Timeout (default)     : 5
Retries (default)     : 1
Auth-Type (default)   : pap
Server-Group:Priority  : radius:1
Default-Priority       : 1

```

Showing details of a RADIUS server when the **status-server** tracking method is configured:

```

switch# show radius-server detail
***** Global RADIUS Configuration *****

Shared-Secret: None
Timeout: 5
Auth-Type: pap
Retries: 1
TLS Timeout: 5
Tracking Time Interval (seconds): 300
Tracking Retries: 1
Tracking User-name: radius-tracking-user
Tracking Password: None
Status-Server Time Interval (seconds)      : 600
Number of Servers: 1

***** RADIUS Server Information *****
Server-Name                               : 2.2.2.2
Auth-Port                                 : 2083
Accounting-Port                           : 2083
VRF                                        : default
TLS Enabled                               : Yes
TLS Connection Status                     : tls_connection_established
Timeout                                   : 5
Auth-Type                                 : pap
Server-Group:Priority                      : radius:1
Default-Priority                          : 1
ClearPass-Username                        :
ClearPass-Password                        : None
Tracking                                  : disabled
Tracking-Mode                             : any
Tracking-Method                           : status-server
Reachability-Status                       : unknown
Tracking-Last-Attempted                   : N/A
Next-Tracking-Request                     : N/A
Port-Access session                       : status-server

```

Showing details of a RADIUS server when the **keep-alive** tracking method is configured:

```

switch# show radius-server detail
***** Global RADIUS Configuration *****

```



```

Shared-Secret: None
Timeout: 5
Auth-Type: pap
Retries: 1
TLS Timeout: 5
Tracking Time Interval (seconds): 300
Tracking Retries: 1
Tracking User-name: radius-tracking-user
Tracking Password: None
Status-Server Time Interval (seconds)      : 400
Number of Servers: 1

***** RADIUS Server Information *****
Server-Name                               : 1.1.1.1
Auth-Port                                 : 2083
Accounting-Port                           : 2083
VRF                                        : default
TLS Enabled                               : Yes
TLS Connection Status                     : tcp_connection_failed
Timeout                                   : 5
Auth-Type                                 : pap
Server-Group:Priority                     : radius:1
ClearPass-Username                        :
ClearPass-Password                        : None
Tracking                                  : disabled
Tracking-Mode                             : any
Tracking-Method                           : keep-alive
Reachability-Status                       : unknown
Tracking-Last-Attempted                   : N/A
Next-Tracking-Request                     : N/A
Port-Access session                       : status-server

```

Showing details of a RADIUS server when the **access-request** tracking method is configured:

```

switch# show radius-server detail
***** Global RADIUS Configuration *****

Shared-Secret: None
Timeout: 5
Auth-Type: pap
Retries: 1
TLS Timeout: 5
Tracking Time Interval (seconds): 300
Tracking Retries: 1
Tracking User-name: radius-tracking-user
Tracking Password: None
Status-Server Time Interval (seconds)      : 500
Number of Servers: 1

***** RADIUS Server Information *****
Server-Name                               : 4.4.4.4
Auth-Port                                 : 2083
Accounting-Port                           : 2083
VRF                                        : default
TLS Enabled                               : Yes
TLS Connection Status                     : tcp_connection_failed
Timeout                                   : 5
Auth-Type                                 : pap
Server-Group:Priority                     : radius:1
ClearPass-Username                        :

```

```

ClearPass-Password           : None
Tracking                     : disabled
Tracking-Mode                 : any
Tracking-Method               : access-request
Reachability-Status           : unknown
Tracking-Last-Attempted       : N/A
Next-Tracking-Request         : N/A
Port-Access session          : keep-alive

```

Showing details of a RADIUS server when the server group is configured:

```

switch# show radius-server detail
***** Global RADIUS Configuration *****

Shared-Secret: None
Timeout: 10
Auth-Type: pap
Retries: 5
TLS Timeout: 5
Tracking Time Interval (seconds): 60
Tracking Retries: 5
Tracking User-name: radius
Tracking Password: None
Status-Server Time Interval (seconds): 300
Number of Servers: 12
AAA Server Status Trap: Enabled

***** RADIUS Server Information *****
Server-Name           : cppm2.cxsecurity.com
Auth-Port              : 1812
Accounting-Port        : 1813
VRF                    : sss
TLS Enabled            : No
Shared-Secret          : ***
Timeout                : 10
Retries                : 5
Auth-Type              : pap
Server-Group:Priority   : RG1:1, RG2:1, RG3:1, RG4:1
ClearPass-Username      :
ClearPass-Password     : None
Tracking               : enabled
Tracking-Mode           : any
Reachability-Status     : reachable, Since Tue Mar 14 19:58:45 UTC 2023
Tracking-Last-Attempted : Thu Mar 16 10:23:46 UTC 2023
Next-Tracking-Request   : 36 seconds

```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager	Operators or Administrators or local user group members with

Platforms	Command context	Authority
	(#)	execution rights for this command. Operators can execute this command from the operator context (>) only.

show radius-server secure ipsec

```
show radius-server secure ipsec { server-list | host {<FQDN> | <IPv4> | <IPv6>}
[port <PORT-NUMBER>] [vrf <VRF-NAME>] [vsx-peer] }
```

Description

Shows information for one or all RADIUS servers configured with IPsec.

Parameter	Description
server-list	Selects all servers for showing.
{<FQDN> <IPv4> <IPv6>}	Specifies the RADIUS server as: ▪ <FQDN>: a fully qualified domain name. ▪ <IPv4>: an IPv4 address. ▪ <IPv6>: an IPv6 address.
port <PORT-NUMBER>	Specifies the authentication port number. Range: 1 to 65535. Default: 1812.
vrf <VRF-NAME>	Specifies the VRF name to be used for communicating with the server. If no VRF name is provided, the default VRF named default is used.
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Usage

The IPsec key is shown in an exportable ciphertext format.

Examples

Showing information for RADIUS server 1.1.1.1 secured with IPsec:

```
switch# show radius-server secure ipsec host 1.1.1.1
IPsec           : enabled
Protocol        : ESP
Authentication   : MD5
Encryption       : AES
SPI             : 1234
```

Showing information for all RADIUS servers secured with IPsec:

```
switch# show radius-server secure ipsec server-list
Server          : 1.1.1.1
IPsec           : enabled
```

```

Protocol          : ESP
Authentication    : MD5
Encryption        : AES
SPI               : 1234

Server            : 1.1.1.2
IPsec             : enabled
Protocol          : ESP
Authentication    : MD5
Encryption        : AES
SPI               : 12341

```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platorms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show radius-server authentication statistics

`show radius-server statistics authentication [vsx-peer]`

Description

Shows authentication statistics for all configured RADIUS servers.

Parameter	Description
<code>vsx-peer</code>	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Examples

Showing RADIUS server authentication statistics:

```

switch# show radius-server statistics authentication
Server Name      : rad1
Auth-Port        : 1812
Accounting-Port  : 1813
VRF              : mgmt

Authentication Statistics
-----

```

```

Round Trip Time      : 100
Pending Requests    : 0
Timeouts            : 6
Bad Authenticators   : 2
Packets Dropped     : 0
Access Requests     : 20
Access Challenge     : 8
Access Accepts      : 14
Access Rejects      : 0
Access Response Malformed : 0
Access Retransmits  : 0
Tracking Requests   : 5
Tracking Responses  : 5
Unknown Response Code : 0

```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
8100 8360	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show radius-server authentication statistics host

```

show radius-server statistics authentication host {<FQDN> | <IPv4> | <IPv6>}
[port <PORT-NUMBER>] [vrf <VRF-NAME>] [vsx-peer]

```

Description

Shows authentication statistics for the specified RADIUS server.

Parameter	Description
{<FQDN> <IPv4> <IPv6>}	Specifies the RADIUS server as: ▪ <FQDN>: a fully qualified domain name. ▪ <IPv4>: an IPv4 address. ▪ <IPv6>: an IPv6 address.
port <PORT-NUMBER>	Specifies the authentication port number. Range: 1 to 65535. Default: 1812.
vrf <VRF-NAME>	Specifies the VRF name to be used for communicating with the server. If no VRF name is provided, the default VRF named default is used.
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Examples

Showing RADIUS server authentication statistics:

```
switch# show radius-server statistics authentication host 20.1.1.49
Server Name       : 20.1.1.49
Auth-Port        : 2083
Accounting-Port   : 2083
VRF              : default

Authentication Statistics
-----
Round Trip Time   : 3
Pending Requests  : 0
Timeouts         : 0
Bad Authenticators : 0
Packets Dropped   : 0
Access Requests   : 13
Access challenge   : 6
Access Accepts    : 3
Access Rejects    : 4
Access Response Malformed : 0
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
8100 8360	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show tacacs-server

```
show tacacs-server [detail] [vsx-peer]
```

Description

Shows the configured TACACS+ servers.

Parameter	Description
detail	Selects additional TACACS+ server details and global parameters for showing.
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Examples

Showing a summary of a global TACACS+ configuration with a shared-secret:

```
switch# show tacacs-server
***** Global TACACS+ Configuration *****

Shared-Secret: AQBapb+HsdpqVlQ3CPCBMQTG8e1cA+CyD0RvfbeA8BEgikCgAAAJOWZSNzA2SWrLA=
Timeout: 5
Auth-Type: pap
Number of Servers: 5

-----
SERVER NAME                               | PORT | VRF
-----
1.1.1.1                                  | 49   | mgmt
1.1.1.2                                  | 12   | mgmt
abc.com                                  | 32   | vrf_blue
2001:0db8:85a3:0000:0000:8a2e:0370:7334 | 49   | default
1.1.1.3                                  | 32   | vrf_red
-----
```

Showing details of a global TACACS+ configuration:

```
switch# show tacacs-server detail
***** Global TACACS+ Configuration *****

Shared-Secret: AQBapb+HsdpqVlQ3CPCBMQTG8e1cA+CyD0RvfbeA8BEgikCgAAAJOWZSNzA2SWrLA=
Timeout: 5
Auth-Type: pap
Number of Servers: 5

***** TACACS+ Server Information *****

Server-Name      : 1.1.1.2
Auth-Port        : 12
VRF              : mgmt
Shared-Secret (default) : AQBapb+HsdpqVlQ3CPCBMQTG8eeA8BEgikCgAAAJOWZSNzA2SWrLA=
Timeout (default)  : 5
Auth-Type (default) : pap
Server-Group      : sg1
Group-Priority    : 1

Server-Name      : 2001:0db8:85a3:0000:0000:8a2e:0370:7334
Auth-Port        : 49
VRF              : default
Shared-Secret (default) : AQBapb+HsdpqVlQ3CPCBMQTG8eeA8BEgikCgAAAJOWZSNzA2SWrLA=
Timeout (default)  : 5
Auth-Type (default) : pap
Server-Group      : sg2
Group-Priority    : 1

Server-Name      : 1.1.1.1
Auth-Port        : 49
VRF              : mgmt
Shared-Secret (default) : AQBapb+HsdpqVlQ3CPCBMQTG8eeA8BEgikCgAAAJOWZSNzA2SWrLA=
Timeout (default)  : 5
Auth-Type (default) : pap
Server-Group (default) : tacacs
Default-Priority   : 1

Server-Name      : abc.com
Auth-Port        : 32
VRF              : vrf_red
```

```

Shared-Secret (default) : AQBapb+HsdpqVlQ3CPCBMQTG8eeA8BEgikCgAAAJOWZSNzA2SWrLA=
Timeout                  : 15
Auth-Type (default)     : pap
Server-Group (default)  : tacacs
Default-Priority         : 3

Server-Name              : 1.1.1.3
Auth-Port                : 32
VRF                      : vrf_blue
Shared-Secret           : AQBapfnqbSswqKC476tdUFZ+AncIRY92hDTYkQCAAAAFEaHn43vNC
Timeout                  : 15
Auth-Type                : chap
Server-Group (default)  : tacacs
Default-Priority         : 5

```

Showing TACACS+ server when per-server shared key and global TACACS+ shared key is not set:

```

switch# show tacacs-server
***** Global TACACS+ Configuration *****

Shared-Secret: None
Timeout: 5
Auth-Type: pap
Number of Servers: 1

-----
SERVER NAME | PORT | VRF
-----
1.1.1.1    | 49   | default
-----

```

Showing TACACS+ server details when per-server shared key and global TACACS+ shared key is not set:

```

switch# show tacacs-server detail
***** Global TACACS+ Configuration *****

Shared-Secret: None
Timeout: 5
Auth-Type: pap
Number of Servers: 1

***** TACACS+ Server Information *****
Server-Name      : 1.1.1.1
Auth-Port        : 49
VRF              : default
Shared-Secret (default) : None
Timeout (default) : 5
Auth-Type (default) : pap
Server-Group (default) : tacacs
Default-Priority  : 1

```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show tacacs-server statistics

show tacacs-server statistics [vsx-peer]

Description

Shows authentication statistics for all configured TACACS+ servers.

Parameter	Description
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Examples

Showing TACACS+ server authentication statistics:

```
switch# show tacacs-server statistics
Server Name      : tac1
Auth-Port       : 49
VRF             : mgmt
Authentication Statistics
-----
Round Trip Time      : 1
Pending Requests    : 0
Timeout            : 0
Unknown Types       : 0
Packet Dropped      : 0
Auth Start         : 8
Auth challenge      : 0
Auth Accepts       : 4
Auth Rejects       : 4
Auth reply malformed : 0
Tracking Requests   : 0
Tracking Responses  : 0
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show tech aaa

show tech aaa

Description

Shows the AAA configuration settings.

Example

Showing the AAA configuration settings:

```
switch# show tech aaa

=====
Show Tech executed on Tue Feb 14 02:19:11 2017
=====

[Begin] Feature aaa
=====

*****
Command : show aaa authentication
*****

AAA Authentication:
  Fail-through           : Enabled
  Limit Login Attempts   : Not set
  Lockout Time           : 300
  Minimum Password Length : Not set

Authentication for ssh channel:

-----
GROUP NAME                | GROUP PRIORITY
-----
local                      | 0
-----

Authentication for https-server channel:

-----
GROUP NAME                | GROUP PRIORITY
-----
local                      | 0
-----

Authentication for console channel:

-----
GROUP NAME                | GROUP PRIORITY
-----
local                      | 0
-----

Authentication for default channel:
-----
```

GROUP NAME		GROUP PRIORITY
tacacs		0
local		1

tacacs		0
local		1

Authentication for telnet channel:

GROUP NAME		GROUP PRIORITY
local		0

local		0

Command : show aaa accounting

AAA Accounting:

Accounting for default channel:

Accounting Type : all

Accounting Mode : start-stop

Default Accounting for login Channels:

GROUP NAME		GROUP PRIORITY
local		0

local		0

Accounting for ssh channel:

GROUP NAME		GROUP PRIORITY
tacacs		0
local		1

tacacs		0
local		1

Accounting for https-server channel:

GROUP NAME		GROUP PRIORITY
tacacs		0

tacacs		0

Accounting for telnet channel:

GROUP NAME		GROUP PRIORITY
tacacs		0
local		1

tacacs		0
local		1

Command : show aaa accounting port-access

...

AAA Accounting Port Access

=====

Radius Accounting Enabled : yes

Radius Server Group : acct_group

Local Accounting Enabled : no

Accounting Mode : start-stop

```

Interim Update Enabled           : true
Interim Interval                 : 12 minutes
Interim Update on-reauth Enabled : true
...

*****
Syntax  : show aaa accounting port-access interface <IFNAME | all> client-status
[mac <MAC-ADDRESS>]
Command : show aaa accounting port-access interface 1/1/1 client-status
*****
...

Port Access Client Status Details

Client 00:50:56:96:5b:9f, steve
=====
Session Details
-----
Port           : 1/1/22
Session Time   : 141s
IPv4 Address   : 10.0.0.3
IPv6 Address   : 2001::1
                2001::3

Accounting Details
-----
Accounting Session ID : 1584556574841
Input Packets         : 265
Input Octets          : 28348
Output Packets        : 341
Output Octets         : 37761
Input Gigaword        : 0
Output Gigaword       : 0
...

...

#### No aaa clients

When there are no port-access accounting sessions:

...

switch# show aaa accounting port-access interface all client-status
Port-access accounting sessions not found.

switch# show aaa accounting port-access interface 1/1/2 client-status
Port-access accounting sessions not found.

switch# show aaa accounting port-access interface 1/1/2 client-status mac
6e:93:79:d9:cb:ee
Port-access accounting sessions not found.
...

*****
Syntax  : show accounting log {all | port-access}
Command : show accounting log port-access
*****
Command to display the Local accounting logs for the network user.
...

-----
May 29 2018 20:29:03.714:53 'acct-id=56789453 type=network user=NWUSER auth-
method=dot1x auth-type=radius rec=ACCT_START mac=00:0d:6a:4f:2a:44 input-pkt=0

```

```

ouput-pkt=0 input-octet=0 output-octets=0'
-----
May 29 2018 20:30:03.714:53 'acct-id=56789453 type=network user=NWUSER auth-
method=dot1x auth-type=radius rec=ACCT_INTRM mac=00:0d:6a:4f:2a:44 input-pkt=2
ouput-pkt=30 input-octet=20 output-octets=50'
-----
May 29 2018 24:29:03.714:53 'acct-id=56789453 type=network user=NWUSER auth-
method=dot1x auth-type=radius rec=ACCT_STOP mac=00:0d:6a:4f:2a:44 input-pkt=20
ouput-pkt=300 input-octet=200 output-octets=500'
-----
May 29 2018 20:29:03.714:53 'acct-id=56789453 type=network user=NWUSER aauth-
method=macauth auth-type=local rec=ACCT_START mac=00:0d:6a:4f:2a:44 input-pkt=0
ouput-pkt=0 input-octet=0 output-octets=0'
-----
...

*****
Syntax : show radius-server statistics {authentication | accounting}
*****
*****
Command : show radius-server statistics authentication
*****
...

Server Name      : 2.2.2.2
Auth-Port       : 1812
Accounting-Port : 1813
VRF             : mgmt

Authentication Statistics
-----
Round Trip Time      : 100
Pending Requests    : 0
Timeouts            : 6
Bad Authenticators   : 2
Packets Dropped     : 0
Access Requests     : 20
Access Challenge    : 8
Access Accepts      : 14
Access Rejects      : 0
Access Response Malformed : 0
Access Retransmits  : 0
Tracking Requests   : 5
Tracking Responses  : 5
Unknown Response Code : 0
...

*****
Command : show radius-server statistics accounting
*****
...

Server Name      : 2.2.2.2
Auth-Port       : 1812
Accounting-Port : 1813
VRF             : mgmt

Accounting Statistics
-----
Round Trip Time      : 100
Pending Requests    : 0
Timeouts            : 5
Bad Authenticators   : 1
Packets Dropped     : 0
Accounting Requests  : 15

```

```

Accounting Responses           : 10
Accounting Response Malformed : 0
Accounting Retransmits         : 0
Unknown Response Code          : 0
...

```

```

*****
Command : show aaa authorization
*****

```

Authorization for default channel:

```

-----
GROUP NAME                | GROUP PRIORITY
-----
local                      | 0
-----

```

Authorization for console channel:

```

-----
GROUP NAME                | GROUP PRIORITY
-----
local                      | 0
-----

```

Authorization for ssh channel:

```

-----
GROUP NAME                | GROUP PRIORITY
-----
tacacs                    | 0
local                     | 1
-----

```

Authorization for telnet channel:

```

-----
GROUP NAME                | GROUP PRIORITY
-----
tacacs                    | 0
local                     | 1
-----

```

```

*****
Command : show aaa server-groups
*****

```

***** AAA Mechanism TACACS+ *****

```

-----
GROUP NAME                | SERVER NAME                | PORT | PRIORITY | VRF
-----
tacacs                    | 1.1.1.1                    | 49   | 1        |
mgmt
-----

```

***** AAA Mechanism RADIUS *****

```

-----
GROUP NAME                | SERVER NAME                | PORT | PRIORITY | VRF
-----

```

```

*****
Command : show tacacs-server detail
*****
***** Global TACACS+ Configuration *****

Shared-Secret: AQBapb+HsdpqVlQ3CPCBMQTG8ekK1c...fbeA8BEgikCgAAAJOWZSNzA2SWrLA=
Timeout: 5
Auth-Type: pap
Tracking Time Interval (seconds): 300
Tracking User-name: tacacs-tracking-user
Tracking Password: None
Number of Servers: 1

***** TACACS+ Server Information *****
Server-Name           : 1.1.1.1
Auth-Port             : 49
VRF                   : mgmt
Shared-Secret         : AQBapfiTREwB7yUKCdmOMT0f...9j2AUxlGAAAF2MkfMTojqX

Timeout              : 5
Auth-Type            : pap
Server-Group         : tacacs
Default-Priority      : 1
Tracking              : disabled
Reachability-Status   : N/A

*****
Command : show radius-server detail
*****
***** Global RADIUS Configuration *****

Shared-Secret: AQBapb+HsdpqVlQ3CPCBMQTG8ekK1cA+Cy...8BEgikCgAAAJOWZSNzA2SWrLA=
Timeout: 5
Auth-Type: pap
Retries: 1
Number of Servers: 0

=====
[End] Feature aaa
=====

=====
Show Tech commands executed successfully
=====

```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Manager (#)	Administrators or local user group members with execution rights for this command.

tacacs-server auth-type

```
tacacs-server auth-type {pap | chap}
no tacacs-server auth-type [pap | chap]
```

Description

Enables the CHAP or PAP authentication protocol, which is used for communication with the TACACS+ servers, at the global level. You can override this command with a fine-grained per server **auth-type** configuration.

The **no** form of this command resets the global authentication mechanism for TACACS+ to PAP, which is the default authentication mechanism for TACACS+.

Parameter	Description
auth-type {pap chap}	Selects either the PAP or CHAP authentication protocol.

Examples

Enabling command for CHAP authentication:

```
switch(config)# tacacs-server auth-type chap
```

Enabling command for PAP authentication:

```
switch(config)# tacacs-server auth-type pap
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

tacacs-server host

```
tacacs-server host {<FQDN> | <IPV4> | <IPV6>}
[key [plaintext <PASSKEY> | ciphertext <PASSKEY>]]
[timeout <TIMEOUT-SECONDS>] [port <PORT-NUMBER>]
[auth-type {pap | chap}] [tracking {enable | disable}] [vrf <VRF-NAME>]
```

```
no tacacs-server host {<FQDN> | <IPV4> | <IPV6>}
[key [plaintext <PASSKEY> | ciphertext <PASSKEY>]]
[timeout <TIMEOUT-SECONDS>] [port <PORT-NUMBER>]
[auth-type {pap | chap}] [tracking {enable | disable}] [vrf <VRF-NAME>]
```


Description

Adds a TACACS+ server. By default, the TACACS+ server is associated with the server group named **tacacs**.

The **no** form of this command removes a previously added TACACS+ server.

Parameter	Description
{<FQDN> <IPv4> <IPv6>}	Specifies the TACACS+ server as: ▪ <FQDN>: a fully qualified domain name. ▪ <IPv4>: an IPv4 address. ▪ <IPv6>: an IPv6 address.
key [plaintext <PASSKEY> ciphertext <PASSKEY>]	Selects either a plaintext or an encrypted local shared-secret passkey for the server. As per RFC 2865, shared-secret can be a mix of alphanumeric and special characters. Plaintext passkeys are between 1 and 32 alphanumeric and special characters. NOTE: When key is entered without either sub-parameter, plaintext passkey prompting occurs upon pressing Enter. Enter must be pressed immediately after the key parameter without entering other parameters. The entered passkey characters are masked with asterisks. When key is omitted, the server uses the global passkey. This command requires either the global or local passkey to be set; otherwise the server will not be contacted. Command tacacs-server key is available for setting the global passkey.
timeout <TIMEOUT-SECONDS>	Specifies the timeout. Range: 1 to 60 seconds. Default : 5 seconds.
port <PORT-NUMBER>	Specifies the TCP authentication port number. Range: 1 to 65535. Default: 49.
auth-type {pap chap}	Selects either the PAP (the default) or CHAP authentication types. If this parameter is not specified, the TACACS+ global default is used.
tracking {enable disable}	Enables or disables server tracking for the RADIUS server. Tracked servers are probed at the start of each server tracking interval to check if they are reachable. Use command tacacs-server tracking to configure TACACS+ server tracking globally.
vrf <VRF-NAME>	Specifies the VRF name to be used for communicating with the server. If no VRF name is provided, the default VRF named default is used.

Usage

If the fully qualified domain name is provided for the TACACS+ server, a DNS server must be configured and accessible through the same VRF which is configured for the TACACS+ server. This configuration is required for the resolution of the TACACS+ server hostname to its IP address. If a DNS server is not available for this VRF, the TACACS+ servers reachable through this VRF must be configured by means of their IP addresses only.

Examples

Adding a TACACS+ server with an IPv4 address, plaintext passkey, timeout, port, authentication type, and VRF name:

```
switch(config)# tacacs-server host 1.1.1.3 key plaintext test-123 timeout 15 port 32 auth-type chap vrf vrf_red
```

Adding a TACACS+ server with an IPv4 address and prompted plaintext passkey:

```
switch(config)# tacacs-server host 1.1.1.5 key
Enter the TACACS server key: *****
Re-Enter the TACACS server key: *****
```

Adding a TACACS+ server with an IPv4 address and a named VRF:

```
switch(config)# tacacs-server host 1.1.1.1 vrf mgmt
```

Adding a TACACS+ server with an IPv4 address, a port, and a named VRF:

```
switch(config)# tacacs-server host 1.1.1.2 port 32 vrf mgmt
```

Adding a TACACS+ server with an FQDN, a timeout, port number, and a named VRF:

```
switch(config)# tacacs-server host abc.com timeout 15 port 32 vrf vrf_blue
```

Adding a TACACS+ server with an IPv6 address:

```
switch(config)# tacacs-server host 2001:0db8:85a3:0000:0000:8a2e:0370:7334
```

Deleting a TACACS+ server with an IPv4 address and specified VRF:

```
switch(config)# no tacacs-server host 1.1.1.1 vrf mgmt
```

Deleting a TACACS+ server with an FQDN, port, and specified VRF:

```
switch(config)# no tacacs-server host abc.com port 32 vrf vrf_blue
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

tacacs-server key

```
tacacs-server key [plaintext <GLOBAL-PASSKEY> | ciphertext <GLOBAL-PASSKEY>]  
no tacacs-server key [plaintext <GLOBAL-PASSKEY> | ciphertext <GLOBAL-PASSKEY>]
```

Description

Creates or modifies a TACACS+ global passkey. The TACACS+ global passkey is used as a shared-secret for encrypting the communication between all TACACS+ servers and the switch. The TACACS+ global passkey is required for authentication unless local passkeys have been set. By default, the TACACS+ global passkey is empty. If the administrator has not set this key, the switch will not be able to perform TACACS+ authentication. The switch will instead rely on the authentication mechanism configured with **aaa authentication login**.



When this command is entered without parameters, plaintext passkey prompting occurs upon pressing Enter. The entered passkey characters are masked with asterisks.

The **no** form of the command removes the global passkey.

Parameter	Description
plaintext <GLOBAL-PASSKEY>	Specifies the TACACS+ global passkey in plaintext format with a length of 1 to 31 characters. As per RFC 2865, a shared-secret can be a mix of alphanumeric and special characters.
ciphertext <GLOBAL-PASSKEY>	Specifies the TACACS+ global passkey in encrypted format.

Examples

Adding the global passkey:

```
switch(config)# tacacs-server key plaintext mypasskey123
```

Adding the global passkey with prompting:

```
switch(config)# tacacs-server key  
Enter the TACACS server key: *****  
Re-Enter the TACACS server key: *****
```

Removing the global passkey:

```
switch(config)# no tacacs-server key
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

tacacs-server timeout

```
tacacs-server timeout [<1-60>]
no tacacs-server timeout [<1-60>]
```

Description

Specifies the number of seconds to wait for a response from the TACACS+ server before trying the next TACACS+ server. If a value is not specified, a default value of 5 seconds is used. You can override this value with a fine-grained per server timeout configured for individual servers.

The **no** form of this command resets the TACACS+ global authentication timeout to the default of 5 seconds.

Parameter	Description
timeout <1-60>	Specifies the timeout interval of 1 to 60 seconds. Default: 5 seconds.

Examples

Specifying the TACACS+ server timeout:

```
switch(config)# tacacs-server timeout 10
```

Resetting the timeout for the TACACS+ server to the default:

```
switch(config)# no tacacs-server timeout
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

tacacs-server tracking

```
tacacs-server tracking interval <INTERVAL>
no tacacs-server tracking interval [<INTERVAL>]
```

```
tacacs-server tracking user-name <NAME>
    [password [plaintext <PASSWORD> | ciphertext <PASSWORD>]]
no tacacs-server tracking [user-name [<NAME>] [ciphertext <PASSWORD>]]
```

Description

Configures TACACS+ server tracking settings globally for all configured TACACS+ servers that have tracking enabled with the **tacacs-server host** command on individual servers.

The **no** form of the command removes the specified configuration, reverting it to its default. The no form with **user-name** also clears the password (resets it to empty).

Parameter	Description
<code>interval <INTERVAL></code>	Specifies the time interval, in seconds, to wait before checking the server reachability status. Default: 300. Range 60 to 84600.
<code>user-name <NAME></code> <code> [password [plaintext <PASSWORD> </code> <code> ciphertext <PASSWORD>]]</code>	Specifies the user name (and optionally a password) to be used for server checking. The default user name is tacacs-tracking-user with an empty password. The password is optional and may be entered as plaintext or pasted in as ciphertext. The plaintext password is visible as cleartext when entered but is encrypted thereafter. Command history does show the password as cleartext. NOTE: When password is entered without a following sub-parameter, plaintext password prompting occurs upon pressing Enter. The entered password characters are masked with asterisks. NOTE: The user does not have to be configured on the server. Server tracking can still be performed with a user which is not configured on the server because authentication failure on the server achieves confirmation that the server is reachable. NOTE: Server tracking uses authentication request and response packets to determine server reachability status. The server tracking user name and password are used to form the request packet which is sent to the server with tracking enabled. Upon receiving a response to the request packet, the server is considered to be reachable.

Examples

Configuring a tracking interval of 120 seconds:

```
switch(config)# tacacs-server tracking interval 120
```

Reverting the tracking interval to its default of 300 seconds:

```
switch(config)# no tacacs-server tracking interval
```

Configuring user **tacacs-tracker** with a plaintext password.

```
switch(config)# tacacs-server tracking user-name tacacs-tracker password plaintext track$1
```

Configuring user **tacacs-tracker** with a prompted plaintext password.

```
switch(config)# tacacs-server tracking user-name tacacs-tracker password
Enter the TACACS server tracking password: *****
Re-Enter the TACACS server tracking password: *****
```

Reverting the tracking user name to its default of **tacacs-tracking-user**:

```
switch(config)# no tacacs-server tracking user-name
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

RADIUS dynamic authorization provides the ability to make changes to a user account session while it is in progress. This ability includes disconnecting a session or updating some aspect of the authorization for the session. It also includes "pot bounce" in which the interface on which a client is connected is brought down and then back up (using COA (change of authorization)).

RADIUS dynamic authorization enables or disables the processing of "Disconnect" and "Change of Authorization (CoA)" messages from the RADIUS server. When enabled, the RADIUS server can dynamically terminate or change the authorization parameters (such as VLAN/user-role assignment) used in an active client session on the switch.



See also *RFC 3576* available at <http://www.ietf.org/rfc/rfc3576.txt> for general information on the dynamic authorization extensions to RADIUS.

Requirements and tips

The switch validates these mandatory attributes that must be present in the CoA/Disconnect Message:

- **NAS IP** or **NAS IPV6** or **NAS Identifier**
- Any one of the following combinations is used to identify the client session:
 - **NAS-Port** and **Calling-Station-ID**
 - **NAS-Port-ID** and **Calling-Station-ID**
 - **Accounting-Session-ID**

RADIUS server requirements:

- For ClearPass to provide CoA capabilities, in the case where the switch sends the NAS-IP address as a routable IP address, the CLI command `ip source interface` must be executed with the `radius` parameter.
- In CISCO ISE, to send the CoA request with the same username as in the RADIUS Accept, the Identity rewrite option has to be configured.

When policy entries are applied via CoA messages, limit the number of entries to 32 entries per policy.

RADIUS dynamic authorization commands

radius dyn-authorization enable

```
radius dyn-authorization enable
no radius dyn-authorization enable
```

Description

Enables RADIUS dynamic authorization. This command must be issued before the configuration set with other **radius dyn-authorization** commands takes effect.

The no form of this command disables RADIUS dynamic authorization.

Examples

Enabling RADIUS dynamic authorization:

```
switch(config)# radius dyn-authorization enable
```

Command History

Release	Modification
10.09	Command introduced on the 8360

Command Information

Platforms	Command context	Authority
8100 8360	config	Administrators or local user group members with execution rights for this command.

radius dyn-authorization client

```
radius dyn-authorization client {<IPV4> | <IPV6> | <HOSTNAME>}  
    [secret-key [plaintext <PASSKEY> | ciphertext <PASSKEY>]]  
    [time-window <WIDTH>] [vrf <VRF-NAME>] [replay-protection {enable|disable}]  
    [rfc5176-enforcement-mode <strict|loose>]  
    no...
```

Description

Configures RADIUS dynamic authorization for the specified client on the specified (or **default**) VRF.

The **no** form of this command unconfigures RADIUS dynamic authorization for the specified client on the specified (or **default**) VRF.

Guidelines

Configure **rfc5176-enforcement-mode loose** when integrating with the Adaptive Network Control (ANC) feature of Cisco ISE, as authorization attributes are sent as part of Disconnect-Requests (code 40) instead of CoA-Requests(code 43).

The following are the only authorization attributes that are accepted in the disconnect requests in the loose mode:

1. Cisco-AVPair='subscriber:command=bounce-host-port'
2. Cisco-AVPair='subscriber:command=disable-host-port'
3. Cisco-AVPair='subscriber:command=reauthenticate' and Cisco-AVPair='subscriber:reauthenticate-type=<last|rerun>'



The **reauthenticate-type=rerun** option is not supported if concurrent onboarding is enabled for the client.

Parameter	Description
<IPV4> <IPV6> <HOSTNAME>	Specifies the client IPv4 address, IPv6 address, or host name.
secret-key [plaintext <PASSKEY> ciphertext <PASSKEY>]	Specifies the dynamic authorization server (RADIUS server) shared secret key required for client access. Provide either a plaintext or an encrypted shared-secret passkey. As per RFC 2865, the shared-secret can be a mix of alphanumeric and special characters. Plaintext passkeys are between 1 and 32 alphanumeric and special characters. NOTE: When secret-key is entered without either sub-parameter, plaintext shared secret prompting occurs upon pressing Enter. Enter must be pressed immediately after the secret-key parameter without entering other parameters. The entered shared secret characters are masked with asterisks.
rfc5176-enforcement-mode <strict loose>	Configure the enforcement mode of RFC5176. The default mode is strict and in this mode, no authorization attributes are allowed as part of disconnect requests. When configured mode is loose , then the authorization attributes are accepted in disconnect requests.
time-window <WIDTH>	Specifies the width of the synchronization window (in seconds) between the RADIUS dynamic authorization client and the RADIUS dynamic authorization server. Default 300. Range: 1 to 65535.
replay-protection {enable disable}	Enables or disables RADIUS dynamic authorization replay protection for the specified client on the specified (or default) VRF. By default, the replay-protection is set to disabled.
vrf <VRF-NAME>	Specifies the VRF on which the identified client is connected. When omitted, VRF default is assumed.

Examples

Configuring RADIUS dynamic authorization with replay protection for a client on the default VRF:

```
switch(config)# radius dyn-authorization client 1.1.2.5 replay-protection enable
```

Configuring RADIUS dynamic authorization with time window and shared secret for a client on the default VRF:

```
switch(config)# radius dyn-authorization client 1.1.2.7 time-window 8
secret-key plaintext skF82#450
```

Configuring loose enforcement of RFC5176:

```
switch(config)# radius dyn-authorization client 1.1.1.1 rfc5176-enforcement-mode
loose
```

Configuring RADIUS dynamic authorization with a prompted shared secret:

```
switch(config)# radius dyn-authorization client 1.1.2.7 secret-key
Enter the RADIUS dyn-authorization key: *****
Re-Enter the RADIUS dyn-authorization key: *****
```

Command History

Release	Modification
10.13	The rfc5176-enforcement-mode parameter was introduced.
10.09	Command introduced on the 8360

Command Information

Platforms	Command context	Authority
8100 8360	config	Administrators or local user group members with execution rights for this command.

radius dyn-authorization client tls (RadSec)

```
radius dyn-authorization client [<IPV4> | <IPV6> | <HOSTNAME>]
    tls [replay-protection {enable|disable}] [time-window <WIDTH>] [vrf <VRF-NAME>]
[rfc5176-enforcement-mode <strict|loose>]
no radius dyn-authorization client [<IPV4> | <IPV6> | <HOSTNAME>]
    tls [replay-protection {enable|disable}] [time-window <WIDTH>] [vrf <VRF-NAME>]
[rfc5176-enforcement-mode <strict|loose>]
```

Description

Enables TLS protection for a RADIUS dynamic authorization client on the specified (or **default**) VRF. RadSec is a protocol that supports RADIUS over TLS. The **no** form of this command deletes TLS protection for the dynamic authorization client.



RadSec server must be configured before configuring dynamic authorization.

Guidelines

Configure **rfc5176-enforcement-mode loose** when integrating with the Adaptive Network Control (ANC) feature of Cisco ISE, as authorization attributes are sent as part of Disconnect-Requests (code 40) instead of CoA-Requests (code 43).

The following are the only authorization attributes that are accepted in the disconnect requests in the loose mode:

1. Cisco-AVPair='subscriber:command=bounce-host-port'
2. Cisco-AVPair='subscriber:command=disable-host-port'
3. Cisco-AVPair='subscriber:command=reauthenticate' and Cisco-AVPair='subscriber:reauthenticate-type=<last|rerun>'



The **reauthenticate-type=rerun** option is not supported if concurrent onboarding is enabled for the client.

Parameter	Description
<IPV4> <IPV6> <HOSTNAME>	Specifies the client IPv4 address, IPv6 address, or host name.
replay-protection {enable disable}	Enables or disables RADIUS dynamic authorization replay protection for the specified client on the specified (or default) VRF. By default, the replay-protection is set to disabled.
time-window <WIDTH>	Specifies the width of the synchronization window (in seconds) between the RADIUS dynamic authorization client and the RADIUS dynamic authorization server. Default 300. Range: 1 to 65535.
vrf <VRF-NAME>	Specifies the VRF on which the identified client is connected. When omitted, VRF default is assumed.
rfc5176-enforcement-mode <strict loose>	Configure the enforcement mode of RFC5176. The default mode is strict and in this mode, no authorization attributes are allowed as part of disconnect requests. When configured mode is loose , then the authorization attributes are accepted in disconnect requests.

Examples

Enables TLS protection for a RADIUS dynamic authorization client with replay protection and time window for a client on the default VRF:

```
switch(config)# radius dyn-authorization client 1.1.2.5 tls replay-protection
enable time-window 8
```

Configuring loose enforcement of RFC5176:

```
switch(config)# radius dyn-authorization client 1.1.1.1 tls rfc5176-enforcement-
mode loose
```

Deleting TLS protection for a dynamic authorization client on the adm2 VRF:

```
switch(config)# no radius dyn-authorization client 1.1.2.7 tls VRF adm2
```

Command History

Release	Modification
10.13	The rfc5176-enforcement-mode parameter was introduced.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
8100 8360	config	Administrators or local user group members with execution rights for this command.

radius dyn-authorization port

radius dyn-authorization port <PORT-NUMBER>

Description

Sets the RADIUS dynamic authorization server UDP or TCP port.

Parameter	Description
<PORT-NUMBER>	Specifies the UDP or TCP port. Default UDP: 3799 and TCP:2083.

Examples

Setting the RADIUS dynamic authorization server UDP port back to its default 3799:

```
switch(config)# radius dyn-authorization port 3799
```

Setting the RADIUS dynamic authorization server TCP port back to its default 2083:

```
switch(config)# radius dyn-authorization port 2083
```

Command History

Release	Modification
10.09	Command introduced on the 8360

Command Information

Platforms	Command context	Authority
8100 8360	config	Administrators or local user group members with execution rights for this command.

show radius dyn-authorization

show radius dyn-authorization

Description

Shows RADIUS dynamic authorization configuration and summarized statistics for all clients configured for dynamic authorization.

Usage

Show command output item identification:

- **Radius Dynamic Authorization:** Enabled or Disabled status, system wide.
- **Radius Dynamic Authorization Port:** The UDP or TCP port used for dynamic authorization (default 3799).
- **Invalid Client Address in CoA Requests:** The number of CoA (change of authorization) requests received with an incorrect DAC (dynamic authorization client) address.
- **Invalid Client Address in Disconnect Requests:** The number of disconnect requests received with incorrect DAC address.
- **Disconnect Requests:** The number of disconnect requests received from the DAC.
- **Disconnect ACKs:** The number of Disconnect-ACKs sent to the DAC.
- **Disconnect NAKs:** The number of Disconnect-NAKs sent to the DAC.
- **CoA Requests:** The number of CoA-requests received from the DAC.
- **CoA ACKs:** The number of CoA-ACKs sent to the DAC.
- **CoA NAKs:** The number of CoA-NAKs sent to the DAC.

Example

Showing RADIUS dynamic authorization summarized statistics for all clients configured for dynamic authorization:

```
switch# show radius dyn-authorization
Status and Counters - RADIUS Dynamic Authorization Information

RADIUS Dynamic Authorization           : Enabled
RADIUS Dynamic Authorization UDP Port   : 3799
Invalid Client Addresses in CoA Requests : 0
Invalid Client Addresses in Disconnect Requests: 0

Dynamic Authorization Client Information
=====

IP Address       : 1.1.2.1
VRF              : adm2
Replay Protection : Disabled
TLS Enabled    : Yes
Time Window      : 20
Disconnect Requests : 1
Disconnect ACKs    : 1
Disconnect NAKs    : 0
CoA Requests      : 7
CoA ACKs          : 2
CoA-NAKs          : 5
Shared-Secret     :
AQBapb+HsdpqV1Q3CPCBMQTG8ekK1cA+CyD0RvfbeA8BEgikCgAAAJOWZSNzA2SWrLA=

IP Address       : 1.1.2.5
VRF              : default
Replay Protection : Enabled
TLS Enabled    : No
Time Window      : 20
Disconnect Requests : 6
Disconnect ACKs    : 6
Disconnect NAKs    : 0
CoA Requests      : 9
CoA ACKs          : 5
CoA-NAKs          : 4
Shared-Secret     :
```

```
AQBapb+HsdpqV1Q3PCBMQTG8ekK1cA+CyD0RvfbeA8BEgikCgAAAJOWZSNzA2SWrLA=
```

```
IP Address      : 1.1.2.7
VRF             : default
Replay Protection : Disabled
TLS Enabled    : Yes
Time Window     : 8
Disconnect Requests : 6
Disconnect ACKs   : 6
Disconnect NAKs   : 0
CoA Requests     : 9
CoA ACKs          : 5
CoA-NAKs         : 4
Shared-Secret    :
AQBapb+HsdpqV1Q3PCBMQTG8ekK1cA+CyD0RvfbeA8BEgikCgAAAJOWZSNzA2SWrLA=
```

Command History

Release	Modification
10.09	Command introduced on the 8360

Command Information

Platforms	Command context	Authority
8100 8360	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show radius dyn-authorization client

```
show radius dyn-authorization client <IP-ADDR> [vrf <VRF-NAME>]
```

Description

Shows RADIUS dynamic authorization statistics for the specified client on the specified VRF.

Parameter	Description
<IP-ADDR>	Specifies the client IPv4 or IPv6 address.
vrf <VRF-NAME>	Specifies the VRF on which the identified client is connected. When omitted, VRF default is assumed.

Usage

Show command output item identification:

- **Total Requests:** The number of Disconnect and CoA (change of authorization) requests received from the DAC (dynamic authorization client).
- **Authorize Only Requests:** The number of Disconnect and CoA requests received from the DAC with an "Authorize only" Service-Type attribute.

- **Malformed Requests:** The number of malformed Disconnect and CoA requests received from the DAC.
- **Bad Authenticator Requests:** The number of Disconnect and CoA requests received from this DAC with an invalid authenticator field.
- **Dropped Requests:** The number of Disconnect and CoA requests from this DAC that have been silently discarded for reasons other than malformed, bad authenticators, or unknown type.
- **Total ACK Responses:** The number of Disconnect-ACKs sent to the DAC.
- **Total NAK Responses:** The number of Disconnect-NAKs sent to the DAC.
- **Session Not Found Responses:** The number of Disconnect-NAKs sent to the DAC because no session context could be found.
- **User Sessions Modified:** The number of user sessions for which authorization changed due to Disconnect and CoA requests received from the DAC.

Example

Showing RADIUS dynamic authorization statistics for client 1.1.2.1 on VRF default:

```
switch# show radius dyn-authorization client 1.1.2.1 vrf default
Status and Counters - RADIUS Dynamic Authorization Client Information

VRF Name           : default
Authorization Client : 1.1.2.1
Unknown Packets    : 55
Message-Type       Disconnect      CoA
-----
Total Requests      2147483647      10
Authorize Only Requests 10          10
Malformed Requests  10          10
Bad Authenticator Requests 2147483647  2147483647
Dropped Requests    10          10
Total ACK Responses  10          10
Total NAK Responses  10          10
Session Not Found Responses 10          10
User Sessions Modified 20          20
```

Command History

Release	Modification
10.09	Command introduced on the 8360

Command Information

Platforms	Command context	Authority
8100 8360	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

IP Flow Information Export (IPFIX) is an embedded network flow analysis tool that compiles characteristic and measured properties of flows and sends flow reports to flow collectors. IPFIX is configurable via the command-line or REST interfaces. With IPFIX, customers configure flow records with match (key) fields and collection (non-key) fields. Match fields are the set of fields that define a flow, such as IP address or UDP port. Collection fields are the set of fields that identify information to collect for a flow, such as packet and byte counters.

A flow exporter defines where and how to export flow reports. Flow exporters are created as standalone entities in the **config** context to provide flow monitors the ability to export flow reports. A single flow exporter can be assigned to one or more flow monitors, and multiple flow exporters can be assigned to a single flow monitor.

IPFIX is a stand alone feature and can work on its own to monitor the traffic flow. On enabling the Application Recognition and Control feature, application information along with flow properties are exported to external or internal IPFIX collectors.



The IPFIX feature on the 8360 switch series are for monitoring only.

For more information about IPFIX, see the *Monitoring Guide*.

Traffic insight allows monitoring of large amount of data that it collects from various flow exporters like IPFIX provide the ability to filter, aggregate, and sort the data based on user flow monitor requests. Traffic insight tracks different monitor requests simultaneously and provides monitor reports per request.

Protocol and feature details

When traffic insight is enabled and clients on the network access SaaS services or public websites, a flow exporter like IPFIX caches flows in both directions and collects traffic statistics and source and destination MAC addresses.

The IPFIX sends the flow record to traffic insight, and the traffic insight feature collects these records and updates the bidirectional traffic information to the Open vSwitch Database (OVSDB). Aruba Central fetches the flow details from OVSDB through REST APIs.

Supported Platforms

The following table list the supported platforms for Traffic Insight.

Table 1: *Supported platforms for Traffic Insight.*

Platform	Traffic Insight
8360	Yes only dns-average-latency

Supported Monitor Types

Traffic insight supports a variety of monitor types. Refer to this section to learn which monitor types are supported on each platform.

The 6300, 6400, and 8360 platforms support the following monitor type:

- DNS Average Latency
 - Monitors dns request and response flows and provides average dns-latency details per client
 - Every 5 minutes the client insights table in the data base is updated with dns average latency details



After enabling the client-insight feature the DNS average latency details are published for clients that onboard the switch.

Caveats for Traffic Insight

The following section provides details on the caveats to be noted for Traffic Insight.

- Only one traffic-insight instance is allowed.
- Maximum number of supported traffic insight monitors on the 8360 Switch Series is 1.

Configuring Traffic Insight

Prerequisite:

- Enable IPFIX—Flow data is exported to Traffic Insight, which is an internal IPFIX collector.
- Both IPFIX and Client Insight feature should be enabled for Traffic Insight to publish the dns average latency.



The Application Recognition feature is only supported on the 6300 and 6400 Switch Series.

Traffic Insight Configuration

Complete the steps below to configure traffic insight.

1. Create and enable Traffic Insight instance and specify the flow source

```
switch(config)# traffic-insight TI_Instance-01 -->Creates a Traffic Insight
                                                    instance with name TI_Instance-01
switch(config-ti)# source ipfix -->Sets the source protocol to
                                                    collect flow information
switch(config-ti)# enable -->Enables Traffic Insight
```

2. Specify the flow configuration

```
switch(config)# flow exporter <EXPORTER_NAME>
  destination type traffic-insight
  destination traffic-insight test
  template data timeout <TIMEOUT_VALUE>

switch(config)# flow record <RECORDED_NAME>
  match ipv4 destination address
  match ipv4 protocol
  match ipv4 source address
  match ipv4 version
  match transport destination port
  match transport source port
  collect counter bytes
  collect counter packets
  collect application dns response-code
  collect timestamp absolute first
  collect timestamp absolute last
switch(config)# flow monitor <MONITOR_NAME>
  cache timeout active <TIMEOUT_VALUE>
  exporter <EXPOTER_NAME>
  record <RECORDED_NAME>
switch(config)# interface <Inboud_Interface>
switch(config-if)#ip flow monitor flow-monitor-1 in -->Enable IPv4 or IPv6 flow
                                                    monitor on both inbound
                                                    and outbound interfaces

switch(config)# interface <Outbound_Interface>
switch(config-if)#ip flow monitor flow-monitor-1 in
```

3. Specify the monitoring parameters for flow monitoring

```
switch(config-ti)# monitor DNSLatency type dns-average-latency
```

4. Specify the show commands to get the desired output

```
switch# show traffic-insight instance-1 monitor-type dns-average-latency mntr2
Name                                     : mntr2
Type                                    : dns-average-latency
Start time for latency calculation       : 10/10/2022 04:47:26.869937 UTC
End time for latency calculation        : 10/10/2022 04:48:26.812820 UTC
client_mac      client_ip      dns_server_ip      dns_avergae_latency(msec)
-----
aa:aa:aa:aa:aa:aa  192.168.11.1  172.0.0.1      200
bb:bb:bb:bb:bb:bb  192.168.12.1  172.1.1.1      300
cc:cc:cc:cc:cc:cc  192.168.13.1  172.2.2.2      150
```

Traffic insight commands

diag-dump traffic-insight basic

diag-dump traffic-insight basic

Description

Displays diagnostic information for Traffic Insight.

Examples

```
Switch# diag-dump traffic-insight basic
=====
[Start] Feature traffic-insight Time : Wed Nov  2 18:26:45 2022
=====
-----
[Start] Daemon traffic-insightd
-----
Printing App cache:
TI CPDI Clients MACs learnt: 0
Printing flows for instance test
Printing flows for instance test
Printing DNS cache received:
CLIENT: 100.10.10.10
  DNS_SERVER_IP    LATENCY    TOTAL_SAMPLES    PORT    REQUEST_TIME    RESPONSE_
TIME
  100.10.10.2      261        4
Printing DNS IP MAC cache:
IP address          MAC address
100.10.10.10        00:50:56:96:8a:67
-----
[End] Daemon traffic-insightd
-----
[End] Feature traffic-insight
=====
Diagnostic-dump captured for feature traffic-insight
```

Command History

Release	Modification
10.11	Command introduced.

Command Information

Platforms	Command context	Authority
8100 8360	Manager (#)	Administrators or local user group members with execution rights for this command.

show capacities traffic-insight

show capacities traffic-insight

Description

Displays the system capacities status and their values for Traffic Insight

Examples

```
Switch# show capacities traffic-insight

System Capacities: Filter TRAFFIC_INSIGHT
Capacities Name                                     Value
-----
--
Maximum number of Traffic-insight instances          1
Maximum number of Traffic-insight monitors           1
```

Command History

Release	Modification
10.11	Command introduced.

Command Information

Platforms	Command context	Authority
8100 8360	Manager (#)	Administrators or local user group members with execution rights for this command.

show debug buffer module trafficinsight

show debug buffer module trafficinsight

Description

Displays Traffic Insight debug logs stored in the debug buffer.

Examples

```
Switch# show debug buffer module trafficinsight
-----
show debug buffer
-----
2022-10-26:11:11:30.689510|traffic-insightd|LOG_
DEBUG|AMM|1/1|TRAFFICINSIGHT|TRAFFICINSIGHT_PACKET|Unsupported record id: 210
2022-10-26:11:11:30.689573|traffic-insightd|LOG_
DEBUG|AMM|1/1|TRAFFICINSIGHT|TRAFFICINSIGHT_PACKET|DMAC: 10:4f:58:88:08:00
2022-10-26:11:11:30.689639|traffic-insightd|LOG_
DEBUG|AMM|1/1|TRAFFICINSIGHT|TRAFFICINSIGHT_PACKET|Unsupported record id: 210
2022-10-26:11:11:30.689700|traffic-insightd|LOG_
DEBUG|AMM|1/1|TRAFFICINSIGHT|TRAFFICINSIGHT_PACKET|octetDeltaCount: 13751
2022-10-26:11:11:30.689761|traffic-insightd|LOG_
DEBUG|AMM|1/1|TRAFFICINSIGHT|TRAFFICINSIGHT_PACKET|packetDeltaCount: 36
2022-10-26:11:11:30.689823|traffic-insightd|LOG_
DEBUG|AMM|1/1|TRAFFICINSIGHT|TRAFFICINSIGHT_PACKET|source interface: 0
2022-10-26:11:11:30.689887|traffic-insightd|LOG_
DEBUG|AMM|1/1|TRAFFICINSIGHT|TRAFFICINSIGHT_PACKET|Unsupported record id: 252
2022-10-26:11:11:30.689949|traffic-insightd|LOG_
DEBUG|AMM|1/1|TRAFFICINSIGHT|TRAFFICINSIGHT_PACKET|App id: 3235
2022-10-26:11:11:30.690159|traffic-insightd|LOG_
DEBUG|AMM|1/1|TRAFFICINSIGHT|TRAFFICINSIGHT|ti_rcv_messages_in_cpdi_layer:
Received message with size 200 from DL
2022-10-26:11:11:30.690184|traffic-insightd|LOG_
DEBUG|AMM|1/1|TRAFFICINSIGHT|TRAFFICINSIGHT|ti_cpdi_layer_handle_events: Handling
message in CPDI event 10
2022-10-26:11:11:30.690321|traffic-insightd|LOG_
DEBUG|AMM|1/1|TRAFFICINSIGHT|TRAFFICINSIGHT|ti_topn_add_record_to_monitor:New TOPN
hash node created for SIP 3501::100, DIP 3701::100, VRF default,dst_port 80
```

Command History

Release	Modification
10.11	Command introduced.

Command Information

Platforms	Command context	Authority
8100 8360	Manager (#)	Administrators or local user group members with execution rights for this command.

show events traffic-insightd

```
show events -d traffic-insightd
```

Description

Displays event logs generated by the switch modules since the last reboot for Traffic Insight.

Examples

Showing event logs of Traffic Insight:

```
Switch# show events -d traffic-insightd
-----
```

```
Event logs from current boot
-----
2022-10-26T07:55:17.369208+00:00 6410 traffic-insightd[2518]: Event|14005|LOG_
INFO|UMM|-|Traffic Insight instance t1 enabled
2022-10-26T07:55:17.369309+00:00 6410 traffic-insightd[2518]: Event|14001|LOG_
INFO|UMM|-|Instance t1 created
2022-10-26T08:09:53.077469+00:00 EdgeInt traffic-insightd[2518]: Event|14003|LOG_
INFO|UMM|-|dns-avergae-latency running-statistics cleared for the monitor top3 and
instance t1
2022-10-26T08:24:52.998692+00:00 EdgeInt traffic-insightd[2518]: Event|14003|LOG_
INFO|UMM|-|dns-avergae-latency running-statistics cleared for the monitor top3 and
instance t1
```

Command History

Release	Modification
10.11	Command introduced.

Command Information

Platforms	Command context	Authority
8100 8360	Manager (#)	Administrators or local user group members with execution rights for this command.

show running-config traffic-insight

```
show running-config traffic-insight
```

Description

Display configuration settings for all traffic insight instances.

Examples

Related Commands

Command	Description
traffic insight	Create and configure a traffic insight instance

Command History

Release	Modification
10.11	Command introduced.

Command Information

Platforms	Command context	Authority
8100 8360	Operator (>) or Manager (#)	Administrators or local user group members with execution rights for this command.

show tech traffic-insight

show tech traffic-insight

Description

Shows the Traffic Insight configuration settings.

Examples

The example shows the Traffic Insight configuration settings.

```
Switch# show tech traffic-insight
=====
Show Tech executed on Wed Oct 26 11:11:37 2022
=====
[Begin] Feature traffic-insight
=====
*****
Command : show running-config traffic-insight
*****
traffic-insight t1
enable
source ipfix
!
monitor dns type dns-average-latency
=====
[End] Feature traffic-insight
=====
Show Tech commands executed successfully
=====
```

Command History

Release	Modification
10.11	Command introduced.

Command Information

Platforms	Command context	Authority
8100 8360	Manager (#)	Administrators or local user group members with execution rights for this command.

show traffic-insight monitor-type

show traffic-insight <INSTANCE_NAME> monitor-type

dns-average-latency <MONITOR_NAME>

Description

Display information for traffic insight monitored flows.

Parameter	Description
<INSTANCE_NAME>	Name of the traffic insight instance, string of maximum length up to 32 characters.
monitor-type	Specifies traffic insight monitor type. NOTE: The dns-average-latency flow is supported only for 8360 switch series.
<MONITOR_NAME>	Specify a monitor name to display information for that monitor.

Examples

The following example shows **dns-average-latency** data for **mntr2** monitoring, for instance **instance-1**:

```
switch# show traffic-insight instance-1 monitor-type dns-average-latency mntr2
Name                                     : mntr2
Type                                     : dns-average-latency
Start time for latency calculation       : 10/10/2022 04:47:26.869937 UTC
End time for latency calculation        : 10/10/2022 04:48:26.812820 UTC
client_mac      client_ip      dns_server_ip      dns_avergae_latency (msec)
-----
aa:aa:aa:aa:aa:aa  192.168.11.1  172.0.0.1      200
bb:bb:bb:bb:bb:bb  192.168.12.1  172.1.1.1      300
cc:cc:cc:cc:cc:cc  192.168.13.1  172.2.2.2      150
```

Related Commands

Command	Description
traffic insight	Create and configure a traffic insight instance.

Command History

Release	Modification
10.12.1000	The dns-onboarding-latency sub-parameter was introduced.
10.11	Command introduced.

Command Information

Platforms	Command context	Authority
8100 8360	Manager (#)	Administrators or local user group members with execution rights for this command.

traffic insight


```

traffic-insight <INSTANCE_NAME>
  [no] enable
  [no] source ipfix
  [no] monitor <NAME> type dns-average-latency

```

Description

Traffic insight monitors data collected from flow exporters like the IP Flow Information Export (IPFIX) flow exporter. Traffic insight tracks multiple monitor requests simultaneously and provides monitor reports for each request.

Parameter	Description
<INSTANCE_NAME>	Name of the traffic insight instance, string of maximum length up to 32 characters.
[no] enable	Enable or disable this traffic insight configuration
[no] source ipfix	The traffic insight configuration uses this source protocol to collect traffic flows. The only available protocol is ipfix .
monitor <INSTANCE_NAME>	Enable flow monitoring on a traffic insight instance and configure rules for filtering and grouping traffic flows.
type	Specifies type of the monitor
dns-average-latency	Monitors DNS request and response flows and provides average dns-latency details per client. The Traffic Insight application flow table in the database is updated every 5 minutes with dns average latency information.
no	Negate a command or set its defaults

Examples

The following example creates a traffic insight instance named **TI_1**:

```
switch(config)# traffic-insight TI_1
```

The following example deletes a traffic insight instance named **TI_1**:

```
switch(config)# no traffic-insight TI_1
```

The following example enables traffic insight instance for **TI_1** instance:

```
switch(config)# traffic-insight TI_1
switch(config-ti)#enable
```

The following example disables traffic insight instance for **TI_1** instance:

```
switch(config)# traffic-insight TI_1
switch(config-ti)#no enable
```

The following example sets the source protocol for **TI_1** instance to collect flows information from IPFIX:

```
switch(config)# traffic-insight TI_1
switch(config-ti)# source ipfix
```

The following example removed the source protocol for **TI_1** instance:

```
switch(config)# traffic-insight TI_1
switch(config-ti)# no source ipfix
```

The following examples create a traffic insight monitor for **dns-average-latency** for the **mti3** instance:

```
switch(config-ti)# monitor mnti3 type dns-average-latency
```

Command History

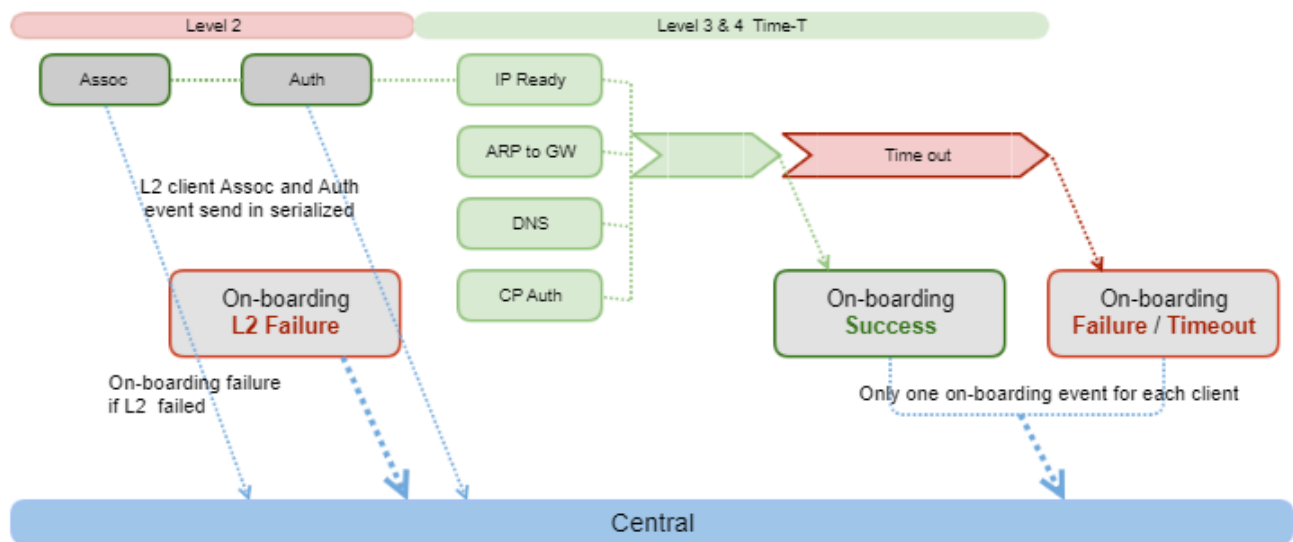
Release	Modification
10.12.1000	The dns-onboarding-latency sub-parameter was introduced.
10.13	The raw-flows sub-parameter introduced.
10.11	Command introduced.

Command Information

Platforms	Command context	Authority
8100 8360	config	Administrators or local user group members with execution rights for this command.

The Client Insight feature captures L2, L3, and L4 onboarding details such as time taken for authentication, acquiring IP address and DNS resolution of the clients. The details published by the Client Insight feature help in providing better insight into the client activities, using the Aruba Central application. Client Insight can also be configured to generate event logs with client onboarding status.

Figure 1 Onboarding Event Workflow



Following is a brief explanation of the various stages in the feature:

- L2 stage—Client undergoes authentication or authorization. If security is disabled on the port, then the client is treated as L2 on-boarded client. For L2 clients undergoing authentication, RADIUS and authentication latencies are published in the Client Insight table. Using the authentication start and end time, port access publishes authentication start timestamp, end timestamp and authentication latencies to the Client Insight table. It also publishes time taken by authentication methods to send request and receive response from the RADIUS server. From these values, the following authentication latency can be derived:
 - `dot1x_radius_latency`—Time taken to complete 802.1x RADIUS authentication.
 - `macauth_radius_latency`—Time taken to complete mac-auth RADIUS authentication.



`radius_latency` values are a subset of `auth_latency`. Depending on the configuration, only one of either 802.1X and mac-auth RADIUS latency values is published. In case of concurrent onboarding or authentication precedence with priority, when both the methods are enabled, both latencies are published.

- L3 stage—Client acquires an IP address through the DHCP process, in case the onboarding latency would be the time taken by the DHCP exchange. Onboarding details are captured for only those clients that onboard the switch after enabling Client Insight configurations. Onboarding data will not be available or published for the existing clients before the Client Insight feature is enabled.

- The DHCP discover, offer, request, and acknowledge (DORA) message exchange between client and server need to be tracked to calculate per-client DHCP latency.
- L4 stage—Client accesses DNS service for its DNS name resolution use cases.

Supported Platforms

Client Insight feature is supported on AOS-CX 4100i, 6000, 6100, 6200, 6300, 6400, 8325, 8360, 8400, and 10000 Switch Series.

Prerequisites

Listed below are the prerequisites to configure Client Insight:

- DHCP snooping must be enabled to capture the L3 onboarding status of clients. If DHCP snooping is not enabled, then all clients are marked with L3 timeout as onboarding status.
- Port access configuration is recommended if the authentication and latency values must be derived. If port access is not configured, MAC learn is considered to be L2 onboarding success.
- For average DNS latency, Traffic Insight instance must be configured for DNS packet sampling.
- On platforms where the Traffic Insight feature is not available, the Average DNS Latency values are not available.

Points to Note

- Onboarding details will not be captured for clients onboarded during process restart.
- There can be multiple onboarding event logs for a client if the client MAC ages out and rejoins repeatedly.
- UBT clients are ignored by Client Insight.
- Upon successful L3 onboarding, if switch relearns the client's MAC after the MAC ages out, L3 onboarding timestamp values would be older than L2 onboarding timestamps.
- In case of unavailability of L2 and L3 timestamps, the timestamp value in the onboarding event log will be displayed as -1.

Following are some of the scenarios where the L3 timestamp could be unavailable:

- For clients onboarded while Client Insight is in disabled state, followed by feature enable and client MAC being aged out and relearned in switch.
In this scenario, the event log generated will have L2 timestamps but not L3 timestamps.
- For successfully onboarded clients who have acquired IP address. Switch reboot will flush client MAC from the system and any traffic other than DHCP exchange will trigger client onboarding.
In this scenario, L3 timestamp will not be available since the DHCP exchange did not take place during client onboarding.
- When a client is authenticated using port access device-mode, all Client Insight entries on the port except device MAC address will be cleared from the database. Further, Client Insight will only monitor device MAC client on the port and ignore other clients.

Limitations

Listed below are the limitations:

- Clients with static IP configuration—Static IP or static binding clients will enter L3 timeout state, as DHCP process will not be triggered for them
- L2 and L3 stage timeout values are configured as 3 minutes and 2 minutes. These values cannot be modified.
- For MAC authenticated clients, with concurrent onboarding or authentication priority, there is a delay in initiating the onboarding event. This is because authentication precedence and priority status is published only after the 802.1X authentication process is complete.
- If the client onboarding is successful after the onboarding timeout, no new event is generated. To check the current onboarding status, Aruba Central must monitor the events from appropriate features (port access, DHCP snooping). The same is applicable for clients where the onboarding fails.
- Old L3 latency values are published when the port to which clients are connected flaps, as the client will not trigger DHCP process after L2 authentication on rejoin.
- ND-snooping binding clients will enter L3 timeout state, as DHCP process will not be triggered for them.
- UBT clients will not be monitored.
- Clients that are onboarded on the LAG interfaces will not be monitored.

Feature Interoperability

- DHCP snooping must be enabled for L3 onboarding stage updates.
- A Traffic Insight instance must be created to check the average DNS latency values.
- Authentication is not required for dynamic clients. Therefore, if port access is disabled on the port, it will be considered as L2 successful soon after the MAC address is learnt.

Troubleshooting Client Insight

How do you check for a client's onboarding history?

To check a client's onboarding history, validate the client's onboarding event logs using the **sh events -c client-insight -r** command.

L3 latency data is not present for a client

if L3 latency data is not present for a client in the diag-dump output, validate the DHCP snooping binding table.

Client details is missing in the client-insight table

If any client MAC address is not present in the MAC address table, the client-insight table will not have any information regarding that client.

Client Insight Commands

client-insight enable

```
client-insight enable
no client-insight enable
```

Description

Enables the Client Insight feature on the device. Client Insight is disabled by default at the device level.

The `no` form of the command disables Client Insight.

Examples

Enabling the Client Insight feature:

```
switch(config)# client-insight enable
```

Disabling the Client Insight feature:

```
switch(config)# no client-insight enable
```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.11	Command introduced.

Command Information

Platforms	Command context	Authority
8100 8360	config	Administrators or local user group members with execution rights for this command.

client-insight on-boarding event logs

```
client-insight  
  event-log  
  client-onboarding
```

Description

Enables generation of event logs that lists the onboarding status of each client. Onboarding event logs are disabled by default. For onboarding event logs to work, the Client Insight feature should be enabled before client onboarding. Use the `no` form of the command to disable onboarding event logs for clients.

Parameter	Description
event-log	Configure client onboarding event logs.
client-onboarding	Enable client onboarding event logs.

Examples

Enabling client onboarding event logs:

```
switch(config)# client-insight event-log client-onboarding
```

Disabling client onboarding event logs:

```
switch(config)# no client-insight event-log client-onboarding
```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.11	Command introduced.

Command Information

Platforms	Command context	Authority
8100 8360	config	Administrators or local user group members with execution rights for this command.

diag-dump client-insight basic

```
diag-dump client-insight basic
```

Description

Displays the status of the Client Insight feature—whether enabled or disabled globally. It also displays latencies for all active clients that are onboarded.

Examples

```
switch# diag-dump client-in basic
=====
[Start] Feature client-insight Time : Tue Jul 25 05:32:14 2023
=====
-----
[Start] Daemon client-insightd
-----

Global client-insight          = ENABLED
Client on-boarding event logs = ENABLED
Client dns on-boarding latency= ENABLED

Displaying client entries with (mac) as key.
Total number of entries: 2

MAC : 00:50:56:96:0e:3f
-----
Overall on-boarding status      : successful
Overall on-boarding failure reason : -

L2 on-boarding detail
-----
L2 on-boarding status          : successful
L2 on-boarding failure reason : -
```

```

L2 on-boarding start time      : 07/25/2023 05:28:50.495425 UTC
L2 on-boarding end time        : 07/25/2023 05:28:50.495425 UTC
L2 on-boarding latency         : 0 min, 0 sec, 0 us
802.1x RADIUS latency          : -
MAC-Auth RADIUS latency        : -

L3 on-boarding detail
-----
IP on-boarding status          : successful
IP on-boarding failure reason   : -
L3 on-boarding latency         : 0 min, 3 sec, 455792 us

VLAN : 20
-----
IP details
-----
IPv4 on-boarding status        : successful
IPv6 on-boarding status        : -

DHCPv4                         DHCPv6
-----
Status          : successful      Status          : -
Failure reason   : -              Failure reason   : -
Start time       : 07/25/2023 05:28:50.485325 UTC Start time       : -
End time         : 07/25/2023 05:28:53.941117 UTC End time         : -

DNS details
-----
DNS on-boarding status : successful
Failure reason         : -

Server IP: 11.11.11.2
-----
On-boarding latency    : 0 min, 0 sec, 306 us
DNS request time       : 07/25/2023 05:28:59.656937 UTC
DNS response time      : 07/25/2023 05:28:59.657243 UTC

Average latency:
Server IP: 11.11.11.2
-----
Average latency          : 7091960 usec
DNS start time for latency calculation : 07/25/2023 05:23:51.335296 UTC
DNS end time for latency calculation   : 07/25/2023 05:28:51.323025 UTC
Number of DNS requests          : 14

Server IP: 12.12.12.2
-----
Average latency          : 7954 usec
DNS start time for latency calculation : 07/25/2023 05:23:51.335296 UTC
DNS end time for latency calculation   : 07/25/2023 05:28:51.323025 UTC
Number of DNS requests          : 12

Server IP: 13.13.13.2
-----
Average latency          : 7388 usec
DNS start time for latency calculation : 07/25/2023 05:23:51.335296 UTC
DNS end time for latency calculation   : 07/25/2023 05:28:51.323025 UTC
Number of DNS requests          : 12
-----
[End] Daemon client-insightd
-----
=====

```



```
[End] Feature client-insight
=====
Diagnostic-dump captured for feature client-insight
```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.11	Command introduced.

Command Information

Platforms	Command context	Authority
8100 8360	Operator (>) or Manager (#)	Administrators or local user group members with execution rights for this command.

show capacities client-insight-client-limit

show capacities client-insight-client-limit

Description

Displays the maximum number of clients supported by the Client Insight feature on the switch.

Examples

```
switch# show capacities client-insight-client-limit

System Capacities: Filter Client-Insight client limit
Capacities Name                                     Value
-----
Maximum number of clients supported by Client-Insight feature 4096
```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.11	Command introduced.

Command Information

Platforms	Command context	Authority
8100 8360	Operator (>) or Manager (#)	Administrators or local user group members with execution rights for this command.

show capacities-status client-insight-client-limit

show capacities-status client-insight-client-limit

Description

Displays the maximum number of clients learnt by the Client Insight feature on the switch.

Examples

```
switch# show capacities-status client-insight-client-limit
System Capacities Status: Filter Client-Insight client limit
Capacities Status Name                                     Value Maximum
-----
Number of clients learnt by Client-Insight feature         0          4096
```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.11	Command introduced.

Command Information

Platforms	Command context	Authority
8100 8360	Operator (>) or Manager (#)	Administrators or local user group members with execution rights for this command.

show events -c client-insight

show events -c client-insight

Description

Displays all the events logged by the Client Insight feature.

Following events are logged by the Client Insight feature:

Table 1: *Events Logged by Client Insight*

Process	Event ID	Severity	Message	Description
client-insightd	14301	Info	Client {mac} {vlans} on {port_name} successfully on-boarded. Client on-boarding started at {ob_start_ts}; L2 complete at {l2_end_ts}; L3 complete at {l3_end_ts}	Client successfully on-boarded with given timestamp values.
client-insightd	14302	Info	Client {mac} {vlans} on {port_name} partial success in on-boarding. L2 status: {l2_ob_state} L3 status: {l3_ob_state}. Client on-boarding started at {ob_start_ts}; L2 complete at {l2_end_ts}; L3 complete at {l3_end_ts}	Client on-boarding is partial-successful with given timestamp values.
client-insightd	14303	Info	Client {mac} on {port_name} failed to on-board with status: {onboarding_status} reason_code: {failure_phase_id}	Client failed to on-board with given status and reason code.
client-insightd	14304	Info	Maximum system wide client limit {client-number} reached	Maximum system wide client limit is reached
client-insightd	14305	Info	Maximum system wide client limit {client-number} reached	Maximum system wide client limit is reached
client-insightd	14306	Info	Client {mac} successfully on-boarded on VLAN {vlans}; Client on-boarding started at {ob_start_ts}; L2 complete at {l2_end_ts}; L3 complete at {l3_end_ts}; ARP to GW response received at {arp_end_ts}; DNS on-boarding to (dns_server_ip)	Client successfully on-boarded with given timestamp values.

Process	Event ID	Severity	Message	Description
			completed at {dns_end_ts}	
client-insightd	14307	Info	Client {mac} on-boarded on VLANs {vlans} and failed on VLANs {failed_vlans}; Client on-boarding started at {ob_start_ts}; L2 complete at {l2_end_ts}; L3 complete at {l3_end_ts}; ARP to GW response received at {arp_end_ts}; DNS on-boarding to (dns_server_ip) completed at {dns_end_ts}; L2 status {l2_ob_state} failure_reason_code - {l2_failure_reason}; L3 status {l3_ob_state} failure_reason_code - {l3_failure_reason}; DNS on-boarding status {dns_status} failure_reason_code - {dns_failure_reason}	Client on-boarding is partial-successful with given timestamp values.
client-insightd	14308	Info	Client {mac} failed to on-board with status: {onboarding_status} in failure phase: {failure_phase_id} with reason: {failure_reason}	Client failed to on-board with given status, phase_id and reason code.



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.11	Command introduced.

Command Information

Platforms	Command context	Authority
8100 8360	Operator (>) or Manager (#)	Administrators or local user group members with execution rights for this command.

show tech client-insight

show tech client-insight

Description

Displays if the global Client Insight and client on-boarding event log features are enabled or disabled. Also displays the latencies for all active clients that are onboarded.

Examples

```
switch# show tech client-insight

=====
Show Tech executed on Thu May 18 15:05:43 2022
=====

[Begin] Feature client-insight
=====
*****
Command : show client-insight
*****
Client Insight Information:
Global client-insight          = ENABLED
Client on-boarding event logs = ENABLED
=====

[End] Feature client-insight
=====

Show Tech commands executed successfully
=====
```

Displaying L2, L3 client latencies and details:

```
switch# show tech client-insight

=====
Show Tech executed on Thu Sep 22 06:34:16 2022
=====

[Begin] Feature client-insight
=====

*****
Command : diag-dump client-insight basic
*****

[Start] Feature client-insight Time : Thu Sep 22 06:34:16 2022
=====
-----
[Start] Daemon client-insightd
-----
```

```

Global client-insight          = ENABLED
Client on-boarding event logs = ENABLED

Displaying client entries with (mac) as key.
Total number of entries: 1

MAC : 00:11:01:00:00:08
-----
Overall on-boarding status      : -
Overall on-boarding failure reason : -

L2 on-boarding detail
-----
L2 on-boarding status          : successful
L2 on-boarding failure reason  : -
L2 authentication start time   : 05/18/22 15:01:01.456789 UTC
L2 authentication end time     : 05/18/22 15:01:02.123456 UTC
L2 authentication latency      : 0 min, 0 sec, 666667 us
802.1x RADIUS latency          : -
MAC-Auth RADIUS latency        : 0 min, 0 sec, 332456 us

L3 on-boarding detail
-----
L3 on-boarding status          : in_progress
L3 on-boarding failure reason  : -
L3 on-boarding latency         : -

VLAN : 10
-----
IP details
-----
IPv4 on-boarding status        : successful
IPv6 on-boarding status        : -

DHCPv4                         DHCPv6
-----
Status          : successful          Status          : -
Failure reason   : -                  Failure reason   : -
Start time       : 05/18/22 15:01:02.456789 UTC Start time       : -
End time         : 05/18/22 15:01:02.999988 UTC End time         : -

VLAN : 20
-----
IP details
-----
IPv4 on-boarding status        : In_Progress
IPv6 on-boarding status        : -

DHCPv4                         DHCPv6
-----
Status          : In_Progress          Status          : -
Failure reason   : -                  Failure reason   : -
Start time       : 05/18/22 15:01:03.256485 UTC Start time       : -
End time         : -                  End time         : -

DNS details
-----
Server IP: 172.16.1.8
-----
Average latency              : 0 min, 0 sec, 432456 us
DNS start time for latency calculation : 05/18/22 15:01:03.123456 UTC
DNS end time for latency calculation   : 05/18/22 15:01:03.425466 UTC

```

```

Number of DNS requests          : 16

Server IP: 2003::1
-----
Average latency                  : 0 min, 0 sec, 432456 us
DNS start time for latency calculation : 05/18/22 15:01:03.123456 UTC
DNS end time for latency calculation   : 05/18/22 15:01:03.425466 UTC
Number of DNS requests            : 16

-----

[End] Daemon client-insightd
-----

[End] Feature client-insight
=====
Diagnostic-dump captured for feature client-insight
=====
[End] Feature client-insight
=====

=====
Show Tech commands executed successfully
=====
Show Tech took 43 seconds for execution

=====
Show Tech executed on Thu Sep 22 06:34:16 2022
=====

[Begin] Feature client-insight
=====

*****
Command : diag-dump client-insight basic
*****

=====
[Start] Feature client-insight Time : Thu Sep 22 06:34:16 2022
=====

-----
[Start] Daemon client-insightd
-----

Global client-insight          = ENABLED
Client on-boarding event logs = ENABLED

Displaying client entries with (mac) as key.
Total number of entries: 1

MAC : 00:11:01:00:00:08
-----
Overall on-boarding status      : -
Overall on-boarding failure reason : -

L2 on-boarding detail
-----
L2 on-boarding status          : successful
L2 on-boarding failure reason : -

```

```

L2 authentication start time : 05/18/22 15:01:01.456789 UTC
L2 authentication end time   : 05/18/22 15:01:02.123456 UTC
L2 authentication latency    : 0 min, 0 sec, 666667 us
802.1x RADIUS latency        : -
MAC-Auth RADIUS latency      : 0 min, 0 sec, 332456 us

L3 on-boarding detail
-----
L3 on-boarding status        : in_progress
L3 on-boarding failure reason : -
L3 on-boarding latency       : -

VLAN : 10
-----
IP details
-----
IPv4 on-boarding status      : successful
IPv6 on-boarding status      : -

DHCPv4                        DHCPv6
-----
Status                        : successful          Status : -
Failure reason                : -                  Failure reason : -
Start time                    : 05/18/22 15:01:02.456789 UTC Start time : -
End time                      : 05/18/22 15:01:02.999988 UTC End time : -

VLAN : 20
-----
IP details
-----
IPv4 on-boarding status      : In_Progress
IPv6 on-boarding status      : -

DHCPv4                        DHCPv6
-----
Status                        : In_Progress          Status : -
Failure reason                : -                  Failure reason : -
Start time                    : 05/18/22 15:01:03.256485 UTC Start time : -
End time                      : -                   End time : -

DNS details
-----
Server IP: 172.16.1.8
-----
Average latency                : 0 min, 0 sec, 432456 us
DNS start time for latency calculation : 05/18/22 15:01:03.123456 UTC
DNS end time for latency calculation   : 05/18/22 15:01:03.425466 UTC
Number of DNS requests          : 16

Server IP: 2003::1
-----
Average latency                : 0 min, 0 sec, 432456 us
DNS start time for latency calculation : 05/18/22 15:01:03.123456 UTC
DNS end time for latency calculation   : 05/18/22 15:01:03.425466 UTC
Number of DNS requests          : 16

-----
[End] Daemon client-insightd
-----

```



```

=====
[End] Feature client-insight
=====
Diagnostic-dump captured for feature client-insight
=====
[End] Feature client-insight
=====

=====
Show Tech commands executed successfully
=====
Show Tech took 43 seconds for execution

```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.11	Command introduced.

Command Information

Platforms	Command context	Authority
8100 8360	Operator (>) or Manager (#)	Administrators or local user group members with execution rights for this command.

The public key infrastructure (PKI) feature enables administrators to manage digital certificates on the switch. The switch uses certificates to validate SSH clients when acting as an SSH server, and when communicating with syslog servers when TLS encryption is used.

PKI concepts

Digital certificate

A digital certificate is an electronic form of identification that stores important information about an entity (such as a computer, program, or website). Certificates help secure digital transactions by enabling the end parties to validate each other's identity. Digital certificates are issued by a certificate authority (CA) and are composed of an encoded string of characters (usually stored in a file). For example:

```
-----BEGIN CERTIFICATE-----
MIIDSDCCApGCCQDJotuPPj9GCDANBgkqhkiG9w0BAQsAADCBCqzELMAkGA1UEBh
VVMxEzARBgNVBAgMCkNhbmG1mb3JuaWExEDA0BgNVBACBM1JvY2tsaW4xDDAKBg
BAoMA0hQTjEVMBMGA1UECwwMSFBOUm9zZXZpbGx1MSokwAYDVQQDDCFocG5zdz
...
MioDy0096DvSMPsnOaI+jnZ3AozN8y+nLgotXUsg36pO/Ncc51oQhyUdcAbgA1
rzSLgyTnpXZKumvlaOTk3pzrIf7m5V103GTbgHGSFCzgO6QWxVxu9d7ju1o59S
aOIT7JSsYI5LsLpVz9ZqS599rj/1LoH+rLN1RDVXpS+J51
-----END CERTIFICATE-----
```

The switch can import PEM encoded ITU-T X.509 v3 certificates. (Certificates can be converted to human-readable form using a software decoder.)

An X.509 digital certificate typically includes the following information:

- Signature algorithm: The cryptographic algorithm used to generate the digital signature.
- Signature value: Digital signature of the certificate generated using the CA's private key.
- Version number: X.509 version number.
- Serial number: Certificate serial number.
- Issuer name: Name of the certificate authority (CA) that issued the certificate.
- Validity period: Beginning and ending dates.
- Subject name: Name of the entity to which the certificate is issued.
- Subject public key and key algorithm.
- Key usage extension: Purpose of the certificate.

Certificate authority

A certificate authority (CA) is an entity that can issue and sign digital certificates. A CA can be a well-known, trusted commercial company, or a private entity controlled by your organization. For a commercial CA, the CA validates the credentials of a user before issuing a certificate and signing it,

guaranteeing a certificate holder's identity. For a private CA, self-signed certificates can be generated as needed for devices on your network without paying a commercial company.

Root certificate

A root certificate is a self-signed certificate that is deemed the root of trust for a certificate chain. This is the certificate that identifies a CA, and is used by the CA to sign any certificates that it issues. When two peers attempt to establish a secure connection, they use the CA's public key to verify that each other's certificates were indeed signed by a trusted certificate authority.

Each root CA certificate has a unique fingerprint, which is the hash value of the certificate content. The fingerprint of a root CA certificate can be used to authenticate the validity of the root CA.

In a certificate chain, the root CA generates a self-signed certificate, and each lower level CA holds a CA certificate (intermediate certificate) issued by the CA immediately above it. The hierarchy of these certificates forms a *chain of trust*.

Leaf certificate

This is the certificate used by a software entity, such as a syslog client, to identify itself to a peer when establishing a secure connection.

Intermediate certificate

An intermediate certificate is a CA which has been issued by the root certificate or by another intermediate certificate. Intermediate CAs can issue leaf certificates and sit in between the root and leaf certificates. The use of an intermediate CA allows administrators to segregate their PKI groups.

Trust anchor

This is the certificate that acts as the base of trust for the validation of other certificates. A trust anchor can be a root or intermediate certificate issued by a CA.

OCSP

The online certificate status protocol (OCSP) is a real-time method for determining the revocation status of a certificate. When two peers attempt to establish a secure connection, they can query an OCSP responder to determine the status (valid or revoked) of each other's certificates. The OCSP responder for a certificate is typically provided by a server managed by the CA that issued the certificate.

PKI on the switch

The AOS-CX Switch Series switches provides for installation of certificate authority (CA) certificates and the generation and installation of leaf certificates.

Trust anchor profiles

The switch supports 64 trust anchor (TA) profiles. Each TA profile stores a trusted CA certificate. The certificate can be either a root CA certificate, which must be self-signed, or an intermediate CA certificate that is issued by another CA.



The certificate must have its `BasicConstraints` field with CA key set to **true**, and its **KeyUsage** extension field set with **keyCertSign** and/or **cRLSign**.

CA certificates are used to:

- Validate the certificates that remote peers present when attempting to establish a secure connection with a service on the switch, for example, the SSH server.
- Validate leaf certificates installed on the switch that are used, for example, by the syslog client, the Web UI, or REST API.

The TA profile also enables configuration of real-time checking of certificate revocation (through OCSP).

Leaf certificates

Leaf certificates can be installed on the switch for use by features such as the syslog client, the Web UI, or REST API. If you are purchasing a certificate from a trusted CA, the switch can generate the certificate signing request (CSR) that is used to obtain the certificate. The switch can also directly generate self-signed certificates. Alternatively, the certificate and private key can be generated outside the switch and then imported. X509 certificate management software such as OpenSSL can be used to generate the private key and CSR and then combine the certificate and private key into one PEM or PKCS#12 file suitable for importation into the switch.

Mandatory matching of peer device hostname

While validating the peer device certificates, the switch checks that the peer device configured hostname matches either the Subject Alternative Name (SAN) field or the Common Name (CN) within the certificate Subject field. If the SAN field is present and matches the hostname, validation succeeds, otherwise it fails. If the SAN field is not present, and the CN matches the hostname, validation succeeds, otherwise it fails.

PKI EST

EST (Enrollment over Secure Transport) (RFC 7030) defines the protocol that devices use to request trusted certificate authority (CA) certificates and to enroll / re-enroll device certificates from CA services using secure channels, specifically HTTP over TLS.

Devices can be configured to request the trusted CA certificates and to request enrollment, and re-enrollment of device certificates automatically, without the need for administrator intervention, while maintaining the security and integrity of the whole enrollment process.

The switch includes an EST client implemented as a part of the PKI infrastructure.

For detailed CLI command descriptions, see:

- [PKI commands](#)
 - [PKI EST commands](#)
-



EST usage overview

- The EST client on the switch requires EST profile configuration, including EST server URL and the VRF providing HTTP connection to the EST server.
- At the time the URL is set in the EST profile, the switch connects to the EST server and downloads the trusted CA certificate chain. To accommodate CA certificate updates, the certificate chain is also downloaded before a certificate enrollment or re-enrollment is attempted.

- EST supports up to:
 - 16 EST profiles
 - 63 trusted CA certificates downloaded from EST servers.
 - 18 device certificates enrolled through EST services.
- EST profile configuration is supported through the CLI and the REST API **PKI_EST_Profile**.
- CA certificate request and device certificate enrollment is supported through the CLI and the REST custom API **CertificateManager /certificate**.

Prerequisites for using EST for certificate enrollment

- Establish the PKI infrastructure for your organization, with the CA chain and service ready to issue certificates. Issue a service certificate for the EST server.
- Install the root CA certificate in a TA profile on the switch that will validate the EST server certificate using CLI commands **crypto pki ta-profile** and **ta-certificate**.
- Optionally, preconfigure an EST client certificate on the switch.
- Make the EST server reachable from the switch. Connect the CA service(s) to the EST server. If there is a client certificate for the EST client, install the root CA certificate on the server that will validate the client certificate.

EST profile configuration

In the global configuration context, create an EST profile and enter its context:

```
crypto pki est-profile <EST-NAME>
```

In an EST profile context, configure the EST profile parameters using these commands:

```
url <URL>
vrf <VRF-NAME>
username <USERNAME> password [ciphertext <CIPHERTEXT-PASSWORD> |plaintext
<PLAINTEXT-PASSWORD>]
retry-interval <INTERVAL>
retry-count <RETRIES>
arbitrary-label <LABEL>
arbitrary-label-enrollment <LABEL>
arbitrary-label-reenrollment <LABEL>
reenrollment-lead-time <LEAD-TIME>
```

Certificate enrollment

In the global configuration context, create a certificate and enter its context:

```
crypto pki certificate <CERT-NAME>
```

In a certificate configuration context, configure the certificate parameters:

```
key-type {rsa [key-size <K-SIZE>] | ecdsa [curve-size <C-SIZE>]}
subject [common-name <COMMON-NAME>]
        [country <COUNTRY>]
        [locality <LOCALITY>]
        [org <ORG-NAME>]
        [org-unit <ORG-UNIT>]
        [state <STATE>]
```

In a certificate configuration context, enroll the certificate using an EST service:

```
enroll est-profile <EST-NAME>
```

Certificate re-enrollment

- The re-enrollment request is sent automatically to the same EST server that was used for the original enrollment.
- The switch presents the enrolled certificate being re-enrolled to the EST server for authentication. If the certificate has expired or authentication fails for any reason, the switch falls back to using the EST client certificate or the username and password in the EST profile, whichever is configured, and performs a new certificate enrollment.
- Re-enrollment lead-time is configurable in the EST profile using CLI command **reenrollment-lead-time**. It sets the number of days before certificate expiry date that certificate re-enrollment will be initiated.

Checking EST profile and certificate configuration

Show the list of EST profiles or details of a specific EST profile:

```
show crypto pki est-profile [<EST-NAME>]
```

Show a list of TA profiles whether directly configured or EST-enrolled, or details of a specific TA profile:

```
show crypto pki ta-profile [<TA-NAME>]
```

Show the list of certificates whether directly configured or EST-enrolled, or details of a specific certificate:

```
show crypto pki certificate [<CERT-NAME> [plaintext | pem]]
```

Show all certificates assigned to the switch EST client as well as certificates that are assigned to other applications on the switch.:

```
show crypto pki application
```

EST best practices

Ensure the following:

- A time synchronization service is used on both the switch (the EST client) and the EST server.
- In all CA certificates, the **Basic Constraints** field has **CA** set to **true**, **pathlen** is set appropriately, and **Key Usage** is set with **keyCertSign**.
- In all leaf certificates, the **Extended Key Usage** field is set with the appropriate purpose as follows:
 - For server certificates, set with **serverAuth**. The **Key Usage field** has at least one of **digitalSignature**, **keyEncipherment**, or **keyAgreement**.
 - For client certificates, set with **clientAuth**. The **Key Usage field** has at least one of **digitalSignature**, or **keyAgreement**.

- The EST server is configured to include the intermediate issuer CA certificates in the trusted CA certificate chain that the EST server sends to the switch (the EST client) upon request.

Example using EST for certificate enrollment

This example illustrates the configuration of an EST profile and enrolling application certificates using an EST server.

Prerequisites:

- An EST server is reachable from the switch management port.
- Availability of the root CA certificate used to validate the server certificate.

This example shows the following:

- Installing the root CA certificate as a TA profile for validation of the EST server certificate.
- Configuring an EST profile with the EST server information, including the username and password for client authentication and the EST server URL.
- Issuing a request to enroll a leaf certificate using the EST server.
- Assigning the enrolled certificate to the EST client and syslog client on the switch.

Each section in the below example is preceded by descriptive text.

Example

```
=====
The switch in its default configuration state.
=====
```

```
switch# show running-config
Current configuration:
!
!Version AOS-CX FL.10.06.0001CM
!export-password: d, TECHPUB-315: AOSCX-197765 Halon 10.09:UBT Fallback Role
efault
user admin group administrators password ciphertext AQBapTLgcT+DNrtd0bmdXIP2L0AY
NUpwWyQEIZX4oMKtwlXcYgAAAOMKlfxH+ugf3Fe2JuWar2uKG7A/R6bqMO/ZHS364NompXV/Ko37ZhCq
cFpaOJsk01+IJPRUkbpigCeEObM67Od8/vrASJaO6EAj+RBnWCrifwdChcUUS3XpbCUl7dmxYHNg
!
!
ssh server vrf default
ssh server vrf mgmt
vsf member 1
    type jl668a
vlan 1
spanning-tree
interface mgmt
    no shutdown
    ip dhcp
interface 1/1/1
    no shutdown
    no routing
    vlan access 1
interface 1/1/2
```

```

    no shutdown
    no routing
    vlan access 1
interface 1/1/3
    no shutdown
    no routing
    vlan access 1
...
interface 1/1/26
    no shutdown
    no routing
    vlan access 1
interface 1/1/27
    no shutdown
    no routing
    vlan access 1
interface 1/1/28
    no shutdown
    no routing
    vlan access 1
interface vlan 1
    ip dhcp
!
!
https-server vrf default
https-server vrf mgmt
switch#

```

```

=====
The mgmt port is connected to a network with DNS available and the
EST server reachable.
=====

```

```

switch# show interface mgmt
  Address Mode           : dhcp
  Admin State           : up
  Mac Address           : 38:21:c7:59:cd:81
  IPv4 address/subnet-mask : 999.100.205.146/24
  Default gateway IPv4   : 999.100.205.1
  IPv6 address/prefix    :
  IPv6 link local address/prefix: fe80::3a21:c7ff:fe59:cd81/64
  Default gateway IPv6   :
  Primary Nameserver     :
  Secondary Nameserver   :
switch#

```

```

=====

  Address Mode           : dhcp
  Admin State           : up
  Mac Address           : 38:21:c7:59:cd:81
  IPv4 address/subnet-mask : 999.100.205.146/24
  Default gateway IPv4   : 999.100.205.1
  IPv6 address/prefix    :
  IPv6 link local address/prefix: fe80::3a21:c7ff:fe59:cd81/64
  Default gateway IPv6   :
  Primary Nameserver     :
  Secondary Nameserver   :
switch#

```


=====
Configure the root CA cert as a TA profile that will validate the server cert.
=====

```
switch# config
switch(config)#
switch(config)# crypto pki ta-profile root-ca-for-est-server
switch(config-ta-root-ca-for-est-server)#
switch(config-ta-root-ca-for-est-server)# ta-certificate import terminal
Paste the certificate in PEM format below, then hit enter and ctrl-D:
switch(config-ta-cert)# -----BEGIN CERTIFICATE-----
NVBAYTonfig-ta-cert)# MIIB2DCCAX6gAwIBAgIJAKtmJvZZy9RdMAoGCCqGSM49BAMCMGIXCzAJBg
QKEwNIonfig-ta-cert)# AlVTMQswCQYDVQQIEwJDQTESMBAGA1UEBxMJUM9zZXZpbGx1MQwwCgYDVQ
0yMDAlonfig-ta-cert)# UEUxDjAMBgNVBAsTBUFydWJhMRQwEgYDVQQDEWtkYW5lc3Qtcm9vdDAeFw
...
YDVR0Ponfig-ta-cert)# VCnKTlhxfmV72nfXypI979UsopuP5nCjHTAbMAwGA1UdEwQFMAMBAf8wCw
eo6yN0onfig-ta-cert)# BAQDAgEGMAoGCCqGSM49BAMCA0gAMEUCIQDb/uHvU8DFRTyfnP9wkli6sd
c=00onfig-ta-cert)# UvU05t7/rrVxRQIgMHGjHhaNlnkjYBG8Ei3C1UDILiKl07McMTCWVo4Ik5
switch(config-ta-cert)# -----END CERTIFICATE-----
switch(config-ta-cert)#
The certificate you are importing has the following attributes:
Subject: C = US, ST = CA, L = Roseville, O = HPE, OU = Aruba, CN = danest-root
Issuer: C = US, ST = CA, L = Roseville, O = HPE, OU = Aruba, CN = danest-root
Serial Number: 0xAB6626FXXXXD45D
TA certificate import is allowed only once for a TA profile
Do you want to accept this certificate (y/n)? y
switch(config-ta-root-ca-for-est-server)#
switch(config-ta-root-ca-for-est-server)# exit
switch(config)#
switch(config)# show crypto pki ta-profile
```

TA Profile Name	TA Certificate	Revocation Check
root-ca-for-est-server	Installed, valid	disabled

```
switch(config)#
```

=====
Configure the EST profile with the EST server URL, username/password.
=====

```
switch(config)# crypto pki est-profile test-est-server
switch(config-est-test-est-server)#
switch(config-est-test-est-server)# user fred password plaintext barney
switch(config-est-test-est-server)#
switch(config-est-test-est-server)# url https://999.0.10.229:8443/.well-known/est
switch(config-est-test-est-server)#
switch(config-est-test-est-server)# exit
switch(config)#
```

=====
At the time the EST URL is set, the switch sends a request to the EST server to get the set of trusted CA certs. If that is successful, TA profiles will be auto-created for those CA certs.

Display the list of TA profiles and EST profile details.
=====

```
switch(config)# show crypto pki ta-profile
```

TA Profile Name	TA Certificate	Revocation Check
test-est-server-est-ta00	Installed, valid	OCSP
test-est-server-est-ta02	Installed, valid	OCSP
test-est-server-est-ta05	Installed, valid	OCSP
test-est-server-est-ta01	Installed, valid	OCSP
root-ca-for-est-server	Installed, valid	disabled
test-est-server-est-ta04	Installed, valid	OCSP
test-est-server-est-ta03	Installed, valid	OCSP

```
switch(config)# show crypto pki est-profile
```

Profile Name	Downloaded TA Profiles	Enrolled Certificates
test-est-server	6	1

```
switch(config)#
```

Profile Name	Downloaded TA Profiles	Enrolled Certificates
test-est-server	6	1

```
switch(config)# show crypto pki est-profile test-est-server
```

```

Profile Name           : test-est-server
Service VRF            : mgmt
Service URL            : https://999.0.10.229:8443/.well-known/est
  Arbitrary Label       : not configured
  Arbitrary Label Enrollment : not configured
  Arbitrary Label Reenrollment : not configured
Authentication Username : fred
Authentication Password :
  AQBapR7ndgoxkMlWQUQvK+Dvd3S6m+s9fdaPQwdkMbIYEMnMBgAAAHRhhlIYwA==
Retry Interval         : 30 seconds
Retry Count            : 3 times
Reenrollment Lead Time : 2 days
Downloaded TA Profiles : 6
Enrolled Certificates  :
  cert-for-app
switch(config)#

```

=====
Originally, the switch only has two built-in certificates.
 =====

```
switch(config)# show crypto pki certificate
```

Certificate Name	Cert Status	EST Status	Associated Applications
device-identity	installed	n/a	none
local-cert	installed	n/a	dot1x-supPLICant, est-client, hsc, https-server, syslog-client

=====
Create a new certificate, configure its key type, key size, and subject fields.

```

=====
switch(config)# crypto pki certificate cert-for-app
switch(config-cert-cert-for-app)#
switch(config-cert-cert-for-app)# key-type ecdsa curve-size 521
switch(config-cert-cert-for-app)#
switch(config-cert-cert-for-app)# subject
Do you want to use the switch serial number as the common name (y/n)? n
Common Name: 999.100.205.146
Org Unit: Aruba-Roseville
Org Name: HPE
Locality: Roseville
State: CA
Country: US
switch(config-cert-cert-for-app)#

```

```

=====
Request to enroll the certificate through the EST server.
=====

```

```

switch(config-cert-cert-for-app)# enroll est-profile test-est-server
You are enrolling a certificate with the following attributes:
Subject: C=US, ST=CA, L=Roseville, OU=Aruba-Roseville, O=HPE,
        CN=999.100.205.146
Key Type: ECDSA (521)

```

```

Continue (y/n)? y
Certificate enrollment via test-est-server has been initiated. Please use
'show crypto pki certificate cert-for-app' to check its status.
switch(config-cert-cert-for-app)#

```

```

=====
Check the cert status to see if enrollment is successful. It is.
=====

```

```

switch(config)# show crypto pki certificate

```

Certificate Name	Cert Status	EST Status	Associated Applications
device-identity	installed	n/a	none
local-cert	installed	n/a	dot1x-supplicant, est-client, hsc, https-server, syslog-client
cert-for-app	installed	enroll success	none

```

switch(config-cert-cert-for-app)#
switch(config-cert-cert-for-app)# exit
switch(config)#
switch(config)# show crypto pki certificate cert-for-app pem
Certificate Name: cert-for-app
Associated Applications:
  est-client
Certificate Status: installed
EST Status: enroll success
Certificate Type: regular
Intermediates:
  Subject: C = US, ST = CA, O = HPE, OU = Aruba, CN = danest-int2
  Issuer: C = US, ST = CA, O = HPE, OU = Aruba, CN = danest-int1

```


In this example, the cert is assigned to the est-client and syslog.

```
switch(config)# crypto pki application est-client certificate cert-for-app
switch(config)# crypto pki application syslog-client certificate cert-for-app
switch(config)#
switch(config)#
switch(config)#
switch(config)# show crypto pki application
```

Associated Applications	Certificate Name	Cert Status
est-client	cert-for-app	valid
https-server		not configured, using local-cert
syslog-client	cert-for-app	valid

```
switch(config)#
```

Example including the use of an intermediate certificate

This example shows the following:

- Installing a root CA as a TA profile.
- Creating a CSR for a leaf certificate.
- Installing the signed leaf certificate issued by an intermediate CA. The intermediate CA certificate is included after the signed leaf certificate.

Each section in the below example is preceded by descriptive text.

Example

Install root CA as a TA profile

```
switch(config)# crypto pki ta-profile root
switch(config-ta-root)# ta-certificate import terminal
Paste the certificate in PEM format below, then hit enter and ctrl-D:
switch(config-ta-cert)# -----BEGIN CERTIFICATE-----
switch(config-ta-cert)# MIIGATCCA+mgAwIBAgIJAL/JIZfJ0GpcMA0GCSqGSIUAMIGOMQswCQYD
switch(config-ta-cert)# VQQGEwJVUzETMBEGA1UECAwKQ2FsaWZvcn5pYTESBwwJUm9zZXZpbGxl
switch(config-ta-cert)# MQwwCgYDVQQKDANIUEUxEzARBgNVBASMCK5ldmcxFTATBgNVBAMMDFRl
...
switch(config-ta-cert)# rvadRXSAsUlevJRNN0yINrEJyOfUX2hAfLaiBYP+In6gKTAwVhlxLiXn
switch(config-ta-cert)# LlryAb2/go4BTYjil3eJyXxweUHheuBeesEslBawLv0cPCQPTTdbc970
switch(config-ta-cert)# iWhyAmfSpD/TS3AgCLnBFPKEKsms0f0LF3/C9dRUXjIHT/LDBr+lgzY3
switch(config-ta-cert)# m2NCvxY=
switch(config-ta-cert)# -----END CERTIFICATE-----
switch(config-ta-cert)#
The certificate you are importing has the following attributes:
Subject: C = US, ST = California, L = Roseville, O = HPE, OU = Networking,
CN = Test CA root, emailAddress = generic@corp.com
Issuer: C = US, ST = California, L = Roseville, O = HPE, OU = Networking,
CN =Test CA root, emailAddress = generic@corp.com
Serial Number: 0xBFC92197xxxxxxxx
TA certificate import is allowed only once for a TA profile
Do you want to accept this certificate (y/n)? y
switch(config-ta-root)# exit
```

=====

Create a CSR for a leaf certificate

=====

```
switch(config)# crypto pki certificate leaf
switch(config-cert-leaf)# subject
Do you want to use the switch serial number as the common name (y/n)? y
Common Name: SG9Zxxxxxx
Org Unit:
Org Name:
Locality:
State:
Country:
switch(config-cert-leaf)# enroll terminal
You are enrolling a certificate with the following attributes:
Subject: C=<empty>, ST=<empty>, L=<empty>, OU=<empty>, O=<empty>,
        CN=SG9Zxxxxxx
Key Type: RSA (2048)
```

Continue (y/n)? **y**

```
-----BEGIN CERTIFICATE REQUEST-----
MIICWjCCAUICAQIwFTETMBEGA1UEAwwKU0c5WktONDAwSoZIhvcN
AQEBBQADggEPADCCAQoCggEBAMKdtoucDEMeuZjPGvCcWTm4D39A
WBA8K/bduJvM1E2B/uirU2TX7mF6lN30akClSxZOoofZAmBPCzI3
...
wZtb5c8fYCSR+TpLwZAdoXrvGJqJ1aGzV6/kVfb7rM6ulBksfBo/
JwO+7x8Vn5hldGCrsl9CPJienni/fq24+1CJzspMbY9BKu9EIL+P
5ND9BmN0IzEmDO26F+Ip74DqFCIYjXtl3uPJk4cwJkXq121hlcrG
UlatpvjNEpZOtfoEryDJSs0pHXky7VjltYABIuDy
-----END CERTIFICATE REQUEST-----
```

=====

```
-----BEGIN CERTIFICATE REQUEST-----
MIICWjCCAUICAQIwFTETMBEGA1UEAwwKU0c5WktONDAwSoZIhvcN
AQEBBQADggEPADCCAQoCggEBAMKdtoucDEMeuZjPGvCcWTm4D39A
WBA8K/bduJvM1E2B/uirU2TX7mF6lN30akClSxZOoofZAmBPCzI3
...
wZtb5c8fYCSR+TpLwZAdoXrvGJqJ1aGzV6/kVfb7rM6ulBksfBo/
JwO+7x8Vn5hldGCrsl9CPJienni/fq24+1CJzspMbY9BKu9EIL+P
5ND9BmN0IzEmDO26F+Ip74DqFCIYjXtl3uPJk4cwJkXq121hlcrG
UlatpvjNEpZOtfoEryDJSs0pHXky7VjltYABIuDy
-----END CERTIFICATE REQUEST-----
```

=====

**Install the signed leaf certificate issued by an intermediate CA. The
lintermediate CA certificate is included after the signed leaf certificate.**

=====

```
switch(config-cert-leaf)# import terminal ta-profile root
Paste the certificate in PEM format below, then hit enter and ctrl-D:
switch(config-cert-import)# -----BEGIN CERTIFICATE-----
switch(config-cert-import)# MIIKTCCAhGgAwIBAgIJA01LS0BmKxtbMA0GCSqGSIYxCzAJBgNV
switch(config-cert-import)# BAYTAKFVMRUwEwYDVQQIDAxJbnRlcm1lZGNVBAoMGEludGVybmV0
switch(config-cert-import)# IFdpZGdpdHMgUHR5IEExOZDENMAsGA1UEAw0yMDA1MTQyMDI3MTla
...
```

```

switch(config-cert-import)# axnZcIaNp4eNi95in+TvckXA0eMLScNyR7IF+Wjn56H0fQKYsHp/
switch(config-cert-import)# jllbCkyB1xKnn6IpzIj/hvAx3NpA0jXx/qJA+V/cltaAL6+QPZmI
switch(config-cert-import)# vr5GZsoV72BHFOXxoteZlmWMUdVldYXXP2DzEUbttr9zojwz0MyK
switch(config-cert-import)# Qz5tc0BlGfJAtghykw==
switch(config-cert-import)# -----END CERTIFICATE-----
switch(config-cert-import)# -----BEGIN CERTIFICATE-----
switch(config-cert-import)# MIIFyzCCA7OgAwIBAgIJA01LS0BmKxtwMA0GCSqGCIgOMQswCQYD
switch(config-cert-import)# VQqGEwJVUzETMBEGA1UECAwKQ2FsaWZvc1UEBwwJUm9zZXZpbGxl
switch(config-cert-import)# MQwwCgYDVQQKDANIUEUxEzARBgNVBASMCmcxFTATBgNVBAMMDFRl
...
switch(config-cert-import)# LM9DV3YNWOM4UMMP2HXaDDfqxZPX9Zsj6G1/stRCh8SVfsF2duYR
switch(config-cert-import)# 5brLfEpiDhXrZVXxF91ljRABO2JPLSUufg7xr6M/K5aCujxVYzK7
switch(config-cert-import)# DQaCEw5NlmC1vpYlY2TG3dlUQPZDeQOAHwuBd4HewqDHWfp/T04=
switch(config-cert-import)# -----END CERTIFICATE-----
switch(config-cert-import)#
Leaf certificate is validated with root and imported successfully.
switch(config-cert-leaf)#

```

Installing a self-signed leaf certificate (created inside the switch)

This procedure describes how to create (wholly inside the switch) and install a self-signed X.509 leaf certificate. And associate it with one of the following switch features: syslog client, HTTPS server, or HSC (hardware switch controller).

Procedure

1. Create a leaf certificate context with the command **crypto pki certificate**. This switches to the leaf certificate configuration context.
2. Define leaf certificate properties with the command **subject**.
3. Set the encryption key type for the leaf certificate with the command **key-type**.
4. Generate and install the self-signed certificate with the command **enroll self-signed**.
5. Exit the leaf certificate context with the command **exit**.
6. Associate the leaf certificate with a switch feature (syslog client, HTTPS server, or HSC) with the command **crypto pki application**.

Example

This example:

- Creates the leaf certificate context.
- Defines the leaf certificate characteristics.
- Creates and installs the self-signed leaf certificate.
- Associates the leaf certificate with the syslog client (application) on the switch.

```

switch(config)# crypto pki cert SS_LC
8400X(config-cert-SS_LC)# subject common-name SSLeaf country US
state CA locality Rocklin org Company org-unit Site
8400X(config-cert-SS_LC)# key-type rsa key-size 3072
8400X(config-cert-SS_LC)# enroll self-signed
You are enrolling a certificate with the following attributes:
Subject: C=US, ST=CA, L=Rocklin, OU=Site, O=Company,
        CN=SSLeaf

```



```
Key Type: RSA (3072)
```

```
Continue (y/n)? y
```

```
Self-signed certificate is created and enrolled successfully.
```

```
8400X(config-cert-SS_LC)# exit
```

```
switch(config)# crypto pki application syslog-client certificate SS_LC
```

Installing a self-signed leaf certificate (created outside the switch)

This procedure describes how to install a self-signed X.509 leaf certificate (that was created outside the switch). And then associate the certificate with one of the following switch features: syslog client, HTTPS server, or HSC (hardware switch controller).

Prerequisites

A self-signed leaf certificate (including private-key data) must be created outside the switch.

Procedure

1. Create the leaf certificate context with the command **crypto pki certificate** which then switches to the created leaf certificate context.
2. Import the leaf certificate data into the switch with the command **import(self-signed leaf certificate)**.
3. Exit the leaf certificate context with the command **exit**.
4. Associate the leaf certificate with a switch feature (syslog client, HTTPS server, or HSC) with the command **crypto pki application**.

Example

This example:

- Creates the leaf certificate context.
- Imports the self-signed leaf certificate.
- Associates the leaf certificate with the syslog client (application) on the switch.

```
switch(config)# switch(config)# crypto pki certificate SS_LC2
switch(config)# switch(config-cert-SS_LC)# import terminal self-signed
Paste the certificate in PEM format below, then hit enter and ctrl-D:
switch(config-cert-import)# -----BEGIN CERTIFICATE-----
switch(config-cert-import)# MIIFRDCCAyYgAwIBAgIQP8nnS2Vp15u07xXMdktDJzANBgkqhkiG9
switch(config-cert-import)# MQswCQYDVQGEwJVUEOMAwwGA1UECgwFXJlYmxDAOgNBAMMB1Jvb3gw
switch(config-cert-import)# HhcNMTkNDEwMjIwNTI1WhcjIwMTA0MjIwNE1WjBzQswQYDVQGEwJV
...
switch(config-cert-import)# 1fIYZYGQyla0AwFuPTTxBXHYwRxTPbUYU5tumJrfwRPmE4OVY8S9D
switch(config-cert-import)# 1NGNm3NG03GqPScs/TF9bVyFA5BOrS5lmm7kNfRYlK8D/kMTfRreS
switch(config-cert-import)# YQ1u1NqShps=
switch(config-cert-import)# -----END CERTIFICATE-----
switch(config-cert-import)# -----BEGIN ENCRYPTED PRIVATE KEY-----
switch(config-cert-import)# MIIFDjBABGkqhkiG9wBBQ0wMzAbBgkqhkiw0QwwDQImNpJMN7sVGwC
switch(config-cert-import)# MBQGCCqGSIB3DQMHAit+2qadNAASCMg5LYJ4AFm3EfffH5p5lGgr8
switch(config-cert-import)# IJ6L/UhEtH523nUkdV6gvoAWgoYaeD83PeswToAGv5VS8OMFTPttr
...
switch(config-cert-import)# OgSecqZsG6arbx0ESaYBir1c/6rPs1pcjbdXw283DiD1MWOpesO2a
```

```

switch(config-cert-import)# iKnXnUMpVPfLc74ty2S41DtH0X9Sgf6aa1LjiStg+N7cND9XfGtj/
switch(config-cert-import)# cb4=
switch(config-cert-import)# -----END ENCRYPTED PRIVATE KEY-----
switch(config-cert-import)#
Enter import password:
Paste the certificate in PEM format below, then hit enter and ctrl-D:
switch(config-cert-import)# -----BEGIN CERTIFICATE-----
switch(config-cert-import)# MIIFRDCCAYygAwIBAgIQP8nnS2Vp15u07xXMdktDJzANBgkqhkiG9
switch(config-cert-import)# MQswCQYDVQGEwJVUEOMAwGA1UECgwFXJ1YmxDAOGNBAMMB1Jvb3gw
switch(config-cert-import)# HhcNMTkNDEwMjIwNT1WhcjIwMTA0MjIwNE1WjBzQswQYDVQGEwJV
...
switch(config-cert-import)# 1fIYZYGQyla0AwFuPTTxBXHYWrxTPbUYU5tumJrfwRPM40VY8S9D
switch(config-cert-import)# 1NGNm3NG03GqPScs/TF9bVyFA5BOrS5lmm7knfRYlK8D/kMTfRreS
switch(config-cert-import)# YQ1ulNqShps=
switch(config-cert-import)# -----END CERTIFICATE-----
switch(config-cert-import)# -----BEGIN ENCRYPTED PRIVATE KEY-----
switch(config-cert-import)# MIIFDjBABGkqhkiG9wBBQ0wMzAbBgkqkiw0QwwDQImNpJMN7sVGwC
switch(config-cert-import)# MBQGCCqGS1b3DQMHAit+2qadNAASCMg5LYJ4AFm3EfffH5p51Ggr8
switch(config-cert-import)# IJ6L/UhEtH523nUkdV6gvoAWgoYaeD83PeswToAGv5VS8OMFTPttr
...
switch(config-cert-import)# OgSecqZsG6arbx0ESaYBir1c/6rPs1pcjbdXw283DiD1MWOpes2a
switch(config-cert-import)# iKnXnUMpVPfLc74ty2S41DtH0X9Sgf6aa1LjiStg+N7cND9XfGtj/
switch(config-cert-import)# cb4=
switch(config-cert-import)# -----END ENCRYPTED PRIVATE KEY-----
switch(config-cert-import)#
Enter import password: *****
Leaf certificate is validated as self-signed certificate and imported
successfully.
switch(config-cert-SS_IC2)# exit
switch(config)# crypto pki application syslog-client certificate SS_IC2

```

Installing a certificate of a root CA

Prerequisites

- A certificate of a root CA (that is used as the signer).
- Revocation checking URLs for the CA (optional).

Procedure

1. Create a TA profile with the command **crypto pki ta-profile** which then switches to the created TA profile context.



Step 2 is optional and suggested only for advanced users.

2. Optionally enable certificate revocation checking with the command **revocation-check ocsp**. Most certificates contain revocation checking URLs for OCSP. If you want to override these URLs, configure custom revocation checking URLs with the command **ocsp url**.
3. Import the certificate of the root CA with the command **ta-certificate**.

Example

This example installs the certificate **root-cert** and defines custom revocation checking URLs:

```

switch(config)# crypto pki ta-profile root-cert
switch(config-ta-root-cert)# revocation-check ocsp
switch(config-ta-root-cert)# ocsp url primary http://ocsp-server.site.com
switch(config-ta-root-cert)# ocsp url secondary http://ocsp-server2.site.com
switch(config-ta-root-cert)# ta-certificate import terminal
Paste the certificate in PEM format below, then hit enter and ctrl-D:
switch(config-ta-cert)# -----BEGIN CERTIFICATE-----
switch(config-ta-cert)# MIIDuTCCAqECCQCuoxeJ2ZNYcjANBgqhkiG9w0BAQsFADCBQzELMAEBh
switch(config-ta-cert)# VVMxEzARBgNVBAGMCkNhbgG1mb3JuaWExEDAOBgNVBACMB1JvY2tsDAKBg
switch(config-ta-cert)# BAoMA0hQTjEVMBMGAlUECwwMSFBOUm9zZXZpbGx1MSowKAYDVQOCG5zd
...
switch(config-ta-cert)# x3WFF3dFZ8o9sd5LVAHneH/ztb9MP34z+le1V346r12L2kpxmTOVJVyTo
switch(config-ta-cert)# BIzD/ST/HaWI+OS+S80rm93PSscEbb9GWk7vshh5EnW/moehBKcE40lzy
switch(config-ta-cert)# 3LvMLZcssSe5J2Ca2XIhfDme8UaNZ7syGYMsAW0nG7yYHWkEOQu9s
switch(config-ta-cert)# -----END CERTIFICATE-----
switch(config-ta-cert)#
The certificate you are importing has the following attributes:
Issuer: C=US, ST=CA, L=Rocklin, O=Company, OU=Site,
       CN=site.com/emailAddress=test.ca@site.com
Subject: C=US, ST=CA, L=Rocklin, O=Company, OU=Site,
        CN=8400/emailAddress=test.ca@site.com
Serial Number: 12121221634631568498 (0xae51217d5945772)

TA certificate import is allowed only once for a TA profile
Do you want to accept this certificate (y/n)? y
TA certificate accepted.
switch(config-ta-root-cert)#

```

Installing a downloadable user role certificate

This procedure describes how to create and install a downloadable user role (DUR) certificate.

Prerequisites

- A certificate of a root CA (that is used as the signer).

Procedure

1. Create a TA profile with the command **crypto pki ta-profile** which then switches to the created TA profile context.
2. Import the certificate of the root CA with the command **ta-certificate**.

Example

```

switch(config)# crypto pki ta-profile DUR-cert
switch(config-ta-DUR-cert)# ta-profile
switch(config-ta-cert)# -----BEGIN CERTIFICATE-----
switch(config-ta-cert)#
MIIGFjCCA/6gAwIBAgIJAMt1KN7Gy9GCMA0GCSqGSIb3DQEBCwUAMIGWMQswCQYD
VQQGEWJTTjESMBAGA1UECAwJS2FybmcF0YwdhMRIwEAYDVQQHDA1CYW5nYWxvcuUx
DDAKBgNVBAoMA0hQRTEMAoGA1UECwwDSFBOUm9zZXZpbGx1MSowKAYDVQOCG5zd
LjE5NDEqMCgGCSqGSIb3DQEJARYbcmFkaGFrcmlzaG5hbi5nb3BhbEBocGUuY29t
MCAXDTIwMDExNTA5MzgWMLoYDzQxODMxMDIyMDkzODAzWjCB1jELMAkGA1UEBhMC
SU4xExJAQBgNVBAGMCUthcm5hdGFhYTESMBAGA1UEBwwJQmFuZ2Fsb3JlMQwwCgYD
VQQKDANIUEUxDDAKBgNVBASMA0hQTjEXMBUGA1UEAwwOMTUuMjE5Y2tsOTQx
KjAoBgqhkiG9w0BCQEWG3JhZGhha3Jpc2huYW4uZ29wYWxhbnB1b3R1b3R1b3R1
DQYJKoZIhvcNAQEBBQADggIPADCCAgCGgIBALs99p/xrJHXgYTAiV4WjwgHgJJt

```

```

aRwisIoA8iKBZN3zmc1HKJNeGHYXJl0QNC7xfAFSptwgmQ+bhawLuGLNWWm1zQdP
68GmJS10jnlxkQ1VIwjrDCfk5t7RAMY/bZKPRjPnfzbZ03Nv3tqp9h/bWTF1y17S
SzYdDF9SiEVfx/4EWicXIDx2ie44kE+9CGB817Q/kovALiIjREJxtv2WJLvE4g/X
2pBu2WMMKhxU95JX2WdIrbHLM1sETUMvb6itg6jfhnpDIzWF5Xbb0c22HsJ6YnvY
FylHqkN5QjTBaWo9UpvVeeNEA12tm8D7UsRGJO5u0Y01j4Xp1bQgDf/S6b6LHYQZ
4TLZIEjBn9tH1hXoPd0wXAdpXnYqBZ0U04ZHaRxvG5wEsvZ3LOyJXNU1J2Z5osC+
HkJRr5tMKV9Dc0gON81LPXj4+JmubyWi7ABM8+ktNyDqTeGqMaUZaB+NvGwQyMUR
Ntgvam9ntI+/njW0ViKYEWQJ4OB9D+0sWXJHFrqfZpbVYTQjZktDDnVhSL9Z5Fce
5+AIBBLCCFcNc933fv29jC0oVWjZ2RHt/8B0DdPY/hDPb0epy+WEosxIQzQ++D+M
s9aBPYVgwCKE2mkT6lnqBhAaNiSK7wiUU92rHvYhRr2W6Zib+wU9BFWZIZFKbXd
D8I7P0Zm0hf/j0wVAgMBAAGjYzBhMB0GA1UdDgQWBBrV0riw2MVuuc/Y9VtGgstN
PTrm+DAfBgNVHSMEGDAWgBRV0riw2MVuuc/Y9VtGgstNPTrm+DAPBgNVHRMBAf8E
BTADAQH/MA4GA1UdDwEB/wQEAWIBhjANBgkqhkiG9w0BAQsFAAOCAgEAU7fff1Ci
lyA7yq37jlxzdnGXiuR+00xiuZ62xBcu6F/p2SwsieesQCJ2odiOcaqeYXIAIiI2
EAHpesan7OQap2KQ/Xw/00H3/q+SQo47LiGiZjWLeGjaJ5NXBBra6MhZXjli1EEG
70Qn0dehM7am5bsLRhYvRR+TesWEceNoFQN1lyiqpGWCPII8Q4eL4MsSTEM16Qki
yaVDzQko2FW9P3sDV7RGwKrxJIYT8HqPrU6WZUaT7+C0G5EwqP8peg7HOaInKM6Z
lsmFXaSlTvhGbgjJm8uReWr1wNr+V3nugzOCUFspy32OexP90fJ873K1glIbEfxw
bmWMq6za1KQ9rzyNVI2ucp9F7oyXz0vy/6/FagulKkv2BoUxExU9AVwCkDsdVnun
IuQMly2CVGpj+5bhcdRS3ZUmKWAMw0uBwky0BiE1A48LN7R/OYbOmr4QkmveAJAD
MOZIGK4KbutsrIGsT0vs+1U9wrfdiG2TiZlHsWIT47EYg/C9ZkeDtQUuilob6uaO
Wt/2il/ePUbsSZn9YX9jLBNEsNWbW9B5wyqhAh1AwOpC5KVkHPOsXPOLJZPNO2RI
UKVv7wqGQMMFwKVnn4MoNEdQCYwRsTt6l0+yY1C1dA6xsG0LUXa2SpuX/gpovaNW
6VA2QAAIJIcSFB4KylgncPvV2gUr+Gbd01M=
switch(config-ta-cert)# -----END CERTIFICATE-----
switch(config-ta-cert)#

switch(config-ta-cert)# -----BEGIN CERTIFICATE-----
switch(config-ta-cert)#
MIIGFjCCA/6gAwIBAgIJAMt1KN7Gy9GCMA0GCSqGSIb3DQEBCwUAMIGWMQswCQYD
VQQGEWJTTjESMBAGA1UECAwJS2FybmF0YWdhMRIwEAYDVQQHDAlCYW5nYXxvcUx
DDAKBgNVBAoMA0hQRTEMMGA1UECwwDSFBOMRcwFQYDVQQDDA4xNS4yMTIuMjIx
LjE5NDEBQMCgGCSqGSIb3DQEJARYBcmFkaGFrcmlzaG5hbi5nb3BhbEBocGUuY29t
MCAXDTIwMDExNTA5MzgWMM1oYDZQxODMxMDIyMDkzODAzWjCB1jELMAkGA1UEBhMC
SU4xejAQBgNVBAgMCUthcm5hdGFnYTE5TE5BAG1UEBwwJQmFuZ2Fsb3JlMQwwCgYD
VQKQDANIUEUxDDAKBgNVBASMA0hQTjEXMBUGA1UEAwwOMTUuMjIxLjE5MS4xOTQx
KjAoBgkqhkiG9w0BCQEWG3JhZGhha3Jpc2huYW4uZ29wYXxwAaHBlLmNvbTCCAIw
DQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBALs99p/xrJHXgYTAiV4WjwgHgJt
aRwisIoA8iKBZN3zmc1HKJNeGHYXJl0QNC7xfAFSptwgmQ+bhawLuGLNWWm1zQdP
68GmJS10jnlxkQ1VIwjrDCfk5t7RAMY/bZKPRjPnfzbZ03Nv3tqp9h/bWTF1y17S
SzYdDF9SiEVfx/4EWicXIDx2ie44kE+9CGB817Q/kovALiIjREJxtv2WJLvE4g/X
2pBu2WMMKhxU95JX2WdIrbHLM1sETUMvb6itg6jfhnpDIzWF5Xbb0c22HsJ6YnvY
FylHqkN5QjTBaWo9UpvVeeNEA12tm8D7UsRGJO5u0Y01j4Xp1bQgDf/S6b6LHYQZ
4TLZIEjBn9tH1hXoPd0wXAdpXnYqBZ0U04ZHaRxvG5wEsvZ3LOyJXNU1J2Z5osC+
HkJRr5tMKV9Dc0gON81LPXj4+JmubyWi7ABM8+ktNyDqTeGqMaUZaB+NvGwQyMUR
Ntgvam9ntI+/njW0ViKYEWQJ4OB9D+0sWXJHFrqfZpbVYTQjZktDDnVhSL9Z5Fce
5+AIBBLCCFcNc933fv29jC0oVWjZ2RHt/8B0DdPY/hDPb0epy+WEosxIQzQ++D+M
s9aBPYVgwCKE2mkT6lnqBhAaNiSK7wiUU92rHvYhRr2W6Zib+wU9BFWZIZFKbXd
D8I7P0Zm0hf/j0wVAgMBAAGjYzBhMB0GA1UdDgQWBBrV0riw2MVuuc/Y9VtGgstN
PTrm+DAfBgNVHSMEGDAWgBRV0riw2MVuuc/Y9VtGgstNPTrm+DAPBgNVHRMBAf8E
BTADAQH/MA4GA1UdDwEB/wQEAWIBhjANBgkqhkiG9w0BAQsFAAOCAgEAU7fff1Ci
lyA7yq37jlxzdnGXiuR+00xiuZ62xBcu6F/p2SwsieesQCJ2odiOcaqeYXIAIiI2
EAHpesan7OQap2KQ/Xw/00H3/q+SQo47LiGiZjWLeGjaJ5NXBBra6MhZXjli1EEG
70Qn0dehM7am5bsLRhYvRR+TesWEceNoFQN1lyiqpGWCPII8Q4eL4MsSTEM16Qki
yaVDzQko2FW9P3sDV7RGwKrxJIYT8HqPrU6WZUaT7+C0G5EwqP8peg7HOaInKM6Z
lsmFXaSlTvhGbgjJm8uReWr1wNr+V3nugzOCUFspy32OexP90fJ873K1glIbEfxw
bmWMq6za1KQ9rzyNVI2ucp9F7oyXz0vy/6/FagulKkv2BoUxExU9AVwCkDsdVnun
IuQMly2CVGpj+5bhcdRS3ZUmKWAMw0uBwky0BiE1A48LN7R/OYbOmr4QkmveAJAD
MOZIGK4KbutsrIGsT0vs+1U9wrfdiG2TiZlHsWIT47EYg/C9ZkeDtQUuilob6uaO
Wt/2il/ePUbsSZn9YX9jLBNEsNWbW9B5wyqhAh1AwOpC5KVkHPOsXPOLJZPNO2RI
UKVv7wqGQMMFwKVnn4MoNEdQCYwRsTt6l0+yY1C1dA6xsG0LUXa2SpuX/gpovaNW
6VA2QAAIJIcSFB4KylgncPvV2gUr+Gbd01M=

```

```
switch(config-ta-cert)# -----END CERTIFICATE-----
switch(config-ta-cert)#
```

Installing a CA-signed leaf certificate (initiated in the switch)

This procedure describes how to create and install an X.509 leaf certificate that is initiated inside the switch but signed outside the switch by a CA. And then associate the certificate with one of the following switch features: syslog client, HTTPS server, or HSC (hardware switch controller).

Prerequisites

Root CA certificate **root-cert** must be installed as described in [Installing a certificate of a root CA](#).

Procedure

1. Create a leaf certificate context with the command **crypto pki certificate** which then switches to the created leaf certificate configuration context.
2. Define leaf certificate properties with the command **subject**.
3. Set the encryption key type for the leaf certificate with the command **key-type**.
4. Generate the certificate signing request (CSR) with the command **enroll terminal**.
5. Use the CSR to obtain a leaf certificate from the root CA, using the root CA directly as the signer CA.
6. Import the leaf certificate into the switch with the command **import(CA-signed leaf certificate)**.
7. Exit the leaf certificate context with the command **exit**.
8. Associate the leaf certificate with a switch feature (syslog client, HTTPS server, or HSC) with the command **crypto pki application**.

Example

This example:

- Creates the leaf certificate context.
- Defines the leaf certificate characteristics.
- Generates the leaf certificate signing request in the switch for getting signed outside the switch by a CA.
- Imports the CA-signed leaf certificate into the switch.
- Associates the leaf certificate with the syslog client (application) on the switch.

```
switch(config)# crypto pki certificate lcert
switch(config-cert-lcert)# subject common-name Leaf country US state CA
locality Rocklin org Company org-unit Site
switch(config-cert-lcert)# key-type rsa key-size 3072
switch(config-cert-lcert)# enroll terminal
You are enrolling a certificate with the following attributes:
Subject: C=US, ST=CA, L=Rocklin, O=Company, OU=Site
        CN=Leaf
Key Type: RSA (2048)

Continue (y/n)? y
```

```

-----BEGIN CERTIFICATE REQUEST-----
MIIBozCCAQAwYzEVMBMGAlUEAxMMcG9kMDEtODQwMC0xMQ4wDAYDV
nViYTEMMAoGA1UEChMDSFBFMRiWEAYDVQQHEw1Sb3Nldm1sbGUxCzAJBg
NBMQswCQYDVQQGEwJVUzCBnzANBqkqhkiG9w0BAQEFAAOBjQAwgYkCgYE
...
GBAJ4L3lFFfWBEL+KAKpOGjZcVmw1BMqSKFtOFNF9nzmUmONmU3SKy6dz
7Au22mf3lWDxzrtCC/dj5RtWJeJekxp2LCIK/3eRXUwbYveQDKcxH7j9Z
ace+2tA68F2vlgRCQ/hcQH0YmNuaq4Ne3w0dhm7H1Urx
-----END CERTIFICATE REQUEST-----

switch(config-cert-lcert) #

-----BEGIN CERTIFICATE REQUEST-----
MIIBozCCAQAwYzEVMBMGAlUEAxMMcG9kMDEtODQwMC0xMQ4wDAYDV
nViYTEMMAoGA1UEChMDSFBFMRiWEAYDVQQHEw1Sb3Nldm1sbGUxCzAJBg
NBMQswCQYDVQQGEwJVUzCBnzANBqkqhkiG9w0BAQEFAAOBjQAwgYkCgYE
...
GBAJ4L3lFFfWBEL+KAKpOGjZcVmw1BMqSKFtOFNF9nzmUmONmU3SKy6dz
7Au22mf3lWDxzrtCC/dj5RtWJeJekxp2LCIK/3eRXUwbYveQDKcxH7j9Z
ace+2tA68F2vlgRCQ/hcQH0YmNuaq4Ne3w0dhm7H1Urx
-----END CERTIFICATE REQUEST-----

switch(config-cert-lcert) # import terminal ta-profile root-cert
Paste the certificate in PEM format below, then hit enter and ctrl-D:
switch(config-cert-import) # -----BEGIN CERTIFICATE-----
switch(config-cert-import) # MIIFRDCCAYygwIBAgIQPnnS2Vp5u07XMdktDJzANBqkqhkiG9w0Bv
switch(config-cert-import) # MQswCQYDVQGEwJVEOMAwG1UECgwFJ1YmxDAOgNBMMB1Jvb3QgQ0Ew
switch(config-cert-import) # HhcNMTkNDEwMjIwNTWcjlwMTA0MjwNE1WBzQswQYDVQQGEwJVUzEL
...
switch(config-cert-import) # 1fIYZYGQyla0AwFuTTxBXYwRxPbUYU5tumrfwRPmE40VY8S9DQgcr
switch(config-cert-import) # 1NGNm3NG03GqPcs/T9bVyF5BOrS5lmm7kNfRYl8D/kMTfRreSdxis
switch(config-cert-import) # YQ1ulNqShps=
switch(config-cert-import) # -----END CERTIFICATE-----
switch(config-cert-import) #
Leaf certificate is validated with root-cert and imported successfully.
switch(config-cert-lcert) # exit
switch(config) # crypto pki application syslog-client certificate lcert

```

Installing a CA-signed leaf certificate (created outside the switch)

This procedure describes how to install an X.509 leaf certificate that was created and signed (by a CA) outside the switch. And then associate the certificate with one of the following switch features: syslog client, HTTPS server, or HSC (hardware switch controller).

Prerequisites

- Root CA certificate `root-cert` installed as described in [Installing a certificate of a root CA](#).
- A CA-signed leaf certificate (including private-key data) created outside the switch.

Procedure

1. Create the leaf certificate context with the command **crypto pki certificate** which then switches to the created leaf certificate context.
2. Import the leaf certificate into the switch with the command **import (CA-signed leaf certificate)**.
3. Exit the leaf certificate context with the command **exit**.

4. Associate the leaf certificate with a switch feature (syslog client, HTTPS server, or HSC) with the command **crypto pki application**.

Example

This example:

- Creates the leaf certificate context.
- imports the CA-signed leaf certificate.
- Associates the leaf certificate with the syslog client (application) on the switch.

```
switch(config)# switch(config)# crypto pki certificate CA_LC
switch(config)# switch(config-cert-CA_LC)# import terminal ta-profile root-cert
Paste the certificate in PEM format below, then hit enter and ctrl-D:
switch(config-cert-import)# -----BEGIN CERTIFICATE-----
switch(config-cert-import)# MIIFRDCCAyYgAwIBAgIQP8nn2Vp15u07XMktDJANBgkqhkiG9w0Bv
switch(config-cert-import)# MQswCQYDVQGEwJVUEOMAaw1UECgwFX1YmxDOgNBAMMB1Jvb3QgQ0Ew
switch(config-cert-import)# HhcNMTkNDEwMjIwNT1WhjIMTA0MjIwNE1jBzQswYDVQQGEwJVUzEL
...
switch(config-cert-import)# 1fIYZYGQyla0AwFuPTTxBXHYRxTPbUYUtmJrwrPmE4OVY8S9DQgcr
switch(config-cert-import)# lNGNm3NG03GqPScs/TF9bVyFABOrlmm7kNfRlK8D/kMTfRreSdxis
switch(config-cert-import)# YQ1ulNqShps=
switch(config-cert-import)# -----END CERTIFICATE-----
switch(config-cert-import)# -----BEGIN ENCRYPTED PRIVATE KEY-----
switch(config-cert-import)# MIIFDjBABGkqhkiG9wBBQ0wMzAbBgkiwQwwQImNpJMN7sVGwCaggA
switch(config-cert-import)# MBQGCCqGS1b3DQMHAit+2qadNAASCMgLYJ4AFefhH5p51Ggr86VqS
switch(config-cert-import)# IJ6L/UhEtH523nUkdV6gvoAWgoYaeD8eswAGv5VS8OMFTPttrn5/K
...
switch(config-cert-import)# OgSecqZsG6arbx0ESaYBir1c6rPslpcbDx283DD1MW0peoS2aEmOX
switch(config-cert-import)# iKnXnUMpVPfLc74ty2S41tH0X9gfaalLiStg+N7cND9XfGtjaV2+/
switch(config-cert-import)# cb4=
switch(config-cert-import)# -----END ENCRYPTED PRIVATE KEY-----
switch(config-cert-import)#
Enter import password:
Paste the certificate in PEM format below, then hit enter and ctrl-D:
switch(config-cert-import)# -----BEGIN CERTIFICATE-----
switch(config-cert-import)# MIIFRDCCAyYgAwIBAgIQP8nn2Vp15u07XMktDJANBgkqhkiG9w0Bv
switch(config-cert-import)# MQswCQYDVQGEwJVUEOMAaw1UECgwFX1YmxDOgNBAMMB1Jvb3QgQ0Ew
switch(config-cert-import)# HhcNMTkNDEwMjIwNT1WhjIMTA0MjIwNE1jBzQswYDVQQGEwJVUzEL
...
switch(config-cert-import)# 1fIYZYGQyla0AwFuPTTxBXHYRxTPbUYUtmJrwrPmE4OVY8S9DQgcr
switch(config-cert-import)# lNGNm3NG03GqPScs/TF9bVyFABOrlmm7kNfRlK8D/kMTfRreSdxis
switch(config-cert-import)# YQ1ulNqShps=
switch(config-cert-import)# -----END CERTIFICATE-----
switch(config-cert-import)# -----BEGIN ENCRYPTED PRIVATE KEY-----
switch(config-cert-import)# MIIFDjBABGkqhkiG9wBBQ0wMzAbBgkiwQwwQImNpJMN7sVGwCaggA
switch(config-cert-import)# MBQGCCqGS1b3DQMHAit+2qadNAASCMgLYJ4AFefhH5p51Ggr86VqS
switch(config-cert-import)# IJ6L/UhEtH523nUkdV6gvoAWgoYaeD8eswAGv5VS8OMFTPttrn5/K
...
switch(config-cert-import)# OgSecqZsG6arbx0ESaYBir1c6rPslpcbDx283DD1MW0peoS2aEmOX
switch(config-cert-import)# iKnXnUMpVPfLc74ty2S41tH0X9gfaalLiStg+N7cND9XfGtjaV2+/
switch(config-cert-import)# cb4=
switch(config-cert-import)# -----END ENCRYPTED PRIVATE KEY-----
switch(config-cert-import)#
Enter import password: *****
Leaf certificate is validated with root-cert and imported successfully.
switch(config-cert-CA_LC)# exit
switch(config)# crypto pki application syslog-client certificate CA_LC
```

PKI commands

crypto pki application

```
crypto pki application <APP-NAME> certificate <CERT-NAME>  
no crypto pki application <APP-NAME> certificate <CERT-NAME>
```

Description

Associates a leaf certificate with a feature (application) on the switch. By default, all features are associated with the default, self-signed certificate **local-cert**. This certificate is created by the switch the first time it starts.

The **no** form of this command associates the specified feature with the default certificate.

Parameter	Description
<APP-NAME>	Specifies the name of a feature on the switch: ▪ dot1x-supplicant: 802.1X supplicant ▪ est-client: EST client ▪ hsc: Hardware switch controller ▪ https-server: HTTPS server ▪ syslog-client: Syslog client syslog-client communicates with syslog server over TLS. You can associate a certificate with the syslog-client application by enrolling the certificate manually or through EST.
<CERT-NAME>	Specifies the name of an installed leaf certificate.

Examples

Associating the EST client with leaf certificate **leaf-cert1**:

```
switch(config)# crypto pki application est-client certificate leaf-cert1
```

Associating the syslog client with leaf certificate **leaf-cert**:

```
switch(config)# crypto pki application syslog-client certificate leaf-cert
```

Setting the syslog client to use the default certificate:

```
switch(config)# no crypto pki application syslog-client certificate
```

Associating the HTTPS server with leaf certificate **leaf-cert2**:

```
switch(config)# crypto pki application https-server certificate leaf-cert2
```

Associating the 802.1X supplicant with leaf certificate **cert1**:

```
switch(config)# crypto pki application dot1x-supplicant certificate cert1
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

crypto pki certificate

```
crypto pki certificate <CERT-NAME>
no crypto pki certificate <CERT-NAME>
```

Description

Creates a leaf certificate and changes to its context **config-cert-<CERT-NAME>**. If the specified leaf certificate exists, this command changes to its context.

The first time the switch starts it creates a self-signed, default leaf certificate called **local-cert**. This certificate is used by any switch application that does not have an associated leaf certificate.

The **no** form of this command deletes the specified leaf certificate. The default leaf certificate **local-cert** cannot be deleted.

Parameter	Description
<CERT-NAME>	Specifies the name of a leaf certificate. Range: 1 to 32 alphanumeric characters (excluding ").

Examples

Creating leaf certificate **leaf-cert**:

```
switch(config)# crypto pki certificate leaf-cert
switch(config-cert-leaf-cert)#
```

Deleting leaf certificate **leaf-cert**:

```
switch(config)# no crypto pki certificate leaf-cert
The leaf certificate has associated applications. Deleting the certificate
will make the applications use the default certificate local-cert.
Continue (y/n)? y
switch(config)#
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

crypto pki ta-profile

```
crypto pki ta-profile <TA-NAME>
no crypto pki ta-profile <TA-NAME>
```

Description

Creates a trust anchor (TA) profile and changes to the **config-ta-<TA-NAME>** context for the profile. Each TA profile stores the certificate for a trusted CA. Up to 64 profiles can be defined.

If the specified TA profile exists, this command changes to the **config-ta-<TA-NAME>** context for the profile.

The **no** form of this command removes the specified TA profile.



When creating a new profile, If you exit the **config-ta-<TA-NAME>** context without importing the TA certificate, the profile is discarded.

Parameter	Description
<TA-NAME>	Specifies the TA profile name. Range: 1 to 48 alphanumeric characters excluding ". NOTE: The TA profile name cannot end with est-ta<nn> where <nn> is 00 to 99 . For example, company-trust-anchor-est-ta01 is not allowed. This TA profile name suffix is reserved for TA profiles that are created for CA certificates from EST servers.

Examples

Creating the TA profile **root-cert**:

```
switch(config)# crypto pki ta-profile root-cert
switch(config-ta-root-cert)#
```

Removing TA profile **root-cert**:

```
switch(config)# no crypto pki ta-profile root-cert
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

enroll self-signed

enroll self-signed

Description

Generates a key pair and generates a self-signed certificate with it.

The subject fields and key type of the current leaf certificate must be defined before running this command. If not, you are prompted to fill in the subject fields, and the key type is set to **RSA 2048**.

Example

Enrolling the leaf certificate **leaf-cert**:

```
switch(config-cert-leaf-cert)# enroll self-signed
You are enrolling a certificate with the following attributes:
Subject: C=US, ST=CA, L=Rocklin, OU=Site, O=Comp,
        CN=Leaf01
Key Type: RSA (2048)

Continue (y/n)? y
Self-signed certificate is created and enrolled successfully.

switch(config-cert-leaf-cert)#
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-cert- <i><CERT-NAME></i>	Administrators or local user group members with execution rights for this command.

enroll terminal

enroll terminal

Description

Generates a key pair and certificate signing request (CSR) for the current leaf certificate. Use the CSR to obtain a signed certificate from a certificate authority (CA), and then import the certificate onto the switch with the command **import terminal**.

The key type, and the certificate common name in the subject fields of the current leaf certificate must be completed before running this command.

Example

Enrolling the leaf certificate **leaf-cert**:

```
switch(config-cert-leaf-cert)# enroll terminal
You are enrolling a certificate with the following attributes:
Subject: C=US, ST=CA, L=Rocklin, OU=Site, O=Comp,
        CN=Leaf01
Key Type: RSA (2048)

Continue (y/n)? y

-----BEGIN CERTIFICATE REQUEST-----
MIIBOzCCAQAQAwYzEVMBMGAlUEAxMMcG9kMDEtODQwMC0xMQ4wDAYDVQQLEwV
nViYTEMMAoGA1UEChMDSFBMRlEwEAYDVQQHEw1Sb3Nldm1sbGUxCzAJBgNVBAGT
NBMQswCQYDVQQGEwJVUzCBnzANBkgqhkiG9w0BAQEFAAOBjQAwYkCgYEAAtKcLS
...
GBAJ4L3lFFfWBEL+KAKpOGjZcVmw1BMqSKFtOFNF9nzmUmONmU3SKy6dzQ+6ynR
7Au22mf3lWDxzrtCC/dj5RtWJeJekxp2LCIK/3eRXUwbYveQDKcxH7j9ZB+BAp2
ace+2tA68F2vlgRCQ/hcQH0YmNuaq4Ne3w0dhm7H1Urx
-----END CERTIFICATE REQUEST-----
switch(config-cert-leaf-cert)#
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-cert-<CERT-NAME>	Administrators or local user group members with execution rights for this command.

import (CA-signed leaf certificate)

```
import terminal ta-profile <TA-NAME> [password <PW>]
import <REMOTE-URL> ta-profile <TA-NAME> [password <PW>] [vrf <VRF-NAME>]
import <STORAGE-URL> ta-profile <TA-NAME> [password <PW>]
```

Description

Imports a CA-signed leaf certificate and then validates the certificate against the specified TA profile. If the imported data includes a private key, the private key must match the leaf certificate being imported. If the imported data does not include a private key, the certificate must match a CSR that was previously generated with the command **enroll terminal** and must be signed by the CA whose root certificate is installed in the specified TA profile. The TA profile must exist and have a TA certificate configured.

Parameter	Description
terminal	Import the certificate by pasting PEM-format data at the console. Upon execution, the config-cert-import context is entered for certificate pasting. To complete certificate data entry press Control-D in your terminal program. Alternatively, the pasted

Parameter	Description
	certificate data can include at its end the delimiter END_OF_CERTIFICATE (after the -----END CERTIFICATE----- line), making entry of Control-D unnecessary.
ta-profile <TA-NAME>	Specifies the TA profile name. Range: 1 to 48 alphanumeric characters excluding ".".
password <PW>	Specifies the plaintext password used to decrypt the private key in the imported certificate data. When this parameter is omitted, the password is prompted for as required. Range: 1 to 32 alphanumeric characters.
<REMOTE-URL>	Specifies a certificate data file on a remote TFTP or SFTP server. The URL syntax is: {tftp:// sftp://<USER>@} {<IP> <HOST>} [:<PORT>] [;blocksize=<SIZE>]/<FILE>
vrf <VRF-NAME>	Specifies the name of the VRF to use for the remote URL file transfer. The default is mgmt .
<STORAGE-URL>	Available on switch families that provide USB device file import capability, specifies a certificate data file on a USB storage device inserted in the switch USB port. The URL syntax is usb:/<FILE> .

Usage

- The imported data must include all the intermediate CA certificates in the certificate chain leading to the certificate imported into the specified TA profile.
- This command cannot be used with the default certificate **local-cert**.
- The PEM data format is supported for all import sources. The PKCS#12 data format is supported for **<REMOTE-URL>** and **<STORAGE-URL>**.
- The PEM data must be delimited with these lines for the certificate data:

```
-----BEGIN CERTIFICATE-----
-----END CERTIFICATE-----
```

And the PEM data must be delimited with either of these line pairs for the private key data:

```
-----BEGIN PRIVATE KEY-----
-----END PRIVATE KEY-----
```

```
-----BEGIN ENCRYPTED PRIVATE KEY-----
-----END ENCRYPTED PRIVATE KEY-----
```

Examples

Importing a leaf certificate from the console:

```
switch(config)# crypto pki certificate leaf-cert
switch(config-cert-leaf-cert1)# import terminal ta-profile root-cert
Paste the certificate in PEM format below, then hit enter and ctrl-D:
switch(config-cert-import)# -----BEGIN CERTIFICATE-----
switch(config-cert-import)# MIIFRDCCAyYgAwIBAgQP8nS2Vp15u0xXMdkDJzANBgkqhkiG9w0Bv
switch(config-cert-import)# MQswCQYDVQGEwJVUEOMAwwGA1UCgwFXJ1YmDAgNBAMM1Jvb3QgQ0Ew
switch(config-cert-import)# HhcNMTkNDEwMjIwNTIWhcJlIwMT0MjwNE1WjzQswQDVQGEwJVUzEL
...
switch(config-cert-import)# 1fIYZYGQyla0AwFuPTTxBXHYwRxTPbUYU5umJfRPmE4VY8S9DQgcr
switch(config-cert-import)# 1NGNm3NG03GqPScs/TF9bVyFA5BOS5lmmkfRYK8D/kMTfRreSdxis
```

```

switch(config-cert-import)# YQ1ulNqShps=
switch(config-cert-import)# -----END CERTIFICATE-----
switch(config-cert-import)# -----BEGIN ENCRYPTED PRIVATE KEY-----
switch(config-cert-import)# MIIFDjBABgkqhkiG9wBBQ0wMzAbBgqkw0QwwDQIPJMN7sVGwCAgga
switch(config-cert-import)# MBQGCCqGSIB3DQMHAit+2qadNAASCgLYJ4Am3EfH5p51Ggr86VqS
switch(config-cert-import)# IJ6L/UhEtH523nUkdV6gvAgoYaD83PswToAGv5VS8OMFTPttrn5/K
...
switch(config-cert-import)# OgSecqZsG6arbx0ESaYBir1c/6rPspcjbx283iD1MWOpes2aEmOX
switch(config-cert-import)# iKnXnUMpVPfLc74ty2S41DtH0X9gf6aa1jStg+7cND9XfGtjaV2+/
switch(config-cert-import)# cb4=
switch(config-cert-import)# -----END ENCRYPTED PRIVATE KEY-----
switch(config-cert-import)#
Enter import password: *****
Leaf certificate is validated with root-cert and imported successfully.
switch(config-cert-leaf-cert)#

```

Importing a leaf certificate from a remote file:

```

switch(config)# crypto pki certificate leaf-cert2
switch(config-cert-leaf-cert2)# import tftp://1.1.1.2/c2.p12 ta-profile root-cert
% Total      % Received % Xferd  Average Speed   Time    Time     Time  Current
           %             %             Dload  Upload   Total     Spent    Left  Speed
100  3722  100  3722    0     0   391k      0  --:--:-- --:--:-- --:--:--  391k
100  3722  100  3722    0     0   376k      0  --:--:-- --:--:-- --:--:--  376k
Enter import password: *****
Leaf certificate is validated with root-cert and imported successfully.
switch(config-cert-leaf-cert2)#

```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-cert-<CERT-NAME>	Administrators or local user group members with execution rights for this command.

import (self-signed leaf certificate)

```

import terminal self-signed [password <PW>]
import <REMOTE-URL> self-signed [password <PW>] [vrf <VRF-NAME>]
import <STORAGE-URL> self-signed [password <PW>]

```

Description

Imports a self-signed leaf certificate including its matching private key.

Parameter	Description
terminal	Import the certificate by pasting PEM-format data at the console. Upon execution, the config-cert-import context is entered for

Parameter	Description
	certificate pasting. To complete certificate data entry press Control-D in your terminal program. Alternatively, the pasted certificate data can include at its end the delimiter END_OF_CERTIFICATE (after the -----END CERTIFICATE----- line), making entry of Control-D unnecessary.
password <PW>	Specifies the plaintext password used to decrypt the private key in the imported certificate data. When this parameter is omitted, the password is prompted for as required. Range: 1 to 32 alphanumeric characters.
<REMOTE-URL>	Specifies a certificate data file on a remote TFTP or SFTP server. The URL syntax is: {tftp:// sftp://<USER>@} {<IP> <HOST>} [:<PORT>] [;blocksize=<SIZE>]/<FILE>
vrf <VRF-NAME>	Specifies the name of the VRF to use for the remote URL file transfer. The default is mgmt .
<STORAGE-URL>	Available on switch families that provide USB device file import capability, specifies a certificate data file on a USB storage device inserted in the switch USB port. The URL syntax is usb:/<FILE> .

Usage

- This command cannot be used with the default certificate **local-cert**.
- The PEM data format is supported for all import sources. The PKCS#12 data format is supported for **<REMOTE-URL>** and **<STORAGE-URL>**.
- The PEM data must be delimited with these lines for the certificate data:

```
-----BEGIN CERTIFICATE-----
-----END CERTIFICATE-----
```

And the PEM data must be delimited with either of these line pairs for the private key data:

```
-----BEGIN PRIVATE KEY-----
-----END PRIVATE KEY-----
```

```
-----BEGIN ENCRYPTED PRIVATE KEY-----
-----END ENCRYPTED PRIVATE KEY-----
```

Example

Importing a self-signed leaf certificate from the console:

```
switch(config)# crypto pki certificate ss-leaf-cert
switch(config-cert-ss-leaf-cert)# import terminal self-signed
Paste the certificate in PEM format below, then hit enter and ctrl-D:
switch(config-cert-import)# -----BEGIN CERTIFICATE-----
switch(config-cert-import)# MIID2TCCAsGgAwIBAgIJAkcrqokm6p9GMA0GCSqGSIb3DQEBCwUAM
switch(config-cert-import)# tDCA5ygAwIBAgICEAEwDQYJKoZIhvcNAQELBQAwgYgx CzABAYTAI
switch(config-cert-import)# VQQGEwJVUzELMAkGA1UECAwCQ0ExDTALBgNVBACMBFJvc2UxDDAKB
...
switch(config-cert-import)# +fWQLxhp+jKJGZGOZz/FENt2uSfZHxlXiu8n3g+EgqExenY1pBRJr
switch(config-cert-import)# VuEEoNb/YfkPXHHva4Zfx223q+f694w1VsHkENSzqr2goHpa2fOzq
switch(config-cert-import)# alewwdmVqCES+x8bvfh3C/6IB6ePkEsnM1HNTEm=
switch(config-cert-import)# -----END CERTIFICATE-----
switch(config-cert-import)# -----BEGIN ENCRYPTED PRIVATE KEY-----
switch(config-cert-import)# MIIFDjBABGkqhkiG9w0BBQ0wMzAbBgkqhkiG9w0BBQwwDgQIt8Ni3
```

```

switch(config-cert-import)# MBQGCCqGSib3DQMHBaiBHrejkcdpdASCBMjVxrrYYPnt3Vlabr9k8
switch(config-cert-import)# 5GE0U99awh9ys4360WR95xOFGThvjKTyRWG511nGwVeLZs/7TPXWI
...
switch(config-cert-import)# hzc5ZT/w2F08icRI5mFbGoTAAw9IIWMOXGweaWQJDyKGrhg89GrnV
switch(config-cert-import)# M2UuP/tYuuO328QcenKZEJmZKCb*78oFRR+pgma4oeMaFTIyXE6Pr
switch(config-cert-import)# GAdCK8tkDiJ9DKbqdm5W0/nTJfqwUQlfl127dNrBAodsHdrrw3UR99H
switch(config-cert-import)# SPo=
switch(config-cert-import)# -----END ENCRYPTED PRIVATE KEY-----
switch(config-cert-import)#
Enter import password: *****
Leaf certificate is validated as self-signed certificate and imported
successfully.
switch(config-cert-ss-leaf-cert)#

```

Importing a leaf certificate from a remote file:

```

switch(config)# crypto pki certificate ss-leaf-cert2
switch(config-cert-ss-leaf-cert2)# import tftp://1.1.1.2/ss2.p12 self-signed
% Total      % Received % Xferd  Average Speed   Time    Time     Time  Current
           Dload  Upload   Total     Spent    Left     Speed
100 3230 100 3230    0    0  875k      0 --:--:-- --:--:-- --:--:-- 875k
100 3230 100 3230    0    0  831k      0 --:--:-- --:--:-- --:--:-- 831k
Enter import password: *****
Leaf certificate is validated as self-signed certificate and imported
successfully.
switch(config-cert-ss-leaf-cert2)#

```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-cert- <i><CERT-NAME></i>	Administrators or local user group members with execution rights for this command.

key-type

```
key-type {rsa [key-size <K-SIZE>] | ecdsa [curve-size <C-SIZE>]}
```

Description

Sets the key type and key size for the current leaf certificate. The key type of the default certificate **local-cert** cannot be changed.

Parameter	Description
rsa	Selects the RSA key type.
key-size <K-SIZE>	Specifies the RSA key size in bits. Supported values: 2048, 3072,

Parameter	Description
	4096. Default: 2048
ecdsa	Selects the ECDSA key type.
curve-size <C-SIZE>	Specifies the ECDSA elliptic curve size in bits. Supported values: 256, 348, 521. Default: 256

Examples

Setting RSA encryption on the leaf certificate **leaf-cert**:

```
switch(config)# crypto pki certificate leaf-cert
switch(config-cert-leaf-cert)# key-type rsa key-size 3072
```

Setting ECDSA encryption on the leaf certificate **leaf-cert**:

```
switch(config)# crypto pki certificate leaf-cert
switch(config-cert-leaf-cert)# key-type ecdsa curve-size 521
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-cert-<CERT-NAME>	Administrators or local user group members with execution rights for this command.

ocsp disable-nonce

```
ocsp disable-nonce
no ocsp disable-nonce
```

Description

Configures exclusion of the nonce from OCSF requests. A nonce is a unique identifier that an OCSF client inserts in an OCSF request and expects the OCSF responder to include it in the corresponding OCSF response. The nonce mechanism helps prevent replay attacks in which a malicious player attempts to masquerade as the OCSF responder. Although the nonce is included by default, it can be excluded. Some OCSF responders choose to not support the use of the nonce due to performance considerations.

The **no** form of this command re-enables nonce inclusion in OCSF requests.

Examples

Disable inclusion of the nonce in OCSF requests for TA profile **root-cert**:

```
switch(config)# crypto pki ta-profile root-cert  
switch(config-ta-root-cert)# ocsp disable-nonce
```

Enable inclusion of the nonce in OCSP requests for TA profile **root-cert**:

```
switch(config)# crypto pki ta-profile root-cert  
switch(config-ta-root-cert)# no ocsp disable-nonce
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-ta- <i><TA-NAME></i>	Administrators or local user group members with execution rights for this command.

ocsp enforcement-level

```
ocsp enforcement-level {strict | optional}  
no enforcement-level
```

Description

Sets either strict or reduced enforcement of the OCSP check of certificates. Strict enforcement is enabled by default.

The **no** form of this command resets enforcement to its default of **strict**.

Parameter	Description
strict	Sets strict OCSP checking of certificates. The certificate is accepted only if all possible checking (including validation failures, software system errors, configuration errors, transactional errors) is successful.
optional	Sets reduced OCSP checking of certificates. The certificate is accepted unless one or more of these validation errors occur: ▪ Response signature invalid. ▪ Nonce in response mismatch. ▪ Certificate revoked, but only when revocation checking is possible. If revocation check is not possible, the certificate is still accepted if there are no other validation errors.

Examples

Setting reduced OCSP checking of certificates:

```
switch(config)# crypto pki ta-profile root-cert  
switch(config-ta-root-cert)# ocsp enforcement-level optional
```

Setting strict OCSP checking of certificates:

```
switch(config)# crypto pki ta-profile root-cert  
switch(config-ta-root-cert)# ocsp enforcement-level strict
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-ta- <i><TA-NAME></i>	Administrators or local user group members with execution rights for this command.

ocsp url

```
ocsp url {primary | secondary} <URL>  
no ocsp url {primary | secondary}
```

Description

Configures the OCSP responder URLs that the current TA profile uses to verify the revocation status of an X.509 digital certificate. These URLs override the OCSP responder URL contained within the peer certificate being verified (as well as URLs defined in any intermediate CAs in the chain of trust).

If no OCSP responder URLs are defined for a TA profile (default setting), then the OCSP responder URL in the peer certificate is used for revocation status checking. (The OCSP responder URL is contained in a certificate's Authority Information Access field, which is an X.509 v3 certificate extension.)

The **no** form of this command deletes the specified OCSP responder URL (primary or secondary) from the current TA profile.

Parameter	Description
{primary secondary} <URL>	Specify the HTTP URL of the primary or secondary OCSP responder using either a fully qualified domain name or IPv4 address.

Examples

Defining the primary OCSP URL for the TA profile **root-cert**:

```
switch(config)# crypto pki ta-profile root-cert  
switch(config-ta-root-cert)# revocation-check ocsp  
switch(config-ta-root-cert)# ocsp url primary http://ocsp-server.site.com
```

Removing the primary OCSP URL from the TA profile **root-cert**:

```
switch(config)# crypto pki ta-profile oot-cert  
switch(config-ta-root-cert)# revocation-check ocsp  
switch(config-ta-root-cert)# no ocsp url primary
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-ta-<TA-NAME>	Administrators or local user group members with execution rights for this command.

ocsp vrf

```
ocsp vrf <VRF-NAME>  
no ocsp vrf
```

Description

Sets the VRF that the switch uses to communicate with OCSP responders for OCSP checking. VRF mgmt is used by default.

The **no** form of this command resets the VRF to its default **mgmt**.

Parameter	Description
<VRF-NAME>	Specifies the name of the VRF the switch uses to communicate with OCSP responders. Default: mgmt .

Examples

Reverting the OCSP responder VRF to its default:

```
switch(config)# crypto pki ta-profile root-cert  
switch(config-ta-root-cert)# no ocsp vrf
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	<code>config-ta-<TA-NAME></code>	Administrators or local user group members with execution rights for this command.

revocation-check ocs

revocation-check ocs
no revocation-check

Description

Enables certificate revocation checking for the current profile using the online certificate status protocol (OCS).

The **no** form of this command disables certificate revocation checking for the current profile.

Examples

Enabling revocation checking for the TA profile **root-cert**:

```
switch(config)# crypto pki ta-profile root-cert
switch(config-ta-root-cert)# revocation-check ocs
```

Disabling revocation checking for the TA profile **root-cert**:

```
switch(config)# crypto pki ta-profile root-cert
switch(config-ta-root-cert)# no revocation-check
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	<code>config-ta-<TA-NAME></code>	Administrators or local user group members with execution rights for this command.

show crypto pki application

show crypto pki application

Description

Shows certificate information for all features (applications) using leaf certificates that are managed by PKI.

Examples

Showing certificate information for all features (applications) using leaf certificates:

```
switch# show crypto pki application1
```

Associated Applications	Certificate Name	Cert Status
https-server		not configured, using local-cert
syslog-client	local-cert	valid
hsc	xhscert	invalid, using local-cert

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Manager (#)	Administrators or local user group members with execution rights for this command.

show crypto pki certificate

```
show crypto pki certificate [<CERT-NAME> [plaintext | pem]]
```

Description

Shows a list of all configured leaf certificates, or detailed information for a specific leaf certificate.

Possible values for Cert Status are: **CSR pending, expired, expires soon, installed, malformed, not yet known**.

Possible values for EST Status are: **enroll failed, enroll pending, enroll retrying, enroll success, n/a** (certificate is not EST-enrolled), **reenroll failed, reenroll pending, reenroll retrying**.

Parameter	Description
<CERT-NAME>	Specifies the leaf certificate name. Range: 1 to 32 alphanumeric characters excluding ".".
plaintext	Shows certificate information in plain text.
pem	Shows certificate information in PEM format.

Examples

Showing a list of all configured leaf certificates:

```
switch# show crypto pki certificate
```

Certificate Name	Cert Status	EST Status	Associated Applications
--			
device-identity	installed	n/a	none
pod01-test-1	installed	n/a	dot1x-suppliant

pod01-99-1	installed	n/a	https-server, est-client
syslog-1	CSR pending	enroll retrying	syslog-client
leaf-cert1	installed	enroll success	none
leaf-cert2	CSR pending	enroll failed	none

Showing detailed information (in plaintext format) for leaf certificate **pod01-99-1**:

```
switch# show crypto pki certificate pod01-99-1 plaintext

Certificate Name: pod01-99-1
Associated Applications:
  https-server, est-client
Certificate Status: installed
EST Status: n/a
Certificate Type: regular
Intermediates:
  Subject: C = US, ST = CA, O = Company, OU = Lab-IT, CN = DeviceCA
    Issuer: C = US, ST = CA, O = Company, OU = Lab-IT, CN = Lab-CA
    Serial Number: 0x02
  Subject: C = US, ST = CA, O = Company, OU = Lab-IT, CN = Lab-CA
    Issuer: C = US, ST = CA, O = Company, OU = Lab-IT, CN = Lab-Root
    Serial Number: 0x01
Certificate:
  Data:
    Version: 1 (0x0)
    Serial Number: 14529416756121781768 (0xc9a2db8f3e3f4608)
  Signature Algorithm: sha256WithRSAEncryption
    Issuer: C=US, ST=CA, OU=Lab-IT, O=Company, CN=DeviceCA
  Validity
    Not Before: Jan 12 23:36:57 2018 GMT
    Not After : Nov 1 23:36:57 2020 GMT
  Subject: C=US, ST=CA, OU=Lab-IT, O=Company, CN=pod01-99-1
  Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
      Public-Key: (2048 bit)
      Modulus:

          00:a0:cd:ef:1b:f9:b8:bd:39:fc:7a:0e:00:17:ff:
          2b:72:d8:4e:d4:df:49:36:ca:3a:f9:05:05:d7:e3:
          d1:97:29:71:e6:33:b8:bb:8e:f0:ee:a6:e4:4a:f8:
          ...
          fe:dd:d9:a0:af:59:47:25:b4:34:06:af:03:1d:33:
          30:c3:85:fe:5c:e7:19:7f:ff:3a:b2:21:b8:e8:ed:
          83:09
      Exponent: 65537 (0x10001)
  Signature Algorithm: sha256WithRSAEncryption
    39:f6:03:86:03:d9:05:61:39:25:5f:0d:75:cc:05:ae:04:7e:
    4c:a3:13:0b:f0:1e:af:68:0e:40:9f:ed:48:b6:5e:56:8c:53:
    46:5b:c9:a4:e0:b0:bc:31:4b:a7:5d:0a:ed:7c:9c:f6:bf:1e:
    ...
    39:f5:26:58:68:e2:13:ec:94:ac:60:8e:4b:b0:ba:45:cf:d6:
    6a:4b:9f:7d:ae:3f:e5:2e:81:fe:ac:b3:65:44:35:47:a5:2f:
    89:e7:58:a0
```

Showing detailed information (in PEM format) for leaf certificate **leaf-cert1** with a status of **CSR pending**:

```
switch# show crypto pki certificate leaf-cert1 pem
```

```

Certificate Name: leaf-cert1

Associated Applications:
  syslog-client
Certificate Status: CSR pending
EST Status: enroll retrying
Certificate Type: regular
-----BEGIN CERTIFICATE REQUEST-----

MIICtTCCAZ0CAQAwcDEWMBQGA1UEAxMNC3lzbG9nLTg0MBYGA1UECxMPQ
XJlYmEtUm9zZXZpbGx1MQ4wDAYDVQQKEYTESMBAGA1EBxMJUm9zZXZpbG
x1MQswCQYDVQQIEwJDQTELMAGA1UEBhMCVVMwgGEiMSIb3DQEBAQUAA4I
...
cw2ytN6Idgh81k59x6DH7V/eORaKd5lq+oO7nkr6+QBf5L3f5Kb+TOFio
lei+EdCHMxxc07MK0n3dkziSW25HFUGsyEXVMK+BiD3zbKDoUe6XVhvqI
mamXyghigLYDcbsn6WVw==
-----END CERTIFICATE REQUEST-----

```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Manager (#)	Administrators or local user group members with execution rights for this command.

show crypto pki ta-profile

show crypto pki ta-profile [<TA-NAME>]

Description

Shows a list of all configured TA profiles, or detailed information for a specific profile.



This command shows information for both directly-configured TA profiles and TA profiles that were dynamically downloaded from EST servers.

Parameter	Description
<TA-NAME>	Specifies the TA profile name. Range: 1 to 48 alphanumeric characters excluding ".".

Examples

Showing a list of all configured TA profiles:

```
switch# show crypto pki ta-profile
```


Profile Name	TA Certificate	Revocation Check
-----	-----	-----
BASE_CA	Installed,valid	disabled
BASE02_CA	Installed,expired	disabled
root-cert	Installed,valid	OCSP
ROOT-A_CA	Not Installed	OCSP
EST-Service1	Installed,valid	None
EST-Service2	Installed,valid	None

Showing detailed information for TA profile **root-cert**:

```
switch# show crypto pki ta-profile root-cert

TA Profile Name      : root-cert
Revocation Check     : OCSP
  OSCP Primary URL   : http://ocsp1.domain.com
  OSCP Secondary URL : Not Configured
  OSCP Disable-nonce : false
  OSCP Enforcement Level: strict
  OSCP VRF           : mgmt
TA Certificate: Installed and valid
Version: 3 (0x2)
Serial Number:
  74:e6:6d:22:3f:52:cc:94:43:41:ab:66:a8:8d:47:b1
Signature Algorithm: sha1withRSAEncryption
Issuer: OU=DeviceTrust, OU=Operations, O=Site, C=US,
       CN=Site Trusted Computing Root CA 1.0
Validity
  Not Before: Sep 14 03:12:06 2007 GMT
  Not After : Sep 14 03:21:14 2032 GMT
Subject: OU=DeviceTrust, OU=Operations, O=Site, C=US,
       CN=Site Trusted Computing Root CA 1.0
Subject Public Key Info:
  Public Key Algorithm: rsaEncryption
  RSA Public Key: (2048 bit)
  Modulus (2048 bit):
    30:0d:06:09:2a:86:48:86:f7:0d:01:01:01:05:33:
    03:82:01:0f:00:30:82:01:3a:02:82:01:01:00:ac:
    3d:60:3a:2e:ca:a4:34:db:5c:3b:6b:07:df:73:62:
    ...
    20:c8:df:63:14:5a:e8:d3:ea:83:d8:47:a3:b5:2e:
    bb:64:51:f0:be:13:b6:91:e4:32:45:58:5e:1f:0d:
    02:03:01:00:01
  Exponent: 65537 (0x10001)
X509v3 extensions:
  X509v3 Key Usage:
    Digital Signature, Certificate Signing, CRL Signing
  X509v3 Basic Constraints:
    CA:TRUE, pathlen:4
  X509v3 Subject Key Identifier:
    eb:d7:ec:db:8a:cb:f2:51:d5:06:e1:42:7b:39:a7:d0:1e:31:6e:bf

Signature Algorithm: sha1withRSAEncryption
  1c:90:f3:a4:f0:0d:e2:e3:e9:ae:01:e1:7d:a7:13:e2:cc:0b:
  17:31:26:92:a2:5d:1d:19:60:54:03:13:9b:e1:73:6c:e4:b3:
  01:4f:4e:ae:61:bd:ae:b6:12:d3:ab:08:ae:8c:47:92:d7:0d:
  ...
  ca:cf:11:78:55:6d:06:49:fa:d4:8d:f3:ef:7f:79:38:35:5d:
  16:5a:57:7f:a8:dc:b0:f8:a2:04:0d:17:0b:bb:58:32:30:e0:
  2d:a8:37:a2
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Manager (#)	Administrators or local user group members with execution rights for this command.

ta-certificate

```
ta-certificate { [import [terminal]] | import {<REMOTE-URL> | <STORAGE-URL>} }
```

Description

Imports a CA certificate for use in the current TA profile. The certificate must be in PEM format. The PEM data must be delimited with these lines:

```
-----BEGIN CERTIFICATE-----
-----END CERTIFICATE-----
```



Only the first certificate in the PEM data is imported. Any additional certificates are ignored.

Parameter	Description
[import [terminal]]	Import the certificate by pasting PEM-format data at the console. Upon execution, the config-cert-import context is entered for certificate pasting. To complete certificate data entry press Control-D in your terminal program. Alternatively, the pasted certificate data can include at its end the delimiter END_OF_CERTIFICATE (after the -----END CERTIFICATE----- line), making entry of Control-D unnecessary.
import <REMOTE-URL>	Import the certificate from a file on a remote TFTP or SFTP server. The URL syntax is: <pre>{tftp:// sftp://<USER>@} {<IP> <HOST>} [:<PORT>] [;blocksize=<SIZE>]/<FILE></pre>
import <STORAGE-URL>	Available on switch families that provide USB device file import capability, import the certificate from a file on a USB storage device inserted in the switch USB port. The URL syntax is usb:/<FILE> .

Example

Importing a certificate into the TA profile **root-cert** by pasting PEM-format certificate data at the console:

```
switch(config)# crypto pki ta-profile root-cert
switch(config-ta-root-cert)# ta-certificate import terminal
Paste the certificate in PEM format below, then hit enter and ctrl-D:
switch(config-ta-cert)# -----BEGIN CERTIFICATE-----
switch(config-ta-cert)# MIIDuTCCAqECCQCuoxeJ2ZNYcjANBgkqhkiG9w0BAQsFADCBqzELMAEBh
switch(config-ta-cert)# VVMxEzARBGNVBAGMCKNhG1mb3JuaWExEDAObGNVBACMB1JvY2tsDAKBg
```

```

switch(config-ta-cert)# BAoMA0hQTjEVMBMGA1UECwwMSFBOUm9zZXZpbGx1MSowKAYDVQocG5zdz
...
switch(config-ta-cert)# x3WFF3dFZ8o9sd5LVAHneH/ztb9MP34z+le1V346r12L2kpxmTOVJVyTO
switch(config-ta-cert)# BIzD/ST/HaWI+OS+S80rm93PSscEbb9GWk7vshh5EnW/moehBKcE40lzy
switch(config-ta-cert)# 3LvMLZcssSe5J2Ca2XIhfdme8UaNZ7syGYMsAW0nG7yYHWkEOQu9s
switch(config-ta-cert)# -----END CERTIFICATE-----
switch(config-ta-cert)#
The certificate you are importing has the following attributes:
Issuer: C=US, ST=CA, L=Rocklin, O=Company, OU=Site,
        CN=site.com/emailAddress=test.ca@site.com
Subject: C=US, ST=CA, L=Rocklin, O=Company, OU=Site,
        CN=9000/emailAddress=test.ca@site.com
Serial Number: 12121221634631568498 (0xaea51217d5945772)

TA certificate import is allowed only once for a TA profile
Do you want to accept this certificate (y/n)? y
TA certificate accepted.
switch(config-ta-root-cert)#

```

Importing a certificate into the TA profile **root-cert2** from file **rcert2-data** on the USB device:

```

switch(config)# crypto pki ta-profile root-cert2
switch(config-ta-root-cert2)# ta-certificate import usb:/rcert2-data
The certificate you are importing has the following attributes:
Issuer: C=US, ST=California, L=Rocklin, O=Company, OU=Site,
        CN=site.com/emailAddress=test.ca@site.com
Subject: C=US, ST=California, L=Rocklin, O=Company, OU=Site,
        CN=9000/emailAddress=test.ca@site.com
Serial Number: 12121221634631568498 (0xaea51217d5945772)

TA certificate import is allowed only once for a TA profile
Do you want to accept this certificate (y/n)? y
TA certificate accepted.
switch(config-ta-root-cert2)#

```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-ta-<TA-NAME>	Administrators or local user group members with execution rights for this command.

subject

```

subject [common-name <COMMON-NAME>] [country <COUNTRY>] [locality <LOCALITY>]
        [org <ORG-NAME>] [org-unit <ORG-UNIT>] [state <STATE>]

```

Description

Sets the subject fields for the current leaf certificate. If the **common-name** parameter is not specified, then you are prompted to define a value for each field. If a configured value exists for any field, it is presented as the default.

The subject fields of the default certificate **local-cert** cannot be changed.

Parameter	Description
<code>common-name <COMMON-NAME></code>	Specifies the common name.
<code>country <COUNTRY></code>	Specifies the country or region.
<code>locality <LOCALITY></code>	Specifies the locality such as city.
<code>org <ORG-NAME></code>	Specifies the organization.
<code>org-unit <ORG-UNIT></code>	Specifies the organizational unit.
<code>state <STATE></code>	Specifies the state.

Examples

Setting subject fields for the leaf certificate **leaf-cert**:

```
switch(config-cert-leaf-cert)# subject common-name Leaf01 country US
locality CA org Company org-unit Site state CA
```

Setting subject fields for the leaf certificate **leaf-cert** interactively:

```
switch(config-cert-leaf-cert)# subject
Do you want to use the switch serial number as the common name (y/n)? n
Enter Common Name : Leaf01
Enter Org Unit : Site
Enter Org Name : Company
Enter Locality : Rocklin
Enter State : CA
Enter Country : US
switch(config-cert-leaf-cert)#
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	<code>config-cert-<CERT-NAME></code>	Administrators or local user group members with execution rights for this command.

PKI EST commands

arbitrary-label

```
arbitrary-label <LABEL>
no arbitrary-label
```

Description

Within the EST profile context, configures the generic optional label (also known as arbitrary label) to be concatenated to the EST server URL that is configured with the **url** command. There is no arbitrary label configured by default. Any existing arbitrary label is replaced by this command. The use of arbitrary labels is optional.

RFC 7030 allows the use of arbitrary labels so that one EST server may serve multiple CAs with the same server URL that gets concatenated with different arbitrary labels. The same label is used for every request made under a particular EST profile.

Some EST schemes use arbitrary labels in a more sophisticated way, defining different labels for different types of requests under the same EST profile. For example, the CA certificate request could use the generic label (configured with this **arbitrary-label** command), the certificate enrollment request could use the enrollment label (configured with the **arbitrary-label-enrollment** command), and the re-enrollment request could use the re-enrollment label (configured with the **arbitrary-label-reenrollment** command). Note that only one label of each of the three available types can be configured in any EST profile.

The **no** form of this command removes the generic arbitrary label.

Parameter	Description
<LABEL>	Specifies the generic arbitrary label. Range: Up to 64 characters.

Examples

Configuring the URL and generic arbitrary label. Note that with the URL and arbitrary label configured in this example, the final URL the switch uses to request CA certificates from the EST server is `https://est-service999.com/.well-known/est/rsa2048/cacerts`.

```
switch(config)# crypto pki est-profile EST-service1
switch(config)# url https://est-service999.com/.well-known/est
switch(config-est-EST-service1)# arbitrary-label rsa2048
```

Removing the generic arbitrary label:

```
switch(config)# crypto pki est-profile EST-service1
switch(config-est-EST-service1)# no arbitrary-label
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	<code>config-est-<EST-NAME></code>	Administrators or local user group members with execution rights for this command.

arbitrary-label-enrollment

```
arbitrary-label-enrollment <LABEL>
no arbitrary-label-enrollment
```

Description

Within the EST profile context, configures the arbitrary enrollment label to be concatenated to the EST server URL that is configured with the **url** command. This label is specific to the enrollment operation. There is no arbitrary enrollment label configured by default. Any existing arbitrary enrollment label is replaced by this command. The use of arbitrary enrollment labels is optional.

When the enrollment label is not configured, the generic arbitrary label (created with the **arbitrary-label** command) is used (if configured) for enrollment.

RFC 7030 allows the use of arbitrary labels so that one EST server may serve multiple CAs with the same server URL that gets concatenated with different arbitrary labels. The same label is used for every request made under a particular EST profile.

Some EST schemes use arbitrary labels in a more sophisticated way, defining different labels for different types of requests under the same EST profile. For example, the CA certificate request could use the generic label (configured with the **arbitrary-label** command), the certificate enrollment request could use the enrollment label (configured with this **arbitrary-label-enrollment** command), and the re-enrollment request could use the re-enrollment label (configured with the **arbitrary-label-reenrollment** command). Note that only one label of each of the three available types can be configured in any EST profile.

The **no** form of this command removes the arbitrary enrollment label.

Parameter	Description
<code><LABEL></code>	Specifies the arbitrary enrollment label. Range: Up to 64 characters.

Examples

Configuring the arbitrary enrollment label:

```
switch(config)# crypto pki est-profile EST-service1
switch(config-est-EST-service1)# arbitrary-label-enrollment ipsec-v7
```

Removing the arbitrary enrollment label :

```
switch(config)# crypto pki est-profile EST-service1
switch(config-est-EST-service1)# no arbitrary-label-enrollment
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-est-<EST-NAME>	Administrators or local user group members with execution rights for this command.

arbitrary-label-reenrollment

```
arbitrary-label-reenrollment <LABEL>
no arbitrary-label-reenrollment
```

Description

Within the EST profile context, configures the arbitrary re-enrollment label to be concatenated to the EST server URL that is configured with the **url** command. This label is specific to the re-enrollment operation. There is no arbitrary re-enrollment label configured by default. Any existing arbitrary re-enrollment label is replaced by this command. The use of arbitrary re-enrollment labels is optional.

When the re-enrollment label is not configured, the generic arbitrary label (created with the **arbitrary-label** command) is used (if configured) for re-enrollment.

RFC 7030 allows the use of arbitrary labels so that one EST server may serve multiple CAs with the same server URL that gets concatenated with different arbitrary labels. The same label is used for every request made under a particular EST profile.

Some EST schemes use arbitrary labels in a more sophisticated way, defining different labels for different types of requests under the same EST profile. For example, the CA certificate request could use the generic label (configured with the **arbitrary-label** command), the certificate enrollment request could use the enrollment label (configured with the **arbitrary-label-enrollment** command), and the re-enrollment request could use the re-enrollment label (configured with this **arbitrary-label-reenrollment** command). Note that only one label of each of the three available types can be configured in any EST profile.

The **no** form of this command removes the arbitrary re-enrollment label.

Parameter	Description
<LABEL>	Specifies the arbitrary re-enrollment label. Range: Up to 64 characters.

Examples

Configuring the arbitrary re-enrollment label:

```
switch(config)# crypto pki est-profile EST-service1
switch(config-est-EST-service1)# arbitrary-label-reenrollment ipsec-v7
```

Removing the arbitrary re-enrollment label :

```
switch(config)# crypto pki est-profile EST-service1
switch(config-est-EST-service1)# no arbitrary-label-reenrollment
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-est- <i><EST-NAME></i>	Administrators or local user group members with execution rights for this command.

crypto pki est-profile

```
crypto pki est-profile <EST-NAME>
no crypto pki est-profile <EST-NAME>
```

Description

Creates a certificate Enrollment over Secure Transport (EST) profile and changes to the **config-est-*<EST-NAME>*** context for the profile. Each EST profile stores information about the EST service, including EST server URL. Up to 16 profiles can be created.

If the specified EST profile exists, this command changes to the **config-est-*<EST-NAME>*** context for the profile.

The **no** form of this command deletes the specified EST profile. It also deletes the TA profiles whose CA certificates were downloaded from the corresponding EST server, and the leaf certificates that were enrolled using this EST profile.



The deletion of the related TA profiles and enrolled certificates is permanent. If the EST profile is in the startup configuration and the EST profile is deleted but this deletion is not updated in the startup configuration before a switch reboot, the EST profile will still exist after the reboot but the related TA profiles and enrolled certificates will not exist.

Parameter	Description
<i><EST-NAME></i>	Specifies the EST profile name. Range: Up to 32 alphanumeric characters (excluding ").

Examples

Creating EST profile **EST-Service1**:

```
switch(config)# crypto pki est-profile EST-Service1
switch(config-est-service1)#
```

Removing EST profile **service1**:


```
switch(config)# no crypto pki est-profile EST-Service1
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

enroll est-profile

```
enroll est-profile <EST-NAME>
```

Description

Enrolls a leaf certificate through a remote EST (Enrollment over Secure Transport) server.

Per RFC 7030, EST enables clients to request certificate signing services over secure TLS connections. The switch generates a key pair and the corresponding CSR. The CSR is sent to the EST server to request signing, and the signed certificate is returned to the switch where it is validated. If the whole process succeeds, the certificate can be used as a leaf certificate on the switch. When the leaf certificate approaches its expiry date, it will be renewed automatically through the same EST server.

Each enrollment or re-enrollment attempt starts with a **/cacerts** request sent to the EST server to get the latest chain of CA certificates. After the enrollment or re-enrollment succeeds, this chain of CA certificates will be compared with those downloaded previously from the same EST server. Updates will be made as appropriate.

The subject fields of the current leaf certificate must be defined before running this command. If the common name subject field is not configured, this command is rejected.

This command cannot be used to enroll or renew the default certificate "local-cert."

Parameter	Description
<EST-NAME>	Specifies an existing EST profile name. Range: Up to 32 alphanumeric characters (excluding ").

Example

Enrolling leaf certificate **leaf-cert1** through the EST server identified in EST profile **EST-service1**:

```
switch(config-cert-leaf-cert1)# enroll est-profile EST-service1
You are enrolling a certificate with the following attributes:
  Subject: C=US, ST=CA, L=Roseville, OU=Aruba-Roseville, O=Aruba,
          CN=leaf-cert1
  Key Type: RSA (2048 bits)

Continue (y/n)? y
```

```
Certificate enrollment via EST-service1 has been initiated.  
Please use `show crypto pki certificate leaf-cert1` to check its status.  
  
switch(config-cert-leaf-cert1)#
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-cert-<CERT-NAME>	Administrators or local user group members with execution rights for this command.

reenrollment-lead-time

```
reenrollment-lead-time <LEAD-TIME>  
no reenrollment-lead-time
```

Description

Within the EST profile context, sets the certificate re-enrollment lead time which is the number of days before certificate expiry date that certificate re-enrollment will be initiated.

The **no** form of this command resets the EST server re-enrollment lead time to its default of 2 days.

Parameter	Description
<LEAD-TIME>	Specifies the certificate re-enrollment lead time in days. Range: 0 to 30 days. Default: 2 days.

Examples

Setting the certificate re-enrollment lead time to 15 days:

```
switch(config)# crypto pki est-profile EST-service1  
switch(config-est-EST-service1)# reenrollment-lead-time 15
```

Resetting the certificate re-enrollment lead time to its default of 2 days :

```
switch(config)# crypto pki est-profile EST-service1  
switch(config-est-EST-service1)# no reenrollment-lead-time
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-est-<EST-NAME>	Administrators or local user group members with execution rights for this command.

retry-count

```
retry-count <RETRIES>  
no retry-count
```

Description

Within the EST profile context, sets the maximum number of retries to be attempted after the initial certificate enrollment request fails.

The **no** form of this command resets the maximum number of certificate enrollment request retries to its default of 3.

Parameter	Description
<RETRIES>	Specifies the maximum number of certificate enrollment request retries. Range: 0 to 32 retries. Default: 3 retries.

Examples

Setting the retry count to 5 retries:

```
switch(config)# crypto pki est-profile EST-service1  
switch(config-est-EST-service1)# retry-count 5
```

Resetting the retry count to its default of 3 retries:

```
switch(config)# crypto pki est-profile EST-service1  
switch(config-est-EST-service1)# no retry-count
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-est-<EST-NAME>	Administrators or local user group members with execution rights for this command.

retry-interval

```
retry-interval <INTERVAL>  
no retry-interval
```

Description

Within the EST profile context, sets the interval at which a failed certificate enrollment request is retried. The **no** form of this command resets the enrollment request retry interval to its default of 30 seconds.

Parameter	Description
<code><INTERVAL></code>	Specifies the enrollment request retry interval in seconds. Range: 30 to 600 seconds. Default: 30 seconds.

Examples

Setting the certificate enrollment request retry interval to 45 seconds:

```
switch(config)# crypto pki est-profile EST-service1  
switch(config-est-EST-service1)# retry-interval 45
```

Resetting the retry interval to its default of 30 seconds:

```
switch(config)# crypto pki est-profile EST-service1  
switch(config-est-EST-service1)# no retry-interval
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	<code>config-est-<EST-NAME></code>	Administrators or local user group members with execution rights for this command.

show crypto pki est-profile

```
show crypto pki est-profile [<EST-NAME>]
```

Description

Shows a list of all configured EST profiles, or detailed information for a specific profile.

Parameter	Description
<code><EST-NAME></code>	Specifies the EST profile name. Range: Up to 32 alphanumeric characters (excluding ").

Examples

Showing a list of all configured EST profiles:

```
switch# show crypto pki est-profile
```

Profile Name	Downloaded TA Profiles	Enrolled Certificates
-----	-----	-----
EST-service1	2	3
EST-service2	1	2
EST-service3	2	0

Showing detailed information for EST profile **EST-service1**:

```
switch# show crypto pki est-profile EST-service1
Profile Name           : EST-service1
Service VRF           : mgmt
Service URL            : https://est-service999.com
Arbitrary Label        : not configured
Arbitrary Label Enrollment : /ipsec-VP7
Arbitrary Label Reenrollment : not configured
Authentication Username : est1
Authentication Password :
AQBapREALpWYm2z7L1LanOtR3vGkqhBN1hBUU2CuvQXUF/ggYgAAnAnGTnKq49P4c
dNQ6UqPbjHL4XzCO0T04djkhsUxPKGfnsWuFEONveh+JbEobqKImfwJjc3eWHiaUb
eNpPx2zN2Q1DdyxAAQi4rmKr8LITMTTmd7qr
Retry Interval         : 45 seconds
Retry Count            : 5 times
Reenrollment Lead Time : 2 days
Downloaded TA Profiles : 2
Enrolled Certificates  :
leaf-cert1
leaf-cert2
leaf-cert3
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Manager (#)	Administrators or local user group members with execution rights for this command.

url

```
url <URL>
no url
```

Description

Within the EST profile context, configures the URL of the certificate enrollment EST server. This is not configured by default. Any existing URL is replaced by this command.

The **no** form of this command removes the EST server URL within the selected EST profile. The removal of the URL does not affect the TA profiles and enrolled certificates from the EST server.

Parameter	Description
<URL>	Specifies the EST server URL. Range: Up to 192 characters.

Usage

- The configuration and update of the EST profile URL triggers the sending of a **/cacerts** request to the EST server. A successful request will result in a chain of trusted CA certificates being downloaded from the EST server. Each CA certificate, either root CA certificates or intermediate CA certificates, will be saved as a TA profile, with TA profile name **<est-name>-est-taNN** with **NN** representing two numerical digits. This TA profile naming scheme with the **-est-taNN** suffix is reserved for TA profiles downloaded from EST servers.
- Upon connection with an EST server, the switch authenticates the server by validating the server certificate. For this validation to succeed, a TA profile needs to pre-exist in the switch with a CA certificate from the issuer chain of the server certificate. Once the server is authenticated, all CA certificates in its **/cacerts** response will be trusted, with no further validation occurring for them.
- The TA profiles with CA certificates downloaded from an EST server will have their revocation check set to OCSP, enforcement set to optional, and the OCSP VRF set to the same as that of the EST profile.

Examples

Configuring the EST server URL:

```
switch(config)# crypto pki est-profile EST-service1
switch(config-est-EST-service1)# url https://est-service999.com/.well-known/est
```

Removing the EST server URL:

```
switch(config)# crypto pki est-profile EST-service1
switch(config-est-EST-service1)# no url
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-est-<EST-NAME>	Administrators or local user group members with execution rights for this command.

username

```
username <USERNAME> password [ciphertext <CIPHERTEXT-PASSWORD> |
    plaintext <PLAINTEXT-PASSWORD>]
no username
```

Description

Within the EST profile context, configures the user account information for the EST server that is used to authenticate the switch before accepting requests from the switch. This is not configured by default. Any existing username and password is replaced by this command.

When entered without either optional **ciphertext** or **plaintext** parameters, the plaintext password is prompted for twice, with the characters entered masked with "*" symbols.

The **no** form of this command removes the user account information within the selected EST profile.

There are two ways the EST client on a CX switch can prove itself to an EST server: a certificate, and/or username and password. At least one of the two must be configured for the EST request to succeed. If both are configured, certificate authentication will be used. If a certificate is not configured or certificate authentication fails, and username and password is configured, the username and password will be sent to the EST server for authentication.

Parameter	Description
<USERNAME>	Specifies the EST server account user name. The exact user name requirements are set by the chosen EST service. Range: Up to 32 alphanumeric characters.
ciphertext <CIPHERTEXT-PASSWORD>	Specifies the EST server account password as Base64 ciphertext. No password prompts are provided and the ciphertext password is validated before the configuration is applied for the user. NOTE: The ciphertext password must be gotten from the EST service.
plaintext <PLAINTEXT-PASSWORD>	Specifies the password without prompting. The password is visible as cleartext when entered but is encrypted thereafter. The exact password requirements are set by the chosen EST service. Range: Up to 64 alphanumeric characters.

Examples

Configuring an EST user with prompted cleartext password entry :

```
switch(config)# crypto pki est-profile EST-service1
switch(config-est-EST-service1)# username est1 password
Enter password: *****
Confirm password: *****
switch(config-est-EST-service1)#
```

Configuring an EST user with direct cleartext password entry:

```
switch(config)# crypto pki est-profile EST-service2
switch(config-est-EST-service2)# username est1 password plaintext concept_leap739
```

Configuring an EST user with ciphertext password entry :

```
switch(config)# crypto pki est-profile EST-service3
switch(config-est-EST-service3)# username est1 password ciphertext
AQBpRALpWYm2z7L1LanOtR3vGkqhN1hBU2CuvQXUF/ggYgAAAHWaPqxU6nAnGTnKq49P4cdNQ6U
qPbjHL4XzO0T04djKUPKGfnsWuFEONveh+JbEobq63+1k80qBKImfwJjc3eWHiaUbeNpPx2zN2Q
1DdyxAAQi4rmKr8LITMTTmd7qr
```

Removing the EST user account information for EST profile EST-service2:

```
switch(config)# crypto pki est-profile EST-service2  
switch(config-est-EST-service2)# no username
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-est- <i><EST-NAME></i>	Administrators or local user group members with execution rights for this command.

vrf

```
vrf <VRF-NAME>  
no vrf
```

Description

Within the EST profile context, selects the VRF through which the EST server can be reached. Any existing VRF selection is replaced by this command. When this command is not used, VRF **mgmt** is used by default on switch families supporting the **mgmt** VRF, otherwise the default VRF named **default** is used.

The **no** form of this command selects the default VRF either **mgmt** or **default**.

Parameter	Description
<i><VRF-NAME></i>	Specifies the name of the VRF to use for EST server communication.

Examples

Selecting VRF **it-services** for EST server communications:

```
switch(config)# crypto pki est-profile EST-service1  
switch(config-est-EST-service1)# vrf it-services
```

Resetting the VRF to its default of **mgmt** for EST server communications:

```
switch(config)# crypto pki est-profile EST-service1  
switch(config-est-EST-service1)# no vrf
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-est-<EST-NAME>	Administrators or local user group members with execution rights for this command.



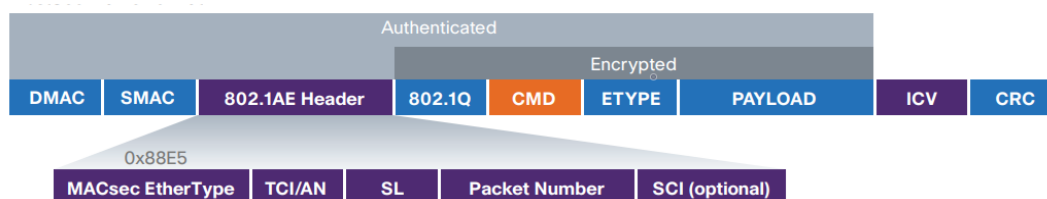
MACsec is available on the 8360 Switch Series.

Media Access Control security (MACsec) provides Layer 2 security for wired LANs, protecting network communications against a range of attacks including: denial of service, intrusion, man-in-the-middle, and eavesdropping. These attacks exploit Layer 2 vulnerabilities and often cannot be detected. MACsec appends a header and tail to all Ethernet frames, and encrypts data payload within the frame. Receiving device checks header and tail for integrity. If the check fails, traffic is dropped. If the check is successful, the frame is decrypted.

The Media Access Control security (MACsec) protocol:

- Provides a Layer 2 hop-by-hop encryption on point-to-point Ethernet links, enabling a bi-directional secure link after an exchange and verification of security keys between two connected devices.
- Secures switch-to-switch infrastructure using the MKA (MACsec Key Agreement) protocol and Static CAK (Connectivity Association Key).
- MACsec is primarily used to secure point-to-point links. With some extensions in the feature, it is possible to establish a MACsec tunnel between two endpoints over a layer2 network. These extensions are referred to as MACsec WAN extensions. The MACsec WAN extensions are available only with an advance feature pack. This feature is available on the 8360 Switch Series.
- MACsec encrypts all fields behind the source/destination MAC addresses except for MACsec SecTAG.
- MACsec secures switch to switch infrastructure using the MACsec Key Agreement (MKA) protocol and Static Connectivity Association Key (CAK).
- The pre-shared key (PSK) includes a connectivity association name (CKN) and a connectivity association key (CAK). The CKN and CAK are configured by the administrator and must match on both ends of the link.
- The MACsec frame format includes an additional 32-byte MACsec header, which includes a well-known EtherType field (0x88E5), while allowing the Ethernet source/destination MAC addresses to be left in the clear for Ethernet frame forwarding.

Figure 1 MACsec Frame Format



MACsec in AOS-CX

8360 Switch Series models that support MACsec:

8360 model	Ports	Speed
JL700A, JL701A	1/1/1 - 1/1/4	10G or 25G
JL704C, JL705C, JL719C	1/1/1 - 1/1/4 1/1/53 - 1/1/54 in split mode with breakout cables (1/1/53 when used with QSA28 Adapter (845970-B21) does not support the use of MACsec)	10G or 25G
JL704C, JL705C, JL719C	1/1/53, 1/1/54	40G or 100G

MACsec is also supported on split interfaces.

MACsec provides:

- **Connectionless data integrity:** Unauthorized changes to data cannot be made without being detected. Each MAC frame carries a separate integrity verification code.
- **Replay protection:** When enabled, packets are expected to arrive within the replay protection window number of packets. MAC frames copied from the network by an attacker cannot be resent into the network without being detected.
- **Secure Channel Identifier (SCI) tag:** Enables inclusion of the Secure Channel Identifier (SCI) tag in the Security TAG (SecTAG) field of the MACsec header. The Secure Channel Identifier (SCI) tag in the Security TAG (SecTAG) field of the MACsec header is comprised of a globally unique MAC Address and a port identifier that is unique within the system. An explicitly encoded SCI field in the SecTAG is not required on point-to-point links if the transmitting link has only one MACsec peer.
- **Data origin authenticity:** A received MAC frame is guaranteed to have been sent by the authenticated device.
- **Confidentiality:** The data payload of each MAC frame is encrypted to prevent it from being eavesdropped by unauthorized parties. The start-of-encryption offset is configurable, with available offset options of 0, 30 or 50 bytes. The default offset of 0 causes the entire data payload to be encrypted.
- **Bounded receive delay:** MAC frames cannot be intercepted by a man-in-the-middle attack and delayed by more than a few seconds without being detected.
- **Multiple Cipher Suites:**
 - gcm-aes-128: AES-128 encryption with Galois/Counter mode.
 - gcm-aes-256: AES-256 encryption with Galois/Counter mode.
 - gcm-aes-xpn-128: AES-128 encryption with Galois/Counter mode and extended packet numbering.
 - gcm-aes-xpn-256: AES-128 encryption with Galois/Counter mode and extended packet numbering. (Default)

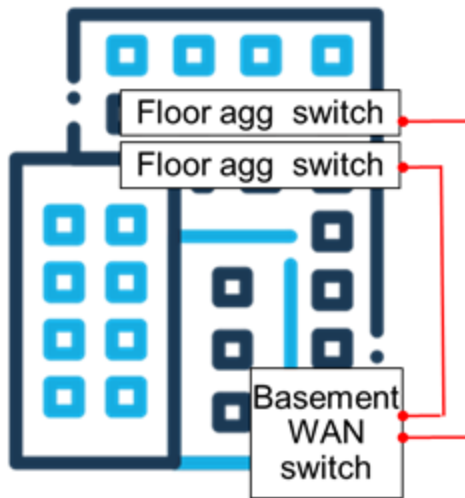
MACsec use cases

The following deployments include point-to-point links between directly connected MACsec-capable devices. In these diagrams, potential MACsec links appear in red.

Use Case 1: *Central campus*

In this example, a company is leasing several floors on a building, where fiber is in the riser of the building.

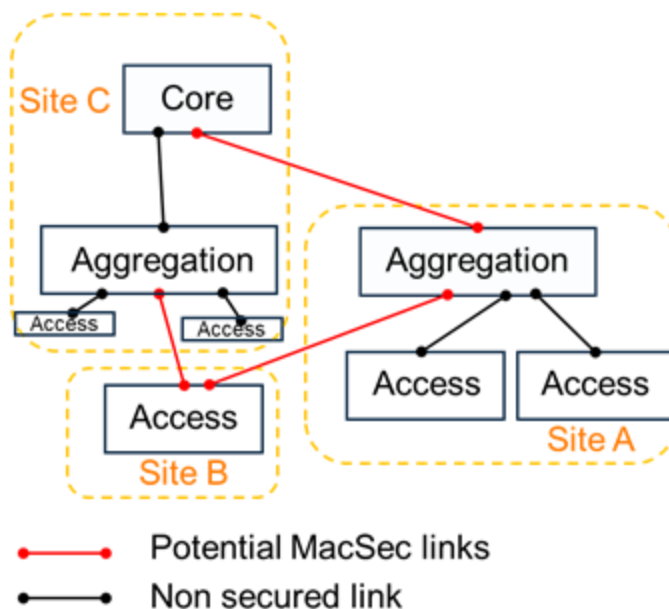
Figure 1 Central campus building with switches on different floors



Use Case 2: Distributed campus

In this low-density distributed campus, multiple sites are linked with both MACsec and non-secured links.

Figure 2 Distributed campus deployments



Use Case 3: ERPS connected campus

In this example, a multi-site campus is connected using Ethernet Ring Protection Switching (ERPS).

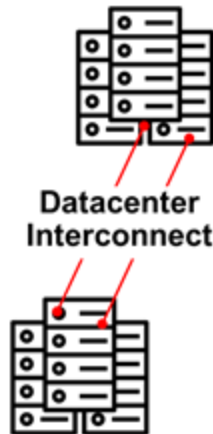
Figure 3 *ERPS Campus*



Use Case 4: Multi-Site Datacenter

A multi-site datacenter can use MACsec links between the sites.

Figure 4 *Datacenter deployment*



MACsec configuration (using 802.1X EAP TLS)



For more information on this feature, see this related video on the [Aruba AirHeads Broadcasting Channel](#).



MACsec with 802.1X EAP TLS requires at least AOS-CX 10.10.



MACsec with EAP TLS is 802.1X standard compliant and interoperates with other vendor NAS servers.

Using MACsec with 802.1X EAP TLS makes it unnecessary to manually configure an MKA policy with its pre-shared keys on the authenticator and supplicant. The MKA policy is dynamically generated on both the authenticator and the supplicant after 802.1X authentication. This simple example illustrates the basic configuration required on both the authenticator switch and the supplicant switch.

In the following command sequences, the authenticator switch is identified with the CLI prompt **auth** and the supplicant switch is identified with the CLI prompt **supp**.

Configure the authenticator

- Configure the RADIUS server for authentication over the OOBM port:

```
auth(config)# radius-server host 192.168.1.1 key ciphertext AQBa...A/g8= vrf mgmt
```

- Associate the RADIUS server with a server group:

```
auth(config)# aaa group server radius dot1x
auth(config-sg)# server 192.168.1.1 vrf mgmt
auth(config-sg)# exit
```

- Create and configure a MACsec policy:

```
auth(config)# macsec policy macsec-aoscx
auth(config-macsec-policy)# cipher-suite gcm-aes-256 gcm-aes-xpn-256
```

- Create a port access role to assign to the switch authenticating itself using 802.1X. The role puts the port in device mode (since the authenticating client is a device), enables access on a set of VLANs, and includes the MACsec policy to use after authentication.

```
auth(config)# port-access role AOSCX-Switch
auth(config-pa-role)# associate macsec-policy macsec-aoscx
auth(config-pa-role)# auth-mode device-mode
auth(config-pa-role)# vlan trunk native 10
auth(config-pa-role)# vlan trunk allowed 10,30
```

- Enable 802.1X globally and associate the RADIUS server group:

```
auth(config)# aaa authentication port-access dot1x authenticator enable
auth(config)# aaa authentication port-access dot1x authenticator radius server-  
group dot1x
```

- Configure the interface for the 802.1X authenticator with MACsec. Set the client-limit to 2 to ensure any traffic sourced directly from the authenticating device (base MAC of the authenticating device) does not cause the 802.1X authentication of the device itself (using the interface MAC) to fail due to client limit. Optionally, set the CAK length for MKA to 16 bytes if the supplicant derives a 16 byte CAK post EAP-TLS authentication.

```
auth(config)# interface 1/1/1
auth(config-if)# no shutdown
auth(config-if)# no routing
auth(config-if)# vlan access 1
auth(config-if)# aaa authentication port-access client-limit 2
auth(config-if)# aaa authentication port-access dot1x authenticator
auth(config-if-dot1x-auth)# mka cak-length 16
auth(config-if-dot1x-auth)# macsec
auth(config-if-dot1x-auth)# enable
```

Configure the supplicant

- Use a signed certificate named “supplicant” installed on the switch for 802.1X EAP TLS authentication. Note that the root certificate should also be installed on switch.

```
supp(config)# crypto pki application dot1x-supplicant certificate supplicant
```

- Create and configure a MACsec policy:

```
supp(config)# macsec policy macsec-aoscx
supp(config-macsec-policy)# cipher-suite gcm-aes-256 gcm-aes-xpn-256
```

- Create a supplicant policy to use for 802.1X EAP TLS authentication. This policy also sets the MACsec policy that is to be used after authentication. Optionally, set the CAK length for MKA to 16 bytes if the authenticator derives a 16 byte CAK post EAP-TLS authentication.

```
supp(config)# aaa authentication port-access dot1x supplicant
supp(config-dot1x-supp)# policy supplicant-aoscx
supp(config-dot1x-supp-policy)# eap-identity identity AOSCX
supp(config-dot1x-supp-policy)# macsec-policy macsec-aoscx
supp(config-dot1x-supp-policy)# mka cak-length 16
```

- Enable the 802.1X supplicant globally:

```
supp(config)# aaa authentication port-access dot1x supplicant
supp(config-dot1x-supp)# enable
```

- Configure the interface for the 802.1X supplicant with MACsec.

```
supp(config)# interface 1/1/1
supp(config-if)# no shutdown
supp(config-if)# no routing
supp(config-if)# vlan access 1
supp(config-if)# aaa authentication port-access dot1x supplicant
supp(config-if-dot1x-supp)# macsec
supp(config-if-dot1x-supp)# associate policy supplicant-aoscx
supp(config-if-dot1x-supp)# enable
```

MACsec configuration (using pre-shared keys)

A simple configuration example is provided here to illustrate MACsec configuration using pre-shared keys in the MKA policy:

- Create and configure a MACsec policy:

```
switch(config)# macsec policy MS_Policy1
switch(config-macsec-policy)# cipher-suite gcm-aes-256 gcm-aes-xpn-256
switch(config-macsec-policy)# replay-protection window-size 100
switch(config-macsec-policy)# exit
switch(config)#
```

- Create and configure an MKA policy:

```
switch(config)# mka policy MKA_Policy1
switch(config-mka-policy)# pre-shared-key ckn abcdef12 cak plaintext 123abcdef
switch(config-mka-policy)# key-server-priority 5
```

```
switch(config-mka-policy) # exit
switch(config) #
```

- Apply the MACsec and MKA policy to a port range:

```
switch(config) # interface 1/1/1-1/1/4
switch(config-if-<1/1/1-1/1/4>) # apply macsec policy MS_Policy1
switch(config-if-<1/1/1-1/1/4>) # apply mka policy MKA_Policy1
switch(config-if-<1/1/1-1/1/4>) # exit
switch(config) #
```

- Show commands are provided for showing policy information and monitoring MACsec and MKA status and statistics:

```
switch(config) # show macsec policy MS_Policy1
...
switch# show macsec status
...
switch# show macsec statistics
...
switch# show mka policy MKA_Policy1
...
switch# show mka status
...
switch# show mka statistics
...
```

MACsec limitations

Listed below are the limitations:

- Only use MACsec-supported interfaces. Not all interfaces on a system may support the MACsec capability. The switch will display an error message when a policy is associated with a physical interface that is not capable of MACsec.
- ROP, L2/L3 LAGs and VSX LAGs are not supported for 802.1X EAP TLS MACsec.
- Only configure a single MACsec/802.1x supplicant and a MACsec instance on an authenticator interface (i.e., client limit = 1).
- Complete MKA policy is dynamically generated on the switch.
- The MACsec role must come via the role in the case of the Authenticator and the supplicant policy in the case of the supplicant.
- Cannot use RADIUS VSAs to configure a MACsec policy for 802.1X EAP TLS MACsec.
- The controlled port falls back to a non-MACsec channel if the supplicant is not MACsec capable and the supplicant falls back to a non-MACsec channel if the authenticator is not MACsec capable.
- WAN MACsec on a LAG interface is not supported.
- When packets transit over a WAN MACsec tunnel, it is possible that they arrive out of order on the destination. By default, replay protection is enabled on a MACsec channel with a window size of 0. All out of order packets in such cases would be dropped. When configuring a MACsec policy for use on a WAN MACsec channel, also configure the replay window to account for out of order packets.
- WAN MACsec with an Aruba controller as nexthop will be established only if the controller has ArubaOS versions 8.10, 10.6, or later.

- When using WAN MACsec, it is possible that the packet size exceeds the link MTU due to the overhead of the MACsec SecTAG header. This can lead to packets being dropped on the next hop device due to larger MTU. Configure the link MTU to account for the additional overhead of the MACsec header in such instances.
- MACsec with custom ether type will not be established between CX devices when there are PVOS switches in bypass.

MACsec WAN extension



- The MACsec WAN extensions are available only with an advance feature pack.
- This feature is available on the 8360 Switch Series.

The MACsec WAN extension allows the establishment of a MACsec channel between two remote endpoints. This process initially requires securing the MKA channel between these endpoints, which is achieved by changing the destination MAC associated with EAPoL frames for MKA. The switch continues to use Ether-Type 0x888e for MKA. It is possible that MKA frames intended for the remote peer are used by an intermediate device when 802.1X or MACsec is enabled on the link of that intermediate device. Hence, it is important to note that a remote MACsec channel establishment will fail, if 802.1X or MACsec is enabled on any of the hops between the two remote endpoints.

8360 Switch Series models that support MACsec WAN extension:

8360 model	Ports
JL717A, JL717C	1/1/1 - 1/1/4
JL719C	1/1/1 - 1/1/4 1/1/53 - 1/1/54

WAN MACsec on a LAG interface

It is recommended not to configure a LAG interface as a WAN MACsec endpoint. If configured, both the LAG state and MACsec state on the member interfaces of the LAG will go down.

Replay protection with WAN MACsec

When packets transit over a WAN MACsec tunnel, it is possible they may arrive out of order at the destination. By default, replay protection is enabled on a MACsec channel with a window size of 0. In this case, all out-of-order packets will be dropped. Hence, when configuring a MACsec policy for a WAN MACsec channel, it is recommended to configure the replay window to account for out-of-order packets.

MACsec WAN extension configuration

The following example shows the tasks that need to be performed to configure MACsec WAN extension:

Configure MACsec bypass

```
switch(config)# macsec policy Aggregator-Connect
switch(config-macsec-policy)# bypass ieee-bpdu
OR
switch(config)# macsec policy Aggregator-Connect bypass ieee-bpdu
```

Configure the clear-tag mode in the MACsec policy

```
switch(config)# macsec policy Aggregator-Connect
switch(config-macsec-policy)# clear-tag-mode dot1q
OR
switch(config)# macsec policy Aggregator-Connect clear-tag-mode dot1q
```

Configure EAPoL-Destination Mac Address

```
switch(config)# mka policy Agg-To-Agg
switch(config-mka-policy)# eapol-destination-mac ff:ff:ff:ff:ff:ff
OR
switch(config)# mka policy Agg-To-Agg eapol-destination-mac ff:ff:ff:ff:ff:ff
```

Enable 802.1q tag for EAPoL MKA frames

```
switch(config)# mka policy Agg-To-Agg
switch(config-mka-policy)# eapol-dot1q-tagged
OR
switch(config)# mka policy Agg-To-Agg eapol-dot1q-tagged
```

Sample configuration

```
vlan 1,10,20
macsec policy <macsec-policy-name>
    bypass ieee-bpdu
    clear-tag-mode dot1q
mka policy <mka-policy-name>
    pre-shared-key ckn <ckn> cak plaintext <cak>
    eapol-destination-mac <<MAC-ADDRESS>>
    eapol-dot1q-tagged
interface 1/1/1
    no shutdown
    no routing
    vlan trunk native 10 tag
    vlan trunk allowed all
    apply mka policy <mka-policy-name>
    apply macsec policy <macsec-policy-name>
```

MACsec WAN extension use cases

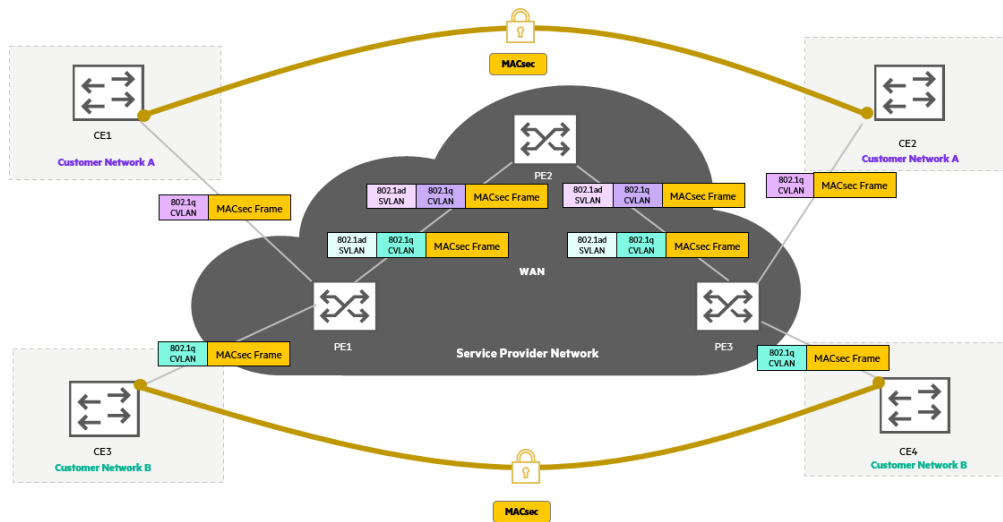
The following deployments include point-to-point links between directly connected MACsec-capable devices.

Use Case 1: QinQ – Service Provider Bridging

The IEEE 802.1ad specification, commonly known as QinQ or provider bridging, extends the IEEE 802.1Q standard by providing a second tier of VLANs in a bridged network. The general purpose of QinQ is to

allow frames from multiple customers to be forwarded in the provider network using service VLANs or S-VLANs. The provider bridge, which may comprise multiple devices in the service provider domain, appears as a simple bridge port to the customer's traffic and maintains the customer's VLAN. In this example, Customer Network A, spread across multiple site locations, wants to link them together in a single logical network. The same applies to customer B. Customer VLANs are not used to make any forwarding decisions inside the provider network, where customer frames get assigned to service VLANs (S-VLANs). Inside the Service Provider Network, frames are forwarded based on the S-VLAN tag only, while the C-VLAN tag remains protected during data transmission. The S-VLAN tag is removed when the frame exits the provider network, restoring the original customer frame. By enabling MACsec, customer frames are encrypted along this path. Hence, the secure customer traffic isolation is achieved at Layer 2 within a Service Provider network.

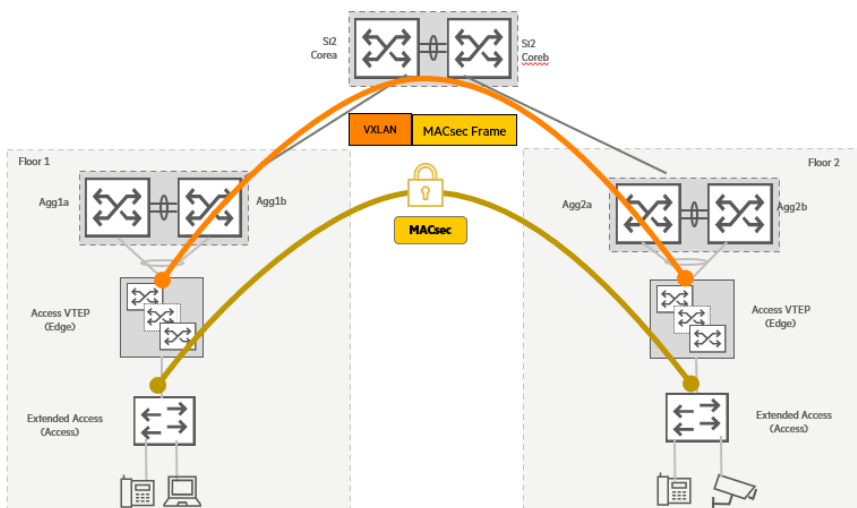
Figure 1 QinQ – Service Provider Bridging



Use Case 2: Interconnect using VXLAN

In this example, two floors are interconnected over VXLAN. Access VSF switches act as VTEPs. The WAN MACsec tunnel is established between the extended access edge switches of different floors.

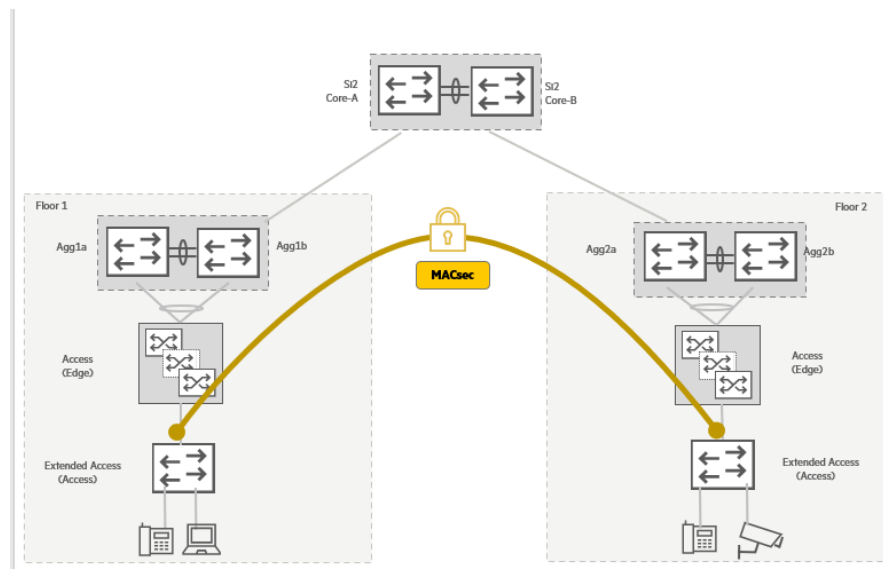
Figure 2 Interconnect using VXLAN



Use Case 3: Interconnect – L2 Only

In this example, two Floors are interconnected over L2-only interfaces. Access VSF switches is connected to extended access standalone switches. The WAN MACsec tunnel is established between the extended access edge switches of different floors.

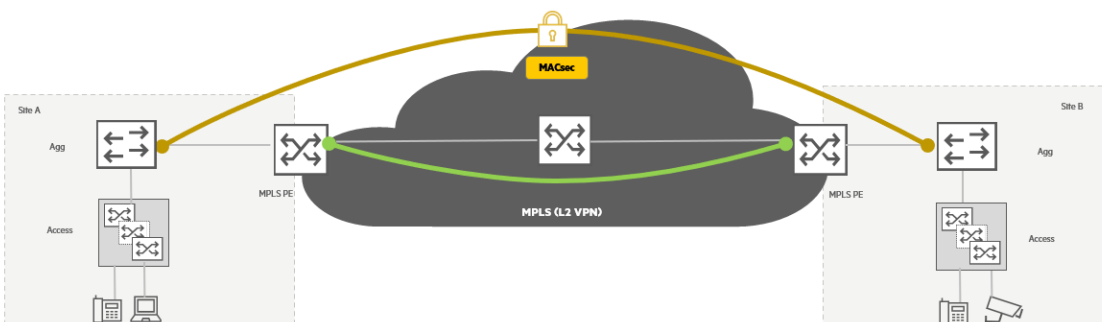
Figure 3 Interconnect – L2 Only



Use Case 4: Pseudo Wire – Site Interconnect using MPLS

In this example, two different sites, Site A and Site B, are connected using MPLS. The WAN MACsec tunnel is established between MACsec tunnel end-points over MPLS cloud. The MPLS PE is a third-party device that supports L2 VPN.

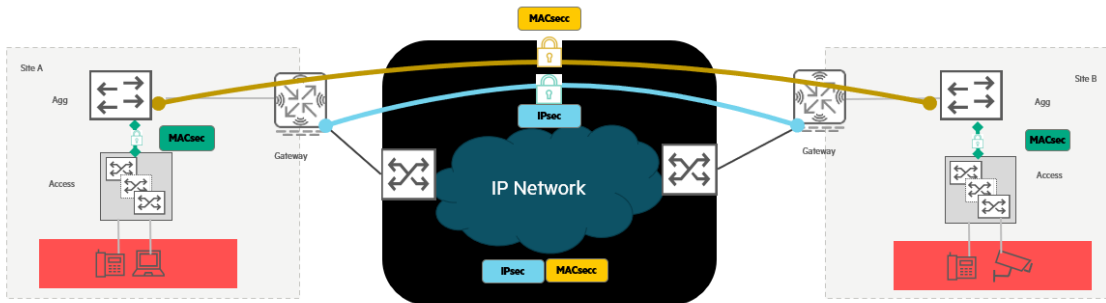
Figure 4 Pseudo Wire – Site Interconnect using MPLS



Use Case 5: Dual Encryption – MACsec over IPsec

In this example, two different sites, Site A and Site B, are protected using IPsec. The LAN MACsec channels are established between Access and Aggregation switches. The WAN MACsec tunnel is established between MACsec tunnel End-Points over IPsec. Gateways are used to establish IPsec tunnels and achieve L2 extension between the sites. The gateways must have an L2 GRE tunnel across the IPsec.

Figure 5 Dual Encryption – MACsec over IPsec



Debugging and troubleshooting

The output of the following show commands can be used to debug and troubleshoot any MACsec WAN extension related configurations:

show mka policy

```
switch# show mka policy Agg-To-Agg

MKA Policy Details

Policy Name: Agg-To-Agg
-----
Mode                : Pre-shared key
CKN                 : abcdef123456
CAK (encrypted)    :
AQBapUwNK5Uf+r1vmhBIncQPw1YPVH0VlnYr7Yjm/bPn3bBVCgAAAHFKt8mcSv/A/g8=
Keychain            : macsec_keys
EAPoL Destination MAC : ff:ff:ff:ff:ff:ff
EAPoL 802.1q Tag    : Enabled
Key-server Priority  : 5
Transmit Interval   : 6 seconds
```

show mka status

```
switch# show mka status interface 1/1/1

MKA Protocol Status

Interface 1/1/1
=====

KA Port Identifier   : 1
MKA Policy Name      : Agg-To-Agg
MKA Session Status   : Secured
Mode                 : Pre-shared key
CKN                  : abcdef123456
CAK (encrypted)     :
AQBapUwNK5Uf+r1vmhBIncQPw1YPVH0VlnYr7Yjm/bPn3bBVCgAAAHFKt8mcSv/A/g8=
Keychain             : macsec_keys
Member Identifier    : 1c64f054f894b5482defdf81
Message Number       : 86
Capability            : Conf, Offset 0
EAPoL Destination MAC : ff:ff:ff:ff:ff:ff
EAPoL 802.1q Tagged  : Enabled
Transmit Interval    : 6 seconds
Key Server Priority   : 5
```

```

Key Server          : No

Live Peer List:
MI                  MN          PRI Capability          Rx-SCI
-----
fb7f82788e4cd38dbc65dc55 119      16  IC, Conf, Offset 0    a45d36489bfe0002

Potential Peer List:
MI                  MN          PRI Capability          Rx-SCI
-----

```

show mka statistics

```
switch# show mka statistics interface 1/1/1
```

```

Interface 1/1/1
=====

KaY
----
SCI : ec0273f72f4d0001

Statistics
-----
MKPDUs With Invalid Version : 0
MKPDUs With Invalid CKN    : 0

Participant
-----
CKN : 1234567890

Statistics
-----
Tx MKPDUs           : 33834
Rx MKPDUs           : 35375
SAKs Distributed    : 1
SAKs Received       : 0
MKPDUs With Invalid ICV : 0
MKPDUs With Duplicate MI : 0
MKPDUs With Invalid MN : 0
...

```

show macsec policy

```
switch# show macsec policy Aggregator-Connect
```

```
MACsec Policy Details
```

```
Policy Name: Aggregator-Connect
```

```

-----
Cipher suite          : GCM-AES-128
Include SCI           : Yes
Confidentiality       : Enabled
Confidentiality offset : 0
Replay protection     : Enabled
Replay protection window : 0
Data delay protection : Enabled
Secure mode           : Must-Secure

```

Bypass	: IEEE-BPDU
Clear tag mode	: 802.1q

MACsec best practices

- Enable MACsec on links that have the potential to be compromised, and can be vulnerable to man-in-the-middle and masquerading attacks.
- Avoid enabling MACsec on links that are operating at 85% or greater capacity. The overhead of a MACsec header can lead to packet drops on a link operating close to full capacity.
- In an environment with devices running AOS-Switch, do not enable UDLD on both links. The UDLD session can toggle between UP and DOWN continuously when both MACsec and UDLD are enabled on the same link.
- Use the default values for the following configurations are recommended for most deployments.
 - **Confidentiality** (Default: Enabled)
 - **Confidentiality-Offset** (Default: 0)
 - **Replay Protection** (Default: Enabled, Window-Size 0)
 - **Transmit-Interval** (Default: 2 seconds)
- Configure the most secure cipher-suite that both the ends of a MACsec channel can support.
- One of the MACsec peers becomes the key-server, which generates and sends secure key information to members of a MACsec CA. When configuring the key-server priority, ensure the device to be elected as the key-server is configured with a lower key-server priority value than the other device on the channel.
- Disable the **Include-SCI tag** option for a slight improvement in performance caused by the reduced overhead in the MACsec header on point-to-point links.
- 802.1X EAP TLS MACsec and Preshared key (PSK) MACsec must not be configured on the same port.
- When running 802.1X EAP TLS MACsec, if it is not clear whether the peer can support MACsec, use a MACsec policy with `secure-mode` configured as `should-secure`. Doing this allows the channel to switch to non-MACsec if the peer does not send any MKA frames after 802.1X authentication.
- In an environment with a Cisco device, the Cisco device must be designated as the key server. Designating the AOS-CX server as the key server results in complete traffic loss.
- In an environment with Cisco and HPE FlexFabric devices, do not update confidentiality-offset on the live channel. There can be complete traffic loss for an extended period on the MACsec channel when confidentiality-offset is updated on both ends.
- In an environment with Cisco devices, when the GCM-AES-XPB-128 or GCM-AES-XPB-256 cipher suite is used for establishing the MACsec channel, the MKA policy on the Cisco device must be configured with **ssci-based-on-sci**.
- The **cak-length** should be configured to 16 under dot1x authenticator mode when Cisco AnyConnect is used as a supplicant.

Switch-to-Host MACsec Limitations

The following limitations apply to switch-to-host MACsec deployments.

- Use only L2 physical interfaces that support MACsec.
- Routed Only Ports (ROPs), Layer-2 or Layer-3 Link Aggregation Groups (LAGs), and VSX LAGs are not supported.

- Configure a single MACsec/802.1X supplicant and MACsec instance only on an authenticator interface, (for example, where client-limit = 1).
- Do not use RADIUS VSAs to configure a MACsec policy.
- The entire MKA policy is dynamically generated on the switch.
- The MACsec role must come via the role for anAuthenticator and the supplicant policy for the supplicant.
- The controlled port falls back to a non-MACsec channel if the supplicant is not MACsec capable. The supplicant falls back to a non-MACsec channel if the authenticator is not MACsec capable.

MACsec troubleshooting

- As a result of standard PHY behavior, the FedCert Event log can indicate that there are packets seen on MACsec interface with a **UNKNOWN_SCI** value, even though other statistics show that this log entry represents combination of packets with either the **not valid** or **UNKNOWN_SCI** values.
- Use the **copy support-files feature macsec** and **copy diag-dump feature macsec** commands to capture diagnostic data specific to MACsec.
- Debug logs are available for MACsec. Issue the **debug macsec all** command for verbose logs when debugging issues.
- When MACsec does not work between two endpoints.
 - Verify the MKA session is **Secured** on both the sides.
 - When the MKA sessions between the two MACsec endpoints flaps continuously between Secured and Unsecured.
 - Verify the cipher-suite advertised by the elected key-server is supported on the peer.
 - Verify the confidentiality-offset configuration is identical on the MACsec peers.
 - Verify the MACsec status shows as **Up** and the state shows as **Retire**.
 - Check the MACsec statistics for packets being dropped.
 - Ok packets must increment on the transmitting channel.
 - **Not Valid** packets incrementing on the transmitting channel indicates an issue with the key programmed on either side of the MACsec channel.

MACsec commands

apply macsec policy

```
apply macsec policy <MACSEC-POLICY-NAME>
no apply macsec policy
```

Description

Within the selected interface context, applies the specified MACsec policy to the selected port. When a MACsec policy is applied to a port, MACsec is enabled on the port and all data traffic is blocked on the port until a secure channel is successfully established.



A MACsec policy can be applied to a physical interface port that is not part of any LAG ports or to a lag port. It can also be applied to an interface that is configured as an MCLAG, VSX keep-alive, or VSX inter-switch-link.

If a MACsec policy is already applied to the selected port, this command replaces the existing policy application.



For MACsec to work, an MKA policy must also be configured and applied to the same ports.

The **no** form of this command dissociates the specified policy from the port.

Parameter	Description
<code><MACSEC-POLICY-NAME></code>	Specifies the MACsec policy name. Range: 1 to 128 alphanumeric characters including only the three special characters "." (period), "-" (hyphen), and "_" (underscore).

Usage

- When any MACsec or MKA policy parameter is updated, any active MACsec session on all interfaces running the MACsec or MKA policy is terminated and restarted. This is indicated with the following prompt that provides an opportunity to not execute the **apply** command.

```
This policy is currently in use by one or more interfaces.
Updating the policy will cause existing MACsec sessions using
the policy to restart.
Continue (y/n)?
```

- For non-LAG ports, a range of ports can be specified in the **interface** command used to enter the interface context. For example, entering the interface context for ports 1/1/1 through 1/1/2:

```
switch(config)# interface 1/1/1-1/1/2
switch(config-if-<1/1/1-1/1/2>)# apply macsec policy MS_Policy1
```

- Not all interfaces on a switch may support the MACsec capability. An error will be generated when a policy is applied to a physical interface that is not capable of MACsec. For LAG ports, any non-MACsec capable interfaces that are part of the LAG will be blocked.
- The 32-port 8360 Switch Series (models JL700A, JL701A) does not support both MACsec and priority-based flow-control (PFC) on same interface. Applying a MACsec policy to an interface associated with an existing PFC configuration will disable the interface. PFC must be unconfigured on the interface before MACsec can be used.

Examples

Applying a MACsec policy to a range of two ports:

```
switch(config)# interface 1/1/1-1/1/2
switch(config-if-<1/1/1-1/1/2>)# apply macsec policy MS_Policy1
```

Attempting to apply a MACsec policy to a port that already has PFC enabled:

```
switch(config)# interface 1/1/3
switch(config-if)# apply macsec policy MS_Policy1

MACsec and priority-based flow control (PFC) cannot be configured at the same time
on
this interface. Applying a MACsec policy will disable the interface until PFC is
```

```
removed.  
Continue (y/n)?
```

Attempting to apply a MACsec policy to a port that is not MACsec capable:

```
switch(config)# interface 1/1/5  
switch(config-if)# apply macsec policy MS_Policy1  
  
MACsec is not supported on the interface.  
switch(config-if)#
```

Removing MACsec policy association from a port:

```
switch(config)# interface 1/1/1  
switch(config-if)# no apply macsec policy
```

Applying a MACsec policy to a LAG port:

```
switch(config)# interface lag 1  
switch(config-if)# apply macsec policy MS_Policy1
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
8360	config-if	Administrators or local user group members with execution rights for this command.

bypass

```
bypass {ieee-bpdu}  
no bypass {ieee-bpdu}
```

Description

Configures the MACsec policy to bypass MACsec for specific features.

When bypass is enabled on the BPDU, packets with a destination MAC matching the IEEE BPDU MAC (01:80:c2:00:00:0*) will bypass MACsec on both the egress and ingress directions.

By default, when MACsec is enabled on an interface, all BPDU frames except EAPoL are protected by MACsec. However, when an interface configured is configured to initiate a MACsec tunnel, the BPDU frames that are essential to the next hop device are sent with MACsec protection. This causes protocols such as LLDP and LACP to fail on the local link since the next hop device will fail to read the MACsec protected frames. To enable these protocols to operate on such links, you must enable BPDU bypass in the MACsec policy.

The **no** form of the command disables MACsec bypass for the specified feature. When no feature is specified, MACsec bypass is disabled for all the features.

Examples

Enabling the MACsec bypass for IEEE BPDUs:

```
switch(config)# macsec policy Aggregator-Connect
switch(config-macsec-policy)# bypass ieee-bpdu
OR
switch(config)# macsec policy Aggregator-Connect bypass ieee-bpdu
```

Disabling the MACsec bypass for IEEE BPDU:

```
switch(config)# macsec policy Aggregator-Connect
switch(config-macsec-policy)# no bypass ieee-bpdu
OR
switch(config)# no macsec policy Aggregator-Connect bypass ieee-bpdu
```

Command History

Release	Modification
10.13	Command introduced.

Command Information

Platforms	Command context	Authority
8360	config config-macsec-policy	Administrators or local user group members with execution rights for this command.

cipher-suite

```
cipher-suite {<CIPHER-SUITE>} [<CIPHER-SUITE>] ... [<CIPHER-SUITE>]
no cipher-suite [<CIPHER-SUITE>] ... [<CIPHER-SUITE>]
```

Description

Within the MACsec policy context, configures one or more cipher suites to be used to generate the SAK (Secure Authentication Key) for when the switch is the key server. When multiple cipher suites are configured, the most secure cipher suite is considered first during negotiation.

The **no** form of this command (without the **<CIPHER-SUITE>** parameter) resets to the default of considering (during negotiation) all supported cipher suites while giving priority to the most secure suite **gcm-aes-xpn-256**. Include the **<CIPHER-SUITE>** parameter to disable a particular cipher suite.

Parameter	Description
<CIPHER-SUITE>	Selects the cipher suite. Available cipher suites are: ▪ gcm-aes-128: AES-128 encryption with Galois/Counter mode. ▪ gcm-aes-256: AES-256 encryption with Galois/Counter mode. ▪ gcm-aes-xpn-128: AES-128 encryption with Galois/Counter

Parameter	Description
	mode and extended packet numbering. gcm-aes-xpn-256: AES-128 encryption with Galois/Counter mode and extended packet numbering. (The default and the most secure.)

Examples

Enabling a single cipher suite:

```
switch(config-macsec-policy)# cipher-suite gcm-aes-128
```

Enabling two cipher suites:

```
switch(config-macsec-policy)# cipher-suite gcm-aes-256 gcm-aes-xpn-256
```

Disabling a particular cipher suite:

```
switch(config-macsec-policy)# no cipher suite gcm-aes-128
```

Resetting to the default of considering all available cipher suites while giving priority to **gcm-aes-xpn-256**:

```
switch(config-macsec-policy)# no cipher-suite
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
8360	config-macsec-policy	Administrators or local user group members with execution rights for this command.

clear macsec statistics

```
clear macsec statistics [interface <IF-RANGE>]
```

Description

Clears MACsec statistics on all MACsec-enabled interfaces or on a specific interface or interface range. MACsec statistics are cleared for the entire switch rather than just in the current user session.

Parameter	Description
interface <IF-RANGE>	Specifies one or more interfaces for which MACsec statistics information is to be cleared.

Examples

Clearing MACsec statistics on an interface range:

```
switch# clear macsec statistics interface 1/1/1-1/1/4
```

Clearing MACsec statistics on all MACsec-enabled interfaces:

```
switch# clear macsec statistics
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
8360	Manager (#)	Administrators or local user group members with execution rights for this command.

clear tag mode

```
clear tag mode {dot1q | none}
no clear tag mode {dot1q | none}
```

Description

Configures the part of the Ethernet payload in a MACsec protected frame that must precede the Security TAG (SecTAG) header in clear text.

The **dot1q** mode allows the 802.1q tag of a MACsec protected frame to be sent in clear text and placed before the MACsec SecTAG header. This enables the establishment of a MACsec tunnel between two MACsec endpoints over a non-MACsec Layer 2 network.

The **no** form of the command will configure the device to place the SecTAG header immediately after the destination and source MAC addresses.



Untagged traffic is not supported on a MACsec channel running clear-tag mode as **dot1q**. All untagged frames will be dropped on ingress.

Parameter	Description
dot1q	Specifies the encoding of a single 802.1q tag in clear text before

Parameter	Description
	Security TAG (SecTAG).
none	Specifies that the Security TAG (SecTAG) directly follows the Ethernet addresses. This is the default option.

Examples

Configuring the clear-tag mode as **dot1q**:

```
switch(config)# macsec policy Aggregator-Connect
switch(config-macsec-policy)# clear-tag-mode dot1q
OR
switch(config)# macsec policy Aggregator-Connect clear-tag-mode dot1q
```

Resetting the clear-tag mode:

```
switch(config)# macsec policy Aggregator-Connect
switch(config-macsec-policy)# no clear-tag-mode dot1q
OR
switch(config)# no macsec policy Aggregator-Connect clear-tag-mode dot1q
```

Command History

Release	Modification
10.13.1000	Added support for the 6400 Switch Series.
10.13	Command introduced.

Command Information

Platforms	Command context	Authority
8360	config config-macsec-policy	Administrators or local user group members with execution rights for this command.

confidentiality

```
confidentiality [offset {0|30|50}]
no confidentiality
```

Description

Within the MACsec policy context, enables Ethernet packet encryption after the MACsec header, optionally including a start-of-encryption offset. Confidentiality is enabled by default with an offset of 0 bytes after the MACsec header.

An offset of 0 causes the entire packet (after the MACsec header) to be encrypted. It is sometimes desirable to offset the start of the encryption deeper into the packet to allow for fields such as MPLS labels and 802.1Q tags to remain unencrypted.

Omitting the **offset** parameter enables confidentiality with whatever offset was configured previously. The **no** form of this command disables confidentiality.

Parameter	Description
offset {0 30 50}	Selects the start-of-encryption offset (in bytes) into the packet after the MACsec header. Default 0 bytes.

Examples

Enabling confidentiality with an offset of 30 bytes:

```
switch(config-macsec-policy)# confidentiality offset 30
```

Disabling confidentiality

```
switch(config-macsec-policy)# no confidentiality
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
8360	config-macsec-policy	Administrators or local user group members with execution rights for this command.

include-sci-tag

```
include-sci-tag
no include-sci-tag
```

Description

Within the MACsec policy context, enables inclusion of the Secure Channel Identifier (SCI) tag in the Security TAG (SecTAG) field of the MACsec header. This is the default.

Inclusion of the SCI tag is not required on point-to-point links if the transmitting link has only one MACsec peer.



On the 8360 Switch Series models JL700A and JL701A, inclusion (or exclusion) of the SCI tag must be set identically at both ends of a MACsec channel. Asymmetric SCI tag settings are not supported.

The **no** form of this command disables inclusion of the Secure Channel Identifier (SCI) tag in the Security TAG (SecTAG) field of the MACsec header.

Examples

Enabling the SCI tag:

```
switch(config-macsec-policy)# include-sci-tag
```

Disabling the SCI tag:

```
switch(config-macsec-policy)# no include-sci-tag
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
8360	config-macsec-policy	Administrators or local user group members with execution rights for this command.

macsec policy

```
macsec policy <MACSEC-POLICY-NAME>  
no macsec policy <MACSEC-POLICY-NAME>
```

Description

Creates the specified MACsec policy and then enters its context (displayed in the CLI as **config-macsec-policy**). If the MACsec policy already exists, this command enters the specified MACsec policy context.

A MACsec policy can be applied to one or more switch ports, enabling MACsec on the ports. An MKA (MACsec Key Agreement) policy must be applied to the same ports.

The **no** form of this command deletes the MACsec policy.

8360 Switch Series models that support MACsec:

8360 model	Ports	Speed
JL700A, JL701A	1/1/1 to 1/1/4	10G or 25G
JL704C, JL705C, JL719C	1/1/1 to 1/1/4 1/1/53 to 1/1/54 in split mode with breakout cables (1/1/53 when used with QSA28 Adapter (845970-B21) does not support the use of MACsec)	10G or 25G
JL704C, JL705C, JL719C	1/1/53, 1/1/54	40G or 100G

MACsec is also supported on split interfaces.



A MACsec policy cannot be deleted if it is currently applied to any ports. All application of the policy must be removed before the policy can be deleted.

Parameter	Description
<code><MACSEC-POLICY-NAME></code>	Specifies the MACsec policy name. Range: 1 to 128 alphanumeric characters including only the three special characters "." (period), "-" (hyphen), and "_" (underscore).

Examples

Creating a MACsec policy:

```
switch(config)# macsec policy MS_Policy1
switch(config-macsec-policy)#
```

Deleting a MACsec policy (the policy cannot be currently applied to any ports):

```
switch(config)# no macsec policy MS_Policy1
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
8360	config	Administrators or local user group members with execution rights for this command.

macsec selftest

```
macsec selftest
no macsec selftest
```

Description

Configures the system to run a self test for MACsec on all MACsec-capable interfaces.

The **no** form of the command disables the MACsec self test on the device.

When enabled, the system will drop traffic on all MACsec capable interfaces until the MACsec selftest completes successfully on the interface. A MACsec selftest will be run in the following scenarios:

- On a VSF stack, the self test will run on a newly added switch
- When member is removed and re-added to stack
- When interface is removed from VSF link
- After every reboot (if enabled)

Examples

Running a MACsec self test:

```
switch(config) # macsec selftest
```

Disabling the MACsec self test:

```
switch(config) # no macsec selftest
```

Command History

Release	Modification
10.11	Command introduced.

Command Information

Platforms	Command context	Authority
8360	config	Administrators or local user group members with execution rights for this command.

replay-protection

```
replay-protection [window-size <WINDOW-SIZE>]  
no replay-protection
```

Description

Within the MACsec policy context, enables replay protection with the default or specified window size. With replay protection enabled, packets are expected to arrive within the replay protection window number of packets. For example with a window size of 10, any packet arriving out-of-sequence by more than 10 packets will be discarded. A window size of 0 (the default) enforces strict order of packet reception, discarding all packets not received in perfect sequence.

The **no** form of this command disables replay protections and resets the window size to its 0 default.

Parameter	Description
<WINDOW-SIZE>	Specifies the replay protection window size in packets. Default 0 packets. Range: 0 to 4294967295 packets.

Examples

Enabling replay protection with the default window size of 0 (strict order of packet reception):

```
switch(config-macsec-policy) # replay-protection
```

Enabling replay protection with a windows size of 100 packets:

```
switch(config-macsec-policy) # replay-protection window-size 100
```

Disabling replay protection.

```
switch(config-macsec-policy)# no replay-protection
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
8360	config-macsec-policy	Administrators or local user group members with execution rights for this command.

secure-mode

```
secure-mode {should-secure|must-secure}  
no secure-mode [should-secure|must-secure]
```

Description

Configures the MACsec protection behavior on the interface when a MACsec Key Agreement (MKA) session is not established. Use **should-secure** to enable fail open mode for MACsec. Fail open mode ensures that traffic continues to flow if the MKA session is not established. Use **must-secure** (the default) to use MACsec in fail closed mode.

The **no** form of the command resets the behavior to the default, **must-secure**.

Parameter	Description
{should-secure must-secure}	With should-secure set: ▪ If the MKA session is not established, traffic is still allowed in clear text without the MACsec header. ▪ If the MKA session is established successfully, traffic is allowed with the MACsec header. With must-secure set: ▪ If the MKA session is not established, traffic is blocked on the data-plane. ▪ If the MKA session is established successfully, traffic is allowed with the MACsec header.

Examples

Configuring **should-secure**:

```
switch(config)# macsec policy Aggregator-Connect  
switch(config-macsec-policy)# secure-mode should-secure  
OR  
switch(config)# macsec policy Aggregator-Connect secure-mode should-secure
```

Configuring **must-secure**:

```
switch(config)# macsec policy Aggregator-Connect
switch(config-macsec-policy)# secure-mode must-secure
OR
switch(config)# macsec policy Aggregator-Connect secure-mode must-secure
```

Resetting to the default (**must-secure**):

```
switch(config)# macsec policy Aggregator-Connect
switch(config-macsec-policy)# no secure-mode
OR
switch(config)# no macsec policy Aggregator-Connect secure-mode
```

Command History

Release	Modification
10.10	Command introduced.

Command Information

Platforms	Command context	Authority
8360	config config-macsec-policy	Administrators or local user group members with execution rights for this command.

show macsec policy

show macsec policy [<MACSEC-POLICY-NAME>]

Description

Shows information for one or all MACsec policies.

Parameter	Description
<MACSEC-POLICY-NAME>	Specifies the MACsec policy name. Range: 1 to 128 alphanumeric characters including only the three special characters "." (period), "-" (hyphen), and "_" (underscore).

Examples

Showing information for a specific MACsec policy:

```
switch# show macsec policy Aggregator-Connect

MACsec Policy Details

Policy Name: Aggregator-Connect
-----
Cipher suite           : GCM-AES-128
Include SCI            : Yes
Confidentiality        : Enabled
Confidentiality offset : 0
```

```
Replay protection      : Enabled
Replay protection window : 0
Data delay protection  : Enabled
Secure mode            : Must-Secure
Bypass                 : IEEE-BPDU
Clear tag mode         : 802.1q
```

Command History

Release	Modification
10.13	Command output updated to display Bypass and Clear tag mode information.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
8360	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show macsec selftest

```
show macsec selftest [interface <IFRANGE>]
```

Description

Shows the status of the MACsec selftest for MACsec capable interfaces. If an interface fails the self test then MACsec selftest should be disabled.

Parameter	Description
<IFRANGE>	Specifies the interface(s) for which to show MACsec selftest information.

Examples

Showing MACsec self test information for all interfaces that are MACsec capable:

```
switch# show macsec selftest
MACsec selftest status

Interface  Status           Failure Reason
-----
1/1/1     Initializing     --
1/1/2     Passed           --
1/1/3     Queued for run   --
1/1/4     Running
1/1/5     Failed           Encryption test failed
1/1/6     Failed           Decryption test failed
1/1/7     Failed           Initialization failed
```

```
1/1/8      Failed      Time out
1/1/9      Initialized
```

Showing MACsec self test information for a specific interface:

```
switch# show macsec selftest interface 1/1/1

MACsec selftest status

Interface  Status  Failure Reason
-----
1/1/1     Passed  --
```

Showing MACsec self test information for an interface range:

```
switch# show macsec selftest interface 1/1/1-1/1/3

MACsec selftest status

Interface  Status  Failure Reason
-----
1/1/1     Passed  --
1/1/2     Running --
1/1/3     Failed  Decryption test failed
```

Command History

Release	Modification
10.10	Command introduced.

Command Information

Platforms	Command context	Authority
8360	Manager (#)	Administrators or local user group members with execution rights for this command.

show macsec statistics

```
show macsec statistics [interface <IF-RANGE>]
```

Description

Shows MACsec statistics for all MACsec-enabled interfaces or a specific interface or interface range.

Parameter	Description
interface <IF-RANGE>	Specifies one or more interfaces for which MACsec statistics information is to be shown.

Examples

Showing MACsec statistics for a specific interface:

```
switch# show macsec statistics interface 1/1/1
```

MACsec Statistics

Interface 1/1/1

=====

Rx Statistics

Unicast Uncontrolled Packets	: 170438363226
Multicast Uncontrolled Packets	: 66586
Broadcast Uncontrolled Packets	: 4399
Rx Uncontrolled Drop Packets	: 0
Rx Uncontrolled Error Packets	: 0
Rx Controlled Unicast Packets	: 170438369232
Rx Controlled Multicast Packets	: 31298
Rx Controlled Broadcast Packets	: 4399
Rx Controlled Drop Packets	: 0
Rx Controlled Error Packets	: 0
Uncontrolled Octets	: 27270198219337
Controlled Octets	: 21816165353719

Tx Statistics

Unicast Uncontrolled Packets	: 0
Multicast Uncontrolled Packets	: 33756
Broadcast Uncontrolled Packets	: 0
Rx Uncontrolled Drop Packets	: 0
Rx Uncontrolled Error Packets	: 0
Unicast Controlled Packets	: 171226945517
Multicast Controlled Packets	: 98215
Broadcast Controlled Packets	: 71894
Rx Controlled Drop Packets	: 0
Rx Controlled Error Packets	: 0
Uncontrolled Octets	: 4658308
Controlled Octets	: 21917110733304
Common Octets	: 27396383670012

SecY Statistics

Port Identifier : 1

Rx Statistics

Transform Error Packets	: 0
Control Packets	: 35288
Untagged Packets	: 0
No Tag Packets	: 0
Bad Tag Packets	: 39
No SCI Packets	: 0
Unknown SCI Packets	: 0
Tagged Control Packets	: 0
Overrun Packets	: 0

Tx Statistics

Transform Error Packets	: 0
Control Packets	: 33756
Untagged Packets	: 0

Transmit Secure Channel

SCI : ec0273f72f4d0001

Statistics

Encrypted Packets : 171227173728
Protected Packets : 0

Secure Association

Association Number : 0

Statistics

Encrypted Packets : 171227173728
Encrypted Octets : 19862392663792
Protected Packets : 0
Protected Octets : 0
Too Long Packets : 0
SA Not In Use Packets : 0

Receive Secure Channel

SCI : 00fd4568f4110001

Statistics

Late Packets : 0
Not Valid Packets : 0
Delayed Packets : 0
Ok Packets : 170438441668

Secure Association

Association Number : 0

Statistics

Unchecked Packets : 0
Delayed Packets : 0
Late Packets : 0
Ok Packets : 170438441668
Invalid Packets : 0
Not Valid Packets : 0
Not Using SA Packets : 0
Unused SA Packets : 0
Decrypted Octets : 19770908750641
Validated Octets : 0

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
8360	Operator (>) or Manager	Operators or Administrators or local user group members with

Platforms	Command context	Authority
	(#)	execution rights for this command. Operators can execute this command from the operator context (>) only.

show macsec status

show macsec status [interface <IF-RANGE>] [detailed]

Description

Shows MACsec status information for all MACsec-enabled interfaces or a specific interface or interface range.

Parameter	Description
interface <IF-RANGE>	Specifies one or more interfaces for which MACsec status information is to be shown.
detailed	Specifies that detailed status information is to be shown.

Usage

Applicable to when the **detailed** parameter is included: The stop time for the MACsec secure channel and secure association is updated only when the secure channel or association entry is being deleted. Therefore, it is never shown as set in the **show macsec status detailed command** output.

Examples

Showing MACsec summary information for all interfaces:

```
switch# show macsec status
```

MACsec Protocol Status

Interface	Port ID	Policy	Protection	Status	State
1/1/1	0	MS_Policy1	Conf, Offset 0	Up	Retire
1/1/2	0	MS_Policy1	IC	Down	Init
...					

Showing detailed MACsec information for a specific interface:

```
switch# show macsec status interface 1/1/1 detailed
```

Interface 1/1/1

=====

Port Identifier: 0

=====

```
Policy      : MS_Policy1
Status      : Up
State       : Retire
Cipher Suite : GCM-AES-128
Protection  : Conf, Offset 0
```

```

Bypass      : IEEE-BPDU
Clear Tag Mode : None

Transmit Secure Channel
-----
SCI   : 000C29F6A4380004C
SSCI  : 1

Secure Association
-----
Association Number : 0 (old)
Key Identifier     : 4F18CE25228178FD15976E4C
Packet Number     : 9500
SA-Start-Time     : Sun Oct 18 04:05:11 UTC 2020
SA-Stop-Time      : Sun Oct 18 04:10:12 UTC 2020

Association Number : 1 (current)
Key Identifier     : 4F18CE25228178FD15976E4C
Packet Number     : 19000
SA-Start-Time     : Sun Oct 18 04:10:13 UTC 2020
SA-Stop-Time      : -

Receive Secure Channel
-----
SCI   : 000C29F6A4360003B
SSCI  : 2

Secure Association
-----
Association Number : 0 (old)
Key Identifier     : 4F18CE25228178FD15976E4C
Lowest Packet Number : 9500
SA-Start-Time     : Sun Oct 18 04:05:12 UTC 2020
SA-Stop-Time      : Sun Oct 18 04:10:12 UTC 2020

Association Number : 1 (current)
Key Identifier     : 4F18CE25228178FD15976E4C
Lowest Packet Number : 19000
SA-Start-Time     : Sun Oct 18 04:10:13 UTC 2020
SA-Stop-Time      : -

```

Command History

Release	Modification
10.13.1000	Command Introduced on the 6400 Switch Series.
10.13	Command output updated to display Bypass and Clear tag mode information.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
8360	Operator (>) or Manager	Operators or Administrators or local user group members with

Platforms	Command context	Authority
	(#)	execution rights for this command. Operators can execute this command from the operator context (>) only.

MKA commands (MACsec)

apply mka policy

```
apply mka policy <MKA-POLICY-NAME>
no apply mka policy
```

Description

Within the selected interface context, applies the specified MKA policy to the selected port. To start the MKA protocol on the port, a MACsec policy must also be applied to the port.



An MKA policy can be applied to a physical interface port that is not part of any LAG ports or to a lag port. It can also be applied to an interface that is configured as an MCLAG, VSX keep-alive, or VSX inter-switch-link.

If an MKA policy is already applied to the selected port, this command replaces the existing policy application.

The **no** form of this command dissociates the specified policy from the port.

Parameter	Description
<MKA-POLICY-NAME>	Specifies the MKA policy name. Range: 1 to 32 alphanumeric characters including only the three special characters "." (period), "-" (hyphen), and "_" (underscore).

Usage

- When any MACsec or MKA policy parameter is updated, any active MACsec session on all interfaces running the MACsec or MKA policy is terminated and restarted. This is indicated with the following prompt that provides an opportunity to not execute the **apply** command.

```
This policy is currently in use by one or more interfaces.
Updating the policy will cause existing MACsec sessions using
the policy to restart.
Continue (y/n)?
```

- For non-LAG ports, a range of ports can be specified in the **interface** command used to enter the interface context. For example, entering the interface context for ports 1/1/1 through 1/1/4:

```
switch(config)# interface 1/1/1-1/1/4
switch(config-if-<1/1/1-1/1/4>)# apply mka policy MKA_Policy1
```

- Not all interfaces on a switch may support the MACsec capability. An error will be generated when a policy is applied to a physical interface that is not capable of MACsec. For LAG ports, any non-MACsec capable interfaces that are part of the LAG will be blocked.

Examples

Applying an MKA policy to a range of two ports:

```
switch(config)# interface 1/1/1-1/1/2
switch(config-if-<1/1/1-1/1/2>)# apply mka policy MKA_Policy1
```

Attempting to apply an MKA policy to a port that is not MACsec capable:

```
switch(config)# interface 1/1/5
switch(config-if)# apply mka policy MKA_Policy1

MACsec is not supported on the interface.
switch(config-if)#
```

Removing MKA policy association from a port:

```
switch(config)# interface 1/1/1
switch(config-if)# no apply mka policy
```

Applying an MKA policy to a LAG port:

```
switch(config)# interface lag 1
switch(config-if)# apply mka policy MKA_Policy1
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
8360	config-if	Administrators or local user group members with execution rights for this command.

clear mka statistics

```
clear mka statistics [interface <IF-RANGE>]
```

Description

Clears MKA statistics on all MACsec-enabled interfaces or on a specific interface or interface range. MKA statistics are cleared for the entire switch rather than just in the current user session.

Parameter	Description
interface <IF-RANGE>	Specifies one or more interfaces (ports) for which MKA statistics information is to be cleared.

Examples

Clearing MKA statistics on an interface range:

```
switch# clear mka statistics interface 1/1/1-1/1/4
```

Clearing MKA statistics on all MACsec-enabled interfaces:

```
switch# clear mka statistics
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
8360	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

data-delay-protection

```
data-delay-protection  
no data-delay-protection
```

Description

Configures the MACsec policy to use data delay protection. Data delay protection allows MKA participants to ensure that the data frames protected by MACsec are not delayed by more than 2 seconds.

Enabling data delay protection necessitates transmission of MKPDUs at a frequency of 0.5 second to meet a maximum data delay of 2 seconds while minimizing connectivity interruption due to the possibility of lost or delayed MKPDUs.

Data delay protection should be enabled only when there is a need to drop MACsec protected frames that are delayed by more than 2 seconds on the wire. It is recommended to not enable data delay protection unless absolutely required as it adds extra load on the system.

Disabled by default.



When data delay protection is enabled, a default of 0.5 second is used as transmit-interval and transmit-interval configuration under MKA policy is ignored.

Examples

Enabling data delay protection:

```
switch(config)# macsec policy Aggregator-Connect data-delay-protection
```

or

```
switch(config)# macsec policy Aggregator-Connect
switch(config-macsec-policy)# data delay protection
```

Disabling data delay protection:

```
switch(config)# no macsec policy Aggregator-Connect data-delay-protection
```

or

```
switch(config)# macsec policy Aggregator-Connect
switch(config-macsec-policy)# no data delay protection
```

Command History

Release	Modification
10.11	Command introduced.

Command Information

Platforms	Command context	Authority
8360	config config-macsec-policy	Administrators or local user group members with execution rights for this command.

eapol-destination-mac

```
eapol-destination-mac <MAC-ADDRESS>
no eapol-destination-mac <MAC-ADDRESS>
```

Description

Configures the destination MAC address to use in EAPoL frames for MKA. When not configured, the switch uses the default EAPoL multicast address (01:80:C2:00:00:03) for MKA.

The **no** form of the command configures the switch to use the default EAPoL multicast address for MKA.

Parameter	Description
<MAC-ADDRESS>	Specifies the EAPoL destination MAC address for MKA.

Examples

Configuring the broadcast MAC as EAPoL destination address:

```
switch(config)# mka policy Agg-To-Agg
switch(config-mka-policy)# eapol-destination-mac ff:ff:ff:ff:ff:ff
OR
switch(config)# mka policy Agg-To-Agg eapol-destination-mac ff:ff:ff:ff:ff:ff
```

Resetting MKA policy to use untagged EAPoL MKA frames:

```
switch(config)# mka policy Agg-To-Agg
switch(config-mka-policy)# no eapol-destination-mac
OR
switch(config-if)# no mka policy Agg-To-Agg eapol-destination-mac
```

Command History

Release	Modification
10.13	Command introduced.

Command Information

Platforms	Command context	Authority
8360	config-if config-mka-policy	Administrators or local user group members with execution rights for this command.

eapol-dot1q-tagged

eapol-dot1q-tagged
no eapol-dot1q-tagged

Description

Configures the EAPoL frames for MKA to be transmitted with an 802.1q tag. The native VLAN associated with the port is used in the MKA frames. This configuration enables the switch to establish a MACsec tunnel over a Layer 2 network with the next hop connected over non-MACsec, 802.1q tagged only link. The **no** form of command configures the switch to send MKA frames as untagged.

- 
- When the configuration is enabled, MKA is restarted on the port if the native VLAN associated with the port is updated.
 - The 802.1q tag added to the MKA frame is also used in the computation of the ICV for the MKA frame. If the 802.1q tag is removed or modified in any way along the path, including changes in VLAN ID or PCP, the MKA frame will be discarded at the destination.

Examples

Configuring the MKA policy to use 802.1q tagged EAPoL MKA frames:

```
switch(config)# mka policy Agg-To-Agg
switch(config-mka-policy)# eapol-dot1q-tagged
OR
switch(config)# mka policy Agg-To-Agg eapol-dot1q-tagged
```

Resetting MKA policy to use untagged EAPoL MKA frames:

```
switch(config)# mka policy Agg-To-Agg
switch(config-mka-policy)# no eapol-dot1q-tagged
OR
switch(config-if)# no mka policy Agg-To-Agg eapol-dot1q-tagged
```

Command History

Release	Modification
10.13	Command introduced on the 8360 and 6300 Switch Series.

Command Information

Platforms	Command context	Authority
8360	config-if config-mka-policy	Administrators or local user group members with execution rights for this command.

eapol-eth-type

```
eapol-eth-type <ETH-TYPE>
no eapol-eth-type <ETH-TYPE>
```

Description

Configures the Ether-Type for use in frames for MKA.

The **no** form of the command uses the default EAPoL ether-type 0x888e for MKA.



- Only values 0x876f and 0x888e are supported.
- Refer to the MACsec WAN extension

Parameter	Description
<ETH-TYPE>	Configures the Ether-Type in EAPoL frames for MKA.

Examples

Configuring the custom Ethernet type for MKA:

```
switch(config)# mka policy Agg-To-Agg eapol-eth-type 876f
OR
switch(config)# mka policy Agg-To-Agg
switch(config-mka-policy)# eapol-eth-type 876f
```

Resetting the custom EAPoL Ethernet Type:

```
switch(config)# no mka policy Agg-To-Agg eapol-eth-type 876f
OR
switch(config)# mka policy Agg-To-Agg
```



```
switch(config-mka-policy) # no eapol-eth-type 876f
```

Using an Ethernet Type value other than 876f or 888e:

```
switch(config) # mka policy Agg-To-Agg
switch(config-mka-policy) # eapol-eth-type 999F
Unsupported Ether-Type. Supported values are 888e and 876f
```

Command History

Release	Modification
10.14	Command introduced on the 6300, 6400, and 8360 Switch Series.

Command Information

Platforms	Command context	Authority
8360	config-mka-policy	Administrators or local user group members with execution rights for this command.

key-server-priority

```
key-server-priority <PRIORITY>
no key-server-priority
```

Description

In the **config-mka-policy** policy context, configures the MKA key server priority. The highest priority is 0 and indicates that this switch strongly wants to be the MKA key server. The lowest priority is 255 and indicates that switch does not want to be the MKA key server, allowing the switch at the other end of the link to be the key server. Set this priority on the switches at either end of the link to achieve the desired effect.

If the key server priority is 0 on both switches then the switch with the lowest system MACsec address is elected as key server.

The **no** form of this command resets the MKA key server priority to its default of 0.

Parameter	Description
<PRIORITY>	Selects the MKA key server priority for this switch. Default 0 (highest priority). Range: 0 to 255.

Examples

Setting the MKA key server priority:

```
switch(config-mka-policy) # key-server-priority 5
```

Resetting the MKA key server priority to its default of 0:

```
switch(config-mka-policy) # no key-server-priority
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
8360	config-mka-policy	Administrators or local user group members with execution rights for this command.

mka policy

```
mka policy <MKA-POLICY-NAME>
no mka policy <MKA-POLICY-NAME>
```

Description

Creates the specified MKA (MACsec Key Agreement) policy and then enters its context (displayed in the CLI as **config-mka-policy**). If the MKA policy already exists, this command enters the specified MKA policy context.

An MKA policy can be applied to one or more switch ports, enabling MKA on the ports. A MACsec policy must be applied to the same ports.

The **no** form of this command deletes the MKA policy.



An MKA policy cannot be deleted if it is currently applied to any ports. All application of the policy must be removed before the policy can be deleted.

Parameter	Description
<MKA-POLICY-NAME>	Specifies the MKA policy name. Range: 1 to 32 alphanumeric characters including only the three special characters "." (period), "-" (hyphen), and "_" (underscore).

Examples

Creating an MKA policy:

```
switch(config) # mka policy MKA_Policy1
switch(config-mka-policy) #
```

Deleting an MKA policy (the policy cannot be currently applied to any ports):

```
switch(config) # no mka policy MKA_Policy1
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
8360	config	Administrators or local user group members with execution rights for this command.

pre-shared-key

```
pre-shared-key keychain <NAME>
pre-shared-key ckn <CA-KEY-NAME> cak {plaintext [<PLAINTEXT-CAK>] | ciphertext
<CIPHERTEXT-CAK>}
```

Description

Configures the Pre-Shared Key (PSK) to use for an MKA policy.

A PSK can be configured one of two ways:

1. Configure the Connectivity Association Key Name (CKN) and Connectivity Association Key (CAK) directly in the PSK.
2. Configure the PSK to use an existing keychain for the CKN (key name) and CAK (key-string).

If both a key chain and a static CKN/CAK are configured in the PSK, then the key chain will be used for MKA operations.



When using a PSK with a key chain, only the send lifetime is considered for CAK lifetime. It is recommended to not configure an accept lifetime in the key chain used for MACsec.

The **no** form of this command deletes the PSK configuration including the key chain association, the CKN and the CAK.

Parameter	Description
<CA-KEY-NAME>	Specifies the CKN (Connectivity Association Key Name). Range: 1 to 64 hexadecimal characters.
<PLAINTEXT-CAK>	Specifies the CAK (Connectivity Association Key) in plaintext. Range: 1 to 64 hexadecimal characters.
<CIPHERTEXT-CAK>	Specifies the CAK (Connectivity Association Key) as ciphertext.
<NAME>	Specifies the keychain name.

Examples

Configuring the pre-shared key with a specified plaintext CAK:

```
switch(config-mka-policy) # pre-shared-key ckn abcdef12 cak plaintext 123abcdef
```

Configuring the pre-shared key with a prompted plaintext CAK:

```
switch(config-mka-policy) # pre-shared-key ckn abcdef12 cak plaintext
Enter CAK: *****
Confirm CAK: *****
```

Configuring the pre-shared key with a ciphertext CAK:

```
switch(config-mka-policy) # pre-shared-key ckn abcdef12 cak ciphertext
AQBapUvjDZgUxtTpgA4NLqnsn7CjXqbDch+BOS7y9fcWExLUBgAAAKUmDYdhew==
```

Configuring a key chain for an MKA policy:

```
switch(config) # mka policy Agg-To-Agg
switch(config-mka-policy) # pre-shared-key keychain macsec_keys
```

Deleting the PSK configuration including its CKN and CAK:

```
switch(config-mka-policy) # no pre-shared-key
```

Deleting a key chain from an MKA policy:

```
switch(config) # mka policy Agg-To-Agg
switch(config-mka-policy) # no pre-shared-key keychain macsec_keys
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
8360	config-mka-policy	Administrators or local user group members with execution rights for this command.

show mka policy

show mka policy [*<MKA-POLICY-NAME>*]

Description

Shows information for one or all MKA policies.

Parameter	Description
<i><MKA-POLICY-NAME></i>	Specifies the MKA policy name. Range: 1 to 32 alphanumeric characters including only the three special characters "." (period), "-" (hyphen), and "_" (underscore).

Examples

Showing information for a specific MKA policy:

```
switch# show mka policy Agg-To-Agg

MKA Policy Details

Policy Name: Agg-To-Agg
-----
Mode                : Pre-shared key
CKN                 : abcdef123456
CAK (encrypted)     :
AQBApUwNK5Uf+r1vmhBIncQPw1YPVH0V1nYr7Yjm/bPn3bBVCgAAAHFKt8mcSv/A/g8=
Keychain            : macsec_keys
EAPoL Destination MAC : ff:ff:ff:ff:ff:ff
EAPoL 802.1q Tag     : Enabled
Key-server Priority  : 5
Transmit Interval    : 6 seconds
```

Command History

Release	Modification
10.13	Command updated to display EAPoL Destination MAC and EAPoL 802.1q Tag in the output.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
8360	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show mka statistics

```
show mka statistics [interface <IF-RANGE>]
```

Description

Shows MKA statistics for all MACsec-enabled interfaces or a specific interface or interface range. The MKA statistics are refreshed periodically, approximately every five seconds.

Parameter	Description
interface <IF-RANGE>	Specifies one or more interfaces for which MKA statistics information is to be shown.

Examples

Showing MKA statistics information for a specific interface:

```
switch# show mka statistics interface 1/1/1
```

```
Interface 1/1/1
=====
```

```
KaY
```

```
----
```

```
SCI : ec0273f72f4d0001
```

```
Statistics
```

```
-----
```

```
MKPDUs With Invalid Version : 0
```

```
MKPDUs With Invalid CKN      : 0
```

```
Participant
```

```
-----
```

```
CKN : 1234567890
```

```
Statistics
```

```
-----
```

```
Tx MKPDUs                : 33834
```

```
Rx MKPDUs                : 35375
```

```
SAKs Distributed         : 1
```

```
SAKs Received            : 0
```

```
MKPDUs With Invalid ICV  : 0
```

```
MKPDUs With Duplicate MI : 0
```

```
MKPDUs With Invalid MN   : 0
```

```
...
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
8360	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show mka status

Shows MKA status information for all MACsec-enabled interfaces or a specific interface or interface range.

```
show mka status [interface <IF-RANGE>]
```

Description

Parameter	Description
interface <IF-RANGE>	Specifies one or more interfaces for which MKA status information is to be shown.

Examples

Showing MKA status information for a specific interface (Pre-shared key):

```
switch# show mka status interface 1/1/1

MKA Protocol Status

Interface 1/1/1
=====

KA Port Identifier      : 1
MKA Policy Name        : Agg-To-Agg
MKA Session Status     : Secured
Mode                   : Pre-shared key
CKN                    : abcdef123456
CAK (encrypted)       :
AQBapUwNK5Uf+r1vmhBIncQPw1YPVH0V1nYr7Yjm/bPn3bBVCgAAAHFKt8mcSv/A/g8=
Keychain               : macsec_keys
Member Identifier      : 1c64f054f894b5482defdf81
Message Number        : 86
Capability             : Conf, Offset 0
EAPoL Destination MAC : ff:ff:ff:ff:ff:ff
EAPoL 802.1q Tagged    : Enabled
Transmit Interval     : 6 seconds
Key Server Priority    : 5
Key Server            : No

Live Peer List:
MI              MN      PRI Capability      Rx-SCI
-----
fb7f82788e4cd38dbc65dc55 119      16 IC, Conf, Offset 0  a45d36489bfe0002

Potential Peer List:
MI              MN      PRI Capability      Rx-SCI
-----
```

Command History

Release	Modification
10.13	Command updated to display EAPoL Destination MAC and EAPoL 802.1q Tagged in the output.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
8360	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

transmit-interval

```
transmit-interval <INTERVAL>
no transmit-interval
```

Description

In the **config-mka-policy** policy context, configures the MKA packet transmit interval.

The **no** form of this command resets the MKA packet transmit interval to its default of 2 seconds.

Parameter	Description
<code><INTERVAL></code>	Selects the MKA packet transmit interval. Default 2 seconds. Range: 2 to 6 seconds.

Examples

Setting the MKA packet transmit interval:

```
switch(config-mka-policy) # transmit-interval 4
```

Resetting the MKA packet transmit interval to its default of 2 seconds:

```
switch(config-mka-policy) # no transmit-interval
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

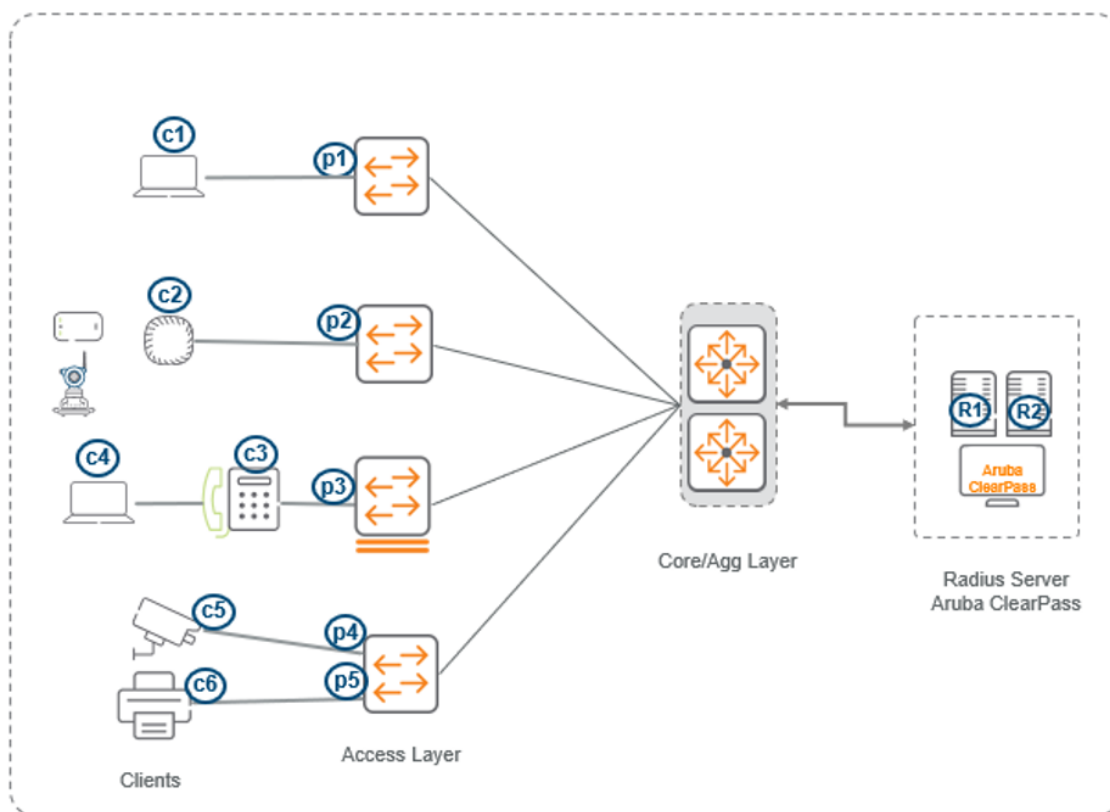
Platforms	Command context	Authority
8360	config-mka-policy	Administrators or local user group members with execution rights for this command.

Local Area Networks are often deployed in a way that allows unauthorized clients to attach to network devices or allow unauthorized users to get access to unattended clients on a network. 802.1X and MAC authentication simplify security management by providing access control plus the ability to control user profiles, allowing a given user entering valid user credentials access from multiple points within the network.

AOS-CX access switches support the following port access authentication types:

- 802.1X authentication
- MAC authentication

Figure 1 802.1X and MAC authentication



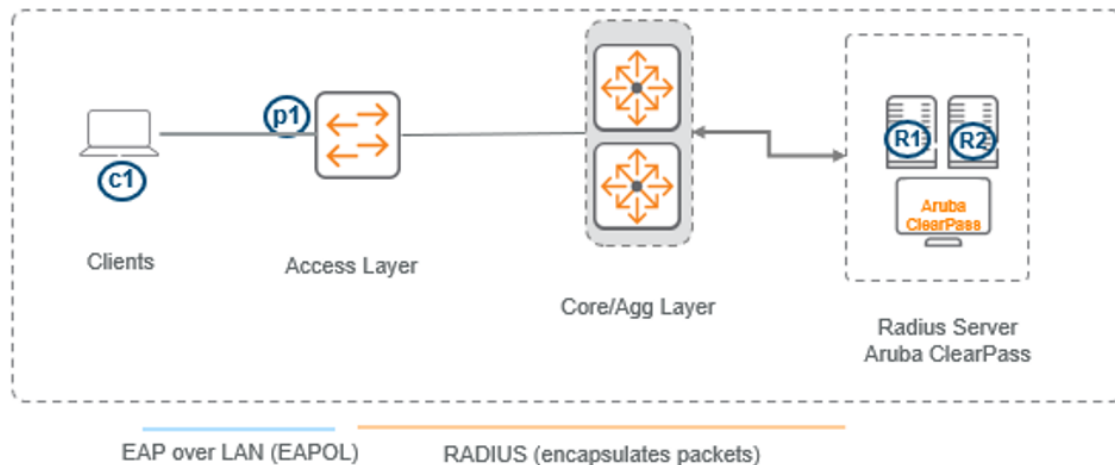
Port access 802.1X authentication

IEEE 802.1X is a standard for port-based authentication. This standard provides administrators with an authentication mechanism for devices trying to access a LAN or WLAN. 802.1X defines the encapsulation of the Extensible Authentication Protocol (EAP) over IEEE 802, which is known as EAP over LAN (EAPOL).

802.1X port-based authentication provides port-level security. It allows LAN access only on ports where a single 802.1X-capable client (supplicant) has entered authorized RADIUS user credentials. 802.1X

authentication is recommended for applications where only one client can connect to the port at a time. Using this option, the port processes all IP traffic as if it comes from the same client.

Figure 1 802.1X authentication



802.1X authentication involves the following entities:

- **Supplicant:** A client device that tries to access the LAN.
- **Authenticator:** A network device (typically a switch) that authenticates the supplicant.
- **Authentication Server:** A host running software supporting the RADIUS and EAP protocols that provides an authentication service to the authenticator.

Until the supplicant is authenticated, the authenticator allows only EAPOL traffic through the port to which the supplicant is connected. Only after the authentication is successful, the authenticator allows normal traffic from the supplicant.

802.1X requires a supplicant (client), authenticator (switch), and authentication server (RADIUS). Aruba ClearPass provides a RADIUS server, as well as other capabilities for monitoring and managing user access.

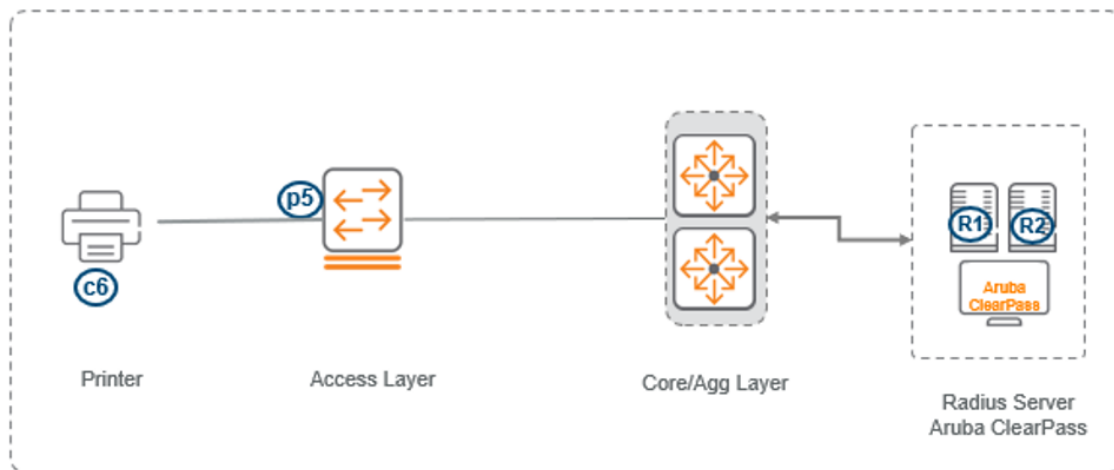
You can alternatively use a third-party RADIUS server such as Microsoft Network Policy Server (NPS) or an open source server such as FreeRADIUS.

In wired deployments, 802.1X is most commonly used in instances where the supplicant is an end-user machine (such as a PC, laptop, phone, and so on) and the authenticator is a switch. In certain deployments, the supplicant can itself be a switch (for example, an access switch). To ensure that the access switch connecting to an upstream switch has the right credentials, a switch should be able to be operate as an 802.1X supplicant.

Port access MAC authentication

MAC authentication is designed to be used at the edge of a network. It provides port-based security measures for protecting private networks and switches from unauthorized access. Because this method does not require clients to run special supplicant software (unlike 802.1X authentication), it is suitable to be used in legacy systems, IoT devices, and temporary access situations where introducing supplicant software is not an attractive option. Only a MAC address is required for authentication.

Figure 1 MAC authentication



MAC authentication relies on a RADIUS server to authenticate clients. This technique simplifies access security management by using a database on a single server to control client access. Up to three RADIUS servers can be used for backup in case access to the primary server fails. It also means that the same credentials can be used for authentication, regardless of which switch or switch port is the current access point into the LAN.

On a port configured for MAC authentication, the switch operates as a port-access authenticator using a RADIUS server, and the Challenge-Handshake Authentication Protocol (CHAP) and Password Authentication Protocol (PAP) protocols. Inbound traffic is processed by the switch alone, until authentication occurs. Some traffic from the switch to an unauthorized client is supported (for example, broadcast or unknown destination packets) before authentication occurs.

How MAC authentication works

MAC authentication grants access to a secure network by authenticating devices. When a device connects to the switch, either by direct link or through the network, the switch forwards the device MAC address to the RADIUS server for authentication. The RADIUS server uses the device MAC address as the user name and password, and grants or denies network access in the same way that it does for clients capable of interactive logons. The process does not use a client device configuration or a logon session. MAC authentication is well suited for clients not capable of providing interactive logons, such as telephones, printers, and wireless access points. Also, because most RADIUS servers allow for authentication to depend on the source switch and port through which the client connects to the network, you can use MAC authentication to lock a particular device to a specific switch and port.

802.1X port access and MAC authentication can be configured at the same time on a port. A total of 256 clients can be configured per port and 16,384 clients on the entire switch, irrespective of the authentication method. After the limit of 16,384 clients is reached, no additional authentication clients are allowed on any port for any method. The default is one client.

MAC authentication, MAC lockout, MACsec, and port security are mutually exclusive on a given port. If you configure any of these authentication methods on a port, you must disable LACP on the port.

How RADIUS server is used in MAC authentication

MAC authentication uses a RADIUS server to temporarily assign a port to a static VLAN to support an authenticated client. During client authentication, the switch port membership is determined according to the following hierarchy:

- A RADIUS-assigned VLAN.
- A static, port-based, untagged VLAN to which the port is configured. A RADIUS-assigned VLAN has priority over switch-port membership in any VLAN.

Supported platforms and standards

Port access is supported on the 4100i, 6000, 6100, 6200, 6300, 6400, 8325, 8360, and 10000 Switch Series.

Scale

Client authentication type	4100i	6000 6100	6200	6300 6400	8325	8360	10000
802.1X authenticated clients per port	32	32	256	256	256	256	256
MAC authenticated clients per port	32	32	256	256	256	256	256
Multiple authenticated clients per system (802.1X or MAC)	736	736	2048	4094	4094	4094	4094

Supported RFCs and standards

- IEEE 2010
- RADIUS (Remote Authentication Dial In User Service) as defined in RFC [2865]
- EAP (Extensible Authentication Protocol) as defined in RFC [3748]

Port access configuration task list

The following example shows the tasks that need to be performed to configure port access.

Note that before enabling 802.1X on the switch, first set up an authentication (RADIUS) server for the switch to use. Identify of the authentication server must be known before the following tasks can be performed.

Port access 802.1X and MAC authentication configuration example

Step 1: Configure the radius server group

The server order defines the priority order.

```
Switch(config)# aaa group server radius AAA-RADIUS
Switch(config-sg)# server tmeswitching1.aaa
Switch(config-sg)# server tmeswitching2.aaa
Switch(config-sg)# server tmeswitching3.aaa
```

Step 2: Configure the DNS server

If you define a FQDN (fully qualified domain name) for the RADIUS server, you must define a DNS server to resolve the name to an IP address:

```
Switch(config)# ip dns domain-name aaa
Switch(config)# ip dns server-address 10.20.10.11
Switch(config)# ip dns server-address 10.20.10.12
```

Step 3: Configure the RADIUS server secret key

```
Switch(config)# radius-server host tmeswitching1.aaa key plaintext admin123
Switch(config)# radius-server host tmeswitching2.aaa key plaintext admin@123
Switch(config)# radius-server host tmeswitching3.aaa key plaintext admin#123
```

Step 4: Configure the Downloadable User Role (DUR) using ClearPass

```
Switch(config)# Switch(config)# radius-server host tmeswitching1.aaa clearpass-
username <USER> clearpass-password plaintext <PASS> vrf <VRF>
```

Step 5: Configure RADIUS server tracking

Configure the tracking:

```
Switch(config)# Switch(config)# radius-server host tmeswitching1.aaa tracking
enable vrf <VRF>Switch(config)# radius-server host tmeswitching1.aaa tracking
enable vrf <VRF>
```

Configure the tracking mode (any or dead-only):

```
Switch(config)# Switch(config)# radius-server host tmeswitching1.aaa tracking-mode
enable vrf <VRF>
```

Step 6: Configure RADIUS dynamic authorization

```
Switch(config)# radius dyn-authorization enable
Switch(config)# radius dyn-authorization client tmeswitching1.aaa secret-key
plaintext admin123
Switch(config)# radius dyn-authorization client tmeswitching2.aaa secret-key
plaintext admin@123
```

Step 7: Configure AAA authentication fail-through

```
Switch(config)# aaa authentication allow-fail-through
```

Step 8: Configure port access authentication on an access port

```
Switch(config)# interface 1/1/1
Switch(config-if)# aaa authentication port-access auth-precedence mac-auth dot1x
Switch(config-if)# aaa authentication port-access client-limit 3
Switch(config-if)# aaa authentication port-access dot1x authenticator
Switch(config-if-dot1x-auth)# cached-reauth
Switch(config-if-dot1x-auth)# cached-reauth-period 60 (default is 30sec)
Switch(config-if-dot1x-auth)# max-eapol-requests 1
Switch(config-if-dot1x-auth)# max-retries 1
Switch(config-if-dot1x-auth)# quiet-period 5
```

```
Switch(config-if-dot1x-auth)# discovery-period 10
Switch(config-if-dot1x-auth)# enable
Switch(config-if-dot1x-auth)# exit
Switch(config-if)#
Switch(config-if)# aaa authentication port-access mac-auth
Switch(config-if-macauth)# enable
Switch(config-if-macauth)# end
Switch# end
```

These commands are available for tuning 802.1X authentication:

- `aaa authentication port-access dot1x authenticator max-eapol-requests`
- `aaa authentication port-access dot1x authenticator max-retries`
- `aaa authentication port-access dot1x authenticator quiet-period`
- `aaa authentication port-access dot1x authenticator discovery-period`

See also:

- [Port access 802.1X authentication commands](#)
- [Port access MAC authentication commands](#)
- [Port access general commands](#)

Use cases

Some port access use cases are as follows.

Use case 1: Faster onboarding of MAC authentication clients using concurrent onboarding

With this default port access authentication precedence configuration, it could take up to 162 seconds to onboard the MAC authentication clients.

```
show running-config interface 1/1/12
interface 1/1/12
no shutdown
no routing
vlan access 1
aaa authentication port-access dot1x authenticator
enable
aaa authentication port-access mac-auth
enable
```

802.1X timers could be tuned to reduce onboarding time, but it could still take 60 seconds to start MAC authentication with the following 802.1X timers configuration. Note that reducing the **eapol-timeout** any further could cause 802.1X to fail in some cases.

```
aaa authentication port-access dot1x authenticator
eapol-timeout 30
max-retries 1
max-eapol-request 1
```

However, with a concurrent onboarding configuration like this, MAC authentication clients can be onboarded quickly.

```
show running-config interface 1/1/12
interface 1/1/12
no shutdown
no routing
vlan access 1
port-access onboarding-method concurrent enable
aaa authentication port-access dot1x authenticator
enable
aaa authentication port-access mac-auth
enable
```

Use case 2: PXE clients that download the supplicant

PXE (Preboot Execution Environment) clients expect the IP address to be assigned within 15 to 20 seconds before continuing the PXE process of connecting to a server to download and install the image and supplicant. With concurrent onboarding, this can be achieved as MAC authentication occurs quickly, gaining access to the PXE network. Once the supplicant is downloaded, the PXE client reboots and starts 802.1X authentication.

Port access 802.1X authentication commands

aaa authentication port-access dot1x authenticator

```
aaa authentication port-access dot1x authenticator {enable | disable}
no aaa authentication port-access dot1x authenticator {enable | disable}
```

Description

Enables or disables 802.1X authentication globally or at the port-level.

The **no** form of the command deletes global 802.1X configuration details and disables 802.1X authentication.

Examples

Enabling 802.1X authentication globally:

```
switch(config)# aaa authentication port-access dot1x authenticator enable
```

Disabling 802.1X authentication globally:

```
switch(config)# aaa authentication port-access dot1x authenticator disable
```

Deleting and disabling global 802.1X authentication:

```
switch(config)# no aaa authentication port-access dot1x authenticator
```

Enabling 802.1X authentication on a port:

```
switch(config-if)# aaa authentication port-access dot1x authenticator enable
```

Disabling 802.1X authentication on a port:

```
switch(config-if)# aaa authentication port-access dot1x authenticator disable
```

Deleting and disabling 802.1X authentication configuration on a port:

```
switch(config-if)# no aaa authentication port-access dot1x authenticator
```

Command History

Release	Modification
10.09	Command introduced on the 8360

Command Information

Platforms	Command context	Authority
8100 8360	config config-if	Administrators or local user group members with execution rights for this command.

aaa authentication port-access dot1x authenticator auth-method

```
aaa authentication port-access dot1x authenticator auth-method eap-radius  
no aaa authentication port-access dot1x authenticator auth-method eap-radius
```

Description

Configures the authentication mechanism used to control access to the network. The configured authentication method will be used to authenticate 802.1X clients.

The **no** form of the command resets the authentication mechanism to the default, **eap-radius**.

Parameter	Description
eap-radius	Specifies the EAP RADIUS as the 802.1X authentication method.

Examples

Enabling the EAP RADIUS 802.1X authentication method on the switch:

```
switch(config)# aaa authentication port-access dot1x authenticator auth-method  
eap-radius
```

Resetting the EAP RADIUS 802.1X authentication method on the switch:

```
switch(config)# no aaa authentication port-access dot1x authenticator auth-method  
eap-radius
```

Command History

Release	Modification
10.09	Command introduced on the 8360

Command Information

Platforms	Command context	Authority
8100 8360	config	Administrators or local user group members with execution rights for this command.

aaa authentication port-access dot1x authenticator cached-reauth

```
aaa authentication port-access dot1x authenticator cached-reauth
no aaa authentication port-access dot1x authenticator cached-reauth
```

Description

Enables cached reauthentication on a port. Cached reauthentication allows 802.1X reauthentications to succeed when the RADIUS server is unavailable. Users already authenticated retain their currently assigned RADIUS attributes.

The **no** form of the command disables the cached reauthentication on a port.

Examples

Enabling cached reauthentication on a port:

```
switch(config-if) # aaa authentication port-access dot1x authenticator cached-
reauth
```

Disabling cached reauthentication on a port:

```
switch(config-if) # no aaa authentication port-access dot1x authenticator cached-
reauth
```

Command History

Release	Modification
10.09	Command introduced on the 8360

Command Information

Platforms	Command context	Authority
8100 8360	config-if	Administrators or local user group members with execution rights for this command.

aaa authentication port-access dot1x authenticator cached-reauth-period

```
aaa authentication port-access dot1x authenticator cached-reauth-period <PERIOD>
```

```
no aaa authentication port-access dot1x authenticator cached-reauth-period
```

Description

Configures the period during which an authenticated client, which has failed to reauthenticate because the RADIUS server is unreachable, remains authenticated.

The **no** form of the command resets the cached reauthentication period to the default, 30 seconds.

Parameter	Description
<code><PERIOD></code>	Specifies the cached reauthentication period (in seconds). Default: 3600. Range: 1 to 4294967295.

Examples

Configuring the cached reauthentication period on a port:

```
switch(config-if)# aaa authentication port-access dot1x authenticator cached-reauth-period 300
```

Resetting the cached reauthentication period to the default value:

```
switch(config-if)# no aaa authentication port-access dot1x authenticator cached-reauth-period
```

Command History

Release	Modification
10.09	Command introduced on the 8360
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
8100 8360	config-if	Administrators or local user group members with execution rights for this command.

aaa authentication port-access dot1x authenticator discovery-period

```
aaa authentication port-access dot1x authenticator discovery-period <PERIOD>  
no aaa authentication port-access dot1x authenticator discovery-period
```

Description

Configures the period the port waits to retransmit the next EAPOL request identity frame on an 802.1X enabled port that has no authenticated clients.

The **no** form of the command resets the discovery period to the default, 30 seconds.

Parameter	Description
<PERIOD>	Specifies the discovery period (in seconds). Default: 30. Range: 1 to 65535.

Examples

Configuring the discovery period on a port:

```
switch(config-if)# aaa authentication port-access dot1x authenticator discovery-period 120
```

Resetting the discovery period to the default value:

```
switch(config-if)# no aaa authentication port-access dot1x authenticator discovery-period
```

Command History

Release	Modification
10.09	Command introduced on the 8360

Command Information

Platforms	Command context	Authority
8100 8360	config-if	Administrators or local user group members with execution rights for this command.

aaa authentication port-access dot1x authenticator eap-tls-fragment

```
aaa authentication port-access dot1x authenticator eap-tls-fragment towards-server <max-fragment-size>
```

```
no aaa authentication port-access dot1x authenticator eap-tls-fragment towards-server
```

Description

Configure the maximum size in bytes of an EAP-TLS fragment encoded in a single RADIUS request packet. The **no** form of the command resets the size to the default value of 3072 bytes.

Examples

Setting the EAP-TLS fragment size for RADIUS request to 1024 bytes:

```
switch(config)# aaa authentication port-access dot1x authenticator eap-tls-fragment towards-server 1024
```

Resetting EAP-TLS fragment size back to the default value of 3072 bytes

```
switch(config-if)# no aaa authentication port-access dot1x authenticator eap-tls-fragment towards-server
```

Command History

Release	Modification
10.11	Command introduced

Command Information

Platforms	Command context	Authority
8100 8360	config-if	Administrators or local user group members with execution rights for this command.

aaa authentication port-access dot1x authenticator eapol-timeout

```
aaa authentication port-access dot1x authenticator eapol-timeout <EAPOL-TIMEOUT>  
no aaa authentication port-access dot1x authenticator eapol-timeout
```

Description

Configure the period the switch waits for a response from a client before retransmitting an EAPOL PDU. If the value is **0**, the time period is calculated as per RFC 2988.



As per RFC 2988 2.1: Before Round-Trip Time (RTT) measurement, set Retransmission Timeout (RTO) to 3 seconds for initial retransmission and then double the RTO to provide back off as per section 5.5. Limit the maximum RTO (RTOmax) to 20 seconds as per section 4.3 of RFC 3748.

The **no** form of the command resets the timeout period to the default.

Parameter	Description
<EAPOL-TIMEOUT>	Specifies the EAPOL timeout period (in seconds). Range: 1 to 65535.

Examples

Configuring EAPOL timeout on a port:

```
switch(config-if)# aaa authentication port-access dot1x authenticator eapol-  
timeout 120
```

Resetting the EAPOL timeout to the default value:

```
switch(config-if)# no aaa authentication port-access dot1x authenticator eapol-  
timeout
```

Command History

Release	Modification
10.09	Command introduced on the 8360

Command Information

Platforms	Command context	Authority
8100 8360	config-if	Administrators or local user group members with execution rights for this command.

aaa authentication port-access dot1x authenticator initial-auth-response-timeout

```
aaa authentication port-access dot1x authenticator
    initial-auth-response-timeout <TIMEOUT>
no aaa authentication port-access dot1x authenticator
    initial-auth-response-timeout [<TIMEOUT>]
```

Description

Configures the period of time (in seconds) the switch waits for the first EAPOL frame from a client before deeming the client to be incapable of 802.1X and therefore attempting the next authentication method, if any. The default is for this timeout to be disabled.

The **no** form of this command disables the timeout.

Parameter	Description
<TIMEOUT>	Specifies the timeout period (in seconds). Range: 1 to 65535.

Examples

Setting a 30 second timeout:

```
switch(config-if)# aaa authentication port-access dot1x authenticator
    initial-auth-response-timeout 30
```

Disabling the timeout:

```
switch(config-if)# no aaa authentication port-access dot1x authenticator
    initial-auth-response-timeout
```

Command History

Release	Modification
10.09	Command introduced on the 8360

Command Information

Platforms	Command context	Authority
8100 8360	config-if	Administrators or local user group members with execution rights for this command.

aaa authentication port-access dot1x authenticator macsec

```
aaa authentication port-access dot1x authenticator macsec
no aaa authentication port-access dot1x authenticator macsec
```

Description

Enables the switch to provision a MACsec channel dynamically when the 802.1X client is authenticated using an EAP method that supports mutual authentication. MACsec is supported in device mode and in client mode with a client limit of one on MACsec-capable ports.



If a MACsec policy is not associated with the role applied to the client on the port with MACsec enabled, a MACsec channel will not be established and the port will be blocked on the data-plane.

The **no** form of the command disables MACsec using EAP on the port.

Examples

Enabling MACsec using EAP on a port:

```
switch(config)# interface 1/1/1
switch(config-if)# aaa authentication port-access dot1x authenticator macsec
OR
switch(config)# interface 1/1/1
switch(config-if)# aaa authentication port-access dot1x authenticator
switch(config-if-dot1x-auth)# macsec
```

Disabling MACsec using EAP on a port:

```
switch(config)# interface 1/1/1
switch(config-if)# no aaa authentication port-access dot1x authenticator macsec
OR
switch(config)# interface 1/1/1
switch(config-if)# aaa authentication port-access dot1x authenticator
switch(config-if-dot1x-auth)# no macsec
```

Command History

Release	Modification
10.10	Command introduced.

Command Information

Platforms	Command context	Authority
8100 8360	config-if config-if-dot1x-auth	Administrators or local user group members with execution rights for this command.

aaa authentication port-access dot1x authenticator max-eapol-requests

```
aaa authentication port-access dot1x authenticator max-eapol-requests <MAX-EAPOL-REQUESTS>
no aaa authentication port-access dot1x authenticator max-eapol-requests
```

Description

Configures the number of EAPOL requests to send to a supplicant that must time out before authentication fails and the authentication session ends.

The **no** form of the command resets the maximum number of EAPOL requests to the default, 5.

Parameter	Description
<MAX-EAPOL-REQUESTS>	Specifies the maximum number of EAPOL requests. Default: 5. Range: 1 to 10.

Examples

Configuring maximum EAPOL requests on a port:

```
switch(config-if) # aaa authentication port-access dot1x authenticator max-eapol-requests 3
```

Resetting the maximum EAPOL requests on a port to default:

```
switch(config-if) # no aaa authentication port-access dot1x authenticator max-eapol-requests
```

Command History

Release	Modification
10.09	Command introduced on the 8360

Command Information

Platforms	Command context	Authority
8100 8360	config-if	Administrators or local user group members with execution rights for this command.

aaa authentication port-access dot1x authenticator mka cak-length

```
aaa authentication port-access dot1x authenticator mka cak-length {16|32}
no aaa authentication port-access dot1x authenticator mka cak-length {16|32}
```

Description

Configures the length of the Connectivity Association Key (CAK) to generate for EAP based MACsec.

The **no** form of this command resets the length to the default value of 32 bytes.

Parameter	Description
{16 32}	Specifies the CAK length. Default: 32.

Examples

Configuring the CAK length to 16 bytes:

```
switch(config)# interface 1/1/1
switch(config-if)# aaa authentication port-access dot1x authenticator mka cak-length 16
OR
switch(config)# interface 1/1/1
switch(config-if)# aaa authentication port-access dot1x authenticator
switch(config-if-dot1x-auth)# mka cak-length 16
```

Configuring the CAK length to default:

```
switch(config)# interface 1/1/1
switch(config-if)# no aaa authentication port-access dot1x authenticator mka cak-length
OR
switch(config)# interface 1/1/1
switch(config-if)# aaa authentication port-access dot1x authenticator
switch(config-if-dot1x-auth)# no mka cak-length
OR
switch(config)# interface 1/1/1
switch(config-if)# aaa authentication port-access dot1x authenticator
switch(config-if-dot1x-auth)# no mka cak-length 16
```

Command History

Release	Modification
10.10.1000	Command introduced.

Command Information

Platforms	Command context	Authority
8100 8360	config-if config-if-dot1x-auth	Administrators or local user group members with execution rights for this command.

aaa authentication port-access dot1x authenticator max-retries

```
aaa authentication port-access dot1x authenticator max-retries <max-retries>
no aaa authentication port-access dot1x authenticator max-retries
```

Description

Configures the maximum number of retries that the switch attempts to authenticate a client on a port before marking the client as unauthenticated.

The **no** form of the command resets the maximum number of retries to the default, 2.

Parameter	Description
<code><max-retries></code>	Indicates the number of authentication attempts. Default: 2. Range: 1 to 10.

Examples

Configuring maximum authentication attempts on a port:

```
switch(config-if) # aaa authentication port-access dot1x authenticator max-retries 5
```

Resetting the maximum authentication attempts on a port to default:

```
switch(config-if) # no aaa authentication port-access dot1x authenticator max-retries
```

Command History

Release	Modification
10.09	Command introduced on the 8360

Command Information

Platforms	Command context	Authority
8100 8360	config-if	Administrators or local user group members with execution rights for this command.

aaa authentication port-access dot1x authenticator quiet-period

```
aaa authentication port-access dot1x authenticator quiet-period <PERIOD>
no aaa authentication port-access dot1x authenticator quiet-period
```

Description

Configures the period during which the port does not try to acquire a supplicant. This period begins after the last authentication attempt, authorized by the maximum retries parameter, fails.

You can configure the number of maximum retries with the **aaa authentication port-access dot1x authenticator max-retries** command.

The **no** form of the command resets the quiet period to the default, 60 seconds.

Parameter	Description
<code><PERIOD></code>	Specifies the quiet period (in seconds). Default: 60. Range: 0 to 65535.

Examples

Configuring quiet period on a port:

```
switch(config-if)# aaa authentication port-access dot1x authenticator quiet-period 100
```

Resetting the quiet period on a port to default:

```
switch(config-if)# no aaa authentication port-access dot1x authenticator quiet-period
```

Command History

Release	Modification
10.09	Command introduced on the 8360

Command Information

Platforms	Command context	Authority
8100 8360	config-if	Administrators or local user group members with execution rights for this command.

aaa authentication port-access dot1x authenticator radius server-group

```
aaa authentication port-access dot1x authenticator radius server-group <GROUP-NAME>  
no aaa authentication port-access dot1x authenticator radius server-group <GROUP_NAME>
```

Description

Configures the switch to use an existing RADIUS server group for 802.1X authentication globally or for a particular port.

The **no** form of the command resets the server group to the default, **radius**.

When configured on a port, the **no** form of the command resets the server group on that port to the globally configured group. If no global RADIUS server group is configured, the **no** form of the command resets the configuration to the default group, **radius**.



When the RADIUS server group for 802.1X authentication is updated on a port, any existing clients on the port that were authenticated using the previous globally configured group will associate with the new group for the port during the next re-authentication cycle. Any new client that is onboarding on the port after the server group update will associate with the new group immediately.

Parameter	Description
<GROUP-NAME>	Specifies the name of the RADIUS server group.

Examples

Configuring the switch to use RADIUS server group **employee**:

```
switch(config)# aaa authentication port-access dot1x authenticator radius server-group employee
```

Resetting RADIUS server group configuration to default:

```
switch(config)# no aaa authentication port-access dot1x authenticator radius server-group
```

Configuring the RADIUS authentication server group on **1/1/1**:

```
switch(config)# interface 1/1/1
switch(config-if)# aaa authentication port-access dot1x authenticator
switch(config-if-dot1x-auth)# radius server-group group2
```

Resetting 802.1X RADIUS server group configuration on **1/1/1**:

```
switch(config)# interface 1/1/1
switch(config-if)# aaa authentication port-access dot1x authenticator
switch(config-if-dot1x-auth)# no radius server-group
```

Command History

Release	Modification
10.12	Command is now configurable on a port
10.09	Command introduced on the 8360

Command Information

Platforms	Command context	Authority
8100 8360	config config-dot1x-auth config-if-dot1x-auth	Administrators or local user group members with execution rights for this command.

aaa authentication port-access dot1x authenticator reauth

```
aaa authentication port-access dot1x authenticator reauth
no aaa authentication port-access dot1x authenticator reauth
```

Description

Enables periodic reauthentication of authenticated clients on the port.
The **no** form of the command disables periodic reauthentication.

Examples

Enabling periodic reauthentication on a port:

```
switch(config-if)# aaa authentication port-access dot1x authenticator reauth
```

Disabling periodic reauthentication on a port:

```
switch(config-if)# no aaa authentication port-access dot1x authenticator reauth
```

Command History

Release	Modification
10.09	Command introduced on the 8360

Command Information

Platforms	Command context	Authority
8100 8360	config-if	Administrators or local user group members with execution rights for this command.

aaa authentication port-access dot1x authenticator reauth-period

```
aaa authentication port-access dot1x authenticator reauth-period <PERIOD>  
no aaa authentication port-access dot1x authenticator reauth-period
```

Description

Configures the period after which the authenticated clients are reauthenticated on the port. You must enable reauthentication on the port before configuring the reauthentication period.

The **no** form of the command resets the reauthentication period to the default, 3600 seconds.

Parameter	Description
<PERIOD>	Specifies the reauthentication period (in seconds). Default: 3600. Range: 1 to 4294967295.

Examples

Configuring reauthentication period on a port:

```
switch(config-if)# aaa authentication port-access dot1x authenticator reauth-  
period 100
```

Resetting the reauthentication period to the default value:

```
switch(config-if)# no aaa authentication port-access dot1x authenticator reauth-  
period
```

Command History

Release	Modification
10.09	Command introduced on the 8360

Command Information

Platforms	Command context	Authority
8100 8360	config-if	Administrators or local user group members with execution rights for this command.

clear dot1x authenticator statistics interface

```
clear dot1x authenticator statistics [interface <IF-NAME>]
```

Description

Clears the 802.1X authentication statistics associated with the port and all the authenticator clients attached to this port.

If no interface is specified, the statistics is cleared for all 802.1X enabled ports.

Parameter	Description
<IF-NAME>	Specifies the interface name.

Examples

Clearing authentication statistics on a port:

```
switch# clear dot1x authenticator statistics interface 1/1/1
```

Clearing authentication statistics on a port:

Clearing authentication statistics on all ports:

```
switch# clear dot1x authenticator statistics
```

Command History

Release	Modification
10.09	Command introduced on the 8360

Command Information

Platforms	Command context	Authority
8100 8360	Manager (#)	Administrators or local user group members with execution rights for this command.

show aaa authentication port-access dot1x authenticator interface client-status

```
show aaa authentication port-access dot1x authenticator interface {all|<IF-NAME>}  
client-status [mac <MAC-ADDRESS>]
```

Description

Shows information about active 802.1X authentication sessions. The output can be filtered by interface or MAC address.

Parameter	Description
all	Specifies all interfaces.
<IF-NAME>	Specifies the interface name.
<MAC-ADDRESS>	Specifies the client MAC address.

Examples

Showing client status information for all ports.

```
switch# show aaa authentication port-access dot1x authenticator interface all  
client-status
```

```
Client  FE:04:D7:50:89:37, johndoe, 1/1/1  
=====
```

Authentication Details

```
-----  
Status           : Authenticated  
Type             : Pass-Through  
EAP-Method       : MD5  
Time Since Last State Change : 10s
```

Authentication Statistics

```
-----  
Authentication           : 0  
Authentication Timeout   : 0  
EAP-Start While Authenticating : 0  
EAP-Logoff While Authenticating : 0  
Successful Authentication : 0  
Failed Authentication     : 0  
Re-Authentication        : 0  
Successful Re-Authentication : 0  
Failed Re-Authentication  : 0  
EAP-Start When Authenticated : 0  
EAP-Logoff When Authenticated : 0  
Re-Auths When Authenticated : 0  
Cached Re-Authentication  : 0
```

```
Client  9A:B4:59:97:D0:7E, janedoe, 1/1/1  
=====
```

Authentication Details

```
-----  
Status           : Authenticated  
Type             : Pass-Through  
EAP-Method       : TLS  
Time Since Last State Change : 5s
```

Authentication Statistics

```
-----  
Authentication           : 0  
Authentication Timeout   : 0  
EAP-Start While Authenticating : 0
```

```
EAP-Logoff While Authenticating      : 0
Successful Authentication             : 0
Failed Authentication                 : 0
Re-Authentication                     : 0
Successful Re-Authentication          : 0
Failed Re-Authentication              : 0
EAP-Start When Authenticated          : 0
EAP-Logoff When Authenticated         : 0
Re-Auths When Authenticated           : 0
Cached Re-Authentication              : 0
```

Command History

Release	Modification
10.09	Command introduced on the 8360

Command Information

Platforms	Command context	Authority
8100 8360	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show aaa authentication port-access dot1x authenticator interface port-statistics

show aaa authentication port-access dot1x authenticator interface {all|<IF-NAME>} port-statistics

Description

Shows information about 802.1X ports. The output can be filtered by interface.

Parameter	Description
all	Specifies all interfaces.
<IF-NAME>	Specifies the interface name.

Examples

Showing information for all ports.

```
switch# show aaa authentication port-access dot1x authenticator interface all
port-statistics

Port 1/1/1
=====

Client Details
-----
  Number of Clients           : 1
  Number of Authenticated Clients : 1
```

```
Number of Unauthenticated Clients : 0
Number of authenticating clients : 0
```

Statistics

```
EAPOL Frames Received           : 4
EAPOL Frames Transmitted         : 3
EAPOL Start Frames Received      : 1
EAPOL Logoff Frames Received     : 0
EAPOL Response ID Frames Received : 2
EAPOL Response Frames Received   : 1
EAPOL Request ID Frames Transmitted : 2
EAPOL Request Frames Transmitted : 1
EAPOL Invalid Frames Received    : 0
EAPOL EAP Length Error Frames Received : 0
EAPOL Last Received Frame Version : 0
EAPOL Last Received Frame Client MAC : 0
```

Port 1/1/2

=====

Client Details

```
Number of Clients                : 1
Number of Authenticated Clients  : 1
Number of Unauthenticated Clients : 0
```

Statistics

```
EAPOL Frames Received           : 4
EAPOL Frames Transmitted         : 3
EAPOL Start Frames Received      : 1
EAPOL Logoff Frames Received     : 0
EAPOL Response ID Frames Received : 2
EAPOL Response Frames Received   : 1
EAPOL Request ID Frames Transmitted : 2
EAPOL Request Frames Transmitted : 1
EAPOL Invalid Frames Received    : 0
EAPOL EAP Length Error Frames Received : 0
EAPOL Last Received Frame Version : 0
EAPOL Last Received Frame Client MAC : 0
```

Command History

Release	Modification
10.09	Command introduced on the 8360

Command Information

Platforms	Command context	Authority
8100 8360	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

Port access MAC authentication commands

aaa authentication port-access allow-lldp-auth [mac {source-mac|chassis-mac}]

```
aaa authentication port-access allow-lldp-auth [mac {source-mac|chassis-mac}]  
[no] aaa authentication port-access allow-lldp-auth [mac {source-mac|chassis-mac}]
```

Description

By default authentication is allowed via LLDP packets which are received on the port. Use the **no** version of this command to prevent authentication using LLDP packets received on the port. Chassis MAC and Source MAC addresses can be used for authentication via LLDP frames.

Examples

Configuring authentication via LLDP packets:

```
switch(config)# interface 1/1/1  
switch(config-if)# aaa authentication port-access allow-lldp-auth  
< pd platform="4100i,6000,6100,6200,6300,6400,8100,8360" >  
switch(config)# interface lag 1  
switch(config-lag-if)# aaa authentication port-access allow-lldp-auth  
< /pd >
```

Enabling authentication via LLDP packets on a MAC source:

```
switch(config)# interface 1/1/1  
switch(config-if)# aaa authentication port-access allow-lldp-auth mac  
source-mac  
  
switch(config-if)# aaa authentication port-access allow-lldp-auth mac  
chassis-mac
```

Enabling authentication via LLDP BDU packets:

```
switch(config-if)# aaa authentication port-access  
allow-lldp-auth Allow or block authentication on LLDP BDU. (Default:  
allow)  
  
switch(config-if)# no aaa authentication port-access  
allow-lldp-auth Allow or block authentication on LLDP BDU. (Default:  
allow)  
  
switch(config-if)# aaa authentication port-access allow-lldp-auth  
switch(config-if)# no aaa authentication port-access allow-lldp-auth
```

Configuring MAC via LLDP packets:

```
switch(config-if)# aaa authentication port-access allow-lldp-auth  
mac Configure the MAC to use for LLDP based authentication (Default: chassis-  
mac)  
  
switch(config-if)# aaa authentication port-access allow-lldp-auth mac  
chassis-mac Use the chassis MAC in LLDP TLV.  
source-mac Use the source MAC in the LLDP frame.
```

Disabling authentication via LLDP packets on a MAC source:

```
switch(config-if)# no aaa authentication port-access allow-lldp-auth mac
chassis-mac      Use the chassis MAC in LLDP TLV.
source-mac       Use the source MAC in the LLDP frame.
```

Command History

Release	Modification
10.13	Command introduced

Command Information

Platforms	Command context	Authority
8100 8360	config-if	Administrators or local user group members with execution rights for this command.

aaa authentication port-access mac-auth

```
aaa authentication port-access mac-auth {enable | disable}
no aaa authentication port-access mac-auth {enable | disable}
```

Description

Enables or disables MAC authentication globally or at the port-level.

Examples

Enabling MAC authentication on all interfaces:

```
switch(config)# aaa authentication port-access mac-auth
switch(config-macauth)# enable
```

Disabling MAC authentication on all interfaces:

```
switch(config)# aaa authentication port-access mac-auth
switch(config-macauth)# disable
```

Enabling MAC authentication on an interface:

```
switch(config-if)# aaa authentication port-access mac-auth
switch(config-if-macauth)# enable
```

Disabling MAC authentication on an interface:

```
switch(config-if)# aaa authentication port-access mac-auth
switch(config-if-macauth)# disable
```

Command History

Release	Modification
10.09	Command introduced on the 8360

Command Information

Platforms	Command context	Authority
8100 8360	config config-if	Administrators or local user group members with execution rights for this command.

aaa authentication port-access mac-auth addr-format

```
aaa authentication port-access mac-auth addr-format {no-delimiter | single-dash |
multi-dash | multi-colon | no-delimiter-uppercase | single-dash-uppercase |
multi-dash-uppercase | multi-colon-uppercase}
no aaa authentication port-access mac-auth addr-format {no-delimiter | single-dash |
multi-dash | multi-colon | no-delimiter-uppercase | single-dash-uppercase |
multi-dash-uppercase | multi-colon-uppercase}
```

Description

Configures the MAC address format that the switch must use in the RADIUS request message. The **no** form of the command resets the MAC address format to the default, **no-delimiter**.

Examples

Setting the MAC address format on the switch:

```
switch(config)# aaa authentication port-access mac-auth
switch(config-macauth)# addr-format single-dash
```

Resetting the MAC address format on the switch to its default:

```
switch(config)# aaa authentication port-access mac-auth
switch(config-macauth)# no addr-format
```

Command History

Release	Modification
10.09	Command introduced on the 8360

Command Information

Platforms	Command context	Authority
8100 8360	config	Administrators or local user group members with execution rights for this command.

aaa authentication port-access mac-auth auth-method

```
aaa authentication port-access mac-auth auth-method {chap | pap}
```

```
no aaa authentication port-access mac-auth auth-method
```

Description

Configures the RADIUS authentication method for MAC authentication.
Following are the MAC authentication methods supported:

- CHAP
- PAP



The PEAP-MSCHAPv2 method of authentication is not supported.

The **no** form of the command resets the authentication method to the default, **chap**.

Examples

Configuring the RADIUS authentication method on the switch:

```
switch# config
switch(config)# aaa authentication port-access mac-auth
switch(config-macauth)# auth-method pap
```

Resetting the RADIUS authentication method on the switch:

```
switch(config)# no aaa authentication port-access mac-auth auth-method
```

Command History

Release	Modification
10.09	Command introduced on the 8360

Command Information

Platforms	Command context	Authority
8100 8360	config	Administrators or local user group members with execution rights for this command.

aaa authentication port-access mac-auth cached-reauth

```
aaa authentication port-access mac-auth cached-reauth
no aaa authentication port-access mac-auth cached-reauth
```

Description

Enables cached reauthentication on a port. Cached reauthentication allows MAC reauthentications to succeed when the RADIUS server is unavailable. Users who are already authenticated, retain their currently assigned RADIUS attributes.

The **no** form of the command disables cached reauthentication.

Examples

Enabling cached reauthentication on a port:

```
switch(config-if)# aaa authentication port-access mac-auth  
switch(config-if-macauth)# cached-reauth
```

Disabling cached reauthentication on a port:

```
switch(config-if)# aaa authentication port-access mac-auth  
switch(config-if-macauth)# no cached-reauth
```

Command History

Release	Modification
10.09	Command introduced on the 8360

Command Information

Platforms	Command context	Authority
8100 8360	config-if	Administrators or local user group members with execution rights for this command.

aaa authentication port-access mac-auth cached-reauth-period

```
aaa authentication port-access mac-auth cached-reauth-period <PERIOD>  
no aaa authentication port-access mac-auth cached-reauth-period
```

Description

Configures the period during which an authenticated client, which has failed to reauthenticate because the RADIUS server is unreachable, remains authenticated.

The **no** form of the command resets the cached reauthentication period to the default, 3600 seconds.

Parameter	Description
<PERIOD>	Specifies the cached reauthentication period (in seconds). Default: 3600. Range: 1 to 4294967295.

Examples

Configuring cached reauthentication period on a port:

```
switch(config-if)# aaa authentication port-access mac-auth  
switch(config-if-macauth)# cached-reauth-period 300
```

Resetting the cached reauthentication period to the default value:

```
switch(config-if)# aaa authentication port-access mac-auth  
switch(config-if-macauth)# no cached-reauth-period
```

Command History

Release	Modification
10.09	Command introduced on the 8360

Command Information

Platforms	Command context	Authority
8100 8360	config-if	Administrators or local user group members with execution rights for this command.

aaa authentication port-access mac-auth password

```
aaa authentication port-access mac-auth password {plaintext|ciphertext}<PASSWORD>  
no aaa authentication port-access mac-auth password
```

Description

Enables and configures the global password that the switch must use for MAC authentication. The password can be either in ciphertext or plaintext format.

The **no** form of the command disables the password for MAC authentication.

Parameter	Description
{plaintext ciphertext}<PASSWORD>	Specifies the global password to be used by all MAC authenticating devices in either plaintext or ciphertext format.

Examples

Setting the MAC authentication password:

```
switch(config)# aaa authentication port-access mac-auth  
switch(config-macauth)# password plaintext maX99J#
```

Disabling the MAC authentication password:

```
switch(config)# aaa authentication port-access mac-auth  
switch(config-macauth)# no password
```

Command History

Release	Modification
10.09	Command introduced on the 8360
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
8100 8360	config	Administrators or local user group members with execution rights for this command.

aaa authentication port-access mac-auth quiet-period

```
aaa authentication port-access mac-auth quiet-period <PERIOD>
no aaa authentication port-access mac-auth quiet-period
```

Description

Configures the period during which the switch does not try to authenticate a rejected client. The **no** form of the command resets the quiet period to the default, 60 seconds.

Parameter	Description
<PERIOD>	Specifies the quiet period (in seconds). Default: 60. Range: 0 to 65535.

Examples

Configuring the quiet period on a port:

```
switch(config-if)# aaa authentication port-access mac-auth
switch(config-if-macauth)# quiet-period 65
```

Resetting the quiet period on a port to default:

```
switch(config-if)# aaa authentication port-access mac-auth
switch(config-if-macauth)# no quiet-period
```

Command History

Release	Modification
10.09	Command introduced on the 8360

Command Information

Platforms	Command context	Authority
8100 8360	config-if	Administrators or local user group members with execution rights for this command.

aaa authentication port-access mac-auth radius server-group

```
aaa authentication port-access mac-auth radius server-group <GROUP-NAME>
no aaa authentication port-access mac-auth radius server-group <GROUP-NAME>
```

Description

Configures the MAC authentication server group globally or for a particular port.

The **no** form of the command resets the authentication server group to the default value, **radius**. When configured on a port, the **no** form of the command resets the server group on that port to the globally configured group. If no global RADIUS server group is configured, the **no** form of the command resets the configuration to the default group, **radius**.



When the RADIUS server group for MAC authentication is updated on a port, any existing clients on the port that were authenticated using the previous globally configured group will associate with the new group for the port during the next re-authentication cycle. Any new client that is onboarding on the port after the server group update will associate with the new group immediately.

Parameter	Description
<i><GROUP-NAME></i>	Specifies the name of the MAC authentication server group.

Examples

Configuring the RADIUS server group for MAC authentication globally:

```
switch# config
switch(config)# aaa authentication port-access mac-auth
switch(config-macauth)# radius server-group group1
```

Configuring the RADIUS server group for MAC authentication on **1/1/5**:

```
switch(config)# interface 1/1/5
switch(config-if)# aaa authentication port-access mac-auth
switch(config-if-macauth)# radius server-group group2
```

Resetting the RADIUS server group configuration on **1/1/5**:

```
switch(config)# interface 1/1/5
switch(config-if)# aaa authentication port-access mac-auth
switch(config-if-macauth)# no radius server-group
```

Command History

Release	Modification
10.12	Command is now configurable on a port
10.09	Command introduced on the 8360

Command Information

Platforms	Command context	Authority
8100 8360	config config-macauth config-if-macauth	Administrators or local user group members with execution rights for this command.

aaa authentication port-access mac-auth reauth

```
aaa authentication port-access mac-auth reauth
no aaa authentication port-access mac-auth reauth
```

Description

Enables periodic MAC reauthentication of authenticated clients on the port.

The **no** form of the command disables periodic MAC reauthentication on the port.

Examples

Enabling reauthentication on a port:

```
switch(config-if)# aaa authentication port-access mac-auth
switch(config-if-macauth)# reauth
```

Disabling reauthentication on a port:

```
switch(config-if)# aaa authentication port-access mac-auth
switch(config-if-macauth)# no reauth
```

Command History

Release	Modification
10.09	Command introduced on the 8360

Command Information

Platforms	Command context	Authority
8100 8360	config-if	Administrators or local user group members with execution rights for this command.

aaa authentication port-access mac-auth reauth-period

```
aaa authentication port-access mac-auth reauth-period <PERIOD>
no aaa authentication port-access mac-auth reauth-period
```

Description

Configures the period after which MAC authenticated clients must be reauthenticated on the port. You must first enable MAC reauthentication on the port before configuring the MAC reauthentication period.

The **no** form of the command resets the MAC reauthentication period to the default, 3600 seconds.

Parameter	Description
<PERIOD>	Specifies the MAC reauthentication period (in seconds). Default: 3600. Range: 1 to 4294967295.

Examples

Configuring the MAC reauthentication period on a port:

```
switch(config-if)# aaa authentication port-access mac-auth
switch(config-if-macauth)# reauth-period 60
```

Resetting the MAC reauthentication period to its default:

```
switch(config-if)# aaa authentication port-access mac-auth
switch(config-if-macauth)# no reauth-period
```

Command History

Release	Modification
10.09	Command introduced on the 8360

Command Information

Platforms	Command context	Authority
8100 8360	config-if	Administrators or local user group members with execution rights for this command.

clear mac-auth statistics

```
clear mac-auth statistics [interface <IF-NAME>]
```

Description

Clears the MAC authentication statistics associated with the port and all the authenticator state machines associated to this port.

If no interface is specified, the statistics is cleared for all MAC authentication enabled ports.

Parameter	Description
<IF-NAME>	Specifies the interface name.

Examples

Clearing MAC authentication statistics on a port:

```
switch# clear mac-auth statistics interface 1/1/1
```

Clearing MAC authentication statistics on all ports:

```
switch# clear mac-auth statistics
```

Command History

Release	Modification
10.09	Command introduced on the 8360

Command Information

Platforms	Command context	Authority
8100 8360	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show aaa authentication port-access mac-auth interface client-status

```
show aaa authentication port-access mac-auth interface {all|<IF-NAME>}  
client-status [mac <MAC-ADDRESS>]
```

Description

Shows information about MAC authentication clients status. The output can be filtered by interface or MAC address.

Parameter	Description
all	Specifies all interfaces.
<IF-NAME>	Specifies the interface name.
<MAC-ADDRESS>	Specifies the client MAC address.

Examples

Showing client status information for all ports:

```
switch# show aaa authentication port-access mac-auth interface all client-status  
  
Port Access Client Status Details  
  
Client AB:CD:DE:FF:AA:BB, 1/1/1  
=====
```

Authentication Details	

Status	: Authenticated
Type	: Pass-Through
Auth-Method	: CHAP
Time Since Last State Change	: 10 secs

```
Authentication Statistics  
-----  
Authentication : 1  
Authentication Timeout : 0  
Successful Authentication : 1  
Failed Authentication : 0  
Re-Authentication : 0  
Successful Re-Authentication : 0  
Failed Re-Authentication : 0  
Re-Auths When Authenticated : 0  
Cached Re-Authentication : 0  
  
Client DD:CD:AB:CS:EE:OI, 1/1/2  
=====
```

```

Authentication Details
-----
Status                : Unauthenticated
Type                  : Pass-Through
Auth-Method           : CHAP
Auth Failure reason    : Server reject/ Server timeout
Time Since Last State Change : 15 secs

Authentication Statistics
-----
Authentication          : 1
Authentication Timeout  : 0
Successful Authentication : 0
Failed Authentication   : 1
Re-Authentication       : 0
Successful Re-Authentication : 0
Failed Re-Authentication : 0
Re-Auths When Authenticated : 0
Cached Re-Authentication : 0

```

Showing status information for a client:

```

switch# show aaa authentication port-access mac-auth interface 1/1/1 client-status
mac ab:cd:de:ff:aa:bb

Port Access Client Status Details

Client AB:CD:DE:FF:AA:BB, 1/1/1
=====
Authentication Details
-----
Status                : Authenticated
Type                  : Pass-Through
Auth-Method           : CHAP
Time Since Last State Change : 10 secs

Authentication Statistics
-----
Authentication          : 1
Authentication Timeout  : 0
Successful Authentication : 1
Failed Authentication   : 0
Re-Authentication       : 0
Successful Re-Authentication : 0
Failed Re-Authentication : 0
Re-Auths When Authenticated : 0
Cached Re-Authentication : 0

```

Command History

Release	Modification
10.09	Command introduced on the 8360

Command Information

Platforms	Command context	Authority
8100 8360	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show aaa authentication port-access mac-auth interface port-statistics

show aaa authentication port-access mac-auth interface {all|<IF-NAME>} port-statistics

Description

Shows information about MAC authentication ports. The output can be filtered by interface.

Parameter	Description
all	Specifies all interfaces.
<IF-NAME>	Specifies the interface name.

Examples

Showing information for all ports.

```
switch# show aaa authentication port-access mac-auth interface all port-statistics

Port 1/1/1
=====

Client Details
-----
Number of Clients           : 3
Number of authenticated clients : 2
Number of unauthenticated clients : 1
Number of authenticating clients : 0

Port 1/1/2
=====

Client Details
-----
Number of Clients           : 4
Number of authenticated clients : 2
Number of unauthenticated clients : 2
Number of authenticating clients : 0
```

Command History

Release	Modification
10.09	Command introduced on the 8360

Command Information

Platforms	Command context	Authority
8100 8360	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

Port access general commands

aaa authentication port-access allow-lldp-auth

```
aaa authentication port-access allow-lldp-auth [mac chassis-mac|source-mac]
no aaa authentication port-access allow-lldp-auth [mac chassis-mac|source-mac]
```

Description

This command is an extension of **aaa authentication port-access allow-lldp-auth**.

By default, authentication on chassis-mac is allowed via LLDP packets which are received on the port. Use the Chassis MAC shown in the LLDP TLV or the source MAC in the LLDP frame.

Use the **no** version of this command to prevent authentication using LLDP packets received on the port. This command can be issued from the interface (**config-if**) or Link Aggregation Group (**config-lag-if**) contexts along with the following commands:

```
interface lag 1
    aaa authentication port access
allow-lldp-bpdu
    aaa authentication port access
allow-lldp-auth mac source-mac
```

Parameter	Description
mac	(Optional) Specify the LLDP authentication-mac type.
chassis-mac	Configure LLDP authentication-mac type as a chassis MAC address. This is the default value.
source-mac	Configure LLDP authentication-mac type as an interface MAC address

Examples

Configuring authentication via LLDP packets:

```
switch(config)# interface 1/1/1
switch(config-if)# aaa authentication port-access allow-lldp-auth
switch(config)# interface lag 1
switch(config-lag-if)# aaa authentication port-access allow-lldp-auth
```

Enabling/disabling authentication via LLDP BPDU packets:

```
switch(config-if)# aaa authentication port-access
allow-lldp-auth Allow or block authentication on LLDP BPDU. (Default:
allow)
```

```
switch(config-if)# no aaa authentication port-access
allow-lldp-auth Allow or block authentication on LLDP BPDU. (Default:
allow)
switch(config-if)# aaa authentication port-access allow-lldp-auth
switch(config-if)# no aaa authentication port-access allow-lldp-auth

switch(config-if)# aaa authentication port-access
block-lldp-auth Allow or block authentication on LLDP BPDU. (Default:
block)
switch(config-if)# no aaa authentication port-access
block-lldp-auth Allow or block authentication on LLDP BPDU. (Default:
block)
```

Configuring the MAC to use for authentication:

```
switch(config)# interface 1/1/1
switch(config-if)# aaa authentication port-access allow-lldp-auth mac source-mac
switch(config-if)# aaa authentication port-access allow-lldp-auth mac chassis-mac
```

```
switch(config-if)# aaa authentication port-access allow-lldp-auth
mac Configure the MAC to use for LLDP based authentication (Default:
chassismac)

switch(config-if)# aaa authentication port-access allow-lldp-auth mac
chassis-mac Use the chassis MAC in LLDP TLV.
source-mac Use the source MAC in the LLDP frame.
```

Disabling authentication via LLDP packets based on MAC source:

```
switch(config-if)# no aaa authentication port-access allow-lldp-auth mac
chassis-mac Use the chassis MAC in LLDP TLV.
source-mac Use the source MAC in the LLDP frame.
```

Disabling authentication via LLDP packets on a LAG port:

```
switch (config) interface lag 1
switch(config-lag if)# no aaa authentication port-access allow-lldp-auth
```



When a client such as dual-homed access points and switches, connects to the switch over multiple physical interfaces and use LLDP packets to onboard, it is recommended to use LLDP authentication MAC as the source MAC on the interfaces. This prevents the switch from learning the client MAC from the chassis MAC in the LLDP TLV (default), similarly to the LLDP BPDUs received on all interfaces connected to the same device. If the MAC learned is the chassis MAC, it will cause the switch to treat the client as moving between the different interfaces each time a LLDP BPDU is received on an interface. Additionally, using a different LLDP authentication MAC type on interfaces connecting to the same device may lead to undesired behavior.

Command History

Release	Modification
10.13	This command can be issued from a Link Aggregation Group (LAG) context.
10.09	Command introduced

Command Information

Platforms	Command context	Authority
8100 8360	config-if config-lag-if	Administrators or local user group members with execution rights for this command.

aaa authentication port-access allow-cdp-auth

```
aaa authentication port-access allow-cdp-auth
no aaa authentication port-access allow-cdp-auth
```

Description

By default authentication is allowed via CDP packets which are received on the port. Use the **no** version of this command to prevent authentication using CDP packets received on the port. This command can be issued from the interface (**config-if**) or Link Aggregation Group (**config-lag-if**) contexts.

Examples

Disabling authentication via CDP packets:

```
switch(config-if)# no aaa authentication port-access allow-cdp-auth
```

Command History

Release	Modification
10.13	This command can be issued on a LAG port
10.09	Command introduced

Command Information

Platforms	Command context	Authority
8100 8360	config-if config-lag-if	Administrators or local user group members with execution rights for this command.

aaa authentication port-access auth-mode

```
aaa authentication port-access auth-mode {client-mode | device-mode | multi-domain}
```

Description

Configures the authentication mode for the port. By default, client mode is enabled. This command can be issued from the interface (**config-if**) or Link Aggregation Group (**config-lag-if**) contexts.

Parameter	Description
client-mode	Selects client mode. In this mode, all clients connecting to the port are sent for authentication. The maximum number of clients allowed to connect to the port is limited by the client limit value configured with the aaa authentication port-access client-limit command.
device-mode	Selects device mode. In this mode, only the first client connecting to the port is sent for authentication. Once this client is authenticated, the port is considered as open and all subsequent clients trying to connect on that port are not sent for authentication.
multi-domain	Selects multidomain mode. In this mode only one voice device is allowed to be authenticated in addition to the configured data devices on a port. By default only one data device is allowed to be authenticated on the multidomain mode along with one voice device. You can configure the maximum number of data devices allowed with the aaa authentication port-access client-limit multi-domain command. If a second voice device or a data device greater than the configured data client limit onboards, a violation is triggered. You must configure a voice VLAN for IP phones to onboard a voice device in the multidomain authentication mode. To authorize a voice device, you must perform one of the following: - Configure the AAA server to send the Aruba-Device-Traffic-Class Aruba VSA with value 1. - Configure the device-traffic-class parameter in the role to be applied to indicate a voice device. Without this VSA value or the device type in the role, the switch considers the voice device as a data device. NOTE: This parameter is not supported when the command is issued from the LAG (config-lag-if) context.

Examples

Configuring device mode authentication for interface 1/1/1:

```
switch(config)# interface 1/1/1
switch(config-if)# aaa authentication port-access auth-mode device-mode
```

Configuring device mode authentication for a LAG port:

```
switch(config)# interface lag 1
switch(config-lag if)# aaa authentication port-access auth-mode device-mode
```

Configuring multidomain mode authentication for a port:

```
switch(config)# interface 1/1/1
switch(config-if)# aaa authentication port-access auth-mode multi-domain
```

Command History

Release	Modification
10.13	This command can be issued from a Link Aggregation Group (LAG) context.
10.09	Command introduced on the 8360

Command Information

Platforms	Command context	Authority
8100 8360	config-if config-lag-if	Administrators or local user group members with execution rights for this command.

aaa authentication port-access auth-precedence

```
aaa authentication port-access auth-precedence [dot1x mac-auth | mac-auth dot1x]
no aaa authentication port-access auth-precedence [dot1x mac-auth | mac-auth dot1x]
no aaa authentication port-access auth-precedence
```

Description

Configures the per port authentication precedence using the space separator.

By default, 802.1X authentication (**dot1x**) takes a higher precedence than MAC authentication (**mac-auth**).

The **no** form of the command resets the port access authentication precedence to the default, 802.1X authentication followed by MAC authentication.

Parameter	Description
dot1x mac-auth	Specifies that the port access authentication precedence is 802.1X authentication followed by MAC authentication.
mac-auth dot1x	Specifies that the port access authentication precedence is MAC authentication followed by 802.1X authentication.

Examples

Configuring MAC authentication precedence on a port:

```
switch(config-if)# aaa authentication port-access auth-precedence mac-auth dot1x
```

Resetting the authentication precedence to the default value:

```
switch(config-if)# no aaa authentication port-access auth-precedence mac-auth dot1x
```

Command History

Release	Modification
10.09	Command introduced on the 8360

Command Information

Platforms	Command context	Authority
8100 8360	config-if	Administrators or local user group members with execution rights for this command.

aaa authentication port-access auth-priority

```
aaa authentication port-access auth-priority [dot1x mac-auth | mac-auth dot1x]
no aaa authentication port-access auth-priority [dot1x mac-auth | mac-auth dot1x]
no aaa authentication port-access auth-priority
```

Description

Configures the authentication priority using the space separator to specific interface.

Default **auth-priority** with concurrent onboarding is 802.1X followed by MAC authentication. With authentication precedence, the default **auth-priority** follows the **auth-precedence** order.

The **no** form of the command resets the port access authentication priority to the default, is same as the configured **auth-precedence** order.

The authentication priority is useful in deployments where clients such as wireless access points (APs), IT-compliant-laptops or phones, or laptops without pre-loaded supplicant software must download the supplicant software or firmware patches before attempting 802.1X authentication. In such cases, configure the MAC authentication as the primary authentication method followed by 802.1X for the authentication order. Meanwhile, configure 802.1X as the primary authentication priority and MAC authentication as secondary to enforce access based on 802.1X. Thus the client (or end access device) will initially be authenticated by MAC authentication with the access required to onboard and install the software or patches, and subsequently attempt the 802.1X authentication.

Reauthentication will be triggered for all high priority methods and not just the final successful authentication method.

Parameter	Description
dot1x mac-auth	Specifies that the port access authentication precedence is 802.1X authentication followed by MAC authentication.
mac-auth dot1x	Specifies that the port access authentication precedence is MAC authentication followed by 802.1X authentication.

Examples

Configuring MAC authentication priority on a port:

```
switch(config-if)# aaa authentication port-access auth-priority mac-auth dot1x
```

Resetting the authentication priority to the default value:

```
switch(config-if)# no aaa authentication port-access auth-priority mac-auth dot1x
switch(config-if)# no aaa authentication port-access auth-priority
```

Sample configuration:

```

interface 1/1/1
  no shutdown
  no routing
  vlan access 1
  aaa authentication port-access auth-precedence mac-auth dot1x
  aaa authentication port-access auth-priority dot1x mac-auth

```

Command History

Release	Modification
10.09	Command introduced on the 8360

Command Information

Platforms	Command context	Authority
8100 8360	config-if	Administrators or local user group members with execution rights for this command.

aaa authentication port-access auth-role

```

aaa authentication port-access [critical-role|preauth-role|reject-role|
  auth-role|critical-voice-role] <ROLE-NAME>
no aaa authentication port-access [critical-role|preauth-role|reject-role|
  auth-role|critical-voice-role]

```

Description

Configures the role to assign to the clients depending on the client authentication state.

The **no** form of the command disassociates the roles that you assign to clients based on the authentication state.

Parameter	Description
critical-role	Specifies the role that is applied when the RADIUS server is unreachable for authentication or when there is a request timeout.
preauth-role	Specifies the role that is applied when authentication is still in progress.
reject-role	Specifies the role that is applied when authentication has failed.
auth-role	Specifies the role that is applied to authenticated clients when a specific role is not assigned in the RADIUS server.
critical-voice-role	Specifies the role for a voice client when the RADIUS server is unreachable for authentication during reauthentication period. This is applicable when multidomain authentication mode is enabled with the aaa authentication port-access auth-mode command.
<ROLE-NAME>	Specifies the role name.

Examples

Configuring critical role for clients:

```
switch(config-if)# aaa authentication port-access critical-role role1
```

Command History

Release	Modification
10.09	Command introduced on the 8360

Command Information

Platforms	Command context	Authority
8100 8360	config-if	Administrators or local user group members with execution rights for this command.

aaa authentication port-access client-auto-log-off final-authentication-failure

```
aaa authentication port-access client-auto-log-off final-authentication-failure
no aaa authentication port-access client-auto-log-off final-authentication-failure
```

Description

Use this command to automatically remove a client when authentication fails due to any reason except **server-reject** or **server-timeout**. This feature is disabled by default.

The **no** form of this command disables this feature if it has been previously enabled.



Automatic client log-off is not supported on Layer-3 interfaces.

Examples

Configuring the client-auto-log-off feature on interface 1/1/1:

```
switch(config)# interface 1/1/1
switch(config-if)# aaa authentication port-access client-auto-log-off final-
authentication-failure
```

Command History

Release	Modification
10.08.1090	Command introduced

Command Information

Platforms	Command context	Authority
8100 8360	config-if	Administrators or local user group members with execution rights for this command.

aaa authentication port-access client-limit

```
aaa authentication port-access client-limit <CLIENTS>
no aaa authentication port-access client-limit
```

Description

Configures the maximum number of clients that can simultaneously connect to a port. This command can be issued from the interface (**config-if**) or Link Aggregation Group (**config-lag-if**) contexts on 8100 and 8360 Switch Series.

The **no** form of this command resets the number of clients to the default.

Parameter	Description
<CLIENTS>	Specifies the maximum number of clients. Default: 1. Range:

Examples

Configuring the client limit for on port **1/1/1**:

```
switch(config)# interface 1/1/1
switch(config-if)# aaa authentication port-access client-limit 25
```

Configuring the client limit for on a LAG port:

```
switch(config)# interface lag 1
switch(config-lag-if)# aaa authentication port-access client-limit 25
```

Command History

Release	Modification
10.13	(For 8100 and 836 Switch Series) This command can be issued from a Link Aggregation Group (LAG) context.
10.09	Command introduced on 8360

Command Information

Platforms	Command context	Authority
8100 8360	config-if config-lag-if	Administrators or local user group members with execution rights for this command.

aaa authentication port-access client-limit multi-domain

```
aaa authentication port-access client-limit multi-domain <DATA-CLIENT-LIMIT>
```

Description

Configures the data client limit on the multidomain enabled interface. By default, the data client limit on a multidomain enabled interface is **1**, and the maximum number of data clients supported on a multidomain enabled port is **5**.

Parameter	Description
<code><DATA-CLIENT-LIMIT></code>	Specifies the maximum data client limit on the multidomain enabled interface. Range: 1 to 5 .

Examples

Configuring data client limit of **4** on the multidomain enabled interface **1/1/4**:

```
switch(config)# interface 1/1/1
switch(config-if)# aaa authentication port-access client-limit multi-domain 4
```

Command History

Release	Modification
10.09	Command introduced on the 8360

Command Information

Platforms	Command context	Authority
8100 8360	config-if	Administrators or local user group members with execution rights for this command.

aaa authentication port-access radius-override

```
aaa authentication port-access radius-override {enable | disable}
no aaa authentication port-access radius-override {enable | disable}
```

Description

Enables or disables **radius-override** support at the interface context. When **radius-override** support is enabled, a new RADIUS overridden role is created with a combination of LUR/DUR along with RADIUS attributes for the corresponding client-role attributes such as VLANs. When the RADIUS override support is disabled, then only the user-roles get applied to the client.

The **no** form of this command disables the support for **radius-override**.



The **radius-override** support is applicable only for Auth-role.

Usage

The following table describes the access-response for the combination of roles with **radius-override** enabled and disabled:

Combination of roles in Access-Accept	Action with <i>radius-override</i> disabled	Action with <i>radius-override</i> enabled
Local User Role and RADIUS attributes	Local User Role is applied	New RADIUS Overridden role with Local User Role and RADIUS attributes is created and applied
Downloadable User Role and RADIUS attributes	Downloadable User Role is applied	New RADIUS Overridden role with Downloadable User Role and RADIUS attribute is created and applied
Local User Role and Downloadable User Role	Local User Role is applied	Local User Role is applied
Local User Role, Downloadable User Role, and RADIUS attributes	Local User Role is applied	New RADIUS Overridden role with Local User Role and RADIUS attributes is created and applied

Examples

Enabling radius-override support:

```
switch(config-if)# aaa authentication port-access radius-override enable
```

```
switch(config-if)# no aaa authentication port-access radius-override disable
```

Disabling radius-override support:

```
switch(config-if)# aaa authentication port-access radius-override disable
```

```
switch(config-if)# no aaa authentication port-access radius-override enable
```

Command History

Release	Modification
10.09	Command introduced on the 8360

Command Information

Platforms	Command context	Authority
8100 8360	config-if	Administrators or local user group members with execution rights for this command.

port-access allow-flood-traffic

```
port-access allow-flood-traffic {enable | disable}
```

Description

Enables or disables transmission of flood traffic, such as broadcast, multicast, and unknown unicast messages through a security enabled port on which no client has been authenticated. This command can be issued from the interface (**config-if**) or Link Aggregation Group (**config-lag-if**) contexts. By default, transmission of flood traffic is disabled.

Usage

This command can be used to allow Wake-on-LAN packets on security enabled ports, before a client is authenticated.

Examples

Enabling flood traffic on a port on interface 1/1/1:

```
switch(config)# interface 1/1/1
switch(config-if)# port-access allow-flood-traffic
```

Enabling flood traffic on a port on a LAG port:

```
switch(config)# interface lag 1
switch(config-lag-if)# port-access allow-flood-traffic
```

Command History

Release	Modification
10.13	(for 8100 and 8360 Switch Series only) This command can be issued from a Link Aggregation Group (LAG) context.
10.09	Command introduced on the 8360

Command Information

Platforms	Command context	Authority
8100 8360	config-if config-lag-if	Administrators or local user group members with execution rights for this command.

port-access auto-vlan

```
port-access auto-vlan
no port-access auto-vlan
```

Description

Creates VLAN automatically for the port-access clients globally, if the VLAN is not configured statically on the switch. By default, **port-access auto-vlan** is disabled.

The **no** form of this command disables the port-access automatic VLAN creation globally on the switch.



The type for the VLAN created using the auto-vlan feature is displayed as **port-access** in the **show vlan** command.

Examples

Enabling automatic VLAN creation for clients:

```
switch(config)# port-access auto-vlan
```

Disabling automatic VLAN creation for clients(default):

```
switch(config)# no port-access auto-vlan
```

Command History

Release	Modification
10.08	Command introduced.

Command Information

Platforms	Command context	Authority
8100 8360	config	Administrators or local user group members with execution rights for this command.

port-access client-move

```
port-access client-move {enable | disable | secure}
```

Description

When client move is enabled (the default), a port access client can move to other port access-enabled interfaces, at which time they will be re-authenticated on the new interface.

When client move is disabled, a client cannot move to other port access-enabled interfaces.



An authenticated client will be moved immediately if the new port to which the client will move has a pre-auth role configured, even when client move is enabled as secure.

Parameter	Description
enable	Enables this feature so port access clients can move to other port access-enabled interfaces.
disable	Disables this feature so port access clients cannot move to other port access-enabled interfaces.
secure	Use this configuration setting to stop a potential attacker from denying a genuine client access by spoofing the client's MAC on a different port-access enabled port of the switch. An authenticated client will be moved immediately if the new port to which the client moved has a pre-authentication role configured, even when client-move is enabled as secure. NOTE: Secure client move is enabled by default.

Examples

Enabling client move:

```
switch(config)# port-access client-move enable
```

Enabling secure client move:

```
switch(config)# port-access client-move enable secure
```

Disabling client move:

```
switch(config)# port-access client-move disable
```

Command History

Release	Modification
10.09	Command introduced on the 8360

Command Information

Platforms	Command context	Authority
8100 8360	config	Administrators or local user group members with execution rights for this command.

port-access event-log client

```
port-access event-log client  
no port-access event-log client
```

Description

Enables port access informational event logs for the client. These event logs help with client telemetry on a remote management station such as Aruba Central. By default, these informational event logs are disabled.



Starting with AOS-CX 10.10, the event IDs 10510 and 10511 are logged when the port access informational event log configuration is enabled.

The **no** form of the command disables port access informational event logs for the client.

Example

Enabling port access event log:

```
switch(config)# port-access event-log client
```

Disabling port access event log:

```
switch(config)# no port-access event-log client
```

Command History

Release	Modification
10.10	Command introduced

Command Information

Platforms	Command context	Authority
8100 8360	config	Administrators or local user group members with execution rights for this command.

port-access fallback-role

```
port-access fallback-role <ROLE-NAME>  
no port-access fallback-role <ROLE-NAME>
```

Description

Configures the fallback role to assign to the clients onboarding on a port. This role is applied only when no derived role is applied to the clients.

The **no** form of the command resets the fallback role.

Parameter	Description
<ROLE-NAME>	Specifies the fallback role name. The maximum number of characters supported is 64.

Usage

Following are the conditions for the fallback role to be applied on onboarding devices:

- The device profile local MAC match feature with block-until-profile-applied mode is configured.
- Device profile along with AAA is configured but no match was found for the device profile client.
- AAA method with no reject or critical role is configured, and the connection to RADIUS server failed.
- 802.1X authentication is enabled on the port, but the supplicant of the device timed out to respond to the authentication request.

Example

Configuring fallback role for a port:

```
switch(config)# interface 1/1/3  
switch(config-if)# port-access fallback-role fallback01
```

Command History

Release	Modification
10.09	Command introduced on the 8360

Command Information

Platforms	Command context	Authority
8100 8360	config-if	Administrators or local user group members with execution rights for this command.

port-access log-off client

```
port-access log-off client mac <MAC-ADDRESS>
port-access log-off client interface <INTERFACE-NAME>
port-access log-off client role <ROLE-NAME>
```

Description

Logs off the client connected to a port access-enabled interface.

Parameter	Description
<MAC-ADDRESS>	Specifies the client MAC address.
<INTERFACE-NAME>	Specifies the client interface.
<ROLE-NAME>	Specifies the client MAC address.

Example

Logging a client off from the switch, specifying the MAC address:

```
switch# port-access log-off client mac 00:50:56:bd:04:2d
```

Logging a client off from the switch, specifying the interface:

```
switch# port-access log-off client interface 1/1/1
```

Logging a client off from the switch, specifying the role:

```
switch# port-access log-off client role r1
```

Command History

Release	Modification
10.09	Command introduced on the 8360

Command Information

Platforms	Command context	Authority
8100 8360	Manager (#)	Administrators or local user group members with execution rights for this command.

port-access onboarding-method precedence

```
port-access onboarding-method precedence [aaa device-profile | device-profile aaa]
no port-access onboarding-method precedence [aaa device-profile | device-profile aaa]
```

Description

Configures the precedence for the method to be used to authenticate onboarding devices for each interface.

The **no** form of the command resets the authentication method precedence to the default precedence of AAA followed by device profile.

AAA includes the 802.1X and MAC authentication methods whose precedence can be configured using the **aaa authentication port-access auth-precedence** command. Here, the default precedence is 802.1X authentication.

For example, if you configure AAA (both 802.1X and MAC) authentication methods and device profile on a port, by default, the authentication precedence would be 802.1X, then MAC, and lastly device profile.



aaa in the parameters refers to the authentication precedence configured using the **aaa authentication port-access auth-precedence** command.

Parameter	Description
aaa device-profile	Specifies that the precedence for per port onboarding authentication method is AAA followed by device profile.
device-profile aaa	Specifies that the precedence for per port onboarding authentication method is device profile followed by AAA.

Examples

Configuring AAA method precedence on a port:

```
switch(config)# interface 1/1/1
switch(config-if)# port-access onboarding-method precedence device-profile aaa
```

Resetting the authentication method precedence:

```
switch(config)# interface 1/1/1
switch(config-if)# no port-access onboarding-method precedence device-profile aaa
```

Command History

Release	Modification
10.09	Command introduced on the 8360

Command Information

Platforms	Command context	Authority
8100 8360	config-if	Administrators or local user group members with execution rights for this command.

port-access onboarding-method concurrent

port-access onboarding-method concurrent <enable | disable>

Description

Configures all methods to start concurrently for faster onboarding process. If authentication priority is not configured when enabling concurrent onboarding, the priority will be 802.1X followed by **mac-auth** and **device-profile**.

Default priority for concurrent onboarding is 802.1X followed by **mac-auth** and **device-profile**.

When enabling concurrent onboarding on the port, existing clients will be de-authenticated and freshly onboarded concurrently.

When concurrent onboarding is enabled, then auth-precedence will be ignored.

If concurrent onboarding is configured, the client will stay in pre-auth role till it gets succeeded by one authentication method or gets failed by all the authentication methods.

When the authentication method with the highest priority fails, the profile of the next successful authentication method is applied.

If all methods fail, the reject or critical role is applied based on the 802.1X authentication failure reason and continues to reauthenticate with the 802.1X method.

Reauthentication will be triggered for all high priority methods and not just the final successful authentication method.

Some RADIUS server may block the client when it receives two requests, **mac-auth** and 802.1X, from the same client at the same time. This is because the RADIUS server allows only one authentication request. In such cases, concurrent onboarding is not feasible. To prevent such scenarios, configure **auth-precedence** with **auth-priority**.

Parameter	Description
enable	Enable clients to be onboarded concurrently.
disable	Disable clients to be onboarded concurrently.

Examples

Enabling concurrent onboarding on a port:

```
switch(config)# interface 1/1/1
switch(config-if)# port-access onboarding-method concurrent enable
```

Disabling concurrent onboarding on a port:

```
switch(config)# interface 1/1/1
switch(config-if)# port-access onboarding-method concurrent disable
```

Sample configuration:

```
interface 1/1/1
  no shutdown
  no routing
  vlan access 999
  !aaa authentication port-access auth-precedence mac-auth dot1x
  port-access onboarding-method concurrent enable
```

Command History

Release	Modification
10.09	Command introduced on the 8360

Command Information

Platforms	Command context	Authority
8100 8360	config-if	Administrators or local user group members with execution rights for this command.

port-access reauthenticate interface

port-access reauthenticate interface <INTERFACE-NAME>

Description

Forcefully reauthenticates all clients connected to an interface.



Clients that are in the **HELD** state are ignored.

Parameter	Description
<INTERFACE-NAME>	Specifies the interface name.

Examples

Configuring reauthentication of all clients on a port:

```
switch# port-access reauthenticate interface 1/1/1
```

Command History

Release	Modification
10.09	Command introduced on the 8360

Command Information

Platforms	Command context	Authority
8100 8360	Manager (#)	Administrators or local user group members with execution rights for this command.

show aaa authentication port-access interface client-status

```
show aaa authentication port-access interface {all | <IFRANGE>}
client-status [mac <MAC-ADDRESS>]
```

Description

Shows information about the status of the role applied on ports. RADIUS overridden user roles are suffixed with *. The role name is not displayed for clients that do not use local, downloaded, or RADIUS overridden role.

Parameter	Description
all	Specifies all interfaces.
<IFRANGE>	Specifies the interface name.
<MAC-ADDRESS>	Specifies the client MAC address.

Examples

Showing information about a client:

```
switch# show aaa authentication port-access interface all client-status
Port Access Client Status Details
RADIUS overridden user roles are suffixed with '*'
Client 00:50:56:96:93:d6, John Doe
=====

Session Details
-----
Port          : 1/1/13
Session Time  : 30s
IPv4 Address  : 10.0.0.1
IPv6 Address  :

Authentication Details
-----
Status          : dot1x Authenticated
Auth Precedence : dot1x - Authenticated, mac-auth - Not attempted
Auth History    : dot1x    - Authenticated, 5s ago
mac-auth - Unauthenticated, Server-Reject, 10s ago
mac-auth - Unauthenticated, Server-Reject, 15s ago
dot1x    - Unauthenticated, Server-Timeout, 15s ago
dot1x    - Attempted, 20s ago

Authorization Details
-----
Role   : Employee*
Status : Applied
```

```

Client 00:50:56:96:50:28
=====
Session Details
-----
Port          : 1/1/14
Session Time  : 10s
IPv4 Address  : 10.0.0.2
IPv6 Address  :

Authentication Details
-----
Status          : mac-auth Authenticated
Auth Precedence : dot1x - Unauthenticated, mac-auth - Authenticated
Auth History    : dot1x - Unauthenticated, Server-Reject, 5s ago
mac-auth - Authenticated, 10s ago

Authorization Details
-----
Status : Applied

```

Command History

Release	Modification
10.12	Command output modified to be suffixed with * for RADIUS overridden user roles. The role name will not be displayed for clients that do not use local, downloaded, or RADIUS overridden role.
10.09	Command introduced on the 8360

Command Information

Platforms	Command context	Authority
8100 8360	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show port-access clients

`show port-access clients [dhcp-info|ubt|vxlan] [interface <INTERFACE-NAME>] [mac <MAC-ADDRESS>]`

Description

Shows summarized active port access client information.

The **User-Role** column in the output will not display any value for clients not using local, downloaded or RADIUS overridden role. When an explicit client name is not available, only the MAC address of the client will be displayed.

The VLANs in the output display the tags, **u**, **t**, and **multi** to indicate untagged VLAN, single tagged VLAN, and multiple VLANs respectively.



Parameter	Description
<i>dhcp</i>	Shows DHCP information of port access clients. NOTE: To view the DHCP information of port access clients, either client IP tracker or DHCP snooping must be enabled. If client IP tracker is enabled, then the command does not display the lease time. This command does not display information about tagged VLAN.
<i>ubt</i>	Shows port access information about UBT clients. NOTE: The output displays information only about untagged VLAN.
<i>vxlan</i>	Shows port access information about VXLAN clients. NOTE: The output displays information about both tagged and untagged VLAN without the tags, u and t .
<INTERFACE-NAME>	Specifies the interface name.
<MAC-ADDRESS>	Specifies the client MAC address.

Examples

Showing information for all clients:

```
switch# show port-access clients
Port Access Clients jhdoadjfoadk

Status Codes: d device-mode, c client-mode, m multi-domain

-----
Port      MAC-Address      Onboarding      Status      Role
Device Type
Method
-----
c 1/1/4      00:50:56:bd:04:c8  port-security  Success
c 1/1/5      00:50:56:bd:32:07  Success      reject-role, reject
c 1/1/5      00:50:56:bd:32:08  Fail        critical-...,
critical
c 1/1/5      00:50:56:cd:32:08  Fail        cached-critical
c 1/1/6      00:50:56:bd:50:43  mac-auth     Success     auth-role, auth
c 1/1/6      00:50:56:bd:50:45  dot1x       Success     RADIUS_773420618
c 1/1/19     08:97:34:ad:e4:00  device-profile Success     ap-role
c 1/1/20     00:50:56:bd:32:08  In-Progress  preauth-role, preauth
c 1/1/20     00:50:56:bd:32:06  In-Progress
c 1/1/20     00:50:56:bd:32:09  Fail
d 1/1/25     08:97:34:ad:f4:03  mac-auth     Success     RADIUS_453420632
c 1/1/212    00:60:56:bd:50:43  mac-auth     Success     fallback-role,
fallback
m 1/1/7      00:50:56:bd:50:45  dot1x       Success     RADIUS_773420620
data
m 1/1/7      00:50:56:bd:50:c5  dot1x       Success     RADIUS_773420621
voice
```

```
m 1/1/8      00:50:56:bd:50:c6  dot1x      Fail      test-voice,critical
voice voice
```

Showing information for clients on a particular interface:

```
switch# show port-access clients interface 1/1/5

Port Access Clients

Status codes: d device-mode, c client-mode, m multi-domain

-----
-
  Port      MAC Address      Onboarded      Status      Role
                Method
-----
-
c 1/1/5     00:50:56:bd:32:07      Success      reject-role, Reject
c 1/1/5     00:50:56:bd:32:08      Fail        critical-...,
Critical
```

Showing information for all clients including multidomain mode clients:

```
switch# show port-access clients

Port Access Clients

Status codes: d device-mode, c client-mode, m multi-domain

-----
-----
  Port      MAC-Address      Onboarding      Status      VLAN      Role
    Device Type      Method
-----
-----
c 1/1/4     00:50:56:bd:04:c8  port-security  Success
c 1/1/5     00:50:56:bd:32:07      Success      10      reject-role,
reject
c 1/1/5     00:50:56:bd:32:08      Fail        20      critical-...,
critical
c 1/1/6     00:50:56:bd:50:43  mac-auth      Success      auth-role,
auth
c 1/1/6     00:50:56:bd:50:45  dot1x         Success      20      RADIUS_
773420618
c 1/1/19    08:97:34:ad:e4:00  device-profile Success
c 1/1/20    00:50:56:bd:32:08      In-Progress  10      ap-role
preauth
c 1/1/20    00:50:56:bd:32:06      In-Progress
c 1/1/20    00:50:56:bd:32:09      Fail
d 1/1/25    08:97:34:ad:f4:03  mac-auth      Success      10      RADIUS_
453420632
c 1/1/212   00:60:56:bd:50:43  mac-auth      Success      fallback-
role, fallback
m 1/1/7     00:50:56:bd:50:45  dot1x         Success      21      RADIUS_
773420620      data
m 1/1/7     00:50:56:bd:50:c5  dot1x         Success      22      RADIUS_
773420621      voice
```

```
m 1/1/8      00:50:56:bd:50:c6  dot1x      Fail      23      test-
voice,critical voice  voice
```

Showing information for all clients including multidomain mode clients and UBT fallback role applied:

```
switch# show port-access clients
Port Access Clients

Status codes: d device-mode

-----
-----
Port      MAC-Address      Onboarding      Status      Role
Device Type      Method
-----
-----
1/1/4      00:50:56:bd:04:c8  port-security   Success
1/1/5      00:50:56:bd:32:07  Success        reject-role, reject
1/1/5      00:50:56:bd:32:08  Fail          critical-...,
critical
1/1/6      00:50:56:bd:50:43  mac-auth       Success      auth-role, auth
1/1/6      00:50:56:bd:50:45  dot1x         Success      RADIUS_773420618
1/1/19     08:97:34:ad:e4:00  device-profile  Success      ap-role
1/1/20     00:50:56:bd:32:08  In-Progress    preauth-role, preauth
1/1/20     00:50:56:bd:32:06  In-Progress
1/1/20     00:50:56:bd:32:09  Fail
d 1/1/25     08:97:34:ad:f4:03  mac-auth       Success      RADIUS_453420632
1/1/212    00:60:56:bd:50:43  mac-auth       Success      fallback-role,
fallback
1/1/7      00:50:56:bd:50:45  dot1x         Success      RADIUS_773420620
data
1/1/7      00:50:56:bd:50:c5  dot1x         Success      RADIUS_773420621
voice
1/1/8      00:50:56:bd:50:c6  dot1x         Fail        test-voice,critical
voice voice
1/1/21     00:50:56:bd:32:13  mac-auth       Success      ubt-role, ubt-
fallback
```

Showing information about a specific client:

```
switch# show port-access clients mac 00:50:56:bd:50:43
Port Access Clients
RADIUS overridden user roles are suffixed with '*'

Flags: Onboarding-Method|Mode|Device-Type|Status

Onboarding-Method: 1x 802.1X, ma MAC-Auth, ps Port-Security, dp Device-Profile,m
Multi-Domain

Mode: c Client-Mode, d Device-Mode, p Proxy-Mode, m Multi-Domain

Device-Type: d Data, v Voice

Status: s Success, f Failed, p In-Progress, d Role-Download-Failed

-----
-----
```

Port VLAN	Client-Name Flags	IPv4-Address	User-Role
1/1/5	00:50:56:bd:50:43 (u)1234, (t)1000 1x c - s		reject-role, reject

Showing information for clients on a particular interface:

```
switch# show port-access clients interface 1/1/5
Port Access Clients
RADIUS overridden user roles are suffixed with '*'

Flags: Onboarding-Method|Mode|Device-Type|Status

Onboarding-Method: 1x 802.1X, ma MAC-Auth, ps Port-Security, dp Device-Profile
Mode: c Client-Mode, d Device-Mode, p Proxy-Mode, m Multi-Domain
Device-Type: d Data, v Voice
Status: s Success, f Failed, p In-Progress, d Role-Download-Failed
```

Port VLAN	Client-Name Flags	IPv4-Address	User-Role
1/1/5	00:50:56:bd:32:07 (u)1234, (t)1000 1x c - s		reject-role, reject
1/1/5	test (u)56 1x c - f		critical-..., critical
1/1/9	00:50:56:bd:50:c7 rp p - s		rp-role

Showing DHCP information of port access clients:

```
switch# show port-access clients dhcp-info
Port Access Clients
```

Port VLAN	Client-Name Lease-Time	IP-Address	
1/1/1 268	Camera-1023	10.10.10.10	10
1/1/2 500 ...	CAP-8-G22	aaaa:bbbb:cccc:dddd:eeee:1234:5678:abcd	20

Showing port access information about UBT clients:

```
switch# show port-access clients ubt
Port Access Clients
RADIUS overridden user roles are suffixed with '*'
```

```

Flags: Onboarding-Method|Mode|Device-Type|Status

Onboarding-Method: 1x 802.1X, ma MAC-Auth, ps Port-Security, dp Device-Profile

Mode: c Client-Mode, d Device-Mode, m Multi-Domain

Device-Type: d Data, v Voice

Status: s Success, f Failed, p In-Progress, d Role-Download-Failed

-----
-----
Port      Client-Name      IPv4-Address      User-Role      Gateway-Role
  Zone      UBT      VLAN  Flags
-----
1/1/12    00:50:56:96:93:d6  10.10.10.10      test_role      authenticated
      zone1      10      ma|c|-|s
1/1/10    CAP-8-G22      10.10.10.11      student
authenticated_gate... zone1      9857  1x|c|-|s

```

Showing port access information about VXLAN clients:

```

switch# show port-access clients vxlan
Port Access Clients
RADIUS overridden user roles are suffixed with '*'

Flags: Onboarding-Method|Mode|Device-Type|Status

Onboarding-Method: 1x 802.1X, ma MAC-Auth, ps Port-Security, dp Device-Profile

Mode: c Client-Mode, d Device-Mode, m Multi-Domain

Device-Type: d Data, v Voice

Status: s Success, f Failed, p In-Progress, d Role-Download-Failed

-----
-----
Port      Client-Name      IPv4-Address      User-Role
  VLAN  VNI  Flags
-----
1/1/21    00:50:56:96:93:d6  10.10.10.10      student
  5678  2432  ma|c|-|s
1/1/21    user_12@gmail.com      employee
  9857  4678  1x|c|-|s

```

Command History

Release	Modification
10.12	The following changes were introduced: ▪ The dhcp-info, ubt, and vxlan parameters were introduced. ▪ Command output modified to display only Port, Client-Name,

Release	Modification
	IPv4-Address, User-Role, VLAN, and Flags.
10.10	Command output updated to display cached-critical role
10.09	Command introduced on the 8360

Command Information

Platforms	Command context	Authority
8100 8360	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show port-access clients detail

```
show port-access clients [interface <INTERFACE-NAME>] [mac <MAC-ADDRESS>] detail
```

Description

Shows detailed active port access clients information including the VLAN group and VLAN association for each of the authenticated clients. The output can be filtered by interface or MAC address.

Parameter	Description
<INTERFACE-NAME>	Specifies the interface name.
<MAC-ADDRESS>	Specifies the client MAC address.

Examples

Showing detailed information for clients on a particular interface (one client):

```
switch# show port-access clients interface 1/1/7 detail
Port Access Client Status Detail
-----

Client 2c:41:38:7f:35:c8, Jamie Doe
=====
Session Details
-----
  Port          : 1/1/8
  Session Time  : 33s
  IPv4 Address  :
  IPv6 Address  :

VLAN Details
-----
  VLANs Assigned : 10,20,30
  Access         :
  Native Untagged : 10
  Allowed Trunk  : 20,30

Authentication Details
```



```
-----
Status           : mac-auth Authenticated
Auth Precedence  : dot1x - Unauthenticated, mac-auth - Authenticated
Auth History     : mac-auth - Authenticated, 5s ago
                  dot1x   - Unauthenticated, Server-Timeout, 10s ago
```

Authorization Details

```
-----
Role      : RADIUS_Overridden_3029903100
Status    : Applied
```

Attributes overridden by RADIUS are prefixed by '*'.

```
Name      : RADIUS_Overridden_3598790787
Type      : radius
Base Role : local, Fri Jul 09 14:34:29 IST 2021
```

```
-----
Reauthentication Period      : 600 secs
Cached Reauthentication Period :
Authentication Mode          :
Session Timeout              : 800 secs
Client Inactivity Timeout    : 1000 secs
Description                   :
*Gateway Zone                 : stdn_ctrl
Access VLAN                   :
Native VLAN                   :
*Allowed Trunk VLANs          : 5
Access VLAN Name              :
Native VLAN Name              :
Allowed Trunk VLAN Names      :
*MTU                           : 9198
QOS Trust Mode                :
STP Administrative Edge Port  :
PoE Priority                   :
Policy                        :
GBP                            :
Device Type                   :
```

```
switch# show port-access clients interface 1/1/7 detail
Port Access Client Status Detail
```

```
-----
Client 2c:41:38:7f:35:c8, Jamie Doe
```

Session Details

```
-----
Port      : 1/1/8
Session Time : 33s
IPv4 Address :
IPv6 Address :
```

VLAN Details

```
-----
VLAN Group Name :
VLANs Assigned  : 10,20,30
Access          :
Native Untagged : 10
Allowed Trunk   : 20,30
```

Authentication Details

```

-----
Status           : mac-auth Authenticated
Auth Precedence  : dot1x - Unauthenticated, mac-auth - Authenticated
Auth History     : mac-auth - Authenticated, 5s ago
                  dot1x   - Unauthenticated, Server-Timeout, 10s ago

```

Authorization Details

```

-----
Role      : RADIUS_Overridden_3029903100
Status    : Applied

```

Attributes overridden by RADIUS are prefixed by '*'.

```

Name      : RADIUS_Overridden_3598790787
Type      : radius
Base Role : MixedRole_XX00_LUR_1, local, Fri Jul 09 14:34:29 IST 2021

```

```

-----
Reauthentication Period      : 600 secs
Cached Reauthentication Period :
Authentication Mode          :
Session Timeout              : 800 secs
Client Inactivity Timeout    : 1000 secs
Description                   :
*Gateway Zone                 : stdn_ctrl
*UBT Gateway Role             : stdn-authenticated-vrfl_dur
UBT Gateway Clearpass Role   :
Access VLAN                   :
Native VLAN                   :
*Allowed Trunk VLANs          : 5
Access VLAN Name              :
Native VLAN Name              :
Allowed Trunk VLAN Names      :
VLAN Group Name               :
*MTU                          : 9198
QOS Trust Mode                :
STP Administrative Edge Port  :
PoE Priority                   :
PVLAN Port Type               :
Captive Portal Profile        :
Policy                         :
GBP                           :
Device Type                   :

```

switch# **show port-access clients interface 1/1/7 detail**

Port Access Client Status Detail

Client 2c:41:38:7f:35:c8, Jamie Doe

=====

Session Details

```

-----
Port      : 1/1/8
Session Time : 33s
IPv4 Address :
IPv6 Address :

```

VLAN Details

```

-----
VLAN Group Name :
VLANs Assigned  : 10,20,30

```

```
Access      :
Native Untagged : 10
Alllowed Trunk : 20,30
```

Authentication Details

```
-----
Status      : mac-auth Authenticated
Auth Precedence : dot1x - Unauthenticated, mac-auth - Authenticated
Auth History  : mac-auth - Authenticated, 5s ago
               dot1x   - Unauthenticated, Server-Timeout, 10s ago
```

Authorization Details

```
-----
Role       : RADIUS_Overridden_3029903100
Status    : Applied
```

Attributes overridden by RADIUS are prefixed by '*'.

```
Name       : RADIUS_Overridden_3598790787
Type       : radius
Base Role  : MixedRole_XX00_LUR_1, local, Fri Jul 09 14:34:29 IST 2021
```

```
-----
Reauthentication Period      : 600 secs
Cached Reauthentication Period :
Authentication Mode          :
Session Timeout              : 800 secs
Client Inactivity Timeout    : 1000 secs
Description                   :
*Gateway Zone                 : stdn_ctrl
*UBT Gateway Role             : stdn-authenticated-vrfl_dur
  UBT Gateway Clearpass Role  :
Access VLAN                   :
Native VLAN                   :
*Allowed Trunk VLANs          : 5
Access VLAN Name              :
Native VLAN Name              :
Allowed Trunk VLAN Names      :
VLAN Group Name               :
*MTU                           : 9198
QOS Trust Mode                :
STP Administrative Edge Port  :
PoE Priority                   :
PVLAN Port Type               :
Captive Portal Profile        :
Policy                         :
GBP                           :
Device Type                   :
```

```
switch# show port-access clients interface 1/1/7 detail
```

```
Port Access Client Status Detail
```

```
-----
Client 2c:41:38:7f:35:c8, Jamie Doe
```

```
=====
```

Session Details

```
-----
Port       : 1/1/8
Session Time : 33s
IPv4 Address :
IPv6 Address :
```

VLAN Details

VLAN Group Name :
VLANs Assigned : 10,20,30
Access :
Native Untagged : 10
Allowed Trunk : 20,30

Authentication Details

Status : mac-auth Authenticated
Auth Precedence : dot1x - Unauthenticated, mac-auth - Authenticated
Auth History : mac-auth - Authenticated, 5s ago
dot1x - Unauthenticated, Server-Timeout, 10s ago

Authorization Details

Role : RADIUS_Overridden_3029903100
Status : Applied

Attributes overridden by RADIUS are prefixed by '*'.

Name : RADIUS_Overridden_3598790787
Type : radius
Base Role : MixedRole_XX00_LUR_1, local, Fri Jul 09 14:34:29 IST 2021

Reauthentication Period	: 600 secs
Cached Reauthentication Period	:
Authentication Mode	:
Session Timeout	: 800 secs
Client Inactivity Timeout	: 1000 secs
Description	:
Access VLAN	:
Native VLAN	:
*Allowed Trunk VLANs	: 5
Access VLAN Name	:
Native VLAN Name	:
Allowed Trunk VLAN Names	:
VLAN Group Name	:
*MTU	: 9198
QOS Trust Mode	:
STP Administrative Edge Port	:
PoE Priority	:
Policy	:
GBP	:
Device Type	:

Showing information for a particular client MAC address:

```
switch# show port-access clients mac 00:00:00:00:00:c8 detail
```

Port Access Client Status Details:

Client 00:00:00:00:00:c8, 00:00:00:00:00:c8

=====

Session Details

Port : 1/1/1
Session Time : 888s
IPv4 Address :
IPv6 Address :

```

VLAN Details
-----
VLAN Group Name : test_group
VLANs Assigned  : 22
Access          : 22
Native Untagged :
Allowed Trunk   :
Authentication Details
-----
Status          : mac-auth Authenticated
Auth Precedence : dot1x - Unauthenticated, mac-auth - Authenticated
Auth History    : mac-auth - Authenticated, 288s ago
dot1x - Unauthenticated, Supplicant-Timeout, 703s ago
dot1x - Unauthenticated, 798s ago
mac-auth - Authenticated, 888s ago
Authorization Details
-----
Role   : RADIUS_2801090107
Status : Applied
Role Information:
Name   : RADIUS_2801090107
Type   : radius
-----
Reauthentication Period           : 600 secs
Cached Reauthentication Period    :
Authentication Mode               :
Session Timeout                  :
Client Inactivity Timeout        :
Description                       :
Gateway Zone                     :
UBT Gateway Role                  :
UBT Gateway Clearpass Role       :
Access VLAN                      :
Native VLAN                      :
Allowed Trunk VLANs              :
Access VLAN Name                 :
Native VLAN Name                 :
Allowed Trunk VLAN Names         :
VLAN Group Name                  : test_group
MTU                              :
QOS Trust Mode                   :
STP Administrative Edge Port     :
PoE Priority                      :
Captive Portal Profile           :
Policy                          :
GBP                              :
switch#

```

Showing detailed information for clients on a particular interface:

```

switch# show port-access clients interface 1/1/7-1/1/8 detail
Port Access Client Status Details:
-----

RADIUS overridden user roles are suffixed with '*'

Client 2c:41:38:7f:35:b9, John Doe
=====
Session Details
-----

```

```

Port          : 1/1/7
Session Time  : 203s
IPv4 Address  : 10.10.10.10
IPv6 Address  :

Authentication Details
-----
Status          : mac-auth Authenticated
Auth Precedence : dot1x - Unauthenticated, mac-auth - Authenticated
Auth History    : mac-auth - Authenticated, 5s ago
dot1x          : Unauthenticated, Server-Reject, 10s ago

Authorization Details
-----
Status : Applied

RADIUS Attributes
-----
User-Name          : Student
Filter-ID          : DHCP, WebServices-Student, DataCenter-Student,
RemoteAccess-Student, Printer-Student
Framed-MTU         : 1500 bytes
Session-Timeout    : 500 seconds
Idle-Timeout       : 200 seconds
Termination-Action : RADIUS-Request
Egress-VLAN-ID     : 10(t), 15(t), 20(u)
Egress-VLAN-Name   : VLAN100(t), VLAN200(u)
Tunnel-Type        : 13
Tunnel-Medium-Type : 6
Tunnel-Private-Group-ID : 20
NAS-Filter-Rule    : permit in 17 from any to any
deny in tcp from any to 10.10.10.3/8
Aruba-Captive-Portal-URL : http://arubanetworks.com/student/captiveportal.php
Aruba-PoE-Priority : Low
Aruba-Port-Auth-Mode : client-mode
Aruba-NAS-Filter-Rule : deny in icmp from 10.10.10.1 to any 27
Aruba-QoS-Trust-Mode : dscp
Aruba-UBT-Gateway-Role : gateway_student_role
Aruba-Gateway-Zone : student_zone
Aruba-STP-Admin-Edge-Port : false
Aruba-UBT-Gateway-CPPM-Role : ubt_gateway_cppm_student_role
Aruba-Device-Traffic-Class : data
Aruba-PVLAN-Port-Type : secondary
RADIUS Role Name : RADIUS_115315236

```

Showing information for a particular client MAC address:

```

switch# show port-access clients mac 2c:41:38:7f:35:c8 detail
Port Access Client Status Detail
-----
RADIUS overridden user roles are suffixed with '*'
Client 2c:41:38:7f:35:c8, John Doe
=====

Session Details
-----
Port          : 1/1/8
Session Time  : 33s
IPv4 Address  :
IPv6 Address  :

```

VLAN Details

VLAN Group Name :
VLANs Assigned : 10,20,30
Access :
Native Untagged : 10
Allowed Trunk : 20,30

Authentication Details

Status : mac-auth Authenticated
Auth Precedence : dot1x - Unauthenticated, mac-auth - Authenticated
Auth History : mac-auth - Authenticated, 5s ago
dot1x - Unauthenticated, Server-Timeout, 10s ago

Authorization Details

Role : student
Status : Applied
Role Information:

Name : student
Type : local

Reauthentication Period : 333 secs
Authentication Mode : device
Native VLAN : 10
Allowed Trunk VLANs : 20,30
PoE Allocation method : usage
PoE Priority : low
Captive Portal Profile : testcpprof_29451201
Policy : PERMIT-ALL_87364653

Captive Portal Profile Configuration:

Name : testcpprof_29451201
Type : local
URL : http://google.com
URL Hash Key : SWNGWyMeYubHPDgVIirpEUwNK5Uf+r1vmhBIncQPw1Y=

Access Policy Details:

Policy Name : PERMIT-ALL_87364653
Policy Type : Local
Policy Status : Applied
Base Policy : N/A
ACL Names : N/A

SEQUENCE	CLASS	TYPE	ACTION
10	dns	ipv4	permit
20	dhcp	ipv4	permit

Class Details:

class ip dns

```
10 match tcp any any
class ip dhcp
20 match any any any
```

Command History

Release	Modification
10.12	The following changes were introduced: ▪ Command output modified to display RADIUS attributes for clients not using local, downloaded or RADIUS overridden role. ▪ Command output modified to display Base Policy and ACL Names.
10.09	Command introduced on the 8360

Command Information

Platforms	Command context	Authority
8100 8360	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show port-access clients onboarding-method

show port-access clients onboarding-method <METHOD>

Description

Shows active port access client information for the specified onboarding method.

Parameter	Description
<METHOD>	Selects the onboarding method. Available methods: device-profile , dot1x , mac-auth , port-security .

Examples

Showing information for clients onboarded using MAC authentication.

```
switch# show port-access clients onboarding-method mac-auth

Port Access Clients

Status codes: device-mode

-----
-
Port      MAC-Address      Onboarding      Status      Role
Method
-----
```



```

-
  1/1/6      00:50:56:bd:50:43  mac-auth      Success      auth-role, auth
  1/1/212    00:60:56:bd:50:43  mac-auth      Success      fallback-role,
fallback

```

Command History

Release	Modification
10.09	Command introduced on the 8360

Command Information

Platforms	Command context	Authority
8100 8360	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show port-access interface

```
show port-access interface all|<ifrange> status
```

Description

Display the interface status for port-access enabled interfaces. It includes the name of the port, the member interfaces associated with the port along with the security state of the interface.

A port-access interface can be in one of the following states:

1. Blocked: Indicates that the interface is blocked by port-access.
2. Secured: Indicates the interface is secured by port-access.
3. Down: Indicates port-access is not yet operational on the interface

Parameter	Description
<i>all</i>	Display port-access information for all interfaces.
<i><ifrange></i>	Display port-access information for the specified interface.

Examples

Showing the port-access status for all interfaces:

```

switch# show port-access interface all status
Port      Interface  Status
-----
1/1/1     1/1/1     Blocked
lag1      1/1/3     Secured
lag1      1/1/4     Down

```

Showing port-access status for interface 1/1/1:

```
switch# show port-access interface 1/1/1 status
Port      Interface  Status
-----
1/1/1     1/1/1      Blocked
```

Showing port-access status for LAG 1:

```
switch# show port-access interface lag1 status
Port      Interface  Status
-----
lag1      1/1/3      Secured
lag1      1/1/4      Down
```

When port-access is not configured on an interface, following message will be displayed:

```
switch# show port-access interface all status
Port-access is not configured
```

Release	Modification
10.13	Command introduced.

Command Information

Platforms	Command context	Authority
8100 8360	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

Port access debugging and troubleshooting

Debugging and troubleshooting Information for RADIUS, MAC authentication, and 802.1X authentication is provided as follows:

- [Radius server reachability debugging and troubleshooting](#)
- [Port access MAC authentication debugging and troubleshooting](#)
- [Port access 802.1X authentication debugging and troubleshooting](#)

Radius server reachability debugging and troubleshooting

Ensure that a valid RADIUS server is correctly identified to the switch and that the RADIUS server is reachable in the network.

Command **radius-server host** is used to identify the RADIUS server to the switch.

The following command sequences show how the RADIUS server is identified to the switch (using command **radius-server host**) and then ping is used to confirm that the RADIUS server is reachable from the switch. Also, RADIUS server information is displayed with related show commands.

```
switch-4# show running-config | in radi
radius-server host cec-cp.ectme.net key ciphertext AQBapdAz4irj...BQAAADY26liu
  tracking enable tracking-mode dead-only clearpass-username cecdur
  clearpass-password ciphertext AQBapXi8CEcB...BgAAAPMfbjuQtw==
radius dyn-authorization enable
ip source-interface radius 192.168.2.4
ipv6 source-interface radius fd00:4:1::b
switch-4#
```

```
switch-4# ping cec-cp.ectme.net
PING cec-cp.ectme.net (192.168.8.50) 100(128) bytes of data.
108 bytes from 192.168.8.50: icmp_seq=1 ttl=62 time=0.314 ms
108 bytes from 192.168.8.50: icmp_seq=2 ttl=62 time=0.331 ms
108 bytes from 192.168.8.50: icmp_seq=3 ttl=62 time=0.355 ms
108 bytes from 192.168.8.50: icmp_seq=4 ttl=62 time=0.424 ms
108 bytes from 192.168.8.50: icmp_seq=5 ttl=62 time=0.341 ms

--- cec-cp.ectme.net ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4098ms
rtt min/avg/max/mdev = 0.314/0.353/0.424/0.037 ms
```

```
switch-4#
switch-4# show radius-server
Unreachable servers are preceded by *
***** Global RADIUS Configuration *****
Shared-Secret: None
Timeout: 5
Auth-Type: pap
Retries: 1
TLS Timeout: 5
Tracking Time Interval (seconds): 300
Tracking Retries: 1
Tracking User-name: radius-tracking-user
Tracking Password: None
Number of Servers: 1
```

```
-----
SERVER NAME | TLS | PORT | VRF
```

```

-----
*cec-cp.ectme.net                               |           | 1812 | default
-----

switch-4# show radius-server detail
***** Global RADIUS Configuration *****

Shared-Secret: None
Timeout: 5
Auth-Type: pap
Retries: 1
TLS Timeout: 5
Tracking Time Interval (seconds): 300
Tracking Retries: 1
Tracking User-name: radius-tracking-user
Tracking Password: None
Number of Servers: 1
***** RADIUS Server Information *****
Server-Name           : cec-cp.ectme.net
Auth-Port             : 1812
Accounting-Port       : 1813
VRF                   : default
TLS Enabled           : No
Shared-Secret         : AQBapdAz4irjSK61Zg/CFArsNYWKbn1LObqDD/v9SH1eMQ6DY26liu
Timeout              : 5
Retries               : 1
Auth-Type             : pap
Server-Group          : radius
Default-Priority      : 1
ClearPass-Username    : cecdur
ClearPass-Password    : AQBapXi8CEcBRKUSLT70WhU6oy+ULtKCc6j9oNBgAAAPMfbjuQtw==
Tracking              : enabled
Tracking-Mode         : dead-only
Reachability-Status   : unreachable, Since Sun Oct 03 23:09:26 PDT 2021
Tracking-Last-Attempted : Sun Oct 03 23:09:16 PDT 2021
Next-Tracking-Request : 234 seconds

```

Port access MAC authentication debugging and troubleshooting

Using show commands

Use command **show aaa authentication port-access mac-auth interface all client-status** to help debug the client/server failure reason.

Example 1: Server timeout (typically caused when RADIUS server becomes unreachable):

```

switch# show aaa authentication port-access mac-auth interface all client-status

Port Access Client Status Details

Client  AB:CD:DE:FF:AA:BB, 1/1/1
=====
Authentication Details
-----
Status           : Unauthenticated
Auth-Method      : CHAP
Auth Failure reason : Server-Timeout
Time Since Last State Change : 200 secs

```

...

Example 2: Server reject (typically caused by invalid user credentials):

```
switch# show aaa authentication port-access mac-auth interface all client-status

Port Access Client Status Details

Client  AB:CD:DE:FF:AA:BB, 1/1/1
=====
Authentication Details
-----
      Status                               : Unauthenticated
      Auth-Method                           : CHAP
      Auth Failure reason                    : Server-reject
      Time Since Last State Change          : 30 secs
...
```

Example 3: Held (caused by a user authentication attempt made sooner than allowed after an earlier failed authentication attempt):

```
switch# show aaa authentication port-access mac-auth interface all client-status

Port Access Client Status Details

Client  AB:CD:DE:FF:AA:BB, 1/1/1
=====
Authentication Details
-----
      Status                               : Unauthenticated
      Auth-Method                           : CHAP
      Auth Failure reason                    : Held
      Time Since Last State Change          : 30 secs
...
```

Using debug commands

The following command sequences illustrate how the debug command can be used to help debug port access MAC authentication:

```
# debug portaccess macauth all
mac      MAC address to filter debug logs
port     PORT name to filter debug logs
severity Minimum log severity to filter debug logs
<cr>
```

Step 1:

```
switch(config-macauth)# 2020-08-02T06:00:05.356+00:00 port-accessd[3250]:
debug|LOG_DEBUG|MSTR|1|PORTACCESS|PORTACCESS_MACAUTH_CONFIG|logID=8378 Posting
event 'MAC-Auth Global Enable' to '15'
2020-08-02T06:00:05.356+00:00 port-accessd[3250]: debug|LOG_
DEBUG|MSTR|1|PORTACCESS|PORTACCESS_MACAUTH_CONFIG|logID=8378 Creating event 'MAC-
Auth Global Enable' for port '(null)'
2020-08-02T06:00:05.356+00:00 port-accessd[3250]: debug|LOG_
```

```

DEBUG|MSTR|1|PORTACCESS|PORTACCESS_MACAUTH_CONFIG|logID=8378 Posting event 'MAC-Auth Global Enable' to '16'
2020-08-02T06:00:05.356+00:00 port-accesssd[3250]: debug|LOG_
DEBUG|MSTR|1|PORTACCESS|PORTACCESS_MACAUTH_PROTOCOL|logID=8379 logID=8379 Handling
event 'MAC-Auth Global Enable' in state 'DISABLED'
2020-08-02T06:00:05.357+00:00 port-accesssd[3250]: debug|LOG_
DEBUG|MSTR|1|PORTACCESS|PORTACCESS_MACAUTH_PROTOCOL|logID=8379 logID=8379 macauth
SM State transition [DISABLED] -> [ENABLED] for object with key 'null'

```

Step 2:

```

switch(config-macauth)# addr-format multi-colon
switch(config-macauth)# 2020-08-02T06:00:39.986+00:00 port-accesssd[3250]:
debug|LOG_DEBUG|MSTR|1|PORTACCESS|PORTACCESS_MACAUTH_CONFIG|logID=8416 Posting
event 'MAC-Auth Address Format Change' to '15'
2020-08-02T06:00:39.986+00:00 port-accesssd[3250]: debug|LOG_
DEBUG|MSTR|1|PORTACCESS|PORTACCESS_MACAUTH_PROTOCOL|logID=8417 logID=8417 Handling
event 'MAC-Auth Address Format Change' in state 'ENABLED'

```

Step 3:

```

switch(config)# interface 1/1/2
switch(config-if)# aaa authentication port-access mac-auth
switch(config-if-macauth)# enable
switch(config-if-macauth)# 2020-08-02T06:01:26.918+00:00 port-accesssd[3250]:
debug|LOG_DEBUG|MSTR|1|PORTACCESS|PORTACCESS_MACAUTH_CONFIG|logID=8464 Posting
event 'MAC-Auth Enabled on Port' to '16'
2020-08-02T06:01:26.918+00:00 port-accesssd[3250]: debug|LOG_
DEBUG|MSTR|1|PORTACCESS|PORTACCESS_MACAUTH_PROTOCOL|logID=8465 logID=8465 Handling
event 'MAC-Auth Enabled on Port' for MACAuthPort '1/1/2' in state 'NULL'
2020-08-02T06:01:26.919+00:00 port-accesssd[3250]: debug|LOG_
DEBUG|MSTR|1|PORTACCESS|PORTACCESS_MACAUTH_PROTOCOL|logID=8465 logID=8465
macauthport SM State transition [INITIALIZED] -> [UP] for object with key '1/1/2'
2020-08-02T06:01:26.919+00:00 port-accesssd[3250]: debug|LOG_
DEBUG|MSTR|1|PORTACCESS|PORTACCESS_MACAUTH_PROTOCOL|logID=8465 logID=8465
switch(config)# interface 1/1/2
switch(config-if)# aaa authentication port-access mac-auth
switch(config-if-macauth)# enable
switch(config-if-macauth)# 2020-08-02T06:01:26.918+00:00 port-accesssd[3250]:
debug|LOG_DEBUG|MSTR|1|PORTACCESS|PORTACCESS_MACAUTH_CONFIG|logID=8464 Posting
event 'MAC-Auth Enabled on Port' to '16'
2020-08-02T06:01:26.918+00:00 port-accesssd[3250]: debug|LOG_
DEBUG|MSTR|1|PORTACCESS|PORTACCESS_MACAUTH_PROTOCOL|logID=8465 logID=8465 Handling
event 'MAC-Auth Enabled on Port' for MACAuthPort '1/1/2' in state 'NULL'
2020-08-02T06:01:26.919+00:00 port-accesssd[3250]: debug|LOG_
DEBUG|MSTR|1|PORTACCESS|PORTACCESS_MACAUTH_PROTOCOL|logID=8465 logID=8465
macauthport SM State transition [INITIALIZED] -> [UP] for object with key '1/1/2'
2020-08-02T06:01:26.919+00:00 port-accesssd[3250]: debug|LOG_
DEBUG|MSTR|1|PORTACCESS|PORTACCESS_MACAUTH_PROTOCOL|logID=8465 logID=8465 Event
handler of MACAuthPort '1/1/2' for event 'MAC-Auth Enabled on Port' in state
'NULL' returned 'OK'

```

Port access 802.1X authentication debugging and troubleshooting

Using show commands

Use command **show aaa authentication port-access dot1x authenticator interface all client-status** to help debug the client/server failure reason.

Example 1: Server timeout (typically caused when RADIUS server becomes unreachable):

```
switch# show aaa authentication port-access dot1x authenticator interface all
client-status
```

```
Client FE:04:D7:50:89:37, userxx1, 1/1/1
=====
```

Authentication Details

Status	: Unauthenticated
Type	: Pass-Through
EAP-Method	: MD5
Auth Failure reason	: Server-Timeout
Time Since Last State Change	: 200s

Authentication Statistics

Authentication	: 0
Authentication Timeout	: 205
EAP-Start While Authenticating	: 0
EAP-Logoff While Authenticating	: 0
Successful Authentication	: 0
Failed Authentication	: 1
Re-Authentication	: 0
Successful Re-Authentication	: 0
Failed Re-Authentication	: 0
EAP-Start When Authenticated	: 0
EAP-Logoff When Authenticated	: 0
Re-Auths When Authenticated	: 0
Cached Re-Authentication	: 0

...

Example 2: Server reject (typically caused by invalid user credentials):

```
switch# show aaa authentication port-access dot1x authenticator interface all
client-status
```

```
Client FE:04:D7:50:89:37, userxx1, 1/1/1
=====
```

Status	: Unauthenticated
Type	: Pass-Through
EAP-Method	: MD5
Auth Failure reason	: Server-reject
Time Since Last State Change	: 30s

Authentication Statistics

Authentication	: 0
Authentication Timeout	: 33
EAP-Start While Authenticating	: 0
EAP-Logoff While Authenticating	: 0
Successful Authentication	: 0
Failed Authentication	: 1
Re-Authentication	: 0
Successful Re-Authentication	: 0
Failed Re-Authentication	: 0
EAP-Start When Authenticated	: 0
EAP-Logoff When Authenticated	: 0

```

Re-Auths When Authenticated      : 0
Cached Re-Authentication        : 0
...

Client  FE:04:D7:50:89:37, userxx1, 1/1/1
=====

Status      : Unauthenticated
Type        : Pass-Through
EAP-Method   : MD5
Auth Failure reason : Server-reject
Time Since Last State Change : 30s

Authentication Statistics
-----
Authentication      : 0
Authentication Timeout : 33
EAP-Start While Authenticating : 0
EAP-Logoff While Authenticating : 0
Successful Authentication : 0
Failed Authentication : 1
Re-Authentication : 0
Successful Re-Authentication : 0
Failed Re-Authentication : 0
EAP-Start When Authenticated : 0
EAP-Logoff When Authenticated : 0
Re-Auths When Authenticated : 0
Cached Re-Authentication : 0
...

```

Example 3: Supplicant timeout (typically occurs when supplicant stops responding):

```

switch# show aaa authentication port-access dot1x authenticator interface all
client-status

Client  FE:04:D7:50:89:37, userxx1, 1/1/1
=====

Status      : Unauthenticated
Type        : Pass-Through
EAP-Method   : MD5
Auth Failure reason : Supplicant-Timeout
Time Since Last State Change : 576s

Authentication Statistics
-----
Authentication      : 631
Authentication Timeout : 631
EAP-Start While Authenticating : 0
EAP-Logoff While Authenticating : 0
Successful Authentication : 0
Failed Authentication : 0
Re-Authentication : 0
Successful Re-Authentication : 0
Failed Re-Authentication : 0
EAP-Start When Authenticated : 0
EAP-Logoff When Authenticated : 0
Re-Auths When Authenticated : 0
Cached Re-Authentication : 0
...

```

Show the EAP handshake statistics:


```

switch# show aaa authentication port-access dot1x authenticator interface all
port-statistics

Port 1/1/1
=====

Authentication Details
-----
Number of Clients           : 2
Number of Authenticated Clients : 1
Number of Unauthenticated Clients : 1
Number of authenticating clients : 0

Authentication Statistics
-----
EAPOL Frames Received           : 25033
EAPOL Frames Transmitted        : 36305
EAPOL Start Frames Received     : 6012
EAPOL Logoff Frames Received    : 0
EAPOL Response ID Frames Received : 18258
EAPOL Response Frames Received  : 763
EAPOL Request ID Frames Transmitted : 34408
EAPOL Request Frames Transmitted : 1137
EAPOL Invalid Frames Received   : 0
EAPOL EAP Length Error Frames Received : 0
EAPOL Last Received Frame Version : 0
EAPOL Last Received Frame Client MAC : 0
...

```

Using other commands

The **debug portaccess dot1x** command:

```

# debug portaccess dot1x
all          Enable all debug modules
config       Enable 802.1X configuration handling logs
packet       Enable 802.1X packet handling logs
protocol     Enable 802.1X protocol handling logs
radius       Enable 802.1X RADIUS request/response logs

```

The **show tech dot1x** and **show events -e** in **port-accessd** commands are also available.

Port access FAQ

1. What 802.1X (dot1x) version is supported?

AOS-CX switches support the 2010 version of 802.1X.

2. What is port access authentication mode client mode?

In client mode, all clients connecting to the port are sent for authentication.

The maximum number of clients allowed to connect to the port is limited by the client limit value configured with the **aaa authentication port-access client-limit** command.

3. What is port access authentication mode device mode?

In device mode, only the first client connecting to the port is sent for authentication. Once this client is authenticated, the port is considered as open and all subsequent clients trying to connect on that port are not sent for authentication.

4. What is default authentication precedence?

The default authentication precedence is 802.1X authentication then MAC authentication. This can be configured differently.

5. What special port access roles are supported?

AOS-CX switches support the following special port access roles:

- Critical role: the role that is applied when the RADIUS server is unreachable for authentication.
- Preauth role: the role that is applied when authentication is still in progress.
- Reject role: the role that is applied when authentication has failed.
- Auth role: the role that is applied to authenticated clients when a specific role is not assigned in the RADIUS server.

6. How do I log off specific interface clients?

Use command **port-access log-off client interface** to log-off any specific interface or all clients.

References

- [AOS-CX Switch Simulator](#)

Multidomain authentication

Multidomain authentication allows a combination of voice and data clients to be authenticated on a port. By default only one voice client and one data client is allowed for authentication. You can configure a maximum of five data clients for authentication. You can enable the multidomain authentication mode with the `aaa authentication port-access auth-mode` command. You can configure only the number of data clients supported with the `aaa authentication port-access client-limit multi-domain` command.

Multidomain authentication requirements

Following are the requirements for multidomain authentication:

- You must configure the multidomain authentication mode by one of the following ways:
 - In the CLI with the **aaa authentication port-access auth-mode** command at the interface level
 - Configure **Aruba-Port-Auth-Mode** and **Aruba-Device-Traffic-Class** VSAs on the RADIUS server
 - In the CLI with the `auth-mode` command at the port access role level (**config-pa-role** context)
- In case the multidomain mode is not enabled on port in the CLI or the **Aruba-Port-Auth-Mode** VSA is not configured, then the switch operates as a client mode on that port, even if the **Aruba-Device-Traffic-Class** VSA is configured.
- To identify the client as a voice client, you must configure either the **device-traffic-class** parameter in the role or the **Aruba-Device-Traffic-Class** VSA (value=1) in the RADIUS server.

- If both are configured, then the **device-traffic-class** configuration overrides the VSA attribute configuration.
- If both are not configured, then the switch considers the client as a data client only.
- A role **critical-voice-role** is applied when an authenticated client fails to reauthenticate because the RADIUS server is unreachable.

This role is not applied when the multidomain authentication mode is not enabled and the client fails to reauthenticate because the RADIUS server is unreachable.



The voice client must first be authenticated successfully with the RADIUS server for the `critical-voice-role` to be applied. If the client is never authenticated, then this role is not applied.

Scenarios with Aruba-Port-Auth-Mode and Aruba-Device-Traffic-Class VSAs

The following table lists the various scenarios when you configure the `Aruba-Port-Auth-Mode` and **Aruba-Device-Traffic-Class** VSAs, and the output in multidomain authentication .

Table 1: *Scenarios configuring authentication mode and traffic class VSAs*

Aruba VSA Configured	Output when Multidomain mode is disabled on port	Output when Multidomain mode is enabled on port
Only Aruba-Device-Traffic-Class VSA is configured	■ Port will be in client mode ■ Client will be authenticated as data or voice client based on Aruba-Device-Traffic-Class VSA	■ Port will be in multidomain mode ■ Client will be authenticated as data or voice client based on Aruba-Device-Traffic-Class VSA
Only Aruba-Port-Auth-Mode VSA configured with multidomain mode	■ Port will be in multidomain mode ■ Client will be authenticated as data client only	
■ <code>Aruba-Port-Auth-Mode</code> VSA configured with multidomain mode ■ Aruba-Device-Traffic-Class VSA is configured	■ Port will be in multidomain mode ■ Client will be authenticated as data or voice client based on <code>Aruba-Device-Traffic-Class</code> VSA	
■ <code>Aruba-Port-Auth-Mode</code> VSA configured with client or device mode ■ Aruba-Device-Traffic-Class VSA is configured	■ Port will be in client or device mode based on Aruba-Port-Auth-Mode VSA ■ Client will be authenticated as data or voice client based on Aruba-Device-Traffic-Class VSA	
Only Aruba-Port-Auth-Mode VSA configured with client or device mode	Port will be in client or device mode based on Aruba-Port-Auth-Mode VSA	

Scenarios with device-traffic-class configuration in role

Following are some of the scenarios of configuring `device-traffic-class` in the role and the output in multidomain authentication.

- Scenario 1: When multidomain mode is enabled on port and the `auth-mode` is not configured in the role.
 - Port will be in multi-domain mode.
 - If **device-traffic-class** is configured in role, then the client will be authenticated as voice, else will be authenticated as data client.
- Scenario 2: When multidomain mode is enabled on port and the **auth-mode** is configured as client or device mode.
 - Port will be in client or device mode based on **auth-mode** configuration in role.
 - If **device-traffic-class** is configured in role, then the client will be authenticated as voice, else will be authenticated as data client.
- Scenario 3: When multidomain mode is not enabled on port and **auth-mode** is configured with multidomain mode in role.
 - Port will be in multi-domain mode.
 - If **device-traffic-class** is configured in role, then the client will be authenticated as voice, else will be authenticated as data client.
- When multidomain mode is not enabled on port and **auth-mode** is not configured in role.
 - Port will be in client mode.
 - If **device-traffic-class** is configured in role, then the client will be authenticated as voice, else will be authenticated as data client.

Port access security violation

A security violation state of a port indicates whether the port is in a state where its client limit has been violated. This state is reset in one of the following ways:

- When the port is shutdown administratively.
- When the port security or authentication method is disabled on the port.
- When the port comes up automatically because of auto recovery.
- When violation action configuration is changed on the port.

Port access security violation commands

port-access security violation action

```
port-access security violation action {notify | shutdown}
no port-access security violation action
```

Description

Configures the action that the switch must take whenever a security violation occurs at a port, such as the number of clients exceeding the configured client limit. This command can be issued from the interface (**config-if**) or Link Aggregation Group (**config-lag-if**) contexts.

The **no** form of the command resets the action to the default action, notify.

Parameter	Description
<code>notify</code>	Specifies that the switch notifies any security violation as an event or log in the syslog server, and also sends an SNMP trap

Parameter	Description
	notification. This action is the default. The format of the event log that is generated for notifying the security violation is: Client limit exceeded on port <PORT> , caused by an unauthenticated client <MAC-ADDRESS> .
shutdown	Specifies that the switch shuts down the port where the client limit has exceeded. A port that is shut down can be configured to auto-recover after a recovery period that can be configured with the port-access security violation action shutdown auto-recovery and port-access security violation action shutdown recovery-timer commands.

Examples

Configuring the shutdown security violation action for interface 1/1/1:

```
switch(config)# interface 1/1/1
switch(config-if)# port-access security violation action shutdown
```

Resetting the security violation action to the default value:

```
switch(config-if)# no port-access security violation action
```

Configuring the shutdown security violation action for a LAG port:

```
switch(config)# interface lag 1
switch(config-lag-if)# port-access security violation action shutdown
```

Command History

Release	Modification
10.13	This command can be issued from a Link Aggregation Group (LAG) context.
10.09	Command introduced on the 8360

Command Information

Platforms	Command context	Authority
8100 8360	config-if config-lag-if	Administrators or local user group members with execution rights for this command.

port-access security violation action shutdown auto-recovery

```
port-access security violation action shutdown auto-recovery {enable | disable}
no port-access security violation action shutdown auto-recovery {enable | disable}
```

Description

Configures auto-recovery of the port when the security violation action is configured as shutdown. This configuration allows the port, that is shut down when a security violation occurs, to be automatically enabled after the recovery timer expires. The **no** form of the command resets auto-recovery to the default, disable.

Parameter	Description
enable	Enables auto-recovery of port when the security violation action is configured as shutdown.
disable	Disables auto-recovery of port when the security violation action is configured as shutdown.

Examples

Enabling auto-recovery of port:

```
switch(config-if)# port-access security violation action shutdown auto-recovery enable
```

Disabling auto-recovery of port:

```
switch(config-if)# no port-access security violation action shutdown auto-recovery
```

Command History

Release	Modification
10.09	Command introduced on the 8360

Command Information

Platforms	Command context	Authority
8100 8360	config-if	Administrators or local user group members with execution rights for this command.

port-access security violation action shutdown recovery-timer

```
port-access security violation action shutdown recovery-timer <RECOVERY-TIME>  
no port-access security violation action shutdown recovery-timer
```

Description

Configures security violation recovery timer for the port when the security violation action is configured as shutdown.

The **no** form of the command resets the shutdown recovery timer to the default, 10.

Parameter	Description
<RECOVERY-TIME>	Specifies the recovery timer (in seconds) after which the port,

Parameter	Description
	which is shut down because of security violation, is automatically enabled. Default: 10. Range: 10 to 600.

Examples

Configuring the shutdown recovery-timer on a port:

```
switch(config-if)# port-access security violation action shutdown recovery-timer 60
```

Resetting the shutdown recovery-timer to the default value:

```
switch(config-if)# no port-access security violation action shutdown recovery-timer
```

Command History

Release	Modification
10.09	Command introduced on the 8360

Command Information

Platforms	Command context	Authority
8100 8360	config-if	Administrators or local user group members with execution rights for this command.

show interface

```
show interface <INTERFACE-NAME>
```

Description

Displays active configurations and operational status information for interfaces including the reason for the port shutdown because of a security violation at the port.

Parameter	Description
<INTERFACE-NAME>	Specifies the interface name.

Examples

The following example shows the status of the interface when it is shutdown because of security violation:

```
switch# show interface 3/1/35

Interface 3/1/25 is down
Admin state is up
```

State information: Disabled by port-access
Link state: down for 53 minutes (since Tue Jun 01 01:27:28 UTC 2021)

Command History

Release	Modification
10.09	Command introduced on the 8360

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show port-access aaa violation interface

show port-access aaa violation interface {all|<INTERFACE>}

Description

Shows information about violations that have occurred and the count of violations for port access authentication methods at the interfaces.

Parameter	Description
all	Specifies all interfaces.
<INTERFACE>	Specifies the interface name or a comma-separated list of interfaces, or a hyphen-separated interface range.

Examples

Showing information for violations for all interfaces:

```
switch# show port-access aaa violation interface all

Client limit exceeded violation status

-----
Port          Violation      Violation-Count
-----
1/1/1         No             0
1/1/2         Yes            10
1/1/5         No             10
```

Showing information for violations on interfaces 1/1/1 to 1/1/2:

```
switch# show port-access aaa violation interface 1/1/1-1/1/2

Client limit exceeded violation status
```


Port	Violation	Violation-Count
1/1/1	No	0
1/1/2	Yes	10

Showing information when no violation action is configured:

```
switch# show port-access aaa violation interface 1/1/1

Port-access aaa violation is not configured
```

Command History

Release	Modification
10.09	Command introduced on the 8360.

Command Information

Platforms	Command context	Authority
8100 8360	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show port-access port-security violation client-limit-exceeded interface

```
show port-access port-security violation client-limit-exceeded interface
{all|<INTERFACE>}
```

Description

Shows information on the number of client-limit-exceeded security violations that have occurred. The output can be filtered by interface.

Parameter	Description
all	Specifies all interfaces.
<INTERFACE>	Specifies the interface name or a comma-separated list of interfaces, or a hyphen-separated interface range.

Examples

Showing information for all ports:

```
switch# show port-access port-security violation client-limit-exceeded interface
all

Client limit exceeded violation status

-----
Port          Violation      Violation-Count
-----
```

```

-----
1/1/1      No      0
1/1/2      Yes     10
1/1/5      No      10

```

Showing information for a port range:

```

switch# show port-access port-security violation client-limit-exceeded interface
1/1/1-1/1/2

```

Client limit exceeded violation status

```

-----
Port      Violation      Violation-Count
-----
1/1/1      No              0
1/1/2      Yes             10

```

Command History

Release	Modification
10.09	Command introduced on the 8360.

Command Information

Platforms	Command context	Authority
8100 8360	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

Port access policy

Port access policy allows network administrators to define a set of rules. These rules are used to restrict or alter the passage of traffic for clients onboarding to a switch that has port security (802.1X, MAC authentication) enabled.

Unlike classifier policies, which are associated with individual front plane port, Link Aggregation Group (LAG), and VLAN or tunnel interface, port-access policies are associated with roles. Based on the role associated with a user after authentication, the policy is applied to the user.

The switch can obtain policies from any of the following sources:

- Local: Policies configured locally on the switch.
- RADIUS: Policies configured using the NAS-Filter-Rule or Aruba-NAS-Filter-Rule RADIUS attributes.



Both local and downloaded type of policies do not have any standards associated with them. Policies that are obtained from the RADIUS server must support all criteria that can be defined using the **NAS-Filter-Rule** attribute.

Classes and actions supported by port access policies

Port access policies support IPv4- and IPv6-based classes, and the following actions.

- **cir**: Set the bandwidth limit for guaranteed traffic.
- **drop**: Drop the packet.
- **dscp**: Remark the 6-bit field in the IP header for packet classification.
- **ip-precedence**: Remark the 3-bit field in the IP header which denotes the priority of the datagram.
- **local-priority**: Change the internal priority that is used to queue the packets for transmission.

RADIUS policies

A RADIUS policy is a port-access policy derived from the combination of the following RADIUS attributes for a client:

- Filter-ID (IETF attribute, Type=11)
- NAS-Filter-Rule (IETF attribute, Type=92)
- Aruba-NAS-Filter-Rule (Aruba VSA, Type=51)

The name of a RADIUS policy is prefixed with RADIUS_. Clients with identical values for these attributes will share the same RADIUS policy on the system. A RADIUS policy cannot be modified by an administrator and is deleted when the last client referring the policy is removed from the system (or switches to a different policy).



The **Base Policy** in **show port-access policy** is the policy associated with the base role that is RADIUS overridden. For non-RADIUS type policies and policies derived from RADIUS attributes (Filter-ID/[Aruba-]NAS-Filter-Rule), N/A (Not Applicable) is shown against the **Base Policy**.



For RADIUS policies derived from the Filter-ID attribute the name associated with each Filter-ID (ACL names) is shown against ACL names. For non-RADIUS policies and policies derived from [Aruba-]NAS-Filter-Rule attribute, an N/A (Not Applicable) is shown against ACL names.

Filter-ID

The Filter-ID attribute is used to apply an existing ACL on the system to a client. Only ACLs of type IPv4 and IPv6 are supported. MAC type ACLs are not supported.

ACLs that match on any of the following fields are not supported:

- Source/destination MAC
- Ether-type
- PCP
- VLAN
- Source/destination IP group
- Source/destination L4 port group

The set of Filter-IDs passed for a client is translated to a RADIUS policy by the system and applied to the client using the ACL definition at that point in time. A change in the ACL after the RADIUS policy is applied will not take affect. The filter-ID attribute can't co-exist with NAS-Filter-Rule or Aruba-NAS-Filter-Rule.

NAS-Filter-Rule

The syntax followed for NAS-Filter-Rule is according to RFC 3588 section 4.3. The syntax is as follows:

action dir proto from src to dst [options]

The keywords supported for each field of a NAS-Filter-Rule are:

- action - (permit|deny)
- dir - in
- proto - (icmp|igmp|tcp|udp|sctp|ah|esp|gre|ospf|pim|ip) and IP protocols from 0 to 255
- src and dst - Both IPV4 and IPV6 address are supported with an optional mask. The keyword "any" is also supported. The L4 port range is supported which is an optional field (0 to 65535). Currently only consecutive port ranges are supported.
- Options:
 - frag
 - ipoptions (ssrr|lsrr|rr|ts) - Not supported.
 - tcptoptions (mss|window|sack|ts|cc) - Not supported.
 - established - This will work only with TCP packets.
 - setup - Not supported.
 - tcpflags (fin|syn|rst|psh|ack|urg) - Only supported with TCP packets. The comma is used to provide more than one TCP flag.
 - icmptypes (0|3|4|5|8|9|10|11|12|13|14|15|16|17|18|echo reply|destination unreachable|source quench|redirect|echo request|router advertisement|router solicitation|time-to-live exceeded|ip header bad|timestamp request|timestamp reply|information request|information reply|address mask request|address mask reply) - This will work only with the ICMP packets. The comma is used to provide more than one ICMP type.

These options can be used in any order after the **dst** field of the NAS-Filter-Rule. All of these keywords are case-sensitive.

Examples

- NAS-Filter-Rule = "permit in 10 from any to any"
- NAS-Filter-Rule = "permit in udp from any 10-100 to 192.10.10.1/24"
- NAS-Filter-Rule = "deny in icmp from 10.10.10.1 to any 27"
- NAS-Filter-Rule = "permit in pim from 10.10.10.1/8 1000 to 192.10.10.1/24 23000"
- NAS-Filter-Rule = "deny in tcp from any 10 to 10.0.10.10 tcpflags ack,fin,rst frag established"
- NAS-Filter-Rule = "permit in icmp from 10.10.10.1 to any 27 icmptypes 0, redirect"
- NAS-Filter-Rule = "deny in tcp from any 50000-55000 to fe80::d1:1/120 65055-65535"
- NAS-Filter-Rule = "permit in udp from any 7,9,17-50,65530-65535 to 40.40.40.3"
- NAS-Filter-Rule = "permit in udp from any to 40.40.40.10 41-58,59,180-224"
- NAS-Filter-Rule = "permit in udp from any 11,13,20-23 to 40.40.40.100 38,39,41-43"

Aruba-NAS-Filter-Rule

The syntax for Aruba-NAS-Filter-Rule is similar to NAS-Filter-Rule with the following extensions:

- cp-redirect - A new action to redirect packets matching the rule to the captive-portal service.
- cnt - Track hit counts for the entry.
- v4/v6 - Create an IPv4 (for v4) or IPv6 (for v6) only entry for a filter rule. When both source and destination IP addresses are wildcarded, hardware entries are created for both IPv4 and IPv6 classes.

Use this option to restrict the switch to only create hardware entries for the specific IP type and save space in the hardware.

Aruba-NAS-Filter-Rule VSA can co-exist with the NAS-Filter-Rule. The system will combine entries across both the attributes and create a single RADIUS policy.

Examples

- Aruba-NAS-Filter-Rule = "cp-redirect in 10 from any to any"
- Aruba-NAS-Filter-Rule = "permit in sctp from 10.0.0.1 to 10.0.0.4"
- Aruba-NAS-Filter-Rule = "permit in icmp from any to any cnt"
- Aruba-NAS-Filter-Rule = "permit in tcp from any to any v4"
- Aruba-NAS-Filter-Rule = "permit in sctp from any to any v6"



A single IPv4 rule consumes 2 hardware entries while a single IPv6 rule consume 4 hardware entries. If an IPv4-only rule is configured, 4 hardware entries otherwise used to match IPv6 frames are saved. Similarly if an IPv6-only rule is configured, 2 hardware entries otherwise used to match IPv4 frames are saved.

Limitations

- If a downloaded role containing one or more unused classes or policies is downloaded again within 30 seconds then client authorization will fail. It is recommended to not have unused classes or policies in a downloaded role.
- When a port-access policy is updated while the port-access daemon is not running all the clients associated with the policy will be logged off when the daemon restarts.
- RADIUS policies can have up to 128 entries in a single class and up to 128 entries in the policy.
- The maximum number of NAS-Filter-Rule attributes in a single RADIUS Access-Accept frame is either the number of rules that can fit inside a single RADIUS packet (4KB) or 128, whichever is lower. RADIUS servers may truncate rules if the frame size goes beyond 4KB. If that occurs then the switch will mark those roles as Invalid and clients associated with those roles will be unauthorized on the switch.

Port access policy commands

port-access policy

```
port-access policy <POLICY-NAME>
  [<SEQUENCE-NUMBER>]
  class {ip|ipv6} <CLASS-NAME> action {<REMARK-ACTIONS> | <POLICE-ACTIONS> | <OTHER-
  ACTIONS>}
  comment <text>
```

Description

Creates or modifies a policy and policy entries. A policy is made up of one or more policy entries ordered and prioritized by sequence numbers. Each entry has an IPv4/IPv6 class and one or more policy actions associated with it.

A policy must be applied to a role using the **associate policy** command.

The **no** form of the command can be used to delete either a policy (use **no** with the policy command) or an individual policy entry (use **no** with the sequence number).

Parameter	Description
<code><POLICY-NAME></code>	Specifies the policy name.
<code><SEQUENCE-NUMBER></code>	Specifies the policy entry sequence number. Range: 1 to 4294967295.
<code>class {ip ipv6} <CLASS-NAME></code>	Specifies the class type and name.
<code><REMARK-ACTIONS></code>	These remark actions are available: <code>ip-precedence <IP-PRECEDENCE-VALUE></code> Specifies the numeric IP precedence value. Range: 0 to 7. <code>dscp <DSCP-VALUE></code> Specifies a Differentiated Services Code Point (DSCP) value. Enter either a keyword or numeric value (0 to 63). See <i>DSCP keywords and corresponding values</i> below. <code>pcp <PCP-VALUE></code> Specifies a pcp value. <code>local-priority <LOCAL-PRIORITY-VALUE></code> Specifies a local priority value. Range: 0 to 7.
<code><POLICE-ACTIONS></code>	These police actions are available: <code>cir kbps <RATE-KBPS></code> Specifies a Committed Information Rate (CIR) value in kbps. Range: 1 to 4294967295. <code>cbs <BYTES></code> Specifies a Committed Burst Size (CBS) value in bytes. Range: 1 to 4294967295. <code>exceed</code> Specifies the action to take on packets that exceed the rate limit.
<code><OTHER-ACTIONS></code>	These other actions are available: <code>drop</code> Selects drop of all traffic. <code>redirect</code> Selects redirect of all traffic to a captive portal server.
<code>comment</code>	Specifies a policy entry comment.

DSCP keywords and corresponding values

Keyword	Value	Description
AF11	10	DSCP 10 (Assured Forwarding Class 1, low drop probability)
AF12	12	DSCP 12 (Assured Forwarding Class 1, medium drop probability)
AF13	14	DSCP 14 (Assured Forwarding Class 1, high drop probability)
AF21	18	DSCP 18 (Assured Forwarding Class 2, low drop probability)
AF22	20	DSCP 20 (Assured Forwarding Class 2, medium drop probability)

Keyword	Value	Description
AF23	22	DSCP 22 (Assured Forwarding Class 2, high drop probability)
AF31	26	DSCP 26 (Assured Forwarding Class 3, low drop probability)
AF32	28	DSCP 28 (Assured Forwarding Class 3, medium drop probability)
AF33	30	DSCP 30 (Assured Forwarding Class 3, high drop probability)
AF41	34	DSCP 34 (Assured Forwarding Class 4, low drop probability)
AF42	36	DSCP 36 (Assured Forwarding Class 4, medium drop probability)
AF43	38	DSCP 38 (Assured Forwarding Class 4, high drop probability)
CS0	0	DSCP 0 (Class Selector 0: Default)
CS1	8	DSCP 8 (Class Selector 1: Scavenger)
CS2	16	DSCP 16 (Class Selector 2: OAM)
CS3	24	DSCP 24 (Class Selector 3: Signaling)
CS4	32	DSCP 32 (Class Selector 4: Real time)
CS5	40	DSCP 40 (Class Selector 5: Broadcast video)
CS6	48	DSCP 48 (Class Selector 6: Network control)
CS7	56	DSCP 56 (Class Selector 7)
EF	46	DSCP 46 (Expedited Forwarding)

Usage

- An applied policy processes the packet sequentially against policy and class entries in the list, until either the last policy entry in the list has been evaluated or the packet matches an entry. If there is no match, the packet will be dropped by one of the implicit **deny all** IPv4 and IPv6 entries.
- Entering an existing **<POLICY-NAME>** value will cause the existing policy to be modified, with any new **<SEQUENCE-NUMBER>** value creating an additional policy entry, and any existing **<SEQUENCE-NUMBER>** value replacing the existing policy entry with the same sequence number.
- If no sequence number is specified, a new policy entry will be appended to the end of the entry list with a sequence number equal to the highest policy entry currently in the list plus 10. The sequence numbers may be reordered with the **port-access policy <POLICY-NAME> resequence <STARTING-SEQ-NUM> <INCREMENT>** command.
- If a policy is configured without any action, the default action, **permit**, is applied for that policy.

Examples

Creating a policy with several class entries:

```

switch(config)# port-access policy POL1
switch(config-pa-policy)# 10 class ip dns
switch(config-pa-policy)# 20 class ip dhcp
switch(config-pa-policy)# 30 class ip test action cir kbps 1024 exceed drop
switch(config-pa-policy)# exit
switch(config)# show port-access policy POL1

Access Policy Details:
=====

Policy Name      : POL1
Policy Type      : Local
Policy Status    :
SEQUENCE        CLASS                                TYPE ACTION
-----
10              dns                                ipv4 permit
20              dhcp                                ipv4 permit
30              test                                ipv4 cir kbps 1024 cbs 2048 exceed drop

```

Adding a comment to an existing class entry:

```

switch(config)# port-access policy POL1
switch(config-pa-policy)# 20 comment DHCP-PERMIT
switch(config-pa-policy)# exit
switch(config)# show run port-access policy POL1

port-access policy POL1
  10 class ip dns
  20 class ip dhcp
  20 comment DHCP-PERMIT
  30 class ip test action cir kbps 1024 cbs 2048      exceed drop

```

Removing a comment from an existing class entry:

```

switch(config)# port-access policy POL1
switch(config-pa-policy)# no 20 comment
switch(config-pa-policy)# exit
switch(config)# show run port-access policy POL1

port-access policy POL1
  10 class ip dns
  20 class ip dhcp
  30 class ip test action cir kbps 1024 cbs 2048 exceed drop

```

Modifying a policy by replacing one class with another at the same sequence number:

```

switch(config)# port-access policy POL1
switch(config-pa-policy)# 10 class ip mds action dscp af21
switch(config-pa-policy)# exit
switch(config)# show port-access policy POL1

Access Policy Details:
=====

Policy Name      : POL1
Policy Type      : Local
Policy Status    : Applied

```


SEQUENCE	CLASS	TYPE	ACTION
10	mds	ipv4	dscp AF21
20	dhcp	ipv4	permit
30	test	ipv4	cir kbps 1024 cbs 2048 exceed drop

Removing a class:

```
switch(config)# port-access policy POL1
switch(config-pa-policy)# no 10
switch(config-pa-policy)# exit
switch(config)# show port-access policy POL1
```

Access Policy Details:
=====

Policy Name : POL1
Policy Type : Local
Policy Status : Applied

SEQUENCE	CLASS	TYPE	ACTION
20	dhcp	ipv4	permit
30	clearpass-web	ipv4	cir kbps 1024 cbs 2048 exceed drop

Command History

Release	Modification
10.13	Added support for reflect action.
10.09	Command introduced on the 8360

Command Information

Platforms	Command context	Authority
8100 8360	config The <code>policy</code> command takes you into the <code>config-pa-policy</code> context where you enter the policy entries.	Administrators or local user group members with execution rights for this command.

port-access policy copy

port-access policy <POLICY-NAME> copy <DESTINATION-POLICY>

Description

Copies an existing policy to a new policy.

Parameter	Description
<POLICY-NAME>	Specifies the existing policy name.
<DESTINATION-POLICY>	Specifies the destination policy name.

Examples

Copying a policy:

```
switch(config)# port-access policy POL1 copy POL1_copy
switch(config)# show port-access policy
```

```
Access Policy Details:
=====
```

```
Policy Name   : POL1
Policy Type   : Local
Policy Status : Applied
```

SEQUENCE	CLASS	TYPE	ACTION
20	dhcp	ipv4	permit
30	test	ipv4	cir kbps 1024 exceed drop

```
Policy Name   : POL1_copy
Policy Type   : Local
Policy Status : Applied
```

SEQUENCE	CLASS	TYPE	ACTION
20	dhcp	ipv4	permit
30	test	ipv4	cir kbps 1024 exceed drop

Command History

Release	Modification
10.09	Command introduced on the 8360

Command Information

Platforms	Command context	Authority
8100 8360	config	Administrators or local user group members with execution rights for this command.

port-access policy resequence

```
port-access policy <POLICY-NAME> resequence <STARTING-SEQ-NUM> <INCREMENT>
```

Description

Resequences numbering in a policy.

Parameter	Description
<POLICY-NAME>	Specifies the policy to be resequenced.
<STARTING-SEQ-NUM>	Specifies the starting sequence number. Range: 1 to 4294967295.
<INCREMENT>	Specifies the sequence number increment.

Examples

Resequencing a policy starting at 5 with an increment of 10:

```
switch(config)# port-access policy POL1 resequence 5 10
switch(config)# show port-access policy POL1
```

Access Policy Details:

=====

```
Policy Name      : POL1
Policy Type      : Local
Policy Status    : Applied
```

SEQUENCE	CLASS	TYPE	ACTION
5	dhcp	ipv4	permit
15	test	ipv4	cir kbps 1024 exceed drop

Command History

Release	Modification
10.09	Command introduced on the 8360

Command Information

Platforms	Command context	Authority
8100 8360	config	Administrators or local user group members with execution rights for this command.

port-access policy reset

```
port-access policy <POLICY-NAME> reset
```

Description

Resets the policy configuration to match the current hardware configuration of the policy.

Parameter	Description
<POLICY-NAME>	Specifies the name of the policy to be reset.

Examples

Resetting a policy:

```

switch(config)# port-access policy POL2
switch(config-pa-policy)# 20 class ip dhcp
switch(config-pa-policy)# 40 class test2 action cir kbps 1024 exceed drop
switch(config-pa-policy)# exit
switch(config)# show port-access policy POL1-V2

Access Policy Details:
=====

Policy Name      : POL2
Policy Type      : Local
Policy Status    : Applied

SEQUENCE      CLASS                                TYPE ACTION
-----
20            dhcp                                ipv4 permit
40            test2                               ipv4 cir kbps 1024 exceed drop

switch(config)# port-access policy POLV2
switch(config-pa-policy)# 50 class ip test3 action cir kbps 1024 exceed drop
switch(config-pa-policy)# no 20
switch(config-pa-policy)# exit
switch(config)# show port-access policy POL2

Access Policy Details:
=====

Policy Name      : POL2
Policy Type      : Local
Policy Status    : Rejected

SEQUENCE      CLASS                                TYPE ACTION
-----
40            test2                               ipv4 cir kbps 1024 exceed drop
50            test3                               ipv4 cir kbps 1024 exceed drop

switch(config)# port-access policy POL2 reset
Following policy entries will be removed:
class ip test3 action cir kbps 1024 exceed drop

Following policy entries will be added:
20 class ip dhcp

Do you want to continue (y/n)? y
switch(config)# show port-access policy POL2

Access Policy Details:
=====

Policy Name      : POL1-V2
Policy Type      : Local
Policy Status    : Applied

SEQUENCE      CLASS                                TYPE ACTION
-----
20            dhcp                                ipv4 permit
40            test2                               ipv4 cir kbps 1024 exceed drop

```

Command History

Release	Modification
10.09	Command introduced on the 8360

Command Information

Platforms	Command context	Authority
8100 8360	config	Administrators or local user group members with execution rights for this command.

clear port-access policy hitcounts

```
clear port-access policy <POLICY-NAME> hitcounts {port|client}
```

Description

Clears statistics and conform rate of a policy applied on a port or client.

Parameter	Description
<POLICY-NAME>	Specifies the policy name.
port	Selects port mode.
client	Selects client mode.

Examples

Clearing policy hit counts:

```
switch# show port-access policy POL6 hitcounts port

Port Access Policy Hit-Counts Details:
=====

Policy Name      : POL4
Policy Type      : Local
Policy Status    : Applied

SEQUENCE CLASS          TYPE ACTION                                CUR-RATE (kbps)
-----
3      test8            ipv4 cir kbps 1024 exceed drop          512

Class Name : dhcp
Class Type : ipv4

SEQUENCE CLASS-ENTRY                                HIT-COUNT
-----
10      match icmp any any count                    0

Class Name : clearpass-web
Class Type : ipv4

SEQUENCE CLASS-ENTRY                                HIT-COUNT
-----
15      match udp any any count                      15101830
```

Class Name : web-traffic
Class Type : ipv4

SEQUENCE	CLASS-ENTRY	HIT-COUNT
10	match any any any count	241
20	match any 10.1.1.1 10.1.1.2 dscp AF11 count	50

Class Name : class6
Class Type : ipv6

SEQUENCE	CLASS-ENTRY	HIT-COUNT
10	match any any any count	173
20	match icmpv6 2001:db8:a::123 2001:db8:a::125 dscp AF11 count	32

```
switch#  
switch# clear port-access policy POL6 hitcounts port  
switch#  
switch# show port-access policy POL6 hitcounts port
```

Port Access Policy Hit-Counts Details:
=====

Policy Name : POL4
Policy Type : Local
Policy Status : Applied

SEQUENCE	CLASS	TYPE	ACTION	CUR-RATE (kbps)
3	test8	ipv4	cir kbps 1024 exceed drop	512

Class Name : dhcp
Class Type : ipv4

SEQUENCE	CLASS-ENTRY	HIT-COUNT
10	match icmp any any count	0

Class Name : clearpass-web
Class Type : ipv4

SEQUENCE	CLASS-ENTRY	HIT-COUNT
15	match udp any any count	0

Class Name : web-traffic
Class Type : ipv4

SEQUENCE	CLASS-ENTRY	HIT-COUNT
10	match any any any count	0
20	match any 10.1.1.1 10.1.1.2 dscp AF11 count	0

Class Name : class6
Class Type : ipv6

SEQUENCE	CLASS-ENTRY	HIT-COUNT
10	match any any any count	0
20	match icmpv6 2001:db8:a::123 2001:db8:a::125 dscp AF11 count	0

Command History

Release	Modification
10.09	Command introduced on the 8360

Command Information

Platforms	Command context	Authority
8100 8360	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show port-access policy

show port-access policy [<POLICY-NAME>]

Description

Shows various aspects of policies and their current usage. Details of a policy including the content of a specific policy is shown.

Policy type values:

- **Local**—User configured policy
- **Downloaded**—Downloaded user policy
- **RADIUS**—Policy obtained from the RADIUS server

Policy status values:

- **Applied**—Policy is successfully applied in the hardware.
- **Rejected**—Policy is not supported in the hardware.
- **In-Progress**—Policy is being processed in the hardware.
- **Failed**—Displayed when the switch fails to apply the policy configuration because the TCAM resources are unavailable or full.

Base Policy Values:

- **Name of the policy**—Policy associated with the RADIUS overridden base role.
- **N/A**—Non-RADIUS policy or policy derived from RADIUS attributes such as Filter ID or [Aruba-]NAS-Filter-Rule

ACL Names Values:

- **Name of the ACL**—Name of the ACL associated with the RADIUS policy derived from RADIUS Filter-ID attribute.
- **N/A**—Non-RADIUS policy or policy derived from [Aruba-]NAS-Filter-Rule RADIUS attribute.



If a policy is configured without any action, the **show** command will represent such an entry with the **permit** action .

Parameter	Description
<POLICY-NAME>	Specifies the policy name.

Examples

Showing information for all policies:

```
switch(config)# show port-access policy

Access Policy Details:
=====

Policy Name      : POL1
Policy Type      : Local
Policy Status    : Applied
Base Policy      : N/A
ACL Name         : N/A

SEQUENCE    CLASS                                TYPE ACTION
-----
20          dhcp                                ipv4 permit
30          test                                ipv4 cir kbps 1024 exceed drop

Policy Name      : POL1_copy
Policy Type      : Local
Policy Status    : Applied
Base Policy      : N/A
ACL Name         : N/A

SEQUENCE    CLASS                                TYPE ACTION
-----
20          dhcp                                ipv4 permit
30          test                                ipv4 cir kbps 1024 exceed drop
```

Showing information for a particular policy:

```
switch(config)# show port-access policy RADIUS_115315236

Access Policy Details:
-----

Policy Name      : RADIUS_115315236
Policy Type      : Radius
Policy Status    : Applied
Base Policy      : N/A
ACL Names        : DHCP, WebServices-Student

SEQUENCE    CLASS                                TYPE ACTION
-----
10          RADIUS_3241199543_2521983626  ipv4 permit

switch(config)# show port-access policy RADIUS_407949976

Access Policy Details:
-----

Policy Name      : RADIUS_407949976
Policy Type      : Radius
Policy Status    : Applied
Base Policy      : test_policy_test_cppm_role-3006-1
ACL Names        : N/A

SEQUENCE    CLASS                                TYPE ACTION
-----
```


Command History

Release	Modification
10.12	Command output modified to display Base Policy and ACL Names .
10.09	Command introduced on the 8360

Command Information

Platforms	Command context	Authority
8100 8360	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show port-access policy hitcounts

```
show port-access policy <POLICY-NAME> hitcounts {port | client}
```

Description

Shows port access hit count statistics.

Parameter	Description
<POLICY-NAME>	Specifies the policy name.
port	Selects port mode.
client	Selects client mode.

Examples

Showing policy hit counts (statistics) with current rate:

```
switch# show port-access policy POL6 hitcounts port

Port Access Policy Hit-Counts Details:
=====

Policy Name   : POL1
Policy Type   : Local
Policy Status : Applied

SEQUENCE CLASS      TYPE ACTION                                CUR-RATE (kbps)
-----
30      test8      ipv4 cir kbps 1024 exceed cbs 2048 drop      512

Class Name : dhcp
Class Type : ipv4
```

SEQUENCE	CLASS-ENTRY	HIT-COUNT
10	match icmp any any count	982150
Class Name : clearpass-web Class Type : ipv4		
SEQUENCE	CLASS-ENTRY	HIT-COUNT
70	match udp any any count	15101830
Class Name : web-traffic Class Type : ipv4		
SEQUENCE	CLASS-ENTRY	HIT-COUNT
4	match any any any count	3194
5	match any 10.1.1.1 10.1.1.2 dscp AF11 count	1716
Class Name : class6 Class Type : ipv6		
SEQUENCE	CLASS-ENTRY	HIT-COUNT
10	match any any any count	0
20	match icmpv6 2001:db8:a::123 2001:db8:a::125 dscp AF11 count	0

Command History

Release	Modification
10.09	Command introduced on the 8360

Command Information

Platforms	Command context	Authority
8100 8360	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

Port access role

Every device that connects to a port is associated with a role. Roles are associated with all clients, both authenticated and unauthenticated, and applied to each user session. By default, roles are enabled on a switch.

Following are a few examples of user role names and the access privileges that can be configured:

- Employee—Provide complete access to network resources.
- Contractor—Provide limited access to network resources.
- Guest—Provide only Internet browsing access.

Each user role determines the client network privileges, frequency of reauthentication, applicable bandwidth contracts, and other permissions.



Active user roles applied on clients are created only on Ternary Content-Addressable Memory (TCAM) resource availability of the switch.

A user role consists of the following optional parameters:

- `Ingress user policy`
L3 (IPv4 and/or IPv6) ordered list of classes with actions.
- `inactivity-timeout`
The inactivity timeout period in seconds with a range of 300 to 4294967295 for the authenticated client for an implicit logoff.
- `reauth-period`
Sets the reauthentication period in seconds or 0 to disable.
- `vlan access`
Sets the untagged VLAN ID.
- `vlan trunk`
Sets the tagged VLAN ID.
- `auth-mode`
Configures the authentication mode for the clients that are associated with the current role. Available modes are: **client-mode**, **device-mode**, **multi-domain**.
- `poe-priority`
Specifies the PoE priority for the interface.
- `mtu`
Configures the MTU support for the client.
- `vlan trunk allowed`
Specifies the list of tagged VLANs configured for the interface.
- `trust-mode`
Configures the QoS trust mode for the client.
- `private-vlan`
Configures PVLAN port type for a user role. The following are the attributes:
 - `promiscuous`
Configures the port type as promiscuous.
 - `secondary`
Configures the port type as secondary.

Operational notes

Following are some of the operational notes to be considered for port access roles:

- When roles are enabled, they are applied to all devices connected to ports where authentication is configured.
- Special roles, such as, critical, reject, pre-auth, and auth are applied depending on the authentication state of the device.
- Roles can be applied in one of the following two ways:
 - Vendor-Specific Attribute (VSA)-Derived Role
Type: **RADIUS: Aruba**

Name: **Aruba-User-Role**

ID: **25**

Value: `<myUserRole>`

See [Vendor-Specific Attributes supported in session authorization](#).

The RADIUS server (ClearPass Policy Manager server) determines how the VSA-Derived Role is applied to the user. The role is sent to the switch through a RADIUS VSA. The VSA derived role will have the same precedence order as the authentication type (802.1X, MAC authentication).

- User Derived Role (UDR)

The UDR is applied when the roles are enabled.

UDR will have the same precedence order as the authentication type (802.1X, MAC authentication).

Downloadable user roles

Downloadable user roles enable AOS-CX switches to download user roles, policy, and class from the ClearPass Policy Manager server. The download facilitates the configuration of policies and attributes for a specific user role which can then be stored locally on the switch. New users can then be assigned the same locally stored version of the user role in ClearPass Policy Manager server, enabling the administrator to save time in reconfiguring each user individually.

The command **radius-server host WORD clearpass-username WORD clearpass-password (plaintext | ciphertext)** can only be used if the user role is going to be downloaded from the ClearPass Policy Manager server.



Avoid unused classes or policies in a downloaded role, as a downloadable user role that contains one or more unused classes or policies can cause client authorization to fail.

Mixed roles

Mixed roles enable users to create a new RADIUS overridden role by overriding client-role attributes such as VLANs, in one of the following scenarios:

- Combination of LUR (Local User Role) and RADIUS attributes received from the RADIUS server.
- Combination of DUR (Downloadable User Role) and RADIUS attributes received from the RADIUS server.

The new RADIUS overridden role contains the attributes present in both LUR/DUR and RADIUS attributes. If any of the attributes are present in both the RADIUS attributes list, and Local User Role or Downloadable User Role, the RADIUS attributes will take precedence and applied to the clients.

You can use the **aaa authentication port-access radius-override enable** command at the interface context to enable the mixed role feature. With this feature enabled, users can have basic configurations that are common to most of the clients as a LUR/DUR and specify only the client-specific attribute as RADIUS attributes from the server as part of the access response.

If this feature is disabled, when a combination of LUR/DUR along with RADIUS attributes is received from the server, the user roles such as LUR or DUR take precedence and are applied to the clients. The RADIUS attributes in the list are not considered.

Important points to note

- Any changes made to LUR after the creation of a mixed role will not affect the mixed roles. Also, the mixed roles will not be affected even on LUR deletion.

- If LUR/DUR contains VLAN ID and RADIUS attribute contains VLAN name or VLAN group, then the final role will contain both VLAN ID and VLAN name or VLAN group. In this case, VLAN ID takes precedence. If both VLAN ID and VLAN name or group are present, VLAN ID takes precedence.
- The description of the LUR will not be copied to the mixed role during an override.

Limitations

Mixed roles cannot be used in the following scenarios:

- A group-based policy (GBP) is present along with LUR or DUR.
- LUR or DUR with more than 1024 class entries.
- DURs with radius-overridden policy. For example: Aruba-Clearpass-User-Role + (NAS-Filter-Rule/Filter-ID) is not supported.

Supported RADIUS attributes in mixed roles

Following are the RADIUS attributes supported in mixed roles:



The RADIUS attributes that are not supported in mixed roles can be still used for testing purposes.

Supported Radius Attributes in mixed roles	Local User Role	Downloadable User Role
Egress-VLAN-ID	Yes	Yes
Aruba-POE-priority	Yes	Yes
Aruba-QOS-trustmode	Yes	Yes
Framed MTU	Yes	Yes
Session timeout	Yes	Yes
Termination-Action	Yes	Yes

Cached-critical role

The cached-critical role allows the authorization of authenticated clients with the previously applied roles when the RADIUS server is unreachable. When the cached-critical user role feature support is enabled, the MAC address of clients and their applied roles are cached in the system during the client log-off or re-authentication. When the RADIUS server is unreachable, the cached-critical role is applied as a special role to the client. Once the RADIUS server is reachable, cache details are cleared from the switch. The cached-critical role can be enabled at the global or per-interface level.

The cached-critical role can be applied only to the authentication-enabled ports. A maximum of 1024 client entries can be cached in the switch. You can configure a timeout period during which the client details remain cached. On a timeout, the cached entry is removed from the switch within the buffer time of 30 minutes. When the number of clients exceeds the maximum limit of 1024, the first in, first out (fifo) replace mode can be used to replace the oldest cached entry in the switch with a new entry. When the maximum limit of 1024 is reached, the following event log is generated: **Reached the maximum cached-clients limit of 1024 on the switch for Limited Auth-Survivability.**



The cached-critical role feature is not supported when the RADIUS server is not configured in the switch.

By enabling the **persistent-storage** configuration, the cached-critical role support for the clients will be available across switch reboots. With this configuration enabled, the client information is cached in the persistent memory of the switch. The information stored in the persistent storage is updated periodically and the interval between the updates is configurable using the **write-interval** CLI option, with a default interval of 3600 seconds. The update to the persistent storage is only done if there is a difference in the client information since the last write.



- For the cached-critical role feature to work across all types of roles such as LUR, DUR, and RADIUS, it is required to configure the **aaa authentication port-access cached-critical-role persistent-storage enable** command before onboarding clients. If the **persistent-storage** configuration is disabled and re-enabled after client onboarding, the cached-critical role feature will not work specifically for clients with DUR and RADIUS roles.
- Enabling **persistent-storage** on the switch might reduce the lifespan of persistent memory.

The cached details are cleared in one of the following scenarios:

- When the client connects back and received a server response.
- When the client is assigned with the cached-critical role and the server becomes reachable.
- When the client attempts for the authentication request and received a response.
- When the client connects back through different on-boarding methods such as device-profile and port-security.
- When the cached-critical role is disabled at the global level.
- When the cached client details are cleared using the `port-access clear cached-client` command.
- When the cached duration exceeds the configured cached-interval timeout period.
- When the number of clients exceeds the maximum limit of 1024.
- When the role is deleted in the case of LUR.



- Clients with roles such as DUR, VSA, LUR, and mixed roles can be cached.
- Cached-critical role can be applied to UBT clients.

For information on this feature, see the related video on the [Aruba AirHeads Broadcasting Channel](#).

Cached-critical role tasks

The cached-critical role tasks are as follows:

Task	Command name	Example
Entering into the cached-critical role (config-aaa-ccr)	<code>aaa authentication port-access cached-critical-role</code>	<code>switch(config)# aaa authentication port-access cached-critical-role</code>

Task	Command name	Example
context at the global level		
Enabling the cached-critical role (global) (disabled by default)	enable	switch(config-aaa-ccr)# enable
Disabling the cached-critical role (global)	disable	switch(config-aaa-ccr)# disable
Setting the cache-timeout (global)	cache-timeout <HOURS>	switch(config-aaa-ccr)# cache-timeout 72
Setting the cached replace mode (global)	cache-replace-mode {fifo none}	switch(config-aaa-ccr)# cache-replace-mode fifo
Configuring the persistent storage for cached clients.	persistent-storage {enable write-interval <900-86400>}	switch(config)#aaa authentication port-access cached-critical-role switch(config-aaa-ccr)# persistent-storage switch(config-aaa-ccr-ps)# enable switch(config-aaa-ccr-ps)# write-interval 7200
Clearing the cached-critical role clients	port-access clear cached-client [all mac <MACADDR> role <ROLENAME>]	switch(config)# port-access clear cached-client ap_role switch(config)# port-access clear cached-client mac 00:0a:0b:0c:0d:0e
Showing summary	show aaa authentication cached-clients	switch# show port-access cached-clients

Task	Command name	Example
zed informati on of all cached port- access clients	<code>[mac <MAC-ADDRESS>] [role <ROLE-NAME>]</code>	
Enabling or disabling cached- critical role at the per- interface level (enabled by default)	<code>[no] aaa authentication port-access cached-critical-role</code>	<code>switch(config)# interface 1/1/1 switch(config-if)# [no] aaa authentication port-access cached-critical-role</code>

Restrictions

The cached-critical role restrictions are as follows:

- Clients with a role associated with the captive portal profile or MACsec policy cannot be cached. If the captive portal clients have a full access role, then the clients can be cached.
- If the cached-critical role is modified with any of the roles such as critical, reject, pre-auth, fallback, critical voice, or auth, then the client details will not be cached.
- When the cached critical role is modified, then the latest role will get applied.
- Accounting is not supported when the cached-critical role is applied to the clients.
- If captive portal clients have a full access role, then the client details can be cached.
- If the client is assigned with the auth role and the radius override is enabled, then the mixed role will have both VSA and auth roles. In this case, the mixed role will be cached with all the attributes of auth role except the description.
- Client details can be cached only when the clients are fully authenticated. In the interim (auth-success), client details will not be cached upon log-off.

Troubleshooting

If the cached-critical role is not applied to a client:

- Check clients MAC using the `show port-access cached-clients` command.
- Check if the client was authenticated successfully and placed in the final authentication state before logging off.
- Check if the client is in the cached-reauthentication state.
- Check if cache limit has reached and cache-replace mode is configured
- Check if the cached interval configured duration has timed out.
- Check if the client has a captive portal profile or MACsec profile in the role.
- Check if the client is applied with any special roles.
- Check whether the client is onboarded with the device profile if local mac-match is enabled.

- Check if the client is replaced when the cached replace mode is set to FIFO.
- Check if the feature is enabled on the particular interface.
- Check if the feature is enabled globally.
- Check if the client is present on any other port.

Special roles

Special roles are always local roles that are created to support instances when the deployments are not yet complete. They are also helpful when any network issues occur during authentication of devices. Special roles are always purpose-based, that is, they are applied only in instances such as the RADIUS server is not reachable for authentication or when a single role has to be applied across all switches.

The following special roles are available:

- Critical role
- Reject role
- Pre-authentication role
- Auth-role
- Fallback role

Critical role

The critical role is applied to devices when the RADIUS server is unreachable during the first authentication process or during reauthentication. This role helps ensure that the devices have limited access to the network even though the authentication is not completed. Once the RADIUS server is available for authentication, the devices are authenticated and the ultimate role is applied.

Reject role

The reject role is applied when the RADIUS server rejects a device during authentication. The reject role gives restricted access to the device compared to a full access role.

Pre-authentication role

The pre-authentication (pre-auth) role allows a device, such as an IP phone, to have network access before the device is authenticated. The pre-auth role is triggered when a MAC-based client is connected to a switch before being authenticated by the RADIUS server. Devices must be assigned a VLAN to provide network connectivity. Two new VLANs are created for pre-auth role functionality, one for voice traffic and one for data traffic. Pre-auth role VLANs can be configured on the switch individually or within a user-role. Devices that can be connected to the switch without authentication are divided into two categories:

- Devices that send voice traffic.
- Devices that send data traffic.



Either one of pre-auth role VLANs (voice and/or data) or a pre-auth role can be configured for a port. However, both a VLAN and role cannot coexist for an interface. Initial traffic on the port is restricted only by Access Control Lists (ACLs) configured for the port or for VLANs or ACLs in the role.

Impact of pre-auth role on existing features

Unauthenticated devices

Configuring pre-auth role VLAN will change the behavior of unauthenticated devices. Normally, authentication-enabled ports will not provide unauthenticated client any network access until the device is authenticated by the RADIUS server. With pre-auth role VLAN configured, the client will be assigned to the pre-auth role VLAN until the RADIUS server authenticates the device.

Unauthenticated clients will be placed into the VLAN specified in the pre-auth role. After authenticated by the RADIUS server, the client will be placed into the VLAN specified in the RADIUS authentication command string or as specified in the RADIUS authentication accept string.

LLDP-bypass

When LLDP-bypass is enabled on the switch, Aruba APs are not authenticated. Therefore pre-auth role VLAN is not applicable.

Bypass using device-identity

Pre-auth role VLAN is not applicable to VoIP devices because they do not need authentication. It is applicable to PCs that need authentication.

ACLs applied on an interface

If an ACL rule is applied on an interface, which is part of a pre-auth role VLAN, traffic coming through that interface will be affected. Traffic will be affected based on the rule in the ACL.

ACLs applied on a VLAN

If an ACL rule is applied on a pre-auth role VLAN, traffic entering that VLAN will be affected. Traffic will be affected based on the rule in the ACL.

Rate-limiting on an interface

If the traffic is rate-limited on an interface as part of a pre-auth role VLAN, the traffic will be impacted. The traffic will be affected based on the rule in the rate-limiting configuration command.

Authenticated or rejected clients

Clients that are authenticated or rejected by the RADIUS server are given different VLANs. These clients are moved from pre-auth role to new VLANs based on the authentication by the RADIUS server.

MAC pinning

Clients whose MAC addresses are pinned and have undergone authentication will always be treated as authenticated. Pre-auth role VLAN is not applicable in this scenario.

Effect of RADIUS tracking on pre-auth role

If RADIUS tracking is enabled and no RADIUS server is available for authentication, the port will be changed from a pre-auth role VLAN to a critical VLAN. The time taken to move from pre-auth role VLAN to critical VLAN depends on the time it takes for RADIUS tracker to inform the subsystem.

Restrictions

The pre-auth role restrictions are as follows:

- It will not support more than one tagged or untagged VLAN membership either through direct VLAN configuration or through user-roles.
- It is not applicable for authentication methods other than MAC-based.
- It is not available to be configured from WebUI, Menu, or REST.

Auth-role

After the RADIUS server authenticates a device, if no role is configured on the server, it sends an empty access accept packet to the switch. The switch translates this empty packet to assign an auth-role to the device. The switch then checks if an auth-role is configured on that port and assigns this role to the device.

Fallback role

The fallback role is applied to onboarding devices when there is no derived role available for the devices. Following are the conditions for the fallback role to be applied on onboarding devices:

- The device profile local MAC match feature with block-until-profile-applied mode is configured.
- Device profile along with AAA is configured but no match was found for the device profile client.
- AAA method with no reject or critical role is configured, and the connection to RADIUS server failed.
- 802.1X authentication is enabled on the port, but the supplicant of the device timed out to respond to the authentication request.

Port access role commands

associate macsec-policy

```
associate macsec-policy <POLICY-NAME>
no associate macsec-policy [<POLICY-NAME>]
```

Description

Associates a MACsec policy with a role. When a role that has a MACsec policy associated is applied to a port, all data traffic is blocked on the port until a secure channel is successfully established.



If a MACsec policy is associated with a role that is applied on a non-MACsec capable interface, the client will be in an unauthorized state and the port will remain in a blocked state.

The **no** form of this command disassociates the policy from the role.

Parameter	Description
<POLICY-NAME>	Specifies the MACsec policy name. Range: Up to 128 characters.

Examples

Associating a MACsec policy with a role.:

```
switch(config)# port-access role role01
switch(config-pa-role)# associate macsec-policy Client-Connect
```

Disassociating a MACsec policy from a role:

```
switch(config-pa-role)# no associate macsec-policy
```

Command History

Release	Modification
10.10	Command introduced.

Command Information

Platforms	Command context	Authority
8100 8360	config-pa-role The <code>port-access role</code> command takes you into the <code>config-pa-role</code> context.	Administrators or local user group members with execution rights for this command.

associate policy

```
associate policy <POLICY-NAME>
no associate policy <POLICY-NAME>
```

Description

Associates the policy with the current role.

The **no** form of this command dissociates the policy from the role.

Parameter	Description
<POLICY-NAME>	Specifies the policy name to associate with the current role. Range: Up to 64 characters. NOTE: Only those policies created by using the port-access policy command are allowed to be associated with a role. Policies created using the policy command are not allowed to be associated with a role. Policies that are of the downloaded type are not allowed to be associated with a role.

Examples

Associating a policy with a role:

```
switch(config)# port-access role role01
switch(config-pa-role)# associate policy policy01
```

Dissociating a policy from the role:

```
switch(config-pa-role)# no associate policy policy01
```

Command History

Release	Modification
10.09	Command introduced on the 8360

Command Information

Platforms	Command context	Authority
8100	config-pa-role	Administrators or local user group members with execution rights

Platforms	Command context	Authority
8360	The <code>port-access role</code> command takes you into the <code>config-pa-role</code> context.	for this command.

auth-mode

`auth-mode {client-mode | device-mode | multi-domain}`

Description

Configures the authentication mode for the clients that are associated with the current role.

Parameter	Description
<code>client-mode</code>	Selects client mode. In this mode, all clients connecting to the port are sent for authentication.
<code>device-mode</code>	Selects device mode. In this mode, only the first client connecting to the port is sent for authentication. Once this client is authenticated, the port is considered as open and all subsequent clients trying to connect on that port are not sent for authentication.
<code>multi-domain</code>	Selects multidomain mode. In this mode only one voice device is allowed to be authenticated in addition to the configured data devices on a port. By default only one data device is allowed to be authenticated on the multidomain mode along with one voice device. You can configure the maximum number of data devices allowed with the aaa authentication port-access client-limit multi-domain command. If a second voice device or a data device greater than the configured data client limit onboards, a violation is triggered. You must configure a voice VLAN for IP phones to onboard a voice device in the multidomain authentication mode. To authorize a voice device, you must perform one of the following: - Configure the AAA server to send the Aruba-Device-Traffic-Class Aruba VSA with value 1. - Configure the device-traffic-class parameter in the role to be applied to indicate a voice device. Without this VSA value or the device type in the role, the switch considers the voice device as a data device.

Examples

Configuring the client authentication mode:

```
switch(config-pa-role) # auth-mode client-mode
```

Command History

Release	Modification
10.09	Command introduced on the 8360

Command Information

Platforms	Command context	Authority
8100 8360	<code>config-pa-role</code> The <code>port-access role</code> command takes you into the <code>config-pa-role</code> context.	Administrators or local user group members with execution rights for this command.

cached-reauth-period

`cached-reauth-period [<PERIOD>]`
`no cached-reauth-period`

Description

Enables cached reauthentication, setting the period after which clients that associated with the current role must be reauthenticated.

The **no** form of this command disables cached authentication.

Parameter	Description
<code><PERIOD></code>	Specifies the cached reauthentication period (in seconds) for clients associated with the role. Default: 30. Range: 30 to 4294967295.

Examples

Enabling cached reauthentication and setting its period to 200 seconds:

```
switch(config-pa-role)# cached-reauth-period 200
```

Disabling cached reauthentication:

```
switch(config-pa-role)# no cached-reauth-period
```

Command History

Release	Modification
10.09	Command introduced on the 8360

Command Information

Platforms	Command context	Authority
8100 8360	<code>config-pa-role</code> The <code>port-access role</code> command takes you into the <code>config-pa-role</code> context.	Administrators or local user group members with execution rights for this command.

client-inactivity timeout

```
client-inactivity timeout {<CLIENT-INACTIVITY-PERIOD> | none}  
no client-inactivity timeout
```

Description

Configures the period that the switch waits for a response from a client after which it removes the client from the role.

The **no** form of the command resets the timeout period to the default.

Parameter	Description
<CLIENT-INACTIVITY-PERIOD>	Specifies the client inactivity time (in seconds). Default: Dynamic client age-out. Range: 60 to 4294967295
none	Selects no client deletion due to inactivity.

Examples

Configuring client inactivity timer for a role:

```
switch(config-pa-role)# client-inactivity timeout 3600
```

Command History

Release	Modification
10.14	The range of the command has been modified from 60 to 4294967295 seconds.
10.09	Command introduced on the 8360

Command Information

Platforms	Command context	Authority
8100 8360	config-pa-role The port-access role command takes you into the config-pa-role context.	Administrators or local user group members with execution rights for this command.

device-traffic-class

```
device-traffic-class voice  
no device-traffic-class [voice]
```

Description

Configures the voice class of client to associate with the role.



This attribute is applicable only to **critical-voice-role** role. It is not applicable to other special roles such as, **preauth-role**, **reject-role**, and **fallback-role**.

The **no** form of the command resets the class of client to the default, data.

Usage

Traffic class of a client will not be considered as voice unless **device-traffic-class** is set to **voice** the role. In the multidomain mode, clients with a role that do not have the value of the **device-traffic-class** attribute set to voice will be considered as data device.

Examples

Configuring voice device traffic class for role **role01**:

```
switch(config)# port-access role role01
switch(config-pa-role)# device-traffic-class voice
```

Command History

Release	Modification
10.09	Command introduced on the 8360

Command Information

Platforms	Command context	Authority
8100 8360	config-pa-role The port-access role command takes you into the config-pa-role context.	Administrators or local user group members with execution rights for this command.

description

description <ROLE-DESCRIPTION>

Description

Configures the role description.

Parameter	Description
<ROLE-DESCRIPTION>	Specifies the role description. Range: Up to 255 characters.

Examples

Configuring the role description:

```
switch(config-pa-role)# description student role
```

Command History

Release	Modification
10.09	Command introduced on the 8360

Command Information

Platforms	Command context	Authority
8100 8360	config-pa-role The port-access role command takes you into the config-pa-role context.	Administrators or local user group members with execution rights for this command.

mtu

mtu <MTU-SIZE>

Description

Configures the MTU (maximum transmission unit) size of a client for a role.

Parameter	Description
<MTU-SIZE>	Specifies the MTU size in bytes. Range: 68 to 9198.

Examples

Configuring client MTU size:

```
switch(config-pa-role) # mtu 9198
```

Command History

Release	Modification
10.09	Command introduced on the 8360

Command Information

Platforms	Command context	Authority
8100 8360	config-pa-role The port-access role command takes you into the config-pa-role context.	Administrators or local user group members with execution rights for this command.

poe-priority

poe-priority {critical | high | low}
no poe-priority

Description

Configures the power distribution priority for the port access roles. High power consumption can be prevented using the **poe-priority** control mechanism.

The **no** form of this command restores the power distribution to its default priority.

Parameter	Description
critical	Selects critical priority.
high	Selects high priority.
low	Selects low priority.

Examples

Configuring PoE priority for a new role:

```
switch(config)# port-access role role01
switch(config-pa-role)# poe-priority critical
```

Resetting PoE priority for the role to its default:

```
switch(config)# port-access role role01
switch(config-pa-role)# no poe-priority
```

Command History

Release	Modification
10.09	Command introduced on the 8360

Command Information

Platforms	Command context	Authority
8100 8360	config-pa-role The <code>port-access role</code> command takes you into the <code>config-pa-role</code> context.	Administrators or local user group members with execution rights for this command.

port-access role

```
port-access role <ROLE-NAME>
no port-access role <ROLE-NAME>
```

Description

Creates a new port access role or modifies an existing role. This command takes you into the **config-pa-role** context. A maximum of 32 port access roles can be created.

The **no** form of this command deletes a role.

Parameter	Description
<ROLE-NAME>	Specifies the role name. Range: Up to 64 characters.

Examples

Creating a new role:

```
switch(config)# port-access role basic01
```

Command History

Release	Modification
10.09	Command introduced on the 8360

Command Information

Platforms	Command context	Authority
8100 8360	config	Administrators or local user group members with execution rights for this command.

reauth-period

```
reauth-period <PERIOD>  
no reauth-period
```

Description

Configures the period after which clients that associated with the current role must be reauthenticated.



The reauthentication period configured here takes precedence over the reauthentication period configured at the port level.

Parameter	Description
<PERIOD>	Specifies the reauthentication period (in seconds) for clients associated with the role. Default: None. Range: 1 to 4294967295. A reauthentication period of less than 60 seconds is not recommended.

Examples

Configuring reauthentication period:

```
switch(config-pa-role)# reauth-period 3000
```

Command History

Release	Modification
10.09	Command introduced on the 8360

Command Information

Platforms	Command context	Authority
8100 8360	config-pa-role The port-access role command takes you into the config-pa-role context.	Administrators or local user group members with execution rights for this command.

session timeout

```
session-timeout <SESSION-TIMEOUT>
no session-timeout
```

Description

Configures the session timeout for the role. After the timeout period, the session is disconnected.

Parameter	Description
<SESSION-TIMEOUT>	Specifies the session timeout (in seconds). Range: 1 to 4294967295. A timeout of less than 60 seconds is not recommended.

Examples

Configuring session timeout for a role:

```
switch(config-pa-role)# session timeout 3600
```

Command History

Release	Modification
10.09	Command introduced on the 8360

Command Information

Platforms	Command context	Authority
8100 8360	config-pa-role The port-access role command takes you into the config-pa-role context.	Administrators or local user group members with execution rights for this command.

show aaa authentication port-access interface client-status

```
show aaa authentication port-access interface {all | <IF-NAME>}
client-status [mac <MAC-ADDRESS>]
```

Description

Shows information about the status of the role applied on ports.

Parameter	Description
all	Specifies all interfaces.
<IF-NAME>	Specifies the interface name.
<MAC-ADDRESS>	Specifies the client MAC address.

Examples

Showing information about a client:

```
switch# show aaa authentication port-access interface all client-status mac
00:00:00:00:00:01
```

Port Access Client Status Details

Client 00:00:00:00:00:01

=====

Session Details

Port : 1/7/24

Session Time : 151s

Authentication Details

Status : mac-auth Authenticated

Auth Precedence : mac-auth - Authenticated, dot1x - Not attempted

Authorization Details

Role : UserRole_1

Status : Applied

Command History

Release	Modification
10.09	Command introduced on the 8360

Command Information

Platforms	Command context	Authority
8100 8360	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show port-access role

```
show port-access role {local | clearpass | radius | name <ROLE-NAME>}
```

Description

Shows information about roles configured locally, or downloaded from ClearPass Policy Manager and the RADIUS server.

Displays information only about the attributes defined for the role. The base policy name will be suffixed with * for RADIUS overridden roles.

Parameter	Description
local	Shows information about locally configured roles.
clearpass	Shows information about roles downloaded from ClearPass Policy Manager.
radius	Shows information about roles downloaded from the RADIUS server.
<ROLE-NAME>	Specifies the role name.

Examples

Showing locally configured role information:

```
switch# show port-access role local
Role Information:
Name   : local_role_01
Type   : local
-----
Reauthentication Period      : 333 secs
Cached Reauthentication Period : 300 secs
Access VLAN Name            : Hpe
VLAN Group Name              : group1
PoE Priority                  : low
Policy                       : deny-http-policy
Private-VLAN Port-Type       : secondar
```

Showing information for roles downloaded from ClearPass Policy Manager:

```
June 2020: Replaced original ClearPass example with a new one from Girish G.
switch# show port-access role clearpass

Role Information:

Name   : CP_GIRI_DUR_GUEST_ROLE-3058-7
Type   : clearpass
Status: Completed
-----
Reauthentication Period      : 300 secs
Authentication Mode          :
Session Timeout              : 1000000 secs
Client Inactivity Timeout    :
Description                   : Guest role for CP6
Gateway Zone                  :
UBT Gateway Role              :
Access VLAN                  : 20
Native VLAN                   :
Allowed Trunk VLANs          :
Access VLAN Name              : vlan20
Native VLAN Name              :
Allowed Trunk VLAN Names     :
MTU                           :
QOS Trust Mode                :
STP Administrative Edge Port  : true
```

```
PoE Priority :
Captive Portal Profile : CP6_CP_GIRI_DUR_GUEST_ROLE-3058-7
Policy : CP6_CP_GIRI_DUR_GUEST_ROLE-3058-7
```

Showing locally configured role information:

```
switch# show port-access role local

Role Information:

Name : local_role_01
Type : local
-----
Reauthentication Period : 333 secs
Cached Reauthentication Period : 300 secs
Access VLAN Name : Hpe
VLAN Group Name : group1
PoE Priority : low
Policy : deny-http-policy
Private-VLAN Port-Type : secondary
```

Showing information for roles downloaded from a RADIUS server:

```
switch# show port-access role radius

Role Information:
Attributes overridden by RADIUS are prefixed by '*'.

Name : RADIUS_21963402
Type : radius
-----
Reauthentication Period: 333 secs
Access VLAN: 10
VLAN Group Name: group1
STP Administrative Edge Port : true
PoE Priority : low
Captive Portal Profile : testcpprof_29451201
Policy : PERMIT-ALL_87364653
Private-VLAN Port-Type : secondary
```

Command History

Release	Modification
10.12	The following changes were introduced: - Command output updated to display information only about the attributes defined for the role. - The base policy name will be suffixed with * for RADIUS overridden roles.
10.09	Command introduced on the 8360.

Command Information

Platforms	Command context	Authority
8100 8360	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

stp-admin-edge-port

```
stp-admin-edge-port
no stp-admin-edge-port
```

Description

Configures the port as a spanning tree administrative edge port for the role. This configuration removes the port participation from STP interactions when onboarding devices. This in turn helps in faster onboarding of devices.

The **no** form of the command disables STP edge port functionality.



If the port receives STP BPDU on the STP administrative edge configured port, the port will move to the STP state. You must configure the port as an STP administrative edge port only if you are sure that the connected device will not participate in STP interactions.

Example

Configuring STP edge port for a role:

```
switch(config)# port-access role role01
switch(config-pa-role)# stp-admin-edge-port
```

Command History

Release	Modification
10.09	Command introduced on the 8360

Command Information

Platforms	Command context	Authority
8100 8360	config-pa-role The <code>port-access role</code> command takes you into the <code>config-pa-role</code> context.	Administrators or local user group members with execution rights for this command.

trust-mode

```
trust-mode [dscp | cos | none]
no trust-mode
```

Description

Configures QoS trust mode for the role.

The **no** form of this command configures the default trust mode for the role.

Parameter	Description
dscp	Selects trust DSCP and retain 802.1p priority.
cos	Selects trust 802.1p and retain DSCP or IP-ToS.
none	Selects no trusting of priority fields.

Examples

Configuring DSCP trust mode for a role:

```
switch(config)# port-access role role01
switch(config-pa-role)# trust-mode dscp
```

Command History

Release	Modification
10.09	Command introduced on the 8360

Command Information

Platforms	Command context	Authority
8100 8360	config-pa-role The <code>port-access role</code> command takes you into the <code>config-pa-role</code> context.	Administrators or local user group members with execution rights for this command.

vlan

```
vlan {access | trunk native | trunk allowed} <VLAN-ID>
no vlan {access | trunk native | trunk allowed} <VLAN-ID>
```

```
vlan {access name | trunk native name | trunk allowed name} <VLAN-NAME>
no vlan {access name | trunk native name | trunk allowed name} [<VLAN-NAME>]
```

Description

Configures VLAN IDs or VLAN names, and VLAN modes for a port access role. You can configure either VLAN IDs or VLAN names, or a combination of both for a role.

The **no** form of the command deletes the VLAN configuration from the role. For trunk allowed VLAN names, you can delete the VLAN names individually or all names at once.

Parameter	Description
access <VLAN-ID>	Specifies the VLAN ID for the access VLAN. Supports a single VLAN ID in the range 1 to 4094.
trunk native <VLAN-ID>	Specifies the native VLAN ID on the trunk interface. Supports a single VLAN ID. Range: 1 to 4094.

Parameter	Description
trunk allowed <VLAN-ID>	Specifies the list of tagged or allowed VLANs on the trunk interface. Supports a list of VLAN IDs. Range: 1 to 4094.
access name <VLAN-NAME>	Specifies the VLAN name for the access VLAN. Supports a single VLAN name. Range: Up to 32 characters.
trunk native name <VLAN-NAME>	Specifies the native VLAN name on the trunk interface. Supports a single VLAN name. Range: Up to 32 characters
trunk allowed name <VLAN-NAME>	Specifies the tagged or allowed VLAN name on the trunk interface. Supports a single VLAN name. Range: Up to 32 characters. The switch supports a maximum of 50 trunk allowed VLAN names.

Usage

Note the following points when configuring the VLAN IDs and names for a role:

- For VLAN access and VLAN trunk native respectively, it is recommended to configure only one of either VLAN ID or name for a role. In case both VLAN ID and name are configured, then VLAN ID takes precedence and is applied with the role.
- For VLAN trunk allowed, you can collectively configure a maximum of 50 names and 1024 VLAN IDs. In case this limit is exceeded in the role, then that role is rejected when applying it to an onboarding device.

Platform	Maximum VLAN IDs per role	Maximum VLAN Names per role	Total VLANs (ID + Name) per role
8360	1024	50	1024
8100	1024	50	1024

Examples

Configuring VLAN modes and VLAN IDs for a new role:

```
switch(config)# port-access role role01
switch(config-pa-role)# vlan trunk native 10
switch(config-pa-role)# vlan trunk allowed 11-15
switch(config-pa-role)# vlan access 50
```

Configuring VLAN modes and VLAN names for a new role:

```
switch(config)# port-access role role10
switch(config-pa-role)# vlan trunk native name hpe01
switch(config-pa-role)# vlan trunk allowed name data
switch(config-pa-role)# vlan trunk allowed name voice
switch(config-pa-role)# vlan trunk allowed name video
```

Deleting VLAN configuration from a role:

```
switch(config-pa-role)# no vlan trunk native 10
switch(config-pa-role)# no vlan trunk allowed 10-15
switch(config-pa-role)# no vlan access 50
```

Deleting trunk allowed VLAN names from a role individually:

```
switch(config-pa-role)# no vlan trunk native name hpe01
switch(config-pa-role)# no vlan trunk allowed name data
switch(config-pa-role)# no vlan trunk allowed name voice
switch(config-pa-role)# no vlan trunk allowed name video
```

Deleting trunk allowed VLAN names from a role all at once:

```
switch(config-pa-role)# no vlan trunk native name hpe01
switch(config-pa-role)# no vlan trunk allowed name
```

Command History

Release	Modification
10.09	Command introduced on the 8360

Command Information

Platforms	Command context	Authority
8100 8360	config-pa-role The port-access role command takes you into the config-pa-role context.	Administrators or local user group members with execution rights for this command.

Port access cached-critical role commands

aaa authentication port-access cached-critical-role (global)

```
aaa authentication port-access cached-critical-role
enable
disable
cache-timeout <HOURS>
cache-replace-mode {fifo|none}
no ...
persistent-storage {enable |write-interval <INTERVAL>}
```

Description

Enters the cached-critical role context (shown in the switch prompt as config-aaa-ccr). The cached-critical role allows the authorization of authenticated clients with the previously applied roles when the RADIUS server is unreachable.

By default, the cached-critical role is disabled at the global level. When the cached-critical user role is enabled, the MAC address of clients and their applied roles are cached in the following cases:

- During the client log-off.
- When a client fails to reach the server during reauthentication.
- All the RADIUS servers in the server group are not reachable. In this case, the details of the clients authenticated with the server group are cached.

When the RADIUS server is unreachable, the cached-critical role is applied as a special role. The cached-critical role can be applied only on authentication-enabled ports.



If a server group configured on a port becomes unreachable, caching is not performed for individual clients dependent that group.

By enabling the **persistent-storage** configuration, the cached-critical role support for the clients will be available across switch reboots. With this configuration enabled, the client information is cached in the persistent memory of the switch. The information stored in the persistent storage is updated periodically and the interval between the updates is configurable using the **write-interval** CLI option, with a default interval of 3600 seconds. The update to the persistent storage is only done if there is a difference in the client information since the last write.

The **no** form of the command disables the cached-critical role. This is the default.



- The **persistent-storage** option must be enabled *before* the clients are onboarded. If the configuration is disabled after a client has onboarded, the feature might not work across a reboot for the clients which are onboarded with DUR/RADIUS roles.
- If the cached-critical user role needs to be modified to add a captive portal profile, use the **port-access clear cached-client role <ROLE>** command to clear the cached clients on the role before it is modified.
- Enabling **persistent-storage** on the switch might reduce the lifespan of persistent memory.

Parameter	Description
enable	Enables the cached-critical role on the authentication-enabled ports.
disable	Disables the cached-critical role. (Default)
cache-timeout <HOURS>	Specifies the timeout period for the client details to be cached in the switch. A timer runs for every 30 minutes interval to check whether the client is valid to stay cached. On a timeout, the cached entry is removed from the switch within the buffer time of 30 minutes. Default: 96 hours. Range: 1 to 168 hours.
cache-replace-mode {fifo none}	Sets the cache replacement mode. ▪ fifo: Sets the cache replace mode to fifo (First in, first out). If the number of cached clients in the system exceeds the limit of 1024, the oldest cache entry of the client is replaced with a new entry. ▪ none: Sets the cache replace mode to none. If the number of cached clients in the system exceeds the limit of 1024, the new client details will not be cached. This is the default.

Parameter	Description
no ...	Negates any existing parameter.
persistent-storage {enable write-interval <900-86400>}	Configures the persistent storage for cached clients. ▪ enable: Enables persistent storage for the cached clients. ▪ write-interval: Configures the interval between consecutive writes to persistent storage in seconds. Range: 900 to 86400 seconds. Default: 3600 seconds.

Examples

Enabling the cached-critical-role at the global level with a cache timeout period of **72** hours and cache replace mode as **fifo**:

```
switch(config)# aaa authentication port-access cached-critical-role
switch(config-aaa-ccr)# enable
switch(config-aaa-ccr)# cache-timeout 72
switch(config-aaa-ccr)# cache-replace-mode fifo
```

Disabling the cached-critical role at the global level:

```
switch(config)# aaa authentication port-access cached-critical-role
switch(config-aaa-ccr)# disable
```

Enabling and configuring persistent storage:

```
switch(config)#aaa authentication port-access cached-critical-role
switch(config-aaa-ccr)# persistent-storage
switch(config-aaa-ccr-ps)# enable
switch(config-aaa-ccr-ps)# write-interval 7200
```

Command History

Release	Modification
10.11.1000	The persistent-storage parameter is added.
10.10	Command introduced on the 4100i, 6200, 6300, 6400, 8100, 8360.

Command Information

Platforms	Command context	Authority
8360	config config-aaa-ccr	Administrators or local user group members with execution rights for this command.

aaa authentication port-access cached-critical-role (per interface)

```
aaa authentication port-access cached-critical-role
no aaa authentication port-access cached-critical-role
```

Description

Enables or disables cached-critical role feature on a specific interface. The cached-critical role allows the authenticated client to be authorized with the previously applied roles when the RADIUS server is unreachable.

By default, the cached-critical role feature is enabled at the port level if the cached-critical role is already enabled globally. This command can be used to configure the cached-user role on the specific ports where the caching is needed.

The **no** form of the command disables the cached-critical role on a specific interface.

Examples

Enabling the cached-critical role on the specific port:

```
switch(config)# interface 1/1/1  
switch(config-if)# aaa authentication port-access cached-critical-role
```

Disabling the cached-critical role on the specific port:

```
switch(config)# interface 1/1/1  
switch(config-if)# no aaa authentication port-access cached-critical-role
```

Command History

Release	Modification
10.10	Command introduced on the 4100i, 6200, 6300, 6400, 8100, 8360.

Command Information

Platforms	Command context	Authority
8100 8360	config-if	Administrators or local user group members with execution rights for this command.

port-access clear cached-client

```
port-access clear cached-client [all | mac <MACADDR> | role <ROLENAME>]
```

Description

Clears all the cached clients or clears cached clients based on the MAC address or role name.

Parameter	Description
all	Clears all the cached clients.
mac <MACADDR>	Clears cached clients based on the MAC address.
role <ROLENAME>	Clears cached clients based on the role.

Examples

Clearing all the cached clients:

```
switch# port-access clear cached-client all
```

Clearing the cached clients based on the MAC address:

```
switch# port-access clear cached-client mac 00:0a:0b:0c:0d:0e
```

Clearing the cached clients based on the role:

```
switch# port-access clear cached-client ap_role
```

Command History

Release	Modification
10.10	Command introduced on the 4100i, 6200, 6300, 6400, 8100, 8360.

Command Information

Platforms	Command context	Authority
8100 8360	config	Administrators or local user group members with execution rights for this command.

show port-access cached-clients

```
show port-access cached-clients [mac <MAC-ADDRESS>] [role <ROLE-NAME>]
```

Description

Shows summarized information of all cached port-access clients on the system. The output can be filtered by MAC address or role.

The role name is not displayed for clients that use a RADIUS role without a base role.

Parameter	Description
<MAC-ADDRESS>	Specifies the MAC address of the client.
<ROLE-NAME>	Specifies the role of the client.

Examples

Showing summarized information for all cached port-access clients on the system:

```
switch# show port-access cached-clients

Port Access Cached-Clients

-----
MAC-Address      Role           Cached-Duration
-----
00:50:56:bd:04:c8 ap-role        3 Days, 22 Hours, 33 Minutes, 44 Seconds
```

```

00:50:56:bd:32:07 RADIUS_773420618 1 Day, 1 Hour, 1 Minute, 1 Second
00:50:56:bd:32:08 RADIUS_773420618 12 Hours, 34 Minutes, 56 Seconds
00:50:56:cd:32:09 ap-role 12 Hours, 56 Seconds
00:50:56:bd:50:43 employee 12 Hours
00:50:56:bd:50:45 printer 34 Minutes
08:97:34:ad:e4:00 role_01_Student 56 Seconds

```

Showing information for a specific client based on the MAC address:

```

switch# show port-access cached-clients clients mac 00:50:56:bd:32:08

Port Access Cached-Clients

-----
MAC-Address      Role              Cached-Time
-----
00:50:56:bd:32:08 RADIUS_773420618 12 Hours, 34 Minutes, 56 Seconds

```

Showing information for a specific client based on the role:

```

switch# show port-access cached-clients role ap-role

Port Access Cached-Clients

-----
MAC-Address      Role              Cached-Time
-----
00:50:56:bd:04:c8 ap-role          3 Days, 22 Hours, 33 Minutes, 44 Seconds
00:50:56:cd:32:09 ap-role          12 Hours, 56 Seconds

```

Showing summarized information for all cached port-access clients on the system:

```

switch# show port-access cached-clients

Port Access Cached-Clients
RADIUS overridden user roles are suffixed with '*'

-----
MAC-Address      Role              Cached-Duration
-----
00:50:56:bd:04:c8 ap-role          3 Days, 22 Hours, 33 Minutes, 44 Seconds
00:50:56:bd:32:07                               1 Day, 1 Hour, 1 Minute, 1 Second
00:50:56:bd:32:08                               12 Hours, 34 Minutes, 56 Seconds
00:50:56:cd:32:09 ap-role          12 Hours, 56 Seconds
00:50:56:bd:50:43 employee          12 Hours
00:50:56:bd:50:45 printer          34 Minutes
08:97:34:ad:e4:00 role_01_Student 56 Seconds
10:2f:09:89:00:35 A-Role*         54 Minutes, 26 Seconds

```

Showing information for a specific client based on the MAC address:

```

switch# show port-access cached-clients clients mac 00:50:57:bd:32:09

Port Access Cached-Clients
RADIUS overridden user roles are suffixed with '*'

-----
MAC-Address      Role              Cached-Duration
-----
00:50:56:bd:32:08                               12 Hours, 34 Minutes, 56 Seconds

```


Showing information for a specific client based on the role:

```
switch# show port-access cached-clients role
ROLE The role name.
switch# show port-access cached-clients role intern
No port-access cached-clients found
switch# show port-access cached-clients role ap-role
Port Access Cached-Clients
RADIUS overridden user roles are suffixed with '*'
-----
MAC-Address           Role                Cached-Duration
-----
00:50:56:bd:04:c8    ap-role             3 Days, 22 Hours, 33 Minutes, 44 Seconds
00:50:56:cd:32:09    ap-role             12 Hours, 56 Seconds
```

Command History

Release	Modification
10.12	Command output modified to be suffixed with * for RADIUS overridden user roles. The role name will not displayed for clients that use a RADIUS role without a base role.
10.10	Command introduced on the 4100i, 6200, 6300, 6400, 8100, 8360.

Command Information

Platforms	Command context	Authority
8100 8360	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show port-access cached-critical-role info

show port-access cached-critical-role info

Description

Shows summarized information of port-access cached-critical role configuration.

Examples

Showing summarized information of the cached-critical role configuration with the status of cached-critical role **Disabled**:

```
switch# show port-access cached-critical-role info

Port Access Cached-Critical-Role
=====

Cached-Critical-Role Status      : Disabled
Cache-Timeout                   : 96 Hours
Cache Replace Mode               : None
Cached-Critical-Role Disabled Ports :
Persistent Storage Status       : Disabled
```

```
Persistent Storage Write Interval : 900 Seconds
Last Write To Persistent Storage : N/A
```

Showing summarized information of the cached-critical role configuration with the status of cached-critical role **Enabled**:

```
switch# show port-access cached-critical-role info

Port Access Cached-Critical-Role
=====

Cached-Critical-Role Status      : Enabled
Cache-Timeout                   : 100 Hours
Cache Replace Mode               : FIFO
Cached-Critical-Role Disabled Ports : 1/1/1-1/1/5,1/1/10
Persistent Storage Status       : Enabled
Persistent Storage Write Interval : 7200 Seconds
Last Write To Persistent Storage : Mon Aug 08 04:40:49 UTC 2022
```

Command History

Release	Modification
10.11.1000	The output is updated to display persistent storage related information.
10.10	Command introduced on the 4100i, 6200, 6300, 6400, 8100, 8360.

Command Information

Platforms	Command context	Authority
8100 8360	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

Port access VLAN groups

VLAN grouping enables user distribution across VLANs in a VLAN group to reduce the size of broadcast domains. This supports dynamic load balancing of users across VLANs by onboarding new users on the least populated VLAN in the group.

A VLAN group is a configuration construct, which contains multiple VLANs allocated to that group. VLAN group leverages the existing standard attribute Tunnel-Group-Private-ID(81). This standard attribute is overloaded to be interpreted as the VLAN group name, if the VLAN name does not exist on the switch with that name. VLAN group is supported only through RADIUS attributes; there is no support available through local roles or downloadable user roles.

VLAN grouping limitations

The following limitations apply to VLAN grouping:

- VLANs must be created to be allocated. Any VLAN that does not exist on the switch is ignored from allocation.
- When a VLAN is allocated from a VLAN group, and is subsequently removed from the VLAN group, no change is performed on the client, until the client expires or a role change is performed. Re-authentication has no effect.
- Deleting a VLAN group after a VLAN from that group is allocated to a client, does not affect the client.
- It is not recommended to use reserved VLANs in the pool. Any VLAN that is reserved for another purpose, is allocated, but fails authorization.
- When the VLAN group and VLAN name are configured with the same name on the switch; upon authentication, the VLAN name takes precedence and clients are applied to the VLAN name.

VLAN group load balancing

VLAN grouping provides distribution of clients across the VLANs in the switch to reduce the broadcast domain of secure clients. This feature enables allocating a VLAN from a preconfigured list of pool, thus reducing the need for the administrator to load balance the network.

Load balancing between VLANs adheres to the following rules:

- A global port access per VLAN client count is maintained.
- For a newly authenticated client with the attribute of a VLAN group, the switch iterates through all VLANs in the VLAN group and assigns the VLAN with the lowest number of clients.
- In cases where more than one VLAN has the same least client count, the switch assigns the VLAN with the lowest VLAN ID to the authenticated client.
- VLAN group load-balancing can be viewed with the *show port-access clients detail* command output, which shows the VLAN association and VLAN group name for each authenticated client.
- The following example configuration shows a VLAN group and 4 VLANs associated with it:

```
port-access vlan-group vgp1
associate-vlan 10,20,30,40
```

For eight newly authenticated clients, the VLAN assignment order is as follows:

Client	VLAN Assignment
Client 1	VLAN 10
Client 2	VLAN 20
Client 3	VLAN 30
Client 4	VLAN 40
Client 5	VLAN 10
Client 6	VLAN 20
Client 7	VLAN 30
Client 8	VLAN 40

- The VLAN client count is across multiple VLAN groups and multiple interfaces.
 - **Example 1:** Client 1 authenticates with group vgp1 containing VLANs 10, 20 where both VLANs have a client count of zero. Client 1 is assigned VLAN 10 since both VLANs have the same client count of zero, and VLAN 10 has the lower VLAN ID. Next, client 2 authenticates with group vgp2 and is assigned VLAN 20 since VLAN 20 has the lower client count, even though it lies within a different VLAN group.
 - **Example 2:** Client 1 authenticates on interface 1/1/1 with group vgp1 containing VLANs 10, 20. Next, client 2 authenticates on interface 1/1/2 on the same or different VLAN group. The order of VLAN assignment for client 1 and client 2 is VLAN 10 and VLAN 20, respectively.

Port access VLAN group commands

associate-vlan

```
associate-vlan <VLAN-ID>
no associate-vlan <VLAN-ID>
```

Description

Associates VLANs with an existing VLAN group.

The **no** form of this command removes the association of the VLAN with the specified VLAN group.

Parameter	Description
<VLAN-ID>	Specifies the VLAN or a specific set of VLANs. Range 1 to 4094.

Examples

Associating VLANs with **group1**:

```
switch(config)# port-access vlan-group group1
switch(config-pa-vlan-group)# associate-vlan 5,10-15,20,21
```

Associating additional VLANs with **group1**:

```
switch(config)# port-access vlan-group group1
switch(config-pa-vlan-group)# associate-vlan 30-40
```

Dissociating VLANs 10-15 from VLAN **group1**:

```
switch(config-pa-vlan-group)# no associate-vlan 10-15
```

Command History

Release	Modification
10.09	Command introduced on the 8360

Command Information

Platforms	Command context	Authority
8100 8360	config-pa-vlan-group	Administrators or local user group members with execution rights for this command.

port-access vlan-group

```
port-access vlan-group <NAME>
no port-access vlan-group <NAME>
```

Description

Creates the specified VLAN group (if it does not already exist) and then enters its context **config-pa-vlan-group**. For an existing VLAN group, this command enters the context of the specified VLAN group. The **no** form of this command removes the specified VLAN group.

In order for the group to be applied to a client, VLANs associated to the group should be configured on the switch. If not, the role displays an error.

Parameter	Description
<NAME>	Specifies the name of the VLAN group. Range 2 to 32 characters.

Examples

Creating VLAN **group1** and associating VLANs with it:

```
switch(config)# port-access vlan-group group1
switch(config-pa-vlan-group)# associate-vlan 5,10-15,20,21
```

Dissociating VLANs 10-15 from VLAN **group1**:

```
switch(config-pa-vlan-group)# no associate-vlan 10-15
```

Command History

Release	Modification
10.09	Command introduced on the 8360

Command Information

Platforms	Command context	Authority
8100 8360	config	Administrators or local user group members with execution rights for this command.

show running-config port-access vlan-group

```
show running-config port-access vlan-group
```

Description

Shows information for all configured VLAN groups.

Example

Showing the port access VLAN group configuration:

```
switch# show running-config port-access vlan-group
...
port-access vlan-group group1
    associate-vlan 5,20,21,30-40
port-access vlan-group group2
    associate-vlan 50-60,75-85
...
```

Command History

Release	Modification
10.09	Command introduced on the 8360

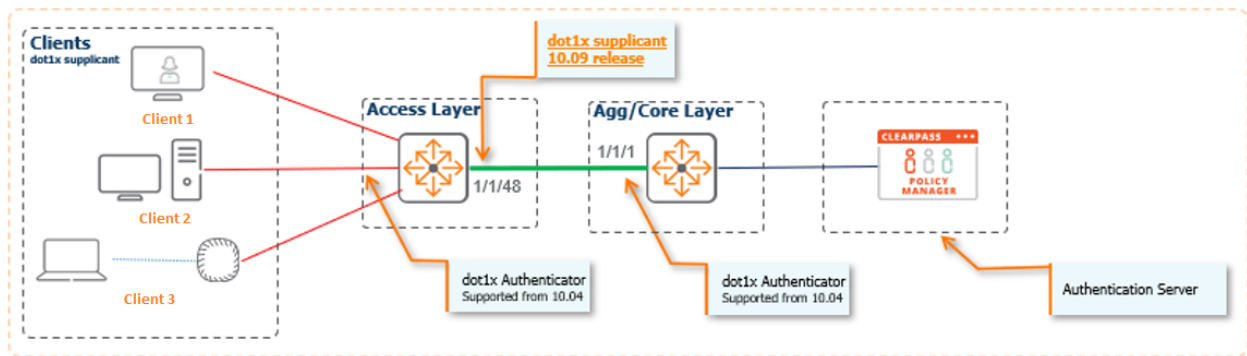
Command Information

Platforms	Command context	Authority
8100 8360	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

Port access 802.1X authentication involves three entities:

- A **supplicant**, such as a PC client, AP, or access switch
- An **authenticator**, which is the Aruba AOS-CX switch
- An **authentication server**, such as Aruba ClearPass

Figure 1 802.1X supplicant overview



Feature details

The following tables list the 802.1X supplicant details.

Table 1: Feature details and limitations

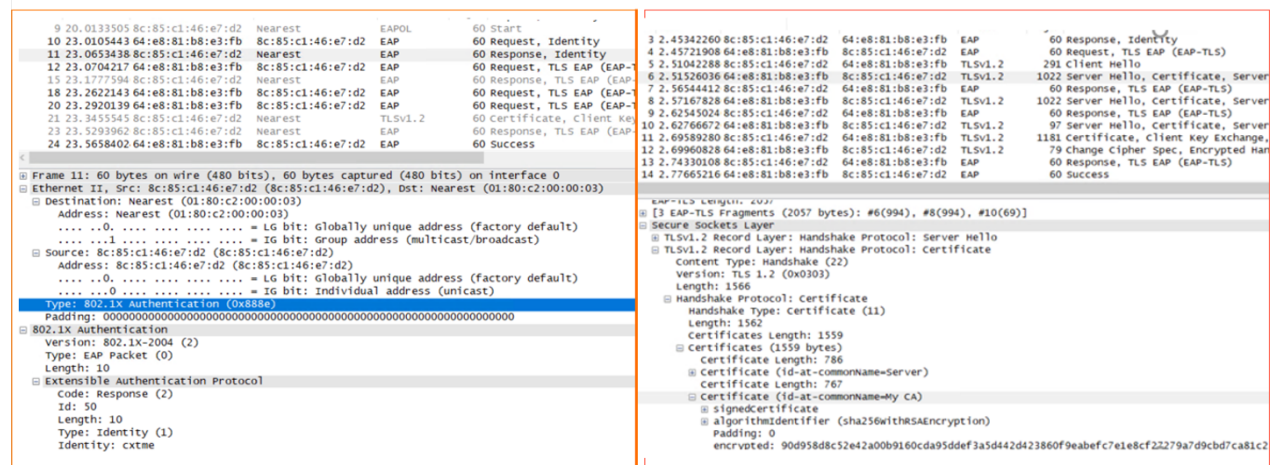
Dot1x Supplicant Features	Supported by AOS-CX
IEEE Standard	802.1X - 2010
EAP Methods	EAP-TLS EAP-MD5
Certificate Types	User Defined EST enrollment
Interface Type	Only L2 Physical Interface
MIB	N/A
Mutual Exclusion Feature	Same interface supports dot1x supplicant and dot1x authenticator

AOS-SW dot1x supplicant	AOS-CX dot1x supplicant
Implements the dot1x 2004 standard.	Implements the dot1x 2010 standard.
Only support EAP-MD5 for authentication.	Supports EAP-TLS and EAP-MD5 for authentication.
Designed to use only base mac address	Designed to use only interface MAC address
eapol-protocol-version 2	eapol-protocol-version 2 & 3(default)

The 802.1X supplicant includes the following sub-features and related packet captures:

- Figure 2** *Packet capture: 802.1X supplicant—eapol-force-multicast*

Without force-multicast



Without canned EAP success

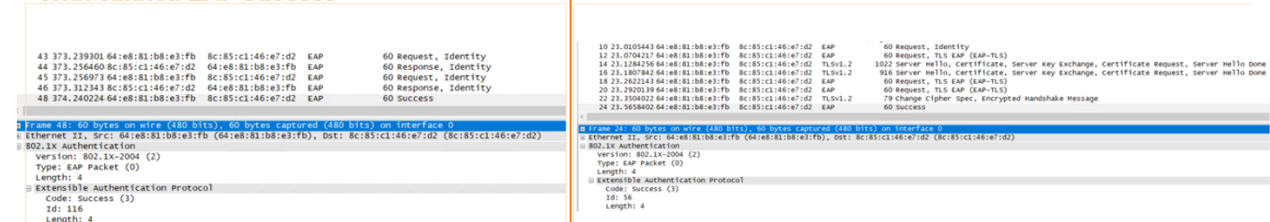


Figure 4 Packet capture: 802.1X supplicant EAP-Method—EAP-TLS EST enrollment certificate

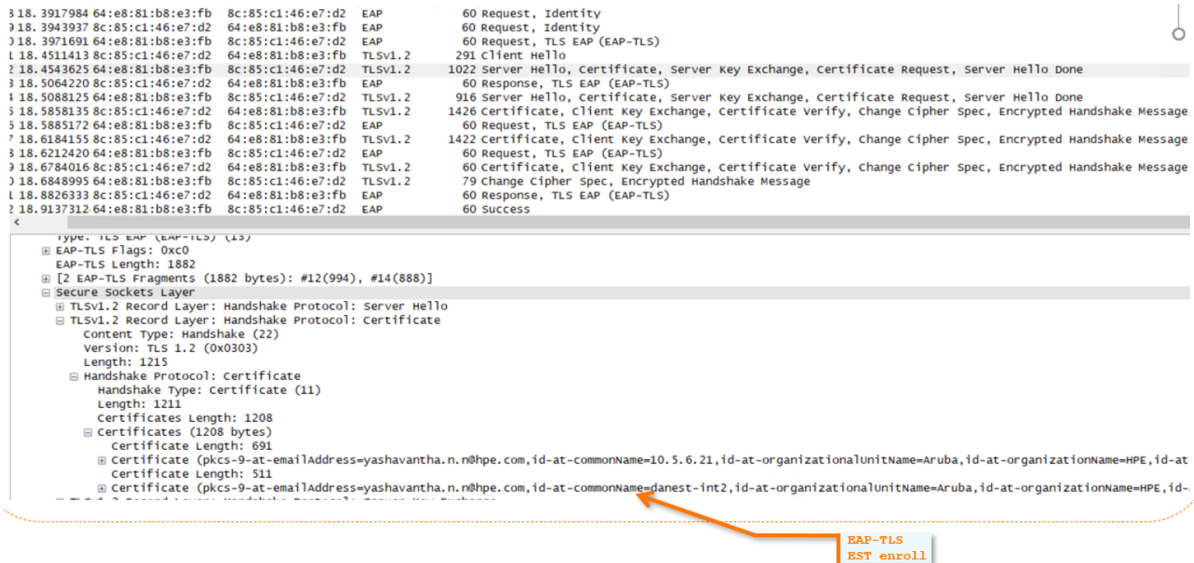
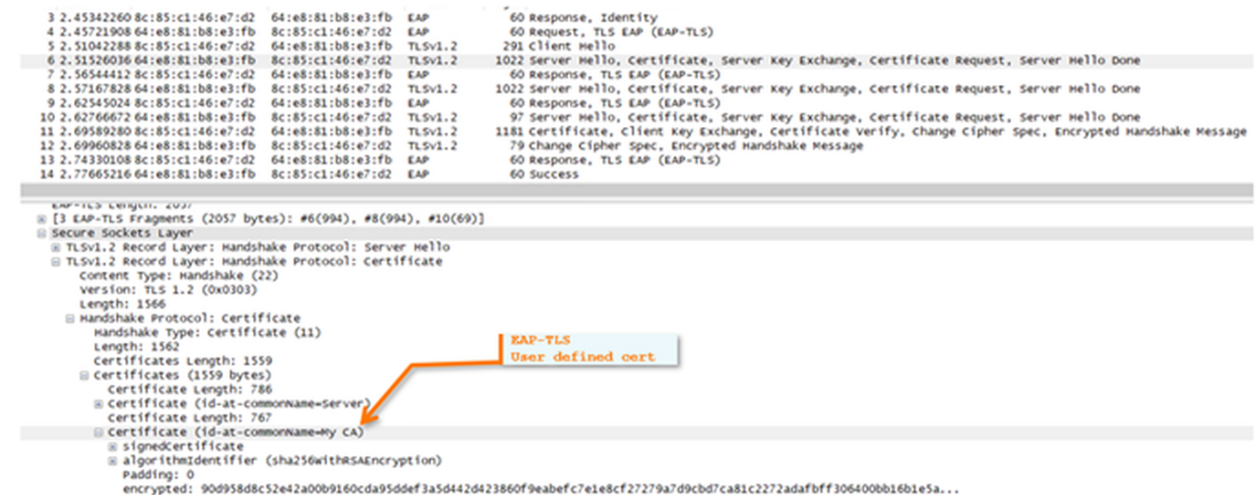


Figure 5 Packet capture: 802.1X supplicant EAP-Method—EAP-TLS - User defined certificate



Validate the same certificate with “show crypto pki certificate client | in Issuer”

Supported platforms

The 802.1X supplicant feature is supported on the 4100i, 6000, 6100 6200, 6300, 6400, and 8360 Switch Series.

802.1X supplicant policy configuration and considerations

802.1X supplicant policy commands include:

- canned EAP success
- discovery timeout
- EAPoL force multicast

- EAP identity
- EAP method
- EAPoL protocol version
- EAPoL timeout
- fail mode
- held period
- max retries
- start-mode

The following general considerations apply to the 802.1X supplicant configuration:

- The 802.1X supplicant only uses the switch interface MAC address for EAP handshake.
- Modifying some policy parameters results in a restart of the 802.1X supplicant state in the interfaces (this does not apply to **EAPoL force multicast**, **max-retries**, or **held period**).
- The IDEVID certificate is not supported by the 802.1X supplicant.

Recommended configuration

The recommended configuration for the 802.1X supplicant is shown below:

```
aaa authentication port-access dot1x supplicant
  enable
  policy cx_dot1x_suppliant_uplink_1
    eap-identity identity cxtme
    eap-identity password plaintext setpasswd ### (EAP-MD5)
    discovery-timeout 60
    start-mode start-closed
    fail-mode fail-closed
    interface 1/1/48
aaa authentication port-access dot1x supplicant
  associate policy cx_dot1x_suppliant_uplink_1
  enable
```

Port access 802.1X supplicant commands

aaa authentication port-access dot1x supplicant (global)

```
aaa authentication port-access dot1x supplicant
```

Description

Enters the 802.1X supplicant global configuration context.

Example

Enter the 802.1X supplicant configuration context:

```
switch(config)# aaa authentication port-access dot1x supplicant
switch(config-dot1x-supp)#
```

Command History

Release	Modification
10.09	Command introduced.

Command Information

Platforms	Command context	Authority
8100 8360	config config-dot1x-supp	Administrators or local user group members with execution rights for this command.

aaa authentication port-access dot1x supplicant (port)

aaa authentication port-access dot1x supplicant

Description

Enters the 802.1X supplicant port context.



The 802.1X supplicant is only supported on L2 physical interfaces that are not members of a LAG.

Example

Enter the 802.1X supplicant port context:

```
switch(config)# interface 1/1/1
switch(config-if)# no routing
switch(config-if)# aaa authentication port-access dot1x supplicant
switch(config-if-dot1x-supp)#
```

When entering the context on a L3 port, an error message displays:

```
switch(config)# interface 1/1/1
switch(config-if)# aaa authentication port-access dot1x supplicant
The operation is allowed only on a L2 physical interface.
```

When entering the context on a LAG, an error message displays:

```
switch(config)# interface lag 1
switch(config-if)# aaa authentication port-access dot1x supplicant
The operation is allowed only on a L2 physical interface.
```

Command History

Release	Modification
10.09	Command introduced.

Command Information

Platforms	Command context	Authority
8100 8360	config config-if config-dot1x-supp	Administrators or local user group members with execution rights for this command.

associate policy

```
associate policy <POLICY-NAME>
no associate policy <POLICY-NAME>
```

Description

Associates a supplicant policy with the port.

The **no** form of the command dissociates the policy from the port and reverts to the default policy.



If an 802.1X supplicant is enabled on the port without associating a policy or dissociating a policy from the port, it results in the port using the default policy.

Parameter	Description
<POLICY-NAME>	Specifies the name of the policy. (Maximum 32 characters).

Examples

Associating a supplicant policy with the port:

```
switch(config)# interface 1/1/1
switch(config)# no routing
switch(config-if)# aaa authentication port-access dot1x supplicant
switch(config-if-dot1x-supp)# associate policy CX_Policy
```

Removing the supplicant policy on the port:

```
switch(config)# interface 1/1/1
switch(config-if)# aaa authentication port-access dot1x supplicant
switch(config-if-dot1x-supp)# no associate policy
OR
switch(config)# interface 1/1/1
switch(config-if)# aaa authentication port-access dot1x supplicant
switch(config-if-dot1x-supp)# no associate policy CX_Policy
```

When the policy being associated does not exist:

```
switch(config)# interface 1/1/1
switch(config-if)# aaa authentication port-access dot1x supplicant
switch(config-if-dot1x-supp)# associate policy New_Supp_Policy
The policy does not exist.
```

When the policy being dissociated is not the one configured on the port:

```
switch(config)# interface 1/1/1
switch(config-if)# aaa authentication port-access dot1x supplicant
switch(config-if-dot1x-supp)# associate policy New_Supp_Policy
The input value does not match the currently configured value.
```

Command History

Release	Modification
10.09	Command introduced.

Command Information

Platforms	Command context	Authority
8100 8360	config config-dot1x-supp config-dot1x-supp-policy	Administrators or local user group members with execution rights for this command.

canned-eap-success

```
canned-eap-success
no canned-eap-success
```

Description

Configures the switch to accept an EAP success from the authenticator without going through the complete authentication cycle. Default: disabled.

The **no** form of the command resets it to the default.

Examples

Configuring the switch to accept a canned EAP success:

```
switch(config)# aaa authentication port-access dot1x supplicant
switch(config-dot1x-supp)# policy CX_Policy
switch(config-dot1x-supp-policy)# canned-eap-success
```

Resetting the allow canned EAP success configuration to the default value in the system:

```
switch(config)# aaa authentication port-access dot1x supplicant
switch(config-dot1x-supp)#policy CX_Policy
switch(config-dot1x-supp-policy)# no canned-eap-success
```

Command History

Release	Modification
10.09	Command introduced.

Command Information

Platforms	Command context	Authority
8100 8360	config config-dot1x-supp config-dot1x-supp-policy	Administrators or local user group members with execution rights for this command.

clear dot1x supplicant statistics

```
clear dot1x supplicant statistics [interface <IFRANGE>]
```

Description

Clears the 802.1X supplicant statistics associated with the interface. If no interface is specified, the statistics are cleared for all 802.1X supplicant-enabled interfaces.

Parameter	Description
<IFRANGE>	Specifies the range of VLAN interfaces for which the supplicant statistics are cleared.

Examples

Clearing authenticator statistics on a specific interface:

```
switch# clear dot1x supplicant statistics 1/1/1
```

Clearing authenticator statistics on all interfaces:

```
switch# clear dot1x supplicant statistics
```

Showing the message when the feature is not enabled on any interface of the system:

```
switch# clear dot1x supplicant statistics
802.1X supplicant is not configured.
```

Showing the message when the feature is not enabled on the interface:

```
switch# clear dot1x supplicant statistics 1/1/1
802.1X supplicant is not configured.
```

Showing the message when there are no 802.1X supplicants on the system:

```
switch# clear dot1x supplicant statistics
No 802.1X supplicants found.
```

Showing the message when there are no 802.1X supplicants on the interface:

```
switch# clear dot1x supplicant statistics 1/1/1
No 802.1X supplicants found.
```

Command History

Release	Modification
10.09	Command introduced.

Command Information

Platforms	Command context	Authority
8100 8360	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

discovery-timeout

```
discovery-timeout <DISCOVERY-TIMEOUT>
no discovery-timeout <DISCOVERY-TIMEOUT>
```

Description

Configures the time period (in seconds) to wait for a potential 802.1X authenticator on the other end before considering the link to be non-802.1X-capable and opening the interface on the data-plane. On a timeout, the switch will not use the authentication result to determine the forwarding behavior of the interface until a link flap. If not set, the switch will wait for the 802.1X authentication cycle to complete before determining the forwarding state of the interface.

The **no** form of the command removes the configuration.

Parameter	Description
<DISCOVERY-TIMEOUT>	Specifies discovery timeout in seconds. Range: 0-300 seconds.

Examples

Configuring a discovery timeout of 15 seconds in the supplicant policy:

```
switch(config)# aaa authentication port-access dot1x supplicant
switch(config-dot1x-supp)# policy CX_Policy
switch(config-dot1x-supp-policy)# discovery-timeout 15
```

Removing the discovery timeout from the policy:

```
switch(config)# aaa authentication port-access dot1x supplicant
switch(config-dot1x-supp)# policy CX_Policy
switch(config-dot1x-supp-policy)# no discovery-timeout 15

OR

switch(config)# aaa authentication port-access dot1x supplicant
switch(config-dot1x-supp)# policy CX_Policy
switch(config-dot1x-supp-policy)# no discovery-timeout 15
```

When the value entered does not match the currently configured non-default value for EAPoL timeout, the following message is displayed:

```
switch(config)# aaa authentication port-access dot1x supplicant
switch(config-dot1x-supp)# policy CX_Policy
switch(config-dot1x-supp-policy)# discovery-timeout 15
switch(config-dot1x-supp-policy)# no discovery-timeout 5
The input value does not match the currently configured value.
```

Command History

Release	Modification
10.09	Command introduced.

Command Information

Platforms	Command context	Authority
8100 8360	config config-dot1x-supp config-dot1x-supp-policy	Administrators or local user group members with execution rights for this command.

eap-identity

```
eap-identity identity <IDENTITY>
no eap-identity identity <IDENTITY>
eap-identity password {plaintext [<PLAINTEXT-PASSWORD>] | ciphertext <CIPHERTEXT-PASSWORD>}
no eap-identity password {plaintext [<PLAINTEXT-PASSWORD>] | ciphertext <CIPHERTEXT-PASSWORD>}
```

Description

Configures the EAP identity to use for authentication including an identity name and an optional password.

The **no** form of the command removes the configuration.

Parameter	Description
<IDENTITY>	Specifies the EAP identity name. Maximum: 64 characters.
<PLAINTEXT-PASSWORD>	Specifies the password associated with the EAP identity in plaintext. Maximum: 32 characters. Specifies the password without prompting. The password is visible as cleartext when entered but is encrypted thereafter. Command history does show the password as cleartext.
<CIPHERTEXT-PASSWORD>	Specifies a ciphertext password. No password prompts are provided and the ciphertext password is validated before the configuration is applied for the user. The variable <CIPHERTEXT-PASSWORD> is Base64 and is typically copied from another switch using the <code>show running-config</code> command output and then

Parameter	Description
	pasted into this command. NOTE: The administrator cannot construct ciphertext passwords themselves. The ciphertext is only created by an AOS-CX switch. The ciphertext is created by setting a password for a user with the <code>user</code> command. The ciphertext is available for copying from the <code>show running-config</code> output and pasting into the configuration on any other AOS-CX switch. The target switch must have the same export password (default or otherwise) as the source switch.

Examples

Configuring the EAP identity and password:

```
switch(config)# aaa authentication port-access dot1x supplicant
switch(config-dot1x-supp)# policy CX_Policy
switch(config-dot1x-supp-policy)# eap-identity identity John Doe
switch(config-dot1x-supp-policy)# eap-identity password plaintext johndoe
```

OR

```
switch(config)# aaa authentication port-access dot1x supplicant
switch(config-dot1x-supp)# policy CX_Policy
switch(config-dot1x-supp-policy)# eap-identity identity John Doe
switch(config-dot1x-supp-policy)# eap-identity password plaintext
Enter password: *****
Confirm password: *****
```

OR

```
switch(config)# aaa authentication port-access dot1x supplicant
switch(config-dot1x-supp)# policy CX_Policy
switch(config-dot1x-supp-policy)# eap-identity identity John Doe
switch(config-dot1x-supp-policy)# eap-identity password ciphertext
AQBapUwNK5Uf+r1vmhBIncQPw1YPVH0V1nYr7Yjm/bPn3bBVCgAAAHFKt8mcSv/A/g8=
```

Removing the EAP identity configuration:

```
switch(config)# aaa authentication port-access dot1x supplicant
switch(config-dot1x-supp)# policy CX_Policy
switch(config-dot1x-supp)# no eap-identity identity
```

OR

```
switch(config)# aaa authentication port-access dot1x supplicant
switch(config-dot1x-supp)# policy CX_Policy
switch(config-dot1x-supp-policy)# no eap-identity identity John Doe
```

Removing the EAP identity password configuration:

```
switch(config)# aaa authentication port-access dot1x supplicant
switch(config-dot1x-supp)# policy CX_Policy
switch(config-dot1x-supp-policy)# no eap-identity password
```

OR

```
switch(config)# aaa authentication port-access dot1x supplicant
switch(config-dot1x-supp)# policy CX_Policy
switch(config-dot1x-supp-policy)# no eap-identity ciphertext
AQBapUwNK5Uf+r1vmhBIncQPw1YPVH0V1nYr7Yjm/bPn3bBVCgAAAHFKt8mcSv/A/g8=
```

When the EAP identity string is longer than 64 characters, the following message is displayed:

```
switch(config)# aaa authentication port-access dot1x supplicant
switch(config-dot1x-supp)# policy CX_Policy
switch(config-dot1x-supp-policy)# eap-identity identity This is a really long
string with more than sixty four characters in it
The EAP identity string is more than 64 characters long.
```

When the EAP identity password string is longer than 32 characters, the following message is displayed:

```
switch(config)# aaa authentication port-access dot1x supplicant
switch(config-dot1x-supp)# policy CX_Policy
switch(config-dot1x-supp-policy)# eap-identity password plaintext This is a
password with more than 32 characters
The password is more than 32 characters long.
```

Command History

Release	Modification
10.09	Command introduced.

Command Information

Platforms	Command context	Authority
8100 8360	config config-dot1x-supp config-dot1x-supp-policy	Administrators or local user group members with execution rights for this command.

eapol-force-multicast

```
eapol-force-multicast
no eapol-force-multicast
```

Description

Configures the switch to send only multicast EAPoL packets irrespective of receiving unicast EAPoL packets from the authenticator. Default: disabled.

The **no** form of the command resets it to the default.

Examples

Configuring the switch to always send EAPoL multicast packets:

```
switch(config)# aaa authentication port-access dot1x supplicant
switch(config-dot1x-supp)# policy CX_Policy
switch(config-dot1x-supp-policy)# eapol-force-multicast
```

Resetting the EAPoL force multicast setting to the default value in the system:

```
switch(config)# aaa authentication port-access dot1x supplicant
switch(config-dot1x-supp)# policy CX_Policy
switch(config-dot1x-supp-policy)# no eapol-force-multicast
```

Command History

Release	Modification
10.09	Command introduced.

Command Information

Platforms	Command context	Authority
8100 8360	config config-dot1x-supp config-dot1x-supp-policy	Administrators or local user group members with execution rights for this command.

eapol-method

```
eapol-method {eap-tls | eap-md5}
no eapol-method {eap-tls | eap-md5}
```

Description

Configures the Extensible Authentication Protocol (EAP) method to use for authentication.

The **no** form of the command resets it to the default. The default is EAP-TLS.

Parameter	Description
eapol-method	Specifies the EAPoL method to use for authentication. Default: eap-tls.
eap-tls	Specifies the EAP method as EAP with TLS (EAP with transport layer security)
eap-md5	Specifies the EAP method as EAP with MD5 digest.

Examples

Configuring the EAP method as EAP-MD5:

```
switch(config)# aaa authentication port-access dot1x supplicant
switch(config-dot1x-supp)# policy CX_Policy
switch(config-dot1x-supp-policy)# eap-method eap-md5
```

Resetting the EAP method to the default value in the system:

```
switch(config)# aaa authentication port-access dot1x supplicant
switch(config-dot1x-supp)# policy CX_Policy
switch(config-dot1x-supp)# no eap-method
```

OR

```
switch(config)# aaa authentication port-access dot1x supplicant
switch(config-dot1x-supp)# policy CX_Policy
switch(config-dot1x-supp-policy)# no eap-method eap-md5
```

When the value entered does not match the currently configured non-default value for EAP method, the following message is displayed:

```
switch(config)# aaa authentication port-access dot1x supplicant
switch(config-dot1x-supp)# policy CX_Policy
switch(config-dot1x-supp-policy)# eap-method eap-md5
switch(config-dot1x-supp-policy)# no eap-method eap-tls
The input value does not match the currently configured value.
```

Command History

Release	Modification
10.09	Command introduced.

Command Information

Platforms	Command context	Authority
8100 8360	config config-dot1x-supp config-dot1x-supp-policy	Administrators or local user group members with execution rights for this command.

eapol-protocol-version

```
eapol-protocol-version
no eapol-protocol-version
```

Description

Configures the EAPoL protocol version to use in EAPoL frames transmitted by the supplicant.

The **no** form of the command resets it to the default.



When the EAPoL protocol version is modified while the policy is in use on one or more ports, all the supplicant sessions on such ports are restarted.

Parameter	Description
<i>protocol-version</i>	Required. Specifies the protocol-version. Options: 2 or 3. Default: 3.

Examples

Configuring the EAPoL protocol version as 2 in the supplicant policy:

```
switch(config)# aaa authentication port-access dot1x supplicant
switch(config-dot1x-supp)# policy CX_Policy
switch(config-dot1x-supp-policy)# eapol-protocol-version 2
```

Reset the EAPoL protocol version to the default value:

```
switch(config)# aaa authentication port-access dot1x supplicant
switch(config-dot1x-supp)# policy CX_Policy
switch(config-dot1x-supp)# no eapol-protocol-version
```

OR

```
switch(config)# aaa authentication port-access dot1x supplicant
switch(config-dot1x-supp)# policy CX_Policy
switch(config-dot1x-supp-policy)# no eapol-protocol-version 2
```

When the value entered does not match the currently configured non-default value for EAPoL protocol version, the following message is displayed:

```
switch(config)# aaa authentication port-access dot1x supplicant
switch(config-dot1x-supp)# policy CX_Policy
switch(config-dot1x-supp-policy)# eapol-protocol-version 2
switch(config-dot1x-supp-policy)# no eapol-protocol-version 3
The input value does not match the currently configured value.
```

Command History

Release	Modification
10.09	Command introduced.

Command Information

Platforms	Command context	Authority
8100 8360	config config-dot1x-supp config-dot1x-supp-policy	Administrators or local user group members with execution rights for this command.

eapol-source-mac

```
eapol-source-mac (interface-mac | system-mac)
no eapol-source-mac (interface-mac | system-mac)
```

Description

Configures the source MAC address to use in the EAPoL frames transmitted by the 802.1X supplicant. The default is interface MAC address.

The **no** form of the command resets to its default EAPoL source MAC value.

Parameter	Description
interface-mac	Specifies the interface MAC address.
system-mac	Specifies the system MAC address.

Examples

Configuring the EAPoL source MAC as system MAC address:

```
switch(config)# aaa authentication port-access dot1x supplicant
switch(config-dot1x-supp)# policy CX_Policy
switch(config-dot1x-supp-policy)# eapol-source-mac system-mac
```

Resetting the EAPoL source MAC to its default address:

```
switch(config)# aaa authentication port-access dot1x supplicant
switch(config-dot1x-supp)# policy CX_Policy
switch(config-dot1x-supp-policy)# no eapol-source-mac system-mac
```

Removing the source MAC address that is not configured for EAPoL source MAC:

```
switch(config)# aaa authentication port-access dot1x supplicant
switch(config-dot1x-supp)# policy CX_Policy
switch(config-dot1x-supp-policy)# eapol-source-mac system-mac
switch(config-dot1x-supp-policy)# no eapol-source-mac interface-mac
The input value does not match the currently configured value.
```

Command History

Release	Modification
10.10.1000	Command introduced.

Command Information

Platforms	Command context	Authority
8100 8360	config config-dot1x-supp config-dot1x-supp-policy	Administrators or local user group members with execution rights for this command.

eapol-timeout

```
eapol-timeout <EAPOL-TIMEOUT>
no eapol-timeout <EAPOL-TIMEOUT>
```

Description

Configures the time period (in seconds) to wait for a response from an authenticator before reattempting authentication.

The **no** form of the command resets it to the default.

Parameter	Description
<EAPOL-TIMEOUT>	Specifies EAPoL timeout in seconds. Default: 30 seconds.

Examples

Configuring an EAPoL timeout of 10 seconds in the supplicant policy:

```
switch(config)# aaa authentication port-access dot1x supplicant
switch(config-dot1x-supp)# policy CX_Policy
switch(config-dot1x-supp-policy)# eapol-timeout 10
```

Resetting the EAPoL timeout to the default value in the system:

```
switch(config)# aaa authentication port-access dot1x supplicant
switch(config-dot1x-supp)# policy CX_Policy
switch(config-dot1x-supp)# no eapol-timeout
```

OR

```
switch(config)# aaa authentication port-access dot1x supplicant
switch(config-dot1x-supp)# policy CX_Policy
switch(config-dot1x-supp-policy)# no eapol-timeout 10
```

When the value entered does not match the currently configured non-default value for EAPoL timeout, the following message is displayed:

```
switch(config)# aaa authentication port-access dot1x supplicant
switch(config-dot1x-supp)# policy CX_Policy
switch(config-dot1x-supp-policy)# eapol-timeout 10
switch(config-dot1x-supp-policy)# no eapol-timeout 5
The input value does not match the currently configured value.
```

Command History

Release	Modification
10.09	Command introduced.

Command Information

Platforms	Command context	Authority
8100 8360	config config-dot1x-supp config-dot1x-supp-policy	Administrators or local user group members with execution rights for this command.

enable

enable
no enable

Description

Enables the 802.1X supplicant on the port. By default, the 802.1X supplicant is disabled on the port. The **no** form of the command disables the 802.1X supplicant on the port.

Example

Enable the 802.1X supplicant on the port:

```
switch(config)# interface 1/1/1
switch(config)# no routing
switch(config-if)# aaa authentication port-access dot1x supplicant
switch(config-if-dot1x-supp)# enable
```

Disable the 802.1X supplicant on the port:

```
switch(config)# interface 1/1/1
switch(config-if)# no aaa authentication port-access dot1x supplicant
switch(config-if-dot1x-supp)# no enable
```

Command History

Release	Modification
10.09	Command introduced.

Command Information

Platforms	Command context	Authority
8100 8360	config config-dot1x-supp	Administrators or local user group members with execution rights for this command.

enable

enable
no enable

Description

Enables the 802.1X supplicant on the system. By default, 802.1X supplicant is disabled on the system. The **no** form of the command disables the 802.1X supplicant on the system.

Example

Enable the 802.1X supplicant on the system:

```
switch(config)# aaa authentication port-access dot1x supplicant
switch(config-dot1x-supp)# enable
```

Disable the 802.1X supplicant on the system:

```
switch(config)# aaa authentication port-access dot1x supplicant
switch(config-dot1x-supp)# no enable
```


Command History

Release	Modification
10.09	Command introduced.

Command Information

Platforms	Command context	Authority
8100 8360	config config-dot1x-supp	Administrators or local user group members with execution rights for this command.

fail-mode

```
fail-mode [fail-closed | fail-open]
no fail-mode [fail-closed | fail-open]
```

Description

Configures the forwarding behavior of the when the 802.1X authentication fails. Default: fail-open. The **no** form of the command resets it to the default.

Examples

Configuring the fail mode as fail-closed:

```
switch(config)# aaa authentication port-access dot1x supplicant
switch(config-dot1x-supp)# policy CX_Policy
switch(config-dot1x-supp-policy)# fail-mode fail-closed
```

Resetting the fail mode to the default value in the system:

```
switch(config)# aaa authentication port-access dot1x supplicant
switch(config-dot1x-supp)#policy CX_Policy
switch(config-dot1x-supp-policy)# no fail-mode
```

OR

```
switch(config)# aaa authentication port-access dot1x supplicant
switch(config-dot1x-supp)#policy CX_Policy
switch(config-dot1x-supp-policy)# no fail-mode fail-closed
```

When the fail-mode value entered does not match the currently configured non-default value:

```
switch(config)# aaa authentication port-access dot1x supplicant
switch(config-dot1x-supp)# policy CX_Policy
switch(config-dot1x-supp-policy)# fail-mode fail-closed
switch(config-dot1x-supp-policy)# no fail-mode fail-open
The input value does not match the currently configured value.
```

Command History

Release	Modification
10.09	Command introduced.

Command Information

Platforms	Command context	Authority
8100 8360	config config-dot1x-supp config-dot1x-supp-policy	Administrators or local user group members with execution rights for this command.

held-period

```
held-period <HELD-PERIOD>
no held-period <HELD-PERIOD>
```

Description

Configure the time period (in seconds) to wait after a failed authentication attempt before another attempt is permitted.

The **no** form of the command resets it to default.

Parameter	Description
<HELD-PERIOD>	Specifies the held period in seconds. Default: 60 seconds.

Usage

When the value entered does not match the currently configured non-default value for held-period, the following message is displayed:

```
switch(config)# aaa authentication port-access dot1x supplicant
switch(config-dot1x-supp)# policy CX_Policy
switch(config-dot1x-supp-policy)# held-period 30
switch(config-dot1x-supp-policy)# held-period 50
The input value does not match the currently configured value.
```

Examples

Configuring a held period of 30 seconds in the supplicant policy:

```
switch(config)# aaa authentication port-access dot1x supplicant
switch(config-dot1x-supp)# policy CX_Policy
switch(config-dot1x-supp-policy)# held-period 30
```

Resetting the held period to the default value in the system:

```
switch(config)# aaa authentication port-access dot1x supplicant
switch(config-dot1x-supp)# policy CX_Policy
switch(config-dot1x-supp)# no held-period
```

OR

```
switch(config)# aaa authentication port-access dot1x supplicant  
switch(config-dot1x-supp)# policy CX_Policy  
switch(config-dot1x-supp-policy)# no held-period 30
```

When the value entered does not match the currently configured non-default value for held-period, the following message is displayed:

```
switch(config)# aaa authentication port-access dot1x supplicant  
switch(config-dot1x-supp)# policy CX_Policy  
switch(config-dot1x-supp-policy)# held-period 30  
switch(config-dot1x-supp-policy)# held-period 50  
The input value does not match the currently configured value.
```

Command History

Release	Modification
10.09	Command introduced.

Command Information

Platforms	Command context	Authority
8100 8360	config config-dot1x-supp config-dot1x-supp-policy	Administrators or local user group members with execution rights for this command.

macsec

```
macsec  
no macsec
```

Description

Enables the switch to provision a MACsec channel dynamically when the 802.1X supplicant is authenticated using an EAP method that supports mutual authentication. By default, MACsec is disabled on the port.

The **no** form of the command disables MACsec for an 802.1X supplicant on the port.



A MACsec policy must be associated with the supplicant policy attached to the port with MACsec enabled. Otherwise, a MACsec channel will not be established and the port will be blocked on the data plane.

Example

Enabling MACsec using EAP for an 802.1X supplicant on the port:

```
switch(config)# interface 1/1/1  
switch(config)# no routing  
switch(config-if)# aaa authentication port-access dot1x supplicant  
switch(config-if-dot1x-supp)# macsec
```

Disabling MACsec using EAP for an 802.1X supplicant on the port:

```
switch(config)# interface 1/1/1
switch(config-if)# aaa authentication port-access dot1x supplicant
switch(config-if-dot1x-supp)# no macsec
```

Attempting to enable MACsec on a port that is not MACsec capable:

```
switch(config)# interface 1/1/10
switch(config)# no routing
switch(config-if)# aaa authentication port-access dot1x supplicant
switch(config-if-dot1x-supp)# macsec
MACsec is not supported on the interface.
```

Command History

Release	Modification
10.10	Command introduced.

Command Information

Platforms	Command context	Authority
8100 8360	config-if-dot1x-supp	Administrators or local user group members with execution rights for this command.

macsec-policy

```
macsec-policy <POLICY-NAME>
no macsec-policy <POLICY-NAME>
```

Description

Associates a MACsec policy with a supplicant policy for the supplicant to use when the supplicant is running MACsec on a port.

The **no** form of the command disassociates the MACsec policy from the supplicant policy.

Parameter	Description
<POLICY-NAME>	Specifies the name of the MACsec policy. (Maximum 128 characters).

Examples

Associating a MACsec policy with the supplicant policy:

```
switch(config)# aaa authentication port-access dot1x supplicant
switch(config-dot1x-supp)# policy Supp_Policy
switch(config-dot1x-supp-policy)# macsec-policy MSec_Policy1
```

Disassociating a MACsec policy from the supplicant policy:

```
switch(config)# aaa authentication port-access dot1x supplicant
switch(config-dot1x-supp)# policy Supp_Policy
switch(config-dot1x-supp-policy)# no macsec-policy
```

Command History

Release	Modification
10.10	Command introduced.

Command Information

Platforms	Command context	Authority
8100 8360	config-dot1x-supp-policy	Administrators or local user group members with execution rights for this command.

max-retries

```
max-retries <MAX-RETRIES>
no max-retries <MAX-RETRIES>
```

Description

Configures the maximum number of authentication attempts before authentication fails. The **no** form of the command resets it to the default.

Parameter	Description
<MAX-RETRIES>	Specifies the maximum retry attempts allowed. Range: 1-5. Default: 2.

Examples

Configuring the maximum retries to 5 in the supplicant policy:

```
switch(config)# aaa authentication port-access dot1x supplicant
switch(config-dot1x-supp)# policy CX_Policy
switch(config-dot1x-supp-policy)# max-retries 5
```

Resetting the max retries to the default value in the system:

```
switch(config)# aaa authentication port-access dot1x supplicant
switch(config-dot1x-supp)# policy CX_Policy
switch(config-dot1x-supp-policy)# no max-retries

OR

switch(config)# aaa authentication port-access dot1x supplicant
switch(config-dot1x-supp)# policy CX_Policy
switch(config-dot1x-supp-policy)# no max-retries 5
```

When the value entered does not match the currently configured non-default value for max-retries, the following message is displayed:

```
switch(config)# aaa authentication port-access dot1x supplicant
switch(config-dot1x-supp)# policy CX_Policy
switch(config-dot1x-supp-policy)# max-retries 5
switch(config-dot1x-supp-policy)# max-retries 3
The input value does not match the currently configured value.
```

Command History

Release	Modification
10.09	Command introduced.

Command Information

Platforms	Command context	Authority
8100 8360	config config-dot1x-supp config-dot1x-supp-policy	Administrators or local user group members with execution rights for this command.

mka cak-length

```
mka cak-length {16|32}
no mka cak-length {16|32}
```

Description

Configures the length of the Connectivity Association Key (CAK) to generate for EAP based MACsec. The **no** form of this command resets it to the default length of 32 bytes.

Parameter	Description
{16 32}	Specifies the CAK length. Default: 32.

Examples

Configuring the CAK length to 16 bytes:

```
switch(config)# aaa authentication port-access dot1x supplicant
switch(config-dot1x-supp)# policy CX_Policy
switch(config-dot1x-supp-policy)# mka cak-length 16
```

Configuring the CAK length to default:

```
switch(config)# aaa authentication port-access dot1x supplicant
switch(config-dot1x-supp)# policy CX_Policy
switch(config-dot1x-supp-policy)# no mka cak-length
OR
switch(config)# aaa authentication port-access dot1x supplicant
```

```
switch(config-dot1x-supp) # policy CX_Policy  
switch(config-dot1x-supp-policy) # no mka cak-length 16
```

Command History

Release	Modification
10.10.1000	Command introduced and on the 8360 switch series.

Command Information

Platforms	Command context	Authority
8100 8360	config-dot1x-supp config-dot1x-supp-policy	Administrators or local user group members with execution rights for this command.

policy (supplicant)

```
policy <POLICY-NAME>  
no policy <POLICY-NAME>
```

Description

Creates an 802.1X supplicant policy on the system.

The **no** form of the command deletes the 802.1X supplicant policy on the system.

Parameter	Description
<POLICY-NAME>	Specifies the name of the policy. (Maximum 32 characters).

Usage

Configure an 802.1X supplicant policy on the system:

Examples

Configure an 802.1X supplicant policy on the system:

```
switch(config) # aaa authentication port-access dot1x supplicant  
switch(config-dot1x-supp) # policy CX_Policy  
switch(config-dot1x-supp-policy) #
```

Delete the 802.1X supplicant policy from the system:

```
switch(config) # aaa authentication port-access dot1x supplicant  
switch(config-dot1x-supp) # no policy CX_Policy
```

Command History

Release	Modification
10.09	Command introduced.

Command Information

Platforms	Command context	Authority
8100 8360	config config-dot1x-supp config-dot1x-supp-policy	Administrators or local user group members with execution rights for this command.

port-access dot1x supplicant restart

port-access dot1x supplicant restart [interface <IFRANGE>]

Description

Restarts the 802.1X supplicant on the specified interface. The current authentication state is discarded and the supplicant restarts the authentication process.

Parameter	Description
<IFRANGE>	Optional. Specifies the range of physical interfaces for which the supplicant is restarted.

Examples

Restarting the 802.1X supplicant on a specific interface:

```
switch# port-access dot1x supplicant restart interface 1/1/1
switch#
```

Restarting the 802.1X supplicant on all interfaces:

```
switch# port-access dot1x supplicant restart
switch#
```

Showing the message when the feature is not enabled on any interface of the system:

```
switch# port-access dot1x supplicant restart
802.1X supplicant is not configured.
```

Showing the message when the feature is not enabled on the given interface:

```
switch# port-access dot1x supplicant restart 1/1/1
802.1X supplicant is not configured.
```

Showing the message when there are no 802.1X supplicants on the system:

```
switch# port-access dot1x supplicant restart
No 802.1X supplicants found.
```

Showing the message when there are no 802.1X supplicants on the interface:


```
switch# port-access dot1x supplicant restart 1/1/1
No 802.1X supplicants found.
```

Command History

Release	Modification
10.09	Command introduced.

Command Information

Platforms	Command context	Authority
8100 8360	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show aaa authentication port-access dot1x supplicant policy

show aaa authentication port-access dot1x supplicant policy <POLICY-NAME>

Description

Shows information about the 802.1X supplicant policies on the system.

Parameter	Description
<POLICY-NAME>	Specifies the name of the policy. (Maximum 32 characters).

Examples

Showing all 802.1X supplicant policies on the system:

```
switch# show aaa authentication port-access dot1x supplicant policy
```

```
802.1X Supplicant Policy Details
```

```
Policy Name: default
```

```
-----
Type                : Default
EAP Method          : EAP-TLS
Held Period         : 60 seconds
Maximum Retries     : 2
EAPoL Timeout       : 30 seconds
EAP Identity        : --
EAP Identity Password : --
EAPoL Force Multicast : False
EAPoL Source MAC    : Interface-MAC
EAPoL Protocol Version : 3
Canned EAP Success  : False
Discovery Timeout    : --
Start Mode          : Start-Open
Fail Mode           : Fail-Open
MKA CAK Length      : 32
```

```

MACsec Policy          : --

Policy Name: CX_Policy
-----
Type                   : Static
EAP Method             : EAP-MD5
Held Period            : 30 seconds
Maximum Retries        : 5
EAPoL Timeout          : 10 seconds
EAP Identity           : John Doe
EAP Identity Password  :
QBapUwNK5Uf+r1vmhBIncQPw1YPVH0V1nYr7Yjm/bPn3bBVCgAAAHFKt8mcSv/A/g8=
EAPoL Force Multicast  : True
EAPoL Source MAC       : Interface-MAC
EAPoL Protocol Version : 2
Canned EAP Success     : True
Discovery Timeout      : 15 seconds
Start Mode             : Start-Closed
Fail Mode              : Fail-Closed
MKA CAK Length         : 16
MACsec Policy          : Aggregator-Connect

```

Showing a specific 802.1X supplicant policy:

```

switch# show aaa authentication port-access dot1x supplicant policy CX_Policy

802.1X Supplicant Policy Details

Policy Name: CX_Policy
-----
Type                   : Static
EAP Method             : EAP-MD5
Held Period            : 30 seconds
Maximum Retries        : 5
EAPoL Timeout          : 10 seconds
EAP Identity           : John Doe
EAP Identity Password  :
AQBapUwNK5Uf+r1vmhBIncQPw1YPVH0V1nYr7Yjm/bPn3bBVCgAAAHFKt8mcSv/A/g8=
EAPoL Force Multicast  : True
EAPoL Source MAC       : Interface-MAC
EAPoL Protocol Version : 2
Canned EAP Success     : True
Discovery Timeout      : 15 seconds
Start Mode             : Start-Closed
Fail Mode              : Fail-Closed
MKA CAK Length         : 16
MACsec Policy          : Aggregator-Connect

```

If the policy with given name does not exist:

```

switch# show aaa authentication port-access dot1x supplicant policy New_CX_Policy
The policy does not exist.

```

Command History

Release	Modification
10.10.1000	Added EAPoL source MAC address and MKA CAK length.
10.09	Command introduced.

Command Information

Platforms	Command context	Authority
8100 8360	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show aaa authentication port-access dot1x supplicant statistics

```
show aaa authentication port-access dot1x supplicant statistics
[interface {<IFRANGE> | vlan <VLAN-ID>}]
```

Description

Shows the 802.1X supplicant statistics on each 802.1X supplicant-enabled interface.

Parameter	Description
<IFRANGE>	Specifies the range of VLAN interfaces for which the supplicant status is shown.
vlan <VLAN-ID>	Specifies a VLAN interface for which the supplicant status is shown.

Examples

Showing the 802.1X supplicant statistics on all enabled interfaces:

```
switch# show aaa authentication port-access dot1x supplicant statistics

802.1X Supplicant Statistics

Interface 1/1/1
=====

EAPOL Frames Received           : 4
EAPOL Frames Transmitted        : 3
EAPOL Start Frames Transmitted  : 1
EAPOL Logoff Frames Transmitted : 0
EAPOL Invalid Frames Received   : 0
EAPOL EAP Length Error Frames Received : 0
Authentication                  : 0
Authentication Timeout          : 0
EAP-Logoff While Authenticating : 0
Successful Authentication       : 0
Failed Authentication           : 0
Re-Authentication               : 0
EAP-Logoff When Authenticated   : 0
```

```
Interface 1/1/2
=====

EAPOL Frames Received           : 0
EAPOL Frames Transmitted        : 1
EAPOL Start Frames Transmitted  : 1
EAPOL Logoff Frames Transmitted : 0
EAPOL Invalid Frames Received   : 0
EAPOL EAP Length Error Frames Received : 0
Authentication                   : 0
Authentication Timeout          : 0
EAP-Logoff While Authenticating : 0
Successful Authentication       : 0
Failed Authentication           : 0
Re-Authentication               : 0
EAP-Logoff When Authenticated   : 0
```

Showing the 802.1X supplicant status on a specific interface:

```
switch# show aaa authentication port-access dot1x supplicant statistics interface
1/1/1

802.1X Supplicant Statistics

Interface 1/1/1
=====

EAPOL Frames Received           : 4
EAPOL Frames Transmitted        : 3
EAPOL Start Frames Transmitted  : 1
EAPOL Logoff Frames Transmitted : 0
EAPOL Invalid Frames Received   : 0
EAPOL EAP Length Error Frames Received : 0
Authentication                   : 0
Authentication Timeout          : 0
EAP-Logoff While Authenticating : 0
Successful Authentication       : 0
Failed Authentication           : 0
Re-Authentication               : 0
EAP-Logoff When Authenticated   : 0
```

Showing the message when the feature is not enabled on any interface of the system:

```
switch# show aaa authentication port-access dot1x supplicant statistics
802.1X supplicant is not configured.
```

Showing the message when the feature is not enabled on the interface:

```
switch# show aaa authentication port-access dot1x supplicant statistics interface
1/1/1
802.1X supplicant is not configured.
```

Showing the message when there are no 802.1X supplicants on the system:

```
switch# show aaa authentication port-access dot1x supplicant status
No 802.1X supplicants found.
```

Showing the message when there are no 802.1X supplicants on the interface:

```
switch# show aaa authentication port-access dot1x supplicant status interface
1/1/1
No 802.1X supplicants found.
```

Command History

Release	Modification
10.09	Command introduced.

Command Information

Platforms	Command context	Authority
8100 8360	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show aaa authentication port-access dot1x supplicant status

```
show aaa authentication port-access dot1x supplicant status
[interface {<IFRANGE> | vlan <VLAN-ID>}]
```

Description

Shows the 802.1X supplicant status on each 802.1X supplicant-enabled interface.

Parameter	Description
<IFRANGE>	Specifies the range of VLAN interfaces for which the supplicant status is shown.
vlan <VLAN-ID>	Specifies a VLAN interface for which the supplicant status is shown.

Usage

- Physical Address Extension (PAE) state:
 - **Initialize**—Authentication is yet to start for the PAE.
 - **Authenticating**—Authentication is in-progress for the PAE.
 - **Authenticated**—Authentication is successful for the PAE.
 - **Held**—Authentication has failed for the PAE and no further authentication attempts will be made till the held period expires.
 - **Unauthenticated**—Authentication has failed for the PAE and no further authentication attempts will be made.
 - **Logoff**—The PAE no longer wishes to be authenticated.

- Status and forwarding state (FS):
 - **Open**—The PAE did not find a 802.1X authenticator within the discovery period. FS: Forwarding
 - **Blocked**—The PAE is currently authenticating and the port is operating in start-mode start-closed or has failed authentication and the port is operating in fail-mode fail-closed. FS: Blocked
 - **Disabled**—The port to which the interface is attached is not ready or has an invalid configuration. FS: Blocked
 - **Secured**—The PAE is authenticated. FS: Forwarding
 - **Start-Open**—The PAE is currently authenticating and the port is operating in start-mode start-open. FS: Forwarding
 - **Fail-Open**—The PAE has failed authentication and the port is operating in fail-mode fail-open. FS: Forwarding

Examples

Showing the 802.1X supplicant status on all enabled interfaces:

```
switch# show aaa authentication port-access dot1x supplicant status
```

802.1X Supplicant Status

Interface	Policy	PAE State	Authenticator	EAP Method	Status
1/1/1	CX_Policy_01	Authenticated	38:21:c7:59:ad:27	EAP-TLS	Secured
1/1/2	CX_Policy_02	Authenticating	38:21:c7:59:ad:28	EAP-MD5	Blocked
1/1/3	CX_Policy_01	Unauthenticated	38:21:c7:59:ad:29	EAP-TLS	Fail-Open
1/1/4	CX_Policy_03	Unauthenticated	--	--	Open

Showing the 802.1X supplicant status on a specific interface:

```
switch# show aaa authentication port-access dot1x supplicant status interface 1/1/1
```

802.1X Supplicant Status

Interface	Policy	PAE State	Authenticator	EAP Method	Status
1/1/1	CX_Policy_01	Authenticated	38:21:c7:59:ad:27	EAP-TLS	Secured

Showing the message when the feature is not enabled on any interface of the system:

```
switch# show aaa authentication port-access dot1x supplicant status
```

802.1X supplicant is not configured.

Showing the message when the feature is not enabled on the interface:

```
switch# show aaa authentication port-access dot1x supplicant status interface 1/1/1
```

802.1X supplicant is not configured.



When an interface range is entered, this message is displayed only if the 802.1X supplicant is disabled either globally or on each interface specified in the user input.

Showing the message when there are no 802.1X supplicants on the system:

```
switch# show aaa authentication port-access dot1x supplicant status
No 802.1X supplicants found.
```

Showing the message when there are no 802.1X supplicants on the interface:

```
switch# show aaa authentication port-access dot1x supplicant status interface
1/1/1
No 802.1X supplicants found.
```

Command History

Release	Modification
10.09	Command introduced.

Command Information

Platforms	Command context	Authority
8100 8360	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

start-mode

```
start-mode[start-closed | start-open]
no start-mode [start-closed | start-open]
```

Description

Configures the forwarding behavior of the interface on the data-plane when the authentication is in-progress during the first run of the supplicant. Default: start-open.

The **no** form of the command resets it to the default.

Examples

Configuring the start mode as start-closed:

```
switch(config)# aaa authentication port-access dot1x supplicant
switch(config-dot1x-supp)# policy CX_Policy
switch(config-dot1x-supp-policy)# start-mode start-closed
```

Resetting the start mode to the default value in the system:

```
switch(config)# aaa authentication port-access dot1x supplicant
switch(config-dot1x-supp)# policy CX_Policy
switch(config-dot1x-supp-policy)# no start-mode
```

OR

```
switch(config)# aaa authentication port-access dot1x supplicant
switch(config-dot1x-supp)#policy CX_Policy
switch(config-dot1x-supp-policy)# no start-mode start-closed
```

When the value does not match the currently configured non-default value for start-mode:

```
switch(config)# aaa authentication port-access dot1x supplicant
switch(config-dot1x-supp)# policy CX_Policy
switch(config-dot1x-supp-policy)# start-mode start-closed
switch(config-dot1x-supp-policy)# no start-mode start-open
The input value does not match the currently configured value.
```

Command History

Release	Modification
10.09	Command introduced.

Command Information

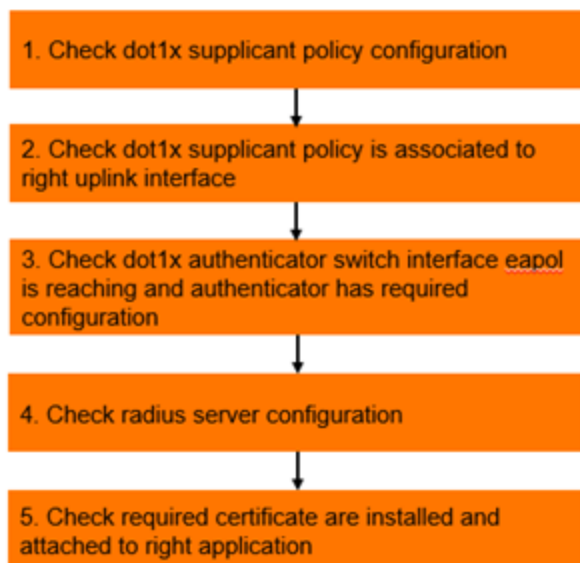
Platforms	Command context	Authority
8100 8360	config config-dot1x-supp config-dot1x-supp-policy	Administrators or local user group members with execution rights for this command.

Troubleshooting

Prerequisites

- Create a diagram for your network topology that includes IP addresses and interface details.
- Check physical cabling.
- Check network status using the **show LLDP neighbor** command, and validate the RADIUS server and authenticator network works by issuing the **ping** and **traceroute** command between loopbacks and interfaces.
- Issue the `show tech` command and save the output prior to contacting customer support, as the output will help support identify issues.

Figure 1 Recommended 802.1X troubleshooting flow



Packet capture

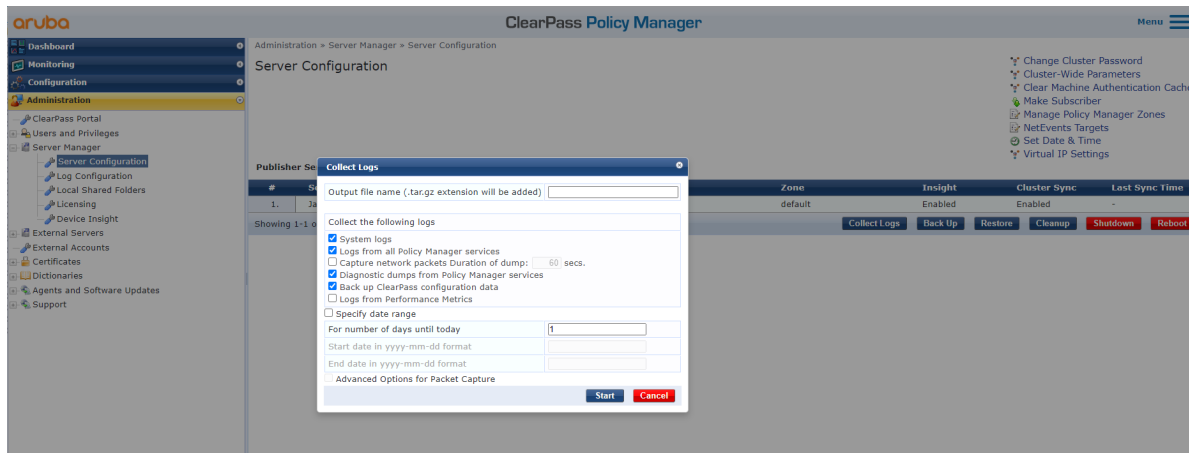
Use the **mirror session** commands for packet capture, as shown in the figure below:

```
mirror session 1
  enable
  destination interface 1/1/40
  source interface 1/1/51 both
```

```
Mirror session 1
Source interface 1/1/1 both
Destination CPU
enable
diag utilities tshark file
copy tshark-pcap tftp://10.80.2.187/supplicant.pcap vrf mgmt
```

If packet capture is required on Aruba ClearPass Policy Manager, navigate to **Administration > Server Manager > Server Configuration** in the Policy Manager WebUI, click **Collect Logs**, then select the following options:

- System logs
- Logs from all Policy Manager services
- Diagnostic dumps from Policy Manager services
- Back up ClearPass configuration data



FAQ

1. What are the EAP methods supported on the 802.1X supplicant?

The following EAP methods are supported on AOS-CX switches:

- eap-md5
- eap-tls

2. How many 802.1X supplicant policies can be configured?

There is exact limit on policies; the maximum number of policies required on an AOS-CX switch is equal to total number of physical L2 interfaces.

3. Can 802.1X authenticator and 802.1X supplicant co-exist?

Yes, the 802.1X supplicant on uplink and 802.1X authenticator on access link can co-exist on a switch.

4. Does the 802.1X supplicant support canned eap success?

Yes, the 802.1X supplicant supports `canned-eap-success`.

5. Does the 802.1X supplicant support both the 2004 and 2010 standards?

Yes, the 802.1X supplicant is based on the 2010 standard and it is backward compatible.

Configurable RADIUS attributes (port access)

RADIUS access request and accounting request packets are sent to a RADIUS server during authentication and accounting of port access clients respectively. These access request packets contain various AVPs (Attribute Value Pairs) that carry the information about the RADIUS server and the client. For example, these AVPs include items such as username and RADIUS server identifier (host name). Similar kinds of details are included in accounting request packets which are sent to accounting servers. Including these attributes in access request packets helps administrators assign appropriate access policies to the clients.

Several commands are provided for configuring RADIUS attributes per RADIUS server group for use with port access client authentication by RADIUS.

Configurable RADIUS attribute commands

aaa radius-attribute group

```
aaa radius-attribute group <GROUP-NAME>
no aaa radius-attribute group <GROUP-NAME>
```

Description

Configures an existing RADIUS server group for which the configured RADIUS attributes will be included in request packets. Enters the **config-radius-attr** context.

The **no** form of this command unconfigures the RADIUS server group for the configured RADIUS attributes.



Nas-id and tunnel-private-group-id attributes only apply to port access requests. Nas-ip-addr attributes only apply to management user requests.

Parameter	Description
<GROUP-NAME>	Specifies an existing RADIUS server group name.

Examples

Configuring port access request RADIUS attributes for **rad_group1**:

```
switch(config)# aaa radius-attribute group rad_group1
switch(config-radius-attr)# nas-id value ARUBA_NAS-01
switch(config-radius-attr)# nas-id request-type authentication
switch(config-radius-attr)# tunnel-private-group-id value static
switch(config-radius-attr)# tunnel-private-group-id request-type authentication
```

Configuring management user request RADIUS attributes for **rad_group2**:

```
switch(config)# aaa radius-attribute group rad_group2
switch(config-radius-attr)# nas-ip-addr request-type authentication
switch(config-radius-attr)# nas-ip-addr service-type user-management
```

Unconfiguring RADIUS attributes for **rad_group1**:

```
switch(config)# no aaa radius-attribute group rad_group1
```

Command History

Release	Modification
10.09	Command introduced on the 8360

Command Information

Platforms	Command context	Authority
8100 8360	config	Administrators or local user group members with execution rights for this command.

nas-id request-type

```
nas-id request-type {authentication | accounting | both}
no nas-id request-type {authentication | accounting | both}
```

Description

For the selected (by context) RADIUS server group, configures the Network Access Server (NAS) ID request type for which the attribute configured with command **nas-id value** will be included.

The no form of this command unconfigures the specified request type.



Nas-id attributes only apply to port access requests.

Parameter	Description
authentication	Selects the authentication request type.
accounting	Selects the accounting request type.
both	Selects both the authentication and accounting request types.

Examples

Configuring the authentication request type for **rad_group1**:

```
switch(config)# aaa radius-attribute group rad_group1
switch(config-radius-attr)# nas-id request-type authentication
```

Configuring both the authentication and accounting request types for **rad_group2**:

```
switch(config)# aaa radius-attribute group rad_group2
switch(config-radius-attr)# nas-id request-type both
```

Unconfiguring the authentication request type for **rad_group1**:

```
switch(config)# aaa radius-attribute group rad_group1
switch(config-radius-attr)# no nas-id request-type authentication
```

Command History

Release	Modification
10.09	Command introduced on the 8360

Command Information

Platforms	Command context	Authority
8100 8360	config-radius-attr	Administrators or local user group members with execution rights for this command.

nas-id value

```
nas-id value <NAS-ID>
no nas-id [value <NAS-ID>]
```

Description

For the selected (by context) RADIUS server group, configures the Network Access Server Identifier (NAS ID) (type 32, RFC 2865). The NAS ID is sent in the RADIUS access request and accounting packets to notify the source of the RADIUS access request.

The **no** form of this command unconfigures the specified NAS ID.



Nas-id attributes only apply to port access requests.

Parameter	Description
<NAS-ID>	Specifies the FQDN or other unique identifying name of the Network Access Server (NAS). Range 1 to 253 characters.

Examples

Configuring the Network Access Server (NAS) ID for **rad_group1**:

```
switch(config)# aaa radius-attribute group rad_group1
switch(config-radius-attr)# nas-id value ARUBA_NAS-01
```

Unconfiguring the NAS ID for **rad_group1**:

```
switch(config)# aaa radius-attribute group rad_group1
switch(config-radius-attr)# no nas-id value ARUBA_NAS-01
```

Unconfiguring both the NAS-ID value and the request type for **rad_group2**:

```
switch(config)# aaa radius-attribute group rad_group2
switch(config-radius-attr)# no nas-id
```

Command History

Release	Modification
10.09	Command introduced on the 8360

Command Information

Platforms	Command context	Authority
8100 8360	config-radius-attr	Administrators or local user group members with execution rights for this command.

nas-ip-addr request-type authentication

```
nas-ip-addr request-type authentication
no nas-ip-addr request-type authentication
```

Description

For the selected (by context) RADIUS server group, configures the **NAS-IP-Address** attribute for inclusion in management user request packets.

The no form of this command unconfigures the **NAS-IP-Address** attribute for inclusion in management user request packets.



Nas-ip-addr attributes only apply to management user requests.

Examples

Configuring the **NAS-IP-Address** attribute for inclusion in management user request packets for **rad_group1**:

```
switch(config)# aaa radius-attribute group rad_group1
switch(config-radius-attr)# nas-ip-addr request-type authentication
```

Unconfiguring the **NAS-IP-Address** attribute for inclusion in management user request packets for **rad_group1**:

```
switch(config)# aaa radius-attribute group rad_group1
switch(config-radius-attr)# no nas-ip-addr request-type authentication
```

Command History

Release	Modification
10.09	Command introduced

Command Information

Platforms	Command context	Authority
8100 8360	config-radius-attr	Administrators or local user group members with execution rights for this command.

nas-ip-addr service-type user-management

```
nas-ip-addr service-type user-management
no nas-ip-addr service-type user-management
```

Description

For the selected (by context) RADIUS server group, configures the **NAS-IP-Address** attribute for inclusion in management user service type request packets.

The no form of this command unconfigures the **NAS-IP-Address** attribute for inclusion in management user service type request packets.



Nas-ip-addr attributes only apply to management user requests.

Examples

Configuring the **NAS-IP-Address** attribute for inclusion in management user service type request packets for **rad_group1**:

```
switch(config)# aaa radius-attribute group rad_group1
switch(config-radius-attr)# nas-ip-addr service-type user-management
```

Unconfiguring the **NAS-IP-Address** attribute for inclusion in management user service type request packets for **rad_group1**:

```
switch(config)# aaa radius-attribute group rad_group1
switch(config-radius-attr)# no nas-ip-addr service-type user-management
```

Command History

Release	Modification
10.09	Command introduced

Command Information

Platforms	Command context	Authority
8100 8360	config-radius-attr	Administrators or local user group members with execution rights for this command.

tunnel-private-group-id request-type

```
tunnel-private-group-id request-type {authentication | accounting | both}
no tunnel-private-group-id request-type {authentication | accounting | both}
```

Description

For the selected (by context) RADIUS server group, configures the request type for which the attribute configured with command **tunnel-private-group-id value** will be included.

The **no** form of this command unconfigures the specified request type.



Tunnel-private-group-id attributes only apply to port access requests.

Parameter	Description
authentication	Selects the authentication request type.
accounting	Selects the accounting request type.
both	Selects both the authentication and accounting request types.

Examples

Configuring the authentication request type for **rad_group1**:

```
switch(config)# aaa radius-attribute group rad_group1
switch(config-radius-attr)# tunnel-private-group-id request-type authentication
```

Configuring both the authentication and accounting request types for **rad_group2**:

```
switch(config)# aaa radius-attribute group rad_group2
switch(config-radius-attr)# tunnel-private-group-id request-type both
```

Unconfiguring the authentication request type for **rad_group2**:

```
switch(config)# aaa radius-attribute group rad_group2
switch(config-radius-attr)# no tunnel-private-group-id request-type authentication
```

Command History

Release	Modification
10.09	Command introduced on the 8360

Command Information

Platforms	Command context	Authority
8100 8360	config-radius-attr	Administrators or local user group members with execution rights for this command.

tunnel-private-group-id value

```
tunnel-private-group-id value {static | dynamic}  
no tunnel-private-group-id value {static | dynamic}
```

Description

For the selected (by context) RADIUS server group, configures the **tunnel-private-group-id** value (type 81, RFC 2868) that will be sent in RADIUS access-request packets. This is used for VLAN identification. The no form of this command unconfigures specified **tunnel-private-group-id** value.



Tunnel-private-group-id attributes only apply to port access requests.

Parameter	Description
static	Causes the switch to send (as an attribute value) the native VLAN of the client port.
dynamic	Causes the switch to send (as an attribute value) the client VLAN assigned by server. This is applicable during re-authentication scenarios.

Examples

Configuring **rad_group1** for the RADIUS attribute to identify the native VLAN of the client port:

```
switch(config)# aaa radius-attribute group rad_group1  
switch(config-radius-attr)# tunnel-private-group-id value static
```

Configuring **rad_group2** for the RADIUS attribute to identify the client VLAN assigned by the server:

```
switch(config)# aaa radius-attribute group rad_group2  
switch(config-radius-attr)# tunnel-private-group-id value dynamic
```

Unconfiguring (for **rad_group1**) the RADIUS attribute to identify the native VLAN of the client port:

```
switch(config)# aaa radius-attribute group rad_group1  
switch(config-radius-attr)# no tunnel-private-group-id value static
```

Unconfiguring (for **rad_group3**) both the group-ID value and request type:

```
switch(config)# aaa radius-attribute group rad_group3  
switch(config-radius-attr)# no tunnel-private-group-id
```

Command History

Release	Modification
10.09	Command introduced on the 8360

Command Information

Platforms	Command context	Authority
8100 8360	<code>config-radius-attr</code>	Administrators or local user group members with execution rights for this command.

AOS-CX supports various RADIUS server attributes to be applied during authentication of clients. This section lists the attributes supported in the following features:

- 802.1X authentication
- MAC authentication
- Dynamic authorization
- Session authorization in 802.1X and MAC authentication, and CoA
- RADIUS server tracking
- RADIUS network accounting



The following terms are used in the list of attributes:

- **Tx:** Attribute added in the request packets that are sent to the RADIUS server.
- **Rx:** Attribute processed in the response packets received from the RADIUS server.

Attributes supported in 802.1X authentication

Following are the RADIUS attributes supported in 802.1X authentication:

Attribute name	Tx	Rx	Notes
User-name	Y	N	RFC2865
Calling-station-id	Y	N	RFC2865/3580
Called-station-id	Y	N	RFC2865/3580
NAS-port-id	Y	N	RFC2869
NAS-port	Y	N	RFC2865
Service-Type	Y	N	RFC2865
EAP-Message	Y	N	RFC2869
Class	N	Y	RFC2865
State	Y	Y	RFC2865
Session-Timeout	N	Y	RFC2865 - Used as EAP timeout in Challenge packet
NAS-IP-Address	Y	N	RFC2865
NAS-Identifier	Y	N	RFC2865
NAS-Ipv6-Address	Y	N	RFC3162
Message-Authenticator	Y	Y	RFC2869
Tunnel-Type	Y	Y	RFC2868
Tunnel-Medium-Type	Y	Y	RFC2868
Tunnel-Private-Group-Id	Y	Y	RFC2868

Attributes supported in MAC authentication

Following are the RADIUS attributes supported in MAC authentication:

Attribute name	Tx	Rx	Notes
User-name	Y	N	RFC2865
Calling-station-id	Y	N	RFC2865/3580

Called-station-id	Y	N	RFC2865/3580
NAS-port-id	Y	N	RFC2869
NAS-port	Y	N	RFC2865
Service-Type	Y	N	RFC2865
State	Y	Y	RFC2865
Class	N	Y	RFC2865
NAS-IP-Address	Y	N	RFC2865
NAS-Identifier	Y	N	RFC2865
NAS-IPv6-Address	Y	N	RFC3162
Message-Authenticator	Y	Y	RFC2869
Chap-Challenge	Y	N	RFC2865
Chap-Password	Y	N	RFC2865
User-Password	Y	N	RFC2865
Tunnel-Type	Y	Y	RFC2868
Tunnel-Medium-Type	Y	Y	RFC2868
Tunnel-Private-Group-Id	Y	Y	RFC2868

Attributes supported in dynamic authorization

Following are the RADIUS attributes supported in dynamic authorization:

Attribute name	Tx	Rx	Notes

User-name	N	Y	RFC2865
Calling-station-id	N	Y	RFC2865/3580
Called-station-id	N	Y	RFC2865/3580
NAS-port-id	N	Y	RFC2869
NAS-port	N	Y	RFC2865
NAS-IP-Address	N	Y	RFC2865
NAS-Identifier	N	Y	RFC2865
NAS-IPv6-Address	N	Y	RFC3162
Error-cause	Y	N	RFC5176
Acct-Terminate-Cause	Y	Y	RFC2866
Acct-Session-Id	N	Y	RFC2866
Message-Authenticator	N	Y	RFC2869
Event-Timestamp	N	Y	RFC2869
State	Y	Y	RFC2865
Proxy-State	Y	Y	RFC2865
Class	N	Y	RFC2865
Tunnel-Type	Y	Y	RFC2868
Tunnel-Medium-Type	Y	Y	RFC2868
Tunnel-Private-Group-Id	Y	Y	RFC2868

- One or more of the following attributes, **NAS-IP-Address**, **NAS-Identifier**, **NAS-IPv6-Address**, is mandatory for processing Change of Authorization (CoA) requests from dynamic authorization clients.
- Either **Acct-Session-Id** attribute, or one or both of **NAS-port** and **NAS-port-id** attributes and the **Calling-station-id** attribute is mandatory to identify the user session for processing CoA requests from dynamic authorization clients.
- The **User-name** attribute is mandatory for processing all CoA requests.
- The **Acct-Terminate-Cause** attribute is used in the CoA disconnect request and response messages.
- All session authorization attributes (both VSA and standard) are supported in the CoA message only, including **Aruba-Port-Bounce**.

Session authorization attributes supported in 802.1X and MAC authentication, and CoA

Standard session attributes supported

Following are the standard session attributes supported in 802.1X and MAC authentication, and CoA:

Attribute name	ID	Type	Notes
Filter-Id	11	String	RFC3580
Egress-VLANID	56	Octet	RFC4675
Egress-VLAN-Name	58	String	RFC4675
Tunnel-Type	64	Octet	RFC2868
Tunnel-Medium-Type	65	Octet	RFC2868
Tunnel-Private-Group-ID	81	String	RFC2868
NAS-Filter-Rule	92	String	RFC4849
Framed-MTU	12	Octet	RFC2865
Session-Timeout	27	Octet	RFC2865
Terminate-Action	29	Octet	RFC2865
Idle-Timeout	28	Octet	RFC2865



When multiple clients request a different MTU value using the **Framed-MTU** attribute, the highest MTU value requested among the clients will be programmed on the port.

Vendor-Specific Attributes supported in session authorization

Following are the Vendor-Specific Attributes (VSAs) supported in session authorization:

Attribute Name	Length	Type	Aruba Vendor ID	Aruba Attribute Type
Aruba-PoE-Priority	4	integer	14823	49
Aruba-Port-Auth-Mode	4	integer	14823	50
Aruba-NAS-Filter-Rule	<=247	string	14823	51
Aruba-QoS-Trust-Mode	4	integer	14823	52
Aruba-User-Role	<=63	string	14823	1
Aruba-Port-Bounce	4	Integer	14823	40
Aruba-STP-Admin-Edge-Port	4	Integer	14823	55
Aruba-UBT-Gateway-CPPM-Role	<=128	string	14823	59
Aruba-Device-Traffic-Class	4	Integer	14823	
Aruba-User-Mgmt-Interface	<=32	string	14823	69
Aruba-PoE-Allocate-By-Method	4	Integer	14823	70



- Change of Authorization of specific attributes in the user role is not supported. Only entire role can be changed.
- Similarly if the session is using RADIUS attributes, CoA can change only the RADIUS session attributes.
- Change of Authorization to user role for a session using RADIUS attributes is not supported either. If this action is attempted, a NAK message is sent.

Description of VSAs

Specifies the PoE priority of onboarding devices post authentication. Following are the supported values:

- **0:** Critical
- **1:** Medium
- **2:** Low

This attribute overrides the PoE priority configured on the port where the device onboards. This attribute is typically used for infrastructure devices. When multiple clients request different priorities, the critical priority takes precedence over medium priority and the medium priority takes precedence over low priority setting.

Specifies the authentication mode of the port post authentication. Following are the supported values:

- **1:** Device mode—In this mode, an infrastructure device, for example, switch or access point, is authenticated first, and all devices connecting to this authenticated device are allowed access. Here, the policy and VLAN attributes are applied at the port-level. In device mode, it is expected that only one device is active and authenticated at any instant. Untagged VLAN will override the port VLAN ID and the tagged VLANs will override the tagged VLANs that are configured on the port using the CLI.
- **2:** Client mode—In this mode, all devices trying to onboard on that port are authenticated. Here, the policy and VLAN attributes are applied per client. Untagged VLAN is configured using MAC-based VLAN. Tagged VLANs are arbitrated among all clients and the result is applied to the port.

Aruba-NAS-Filter-Rule

This attribute is similar to the NAS-Filter-Rule RFC attribute but with additional functionality to support vendor-specific actions in the rule. This attribute can be used to perform actions such as count and rate-limiting. Multiple instances of this attribute are supported, however, the maximum number of filter rules (including this VSA and `NAS-Filter-Rule`) supported per client is 128. A single **NAS-Filter-Rule** attribute split across multiple VSAs is not supported as servers such as FreeRadius and ClearPass Policy Manager do not terminate filter rule with '\0' value. Most policy servers use one filter rule per VSA.

Aruba-QoS-Trust-Mode

Specifies how the switch assigns local priority values to ingress packets. Following are the supported values:

- **0:** Trust mode DSCP
- **1:** Trust mode QoS
- **2:** No trust mode configuration

This attribute overrides the trust mode configured on the port where the device onboards. This attribute is typically used for infrastructure devices. When multiple clients request different trust modes, the DSCP trust mode takes precedence over QoS trust mode and the QoS trust mode takes precedence over no trust mode configuration setting.

Aruba-User-Role

Specifies the role that must be applied for the devices post authentication. The role must be defined on the switch. All the session attributes can be defined in the role. Session authorization attributes (both standard and VSAs) sent with this attribute are ignored.

Aruba-Port-Bounce

Used in the CoA message to signal the switch to shut down the port for the duration specified.

Aruba-STP-Admin-Edge-Port

When enabled, the port will be treated as STP edge port. Even if STP is configured on the port, it will not be executed. Traffic forwarding will occur immediately when a device connects to the port and completes authentication. Following are the supported values:

- **0:** Disable STP admin edge port.
- **1:** Enable STP admin edge port.

Aruba-PoE-Allocate-By-Method

This attribute is used to set the PoE power allocation method for onboarding devices post authentication. Following are the supported values:

- **1:** Class
- **2:** Usage

This feature allows you to change the default PoE allocation method on the port. If multiple clients connected to the same port request different allocation methods, **Class** is given priority.

Attributes supported in RADIUS network accounting

Following are the attributes supported in RADIUS network accounting:

Attribute name	Tx	Rx	Notes

User-name	N	N	RFC2865
Calling-station-id	Y	N	RFC2865
NAS-port-id	Y	N	RFC2869
NAS-port	Y	N	RFC2865
NAS-port-Type	Y	N	RFC2865
Service-Type	Y	N	RFC2865
NAS-IP-Address	Y	N	RFC2865
NAS-Identifier	Y	N	RFC2865
NAS-Ipv6-Address	Y	N	RFC3162
Acct-Authentic	Y	N	RFC2866
Acct-Session-Id	Y	N	RFC2866
Acct-Status-Type	Y	N	RFC2866
Acct-Input-Octets	Y	N	RFC2866 - In Interim and stop pkts
Acct-Output-Octets	Y	N	RFC2866 - In Interim and stop pkts
Acct-Input-Packets	Y	N	RFC2866 - In Interim and stop pkts
Acct-Output-Packets	Y	N	RFC2866 - In Interim and stop pkts
Acct-Input-Gigawords	Y	N	RFC2869 - In Interim and stop pkts
Acct-Output-Gigawords	Y	N	RFC2869 - In Interim and stop pkts
Acct-Session-Time	Y	N	RFC2866 - In Interim and stop pkts
Acct-Terminate-Cause	Y	N	RFC2866 - in Stop Pkt
Class	Y	N	RFC2865
Tunnel-Type	Y	N	RFC2868
Tunnel-Medium-Type	Y	N	RFC2868
Tunnel-Private-Group-Id	Y	N	RFC2868

Attributes supported in RADIUS server tracking

Following are the attributes supported for MAC authentication in RADIUS server tracking:

Attribute name	Tx	Rx	Notes

User-name	Y	N	RFC2865
NAS-IP-Address	Y	N	RFC2865
NAS-Identifier	Y	N	RFC2865
NAS-Ipv6-Address	Y	N	RFC3162
Chap-Challenge	Y	N	RFC2865
Chap-Password	Y	N	RFC2865
User-Password	Y	N	RFC2865

Port security enables you to configure each switch port with a unique list of the MAC addresses of devices that are authorized to access the network through that port. This security enables individual ports to detect, prevent, and log attempts by unauthorized devices to communicate through the switch. MAC Lockdown, also known as Static Addressing, is used to prevent station movement and MAC address hijacking, by allowing a given MAC address to use only an assigned port on the switch. MAC Lockdown also restricts the client device to a specific VLAN.

MAC Lockout enables blocking a specific MAC address so that the switch drops all traffic to or from the specified address.



Port security does not prevent intruders from receiving broadcast and multicast traffic. MAC Lockdown has a higher priority over port security.

Port-security sticky MAC

Sticky MAC is a port security feature that learns MAC addresses on an interface and retains the MAC information. When sticky learning is enabled on a port, all non-static MAC addresses are considered as sticky MACs. Also, all newly on-boarded clients are considered as sticky MACs. The sticky authorized clients are not affected by a switch reboot or link-flap once the MAC addresses are learnt. When disabled, all sticky MACs on the port are made as dynamic clients.

Sticky MACs can be configured statically (sticky-static) and also be learned dynamically (sticky-dynamic) on a sticky-learn enabled port.

-
- If the same MAC address is configured as sticky-static and static on a sticky learning port, sticky MAC configuration takes precedence.
 - Static non-sticky MAC addition is supported on a sticky learning enabled port.
 - Existing static port-security MACs on a port are not changed to sticky MAC on enabling the sticky MAC feature.
 - Moving sticky MAC clients from one port to another is a violation. You can view the violation information using the **show port-access security violation sticky-mac-client-move interface** command. Also, the following event log message will be displayed: **Port security sticky client move violation triggered on port {port} for client with MAC address {mac_addr}**.
 - Downgrading AOS-CX from 10.07 or later versions to earlier versions after learning port-security sticky MACs and upgrading it back to 10.07 or later versions might cause unstable behavior of sticky MACs. So, it is recommended to disable port-security configuration at the global context during migration of software image back to 10.07 or later versions in such scenarios.
-



Basic operation

Default port security operation

The default port security setting for each port is dynamic mode in which the switch learns addresses from inbound traffic from any connected device.

Intruder protection

A port that detects an intruder blocks the intruding device from transmitting to the network through that port.

General operation for port security

On a per-port basis, you can configure security measures to block unauthorized devices, and to send notice of security violations. Once port security is configured, you can then monitor the network for security violations through one or more of the following:

- Alert flags captured by network management tools.
- Alert Log entries in the WebAgent
- Event Log entries in the console interface

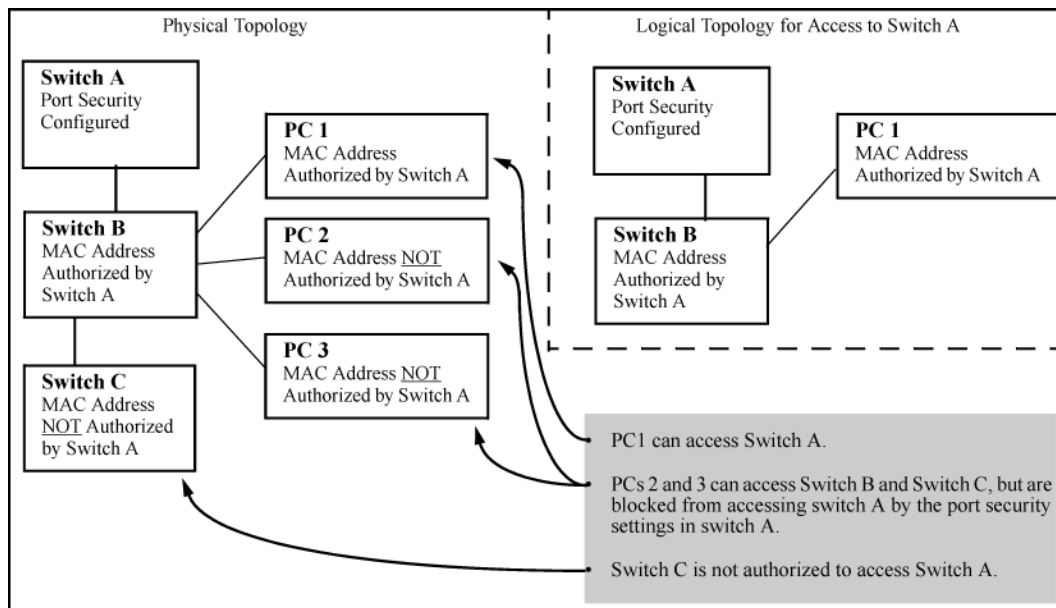
For any port, you can configure the following:

- Action—Used when a port detects an intruder. Specifies whether to send an SNMP trap to a network management station and whether to disable the port.
- Address limit—Sets the number of authorized MAC addresses allowed on the port.
- Static—Enables you to set a fixed limit on the number of MAC addresses authorized for the port and to specify some or all the authorized addresses. (If you specify only some of the authorized addresses, the port learns the remaining authorized addresses from the traffic it receives from connected devices.)
- Configured—Requires that you specify all MAC addresses authorized for the port. The port is not allowed to learn addresses from inbound traffic.
- Authorized (MAC) Addresses—Specify up to eight devices (MAC addresses) that are allowed to send inbound traffic through the port. This feature:
 - Closes the port to inbound traffic from any unauthorized devices that are connected to the port.
 - Provides the option for sending an SNMP trap notifying of an attempted security violation to a network management station and, optionally, disables the port.
- Port Access—Allows only the MAC address of a device authenticated through the switch 802.1X Port-Based access control.

Blocking unauthorized traffic

Unless you configure the switch to disable a port on which a security violation is detected, the switch security measures block unauthorized traffic without disabling the port. This implementation enables you to apply the security configuration to ports on which hubs, switches, or other devices are connected, and to maintain security while also maintaining network access to authorized users.

Figure 1 *How port security controls access*



Broadcast and Multicast traffic is always allowed, and can be read by intruders connected to a port on which you have configured port security.

Trunk group exclusion

Port security does not operate on either a static or dynamic trunk group. If you configure port security on one or more ports that are later added to a trunk group, the switch resets the port security parameters for those ports to the factory default configuration. Ports configured for either Active or Passive LACP, and which are not members of a trunk, can be configured for port security.

Port security commands

port-access port-security

```
port-access port-security {enable | disable}
no port-access port-security {enable | disable}
```

Description

Enables or disables port security globally or at the port level.

Examples

Enabling port security globally:

```
switch(config)# port-access port-security enable
```

Disabling port security globally:

```
switch(config)# port-access port-security disable
```

Enabling port security on a port:

```
switch(config-if)# port-access port-security enable
```

Disabling port security on a port:

```
switch(config-if)# port-access port-security disable
```

Command History

Release	Modification
10.09	Command introduced on the 8360

Command Information

Platforms	Command context	Authority
8100 8360	config config-if	Administrators or local user group members with execution rights for this command.

port-access port-security client-limit

```
port-access port-security client-limit <CLIENTS>  
no port-access port-security client-limit
```

Description

Configures the maximum number of clients that are allowed on a port. After configuring the maximum clients limit, the MAC addresses of the clients can be learned by one of the following methods:

- User can manually configure all MAC addresses by using the **mac-address** command.
- User can allow the port to dynamically learn all MAC addresses.
- User can configure a fixed number of MAC addresses and allow the switch to learn the remaining addresses dynamically.

The **no** form of the command resets the number of clients to the default, 1.

Parameter	Description
<CLIENTS>	Specifies the maximum number of clients. Default: 1. Range: 0 to 32 (4100i, 6000, 6100). 0 to 64 (8325, 10000). 0 to 32 (6200). 0 to 64 (6300, 6400). NOTE: If client limit is configured to 0, the port will not learn any MAC address from inbound traffic and will be blocked indefinitely. An administrator can use this along with the port-access security violation configuration to get notified of a client attempting to connect to a port.

Examples

Configuring client limit on a port:

```
switch(config-if)# port-access port-security enable
switch(config-if-port-security)# client-limit 24
```

Command History

Release	Modification
10.09	Command introduced on the 8360

Command Information

Platforms	Command context	Authority
8100 8360	config-if-port-security	Administrators or local user group members with execution rights for this command.

port-access port-security mac-address

```
port-access port-security mac-address <MAC-ADDRESS>
no port-access port-security mac-address <MAC-ADDRESS>
```

Description

Configures a static client (current interface (port) context) MAC address.

The **no** form of this command removes an authorized static client from the port.

Parameter	Description
<MAC-ADDRESS>	Specifies the static client MAC address.

Examples

Configuring a static client on a port:

```
switch(config-if)# port-access port-security
switch(config-if-port-security)# mac-address aa:bb:cc:dd:ee:ff
```

Deleting a static client on a port:

```
switch(config-if)# port-access port-security
switch(config-if-port-security)# no mac-address aa:bb:cc:dd:ee:ff
```

Command History

Release	Modification
10.09	Command introduced on the 8360

Command Information

Platforms	Command context	Authority
8100 8360	config-if-port-security	Administrators or local user group members with execution rights for this command.

show port-access port-security interface client-status

```
show port-access port-security interface {all|<IF-NAME>}
      client-status [mac <MAC-ADDRESS>]
```

Description

Shows port security clients status information for the ports. The output can be filtered by interface or MAC address.

Parameter	Description
all	Selects all interfaces.
<IF-NAME>	Specifies the interface name.
<MAC-ADDRESS>	Specifies the client MAC address.

Examples

Showing client status information for all ports:

```
switch# show port-access port-security interface all client-status

Port Security Client Status Details

Authorized-Clients    Type                Port
-----
AB:CD:DE:FF:AA:BB    static              1/1/1
DD:CD:AB:CD:EE:01    dynamic             1/1/2
00:50:56:96:7e:fc    sticky-dynamic      1/3/2
```

Showing client status information with sticky-learning enabled for all ports:

```
switch# show port-access port-security interface all client-status

Port Security Client Status Details

Authorized-Clients    Type                Port
-----
AB:CD:DE:FF:AA:BB    sticky-static       1/1/1
DD:CD:AB:CD:EE:01    sticky-dynamic      1/1/2
DE:CD:AB:BB:EE:02    sticky-dynamic      1/1/2
```

Showing client status information for a client:

```
switch# show port-access port-security interface 1/3/2 client-status mac
00:50:56:96:7e:fc

Port Security Client Status Details
```

Authorized-Clients	Type	Port
00:50:56:96:7e:fc	sticky-dynamic	1/3/2

Showing client status information for a port:

```
switch# show port-access port-security interface 1/3/2 client-status
```

Port Security Client Status Details

Authorized-Clients	Type	Port
00:50:56:96:7e:fc	sticky-dynamic	1/3/2

Command History

Release	Modification
10.09	Command introduced on the 8360

Command Information

Platforms	Command context	Authority
8100 8360	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show port-access port-security interface port-statistics

show port-access port-security interface {all|<IF-NAME>} port-statistics

Description

Shows port security statistics for the ports in a switch. The output can be filtered by interface.

Parameter	Description
all	Selects all interfaces.
<IF-NAME>	Specifies the interface name.

Examples

Showing information for all ports.

```
switch# show port-access port-security interface all port-statistics
```

Port 1/1/1
=====

Client Details

```
-----  
Number of authorized clients      : 0  
Number of sticky authorized clients : 2
```

Command History

Release	Modification
10.09	Command introduced on the 8360

Command Information

Platforms	Command context	Authority
8100 8360	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

sticky-learn enable

```
sticky-learn enable  
no sticky-learn enable
```

Description

Enables sticky learning on the port. All the existing and new MACs learned on the port are made sticky. The **no** form of this command disables the sticky learning on the port.

Examples

Enabling sticky learning on the port:

```
switch(config)# interface 1/1/1  
switch(config-if)# port-access port-security  
switch(config-if-port-security)# sticky-learn enable
```

Disabling sticky learning on the port:

```
switch(config)# interface 1/1/1  
switch(config-if)# port-access port-security  
switch(config-if-port-security)# no sticky-learn enable
```

Command History

Release	Modification
10.09	Command introduced on the 8360

Command Information

Platforms	Command context	Authority
8100 8360	config-if-port-security	Administrators or local user group members with execution rights for this command.

sticky-learn mac

```
sticky-learn mac <MAC-ADDRESS> [vlan <VLAN-ID>]
no sticky-learn mac <MAC-ADDRESS> [vlan <VLAN-ID>]
```

Description

Configures the MAC addresses of sticky static clients. After configuring, clients are directly added to the MAC address table.

The **no** form of this command removes an authorized sticky static client from the port.

Parameter	Description
<MAC-ADDRESS>	Specifies the static sticky client MAC address.
vlan <VLAN-ID>	Specifies the static sticky client VLAN ID.

Examples

Configuring a sticky static client on a port:

```
switch(config)# interface 1/1/1
switch(config-if)# port-access port-security
switch(config-if-port-security)# sticky-learn mac-address aa:bb:cc:dd:ee:ff
```

Configuring a sticky static client with a VLAN ID on a port:

```
switch(config)# interface 1/1/1
switch(config-if)# port-access port-security
switch(config-if-port-security)# sticky-learn mac-address aa:bb:cc:dd:ee:ff vlan 4
```

Removing a sticky static client from a port:

```
switch(config)# interface 1/1/1
switch(config-if)# port-access port-security
switch(config-if-port-security)# no sticky-learn mac-address aa:bb:cc:dd:ee:ff
```

Command History

Release	Modification
10.09	Command introduced on the 8360

Command Information

Platforms	Command context	Authority
8100 8360	config-if-port-security	Administrators or local user group members with execution rights for this command.

show port-access security violation sticky-mac-client-move interface

show port-access security violation sticky-mac-client-move interface {all|<IF-NAME>}

Description

Shows information about the sticky-mac client move violation. The output can be filtered by interface.

Parameter	Description
all	Selects all interfaces.
<IF-NAME>	Specifies the interface name.

Examples

Showing information for all ports.

```
switch# show port-access port-security violation sticky-mac-client-move
interface all
```

Sticky MAC Client Move Violation Status Details

Port	Violation	Violation-Count
1/1/1	No	0
1/1/2	Yes	10
1/1/5	No	10

Showing information for a particular port.

```
switch# show port-access port-security violation sticky-mac-client-move
interface 1/1/1
```

Sticky MAC Client Move Violation Status Details

Port	Violation	Violation-Count
1/1/1	No	10

Command History

Release	Modification
10.09	Command introduced on the 8360

Command Information

Platforms	Command context	Authority
8100 8360	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

AOS-CX switches include automatic detection and control for certain link errors and excessive traffic conditions. Fault monitor can be used to log an event or send SNMP traps for these conditions and temporarily disable the port to protect the network. Monitoring can be enabled for all recognized faults or for individual faults, and actions and thresholds for each fault can be configured.

Fault monitor applies only to physical ports and not to LAGs, tunnels, VSF links, or other types of interfaces. Fault monitoring can be applied to the individual members of a LAG.

Fault monitoring conditions

The following fault conditions are available for monitoring:

Excessive broadcasts

An excessive broadcast (broadcast storm) fault is reported when the average ingress traffic rate of broadcast packets exceeds the configured threshold in a 20 second interval.

The default threshold level is configured as a percentage of the bandwidth of the port. Larger the frame size, smaller the converted threshold value in PPS. Hence larger frames require lower threshold percent configurations to hit the fault.

Excessive multicasts

An excessive multicasts (multicast storm) fault is reported when the average ingress traffic rate of multicast packets exceeds the configured threshold in a 20 second interval.

Excessive link flaps

An excessive link flaps fault is reported when the count of transitions between link-up and link-down state exceeds the configured threshold in a 10 second interval.

Excessive oversize packets

An excessive oversized packet fault is reported when the number of ingress oversized frames per 10,000 received frames exceeds the configured threshold value in a 20 second interval. In an oversize packet fault, the packets size is more than the configured MTU on the interface with good cyclic redundancy check (CRC).

Excessive jabbers

An excessive jabbers fault is reported when the number of ingress jabber frames per 10,000 received frames exceeds the configured threshold value in a 20 second interval. In a jabbers fault, the packets size is more than the configured MTU on the interface with bad CRC.

Excessive fragments

An excessive fragments fault is reported when the number of ingress fragment frames per 10,000 received frames exceeds the configured threshold value in a 20 second interval. In a fragments fault, the packet size is less than 64 bytes with bad CRC.

Excessive CRC errors

An excessive CRC errors fault is reported when the number of ingress `crc-error` frames per 10,000 received frames exceeds the configured threshold value in a 20 second interval.

Excessive TX drops

An excessive TX drops fault is reported when egress dropped packets per 10,000 transmitted frames exceeds the configured threshold value in a 20 second interval.

Fault monitor commands

(Fault enabling/disabling)

```
{all | <FAULT>}  
no {all | <FAULT>}
```

Description

Within the selected fault monitor profile context, enables all faults or specific faults for monitoring.

By default, all faults are disabled in a profile and remain disabled until enabled as described here. Configuring the action and threshold does not enable the fault.



Faults enabled with this command use default actions and thresholds unless the actions and thresholds are configured. For information on configuring actions and thresholds for a fault, respectively see [action](#) and [threshold](#).

The **no** form of this command disables faults for monitoring.

Parameter	Description
all	Selects all faults.
<FAULT>	Selects a specific fault. Available fault names: excessive-broadcasts excessive-multicasts excessive-link-flaps excessive-oversize-packets excessive-jabbers excessive-fragments excessive-crc-errors excessive-tx-drops

Examples

Enabling all faults:

```
switch(config-fault-monitor-profile) # all
```

Disabling all faults:

```
switch(config-fault-monitor-profile) # no all
```

Enabling individual faults:

```
switch(config-fault-monitor-profile) # excessive-broadcasts  
switch(config-fault-monitor-profile) # excessive-multicasts  
switch(config-fault-monitor-profile) # excessive-link-flaps  
switch(config-fault-monitor-profile) # excessive-oversize-packets  
switch(config-fault-monitor-profile) # excessive-jabbers  
switch(config-fault-monitor-profile) # excessive-fragments  
switch(config-fault-monitor-profile) # excessive-crc-errors  
switch(config-fault-monitor-profile) # excessive-tx-drops
```

Disabling individual faults:

```
switch(config-fault-monitor-profile) # no excessive-broadcasts  
switch(config-fault-monitor-profile) # no excessive-multicasts  
switch(config-fault-monitor-profile) # no excessive-link-flaps  
switch(config-fault-monitor-profile) # no excessive-oversize-packets  
switch(config-fault-monitor-profile) # no excessive-jabbers  
switch(config-fault-monitor-profile) # no excessive-fragments  
switch(config-fault-monitor-profile) # no excessive-crc-errors  
switch(config-fault-monitor-profile) # no excessive-tx-drops
```

Command History

Release	Modification
10.11.1000	Command introduced on the 8320, 8325, 8360, 9300 and 10000.

Command Information

Platforms	Command context	Authority
All platforms	config-fault-monitor-profile	Administrators or local user group members with execution rights for this command.

action

```
{all | <FAULT>} action {notify | notify-and-disable [auto-enable <TIMEOUT>]}
```

```
no {all | <FAULT>} action {notify | notify-and-disable [auto-enable <TIMEOUT>]}
```

Description

Within the selected fault monitor profile context, configures the fault monitoring action for the specified fault. Default action: **notify** with **auto-enable** disabled.

The no form of this command removes the action and disables **auto-enable**.

Parameter	Description
all	Selects all faults.
<FAULT>	Selects a specific fault. Available fault names: excessive-broadcasts excessive-multicasts excessive-link-flaps excessive-oversize-packets excessive-jabbers excessive-fragments excessive-crc-errors excessive-tx-drops
notify	Selects the <code>notify</code> action. Notifies through events, DLOGs, and SNMP trap. This action is enabled by default.
notify-and-disable	Selects the action as <code>notify-and-disable</code> . Notifies through events, DLOGs, and SNMP trap, and then disables the port.
auto-enable <TIMEOUT>	Sets the number of seconds after which a port disabled by the <code>notify-and-disable</code> action is automatically re-enabled. Range: 1 to 604800 seconds.



The fault parameter values are saved even after a fault is disabled in the profile. The saved values will be used if the fault is later re-enabled in the profile again.

Examples

Configuring the **notify** action for all faults within a given profile:

```
switch(config-fault-monitor-profile) # all action notify
```

Configuring the `notify-and-disable` action for all faults within a given profile:

```
switch(config-fault-monitor-profile) # all action notify-and-disable
```

Configuring the **notify-and-disable** action for all faults with **auto-enable** within a given profile:

```
switch(config-fault-monitor-profile) # all action notify-and-disable auto-enable 80
```

Disabling all fault monitoring for this profile:

```
switch(config-fault-monitor-profile) # no all
```

Restoring all fault monitoring to the default action **notify** within a given profile:

```
switch(config-fault-monitor-profile) # no all action
```

Unconfiguring the auto-enable timer for all fault monitoring within a given profile:

```
switch(config-fault-monitor-profile)# no all action notify-and-disable auto-enable
```

Configuring the **notify** action for specific faults within a given profile:

```
switch(config-fault-monitor-profile)# excessive-oversize-packets action notify
```

Configuring the **notify-and-disable** action for specific faults within a given profile:

```
switch(config-fault-monitor-profile)# excessive-link-flaps action notify-and-disable
switch(config-fault-monitor-profile)# excessive-fragments action notify-and-disable
switch(config-fault-monitor-profile)# excessive-crc-errors action notify-and-disable
```

Configuring the **notify-and-disable** action with **auto-enable** for specific faults within a given profile:

```
switch(config-fault-monitor-profile)# excessive-broadcasts action notify-and-disable auto-enable 80
switch(config-fault-monitor-profile)# excessive-multicasts action notify-and-disable auto-enable 100
switch(config-fault-monitor-profile)# excessive-tx-drops action notify-and-disable auto-enable 70
switch(config-fault-monitor-profile)# excessive-jabbers action notify-and-disable auto-enable 60
```

Restoring fault monitoring to the default action **notify** within a given profile:

```
switch(config-fault-monitor-profile)# no excessive-oversize-packets action
switch(config-fault-monitor-profile)# no excessive-jabbers action
switch(config-fault-monitor-profile)# no excessive-oversize-packets action notify-and-disable
```

Unconfiguring the auto-enable timer within a given profile:

```
switch(config-fault-monitor-profile)# no excessive-jabbers action notify-and-disable auto-enable
```

Command History

Release	Modification
10.11.1000	Command introduced on the 8320, 8325, 8360, 9300 and 10000.

Command Information

Platforms	Command context	Authority
All platforms	config-fault-monitor-profile	Administrators or local user group members with execution rights for this command.

apply fault-monitor profile

```

apply fault-monitor profile <PROFILE-NAME>
no apply fault-monitor profile [<PROFILE-NAME>]

```

Description

Applies a fault monitoring profile to the selected interface or interface range.

The **no** form of this command removes the fault monitoring profile from the selected interface or interface range.

Parameter	Description
<PROFILE-NAME>	Specifies the fault monitor profile name. Range: Up to 64 alphanumeric and special characters.

Examples

Applying the fault monitoring profile to a interface:

```

switch(config)# interface 1/1/1
switch(config-if)# apply fault-monitor profile noisy-ports

```

Applying the fault monitoring profile to a interface range:

```

switch(config)# interface 1/1/2-1/1/24
switch(config-if)# apply fault-monitor profile quiet-ports

```

Command History

Release	Modification
10.11.1000	Command introduced on the 8320, 8325, 8360, 9300 and 10000.

Command Information

Platforms	Command context	Authority
All platforms	config-if	Administrators or local user group members with execution rights for this command.

fault-monitor profile

```

fault-monitor profile <PROFILE-NAME>
no fault-monitor profile <PROFILE-NAME>

```

Description

Creates a fault monitoring profile and enters its context which is indicated as **(config-fault-monitor-profile)**. If the profile already exists, this command enters the profile context. A maximum of 16 fault monitoring profiles are supported.

For information on enabling a fault within a fault monitor profile, see [\(Fault enabling/disabling\)](#).

For information on configuring actions and thresholds for a fault, respectively see [action](#) and [threshold](#).

For information on applying a fault monitor profile to a interface or interface range, see [apply fault-monitor profile](#).

The **no** form of this command deletes the fault monitoring profile.



By default, all faults are disabled in a profile.

Parameter	Description
<code><PROFILE-NAME></code>	Specifies the fault monitor profile name. Range: Up to 64 alphanumeric and special characters.

Examples

Creating a fault monitor profile and entering its context:

```
switch(config) # fault-monitor profile noisy-ports
switch(config-fault-monitor-profile) #
```

Deleting a fault monitor profile:

```
switch(config) # no fault-monitor profile noisy-ports
```

Command History

Release	Modification
10.11.1000	Command introduced on the 8320, 8325, 8360, 9300 and 10000.

Command Information

Platforms	Command context	Authority
All platforms	<code>config</code>	Administrators or local user group members with execution rights for this command.

show fault-monitor profile

```
show fault-monitor profile <PROFILE-NAME>
```

Description

Shows fault monitoring profile information for all profiles or a specific profile.

Parameter	Description
<code><PROFILE-NAME></code>	Specifies the fault monitor profile name. Range: Up to 64 alphanumeric and special characters.

Example

Showing information for all fault monitoring profiles:

```
switch# show fault-monitor profile
```

```
-----
Fault monitor profile: noisy-ports
-----
```

Auto Fault	Enabled	Threshold	Action	Enable
excessive-broadcasts	yes	5%	notify-and-disable	--
excessive-multicasts	yes	1000 pps	notify-and-disable	--
excessive-link-flaps	yes	7	notify-and-disable	--
excessive-oversize-packets	yes	25	notify-and-disable	--
excessive-jabbers	yes	25	notify-and-disable	--
excessive-fragments	yes	25	notify-and-disable	--
excessive-crc-errors	yes	25	notify-and-disable	--
excessive-tx-drops	yes	25	notify-and-disable	--

```
-----
Fault monitor profile: quiet-ports
-----
```

Auto Fault	Enabled	Threshold	Action	Enable
excessive-broadcasts	yes	20%	notify-and-disable	--
excessive-multicasts	yes	25000 pps	notify-and-disable	40
excessive-link-flaps	yes	7	notify	--
excessive-oversize-packets	yes	30	notify-and-disable	--
excessive-jabbers	no	30	notify-and-disable	100
excessive-fragments	yes	30	notify-and-disable	--
excessive-crc-errors	yes	30	notify-and-disable	--
excessive-tx-drops	yes	30	notify-and-disable	--

Showing information for a particular fault monitoring profile:

```
switch# show fault-monitor profile noisy-ports
```

```
-----
Fault monitor profile: noisy-ports
-----
```

Auto Fault	Enabled	Threshold	Action	Enable
excessive-broadcasts	yes	5%	notify-and-disable	--
excessive-multicasts	yes	1000 pps	notify-and-disable	--
excessive-link-flaps	yes	7	notify-and-disable	--
excessive-oversize-packets	yes	25	notify-and-disable	--
excessive-jabbers	yes	25	notify-and-disable	--
excessive-fragments	yes	25	notify-and-disable	--
excessive-crc-errors	yes	25	notify-and-disable	--
excessive-tx-drops	yes	25	notify-and-disable	--

Command History

Release	Modification
10.11.1000	Command introduced on the 8320, 8325, 8360, 9300 and 10000.

Command Information

Platforms	Command context	Authority
All platforms	Manager (#)	Administrators or local user group members with execution rights for this command.

show interface fault-monitor profile

show interface [<INTERFACE>|<IF-RANGE>] fault-monitor profile

Description

Shows fault monitoring profile configuration information for all or specific interfaces.

Parameter	Description
<INTERFACE>	Specifies a single interface.
<IF-RANGE>	Specifies a interface range,

Example

Showing all interfaces with applied fault monitoring profiles:

```
switch# show interface fault-monitor profile
```

```
-----
Port      Fault Monitor Profile
-----
```

```
1/1/1     noisy-ports
1/1/2     quiet-ports
1/1/4     quiet-ports
1/1/5     noisy-ports
1/1/6     noisy-ports
1/1/7     quiet-ports
```

Showing a range of interfaces with applied fault monitoring profiles:

```
switch# show interface 1/1/1-1/1/2,1/1/6 fault-monitor profile
```

```
-----
Port      Fault Monitor Profile
-----
```

```
1/1/1     noisy-ports
1/1/2     quiet-ports
1/1/6     noisy-ports
```

Command History

Release	Modification
10.11.1000	Command introduced on the 8320, 8325, 8360, 9300 and 10000.

Command Information

Platforms	Command context	Authority
All platforms	Manager (#)	Administrators or local user group members with execution rights for this command.

show interface fault-monitor status

```
show interface [<INTERFACE>|<IF-RANGE>] fault-monitor status
```

Description

Shows active fault information for all or specific interfaces.

Parameter	Description
<INTERFACE>	Specifies a single interface.
<IF-RANGE>	Specifies a interface range,

Example

Showing active fault information for all interfaces with applied fault monitoring profiles:

```
switch# show interface fault-monitor status
```

Port	Fault	Fault Elapsed Time	Port State	Time Left
1/1/1	excessive-broadcasts	Tue Apr 14 14:29:09 UTC 2020	down	60
	excessive-jabbers	Tue Apr 15 14:29:09 UTC 2020	--	--
1/1/2	excessive-oversize-packets	Tue Apr 16 14:29:09 UTC 2020	down	--

Showing active fault information for a range of interfaces with applied fault monitoring profiles:

```
switch# show interface 1/3/1,1/3/3 fault-monitor status
```

Port	Fault	Occurring Since	Port State	Time Left
1/1/4	excessive-broadcasts	Tue Apr 14 14:29:09 UTC 2020	down	60
	excessive-jabbers	Tue Apr 15 14:29:09 UTC 2020	--	100

Command History

Release	Modification
10.11.1000	Command introduced on the 8320, 8325, 8360, 9300 and 10000.

Command Information

Platforms	Command context	Authority
All platforms	Manager (#)	Administrators or local user group members with execution rights for this command.

show running-config

show running-config [interface <IFNAME> | current-context | all]

Description

Shows the running configuration including any fault-monitor profile configurations and profile-names applied to an interface. The below examples focus on fault monitor-related configuration items. Other configuration items that may be present are represented by an ellipsis (. . .).

Parameter	Description
interface <IFNAME>	Shows running configuration information for only the specified interface.
current-context	Shows running configuration information for only the current context.
all	Shows all running configuration information.

Examples

Showing the running configuration for a particular interface:

```
switch# show running-config interface 1/1/1
interface 1/1/1
...
    apply fault-monitor profile noisy-ports
...
```

Showing the running configuration for a particular fault monitor profile current context:

```
switch# fault-monitor profile noisy-ports
switch(config-fault-monitor-profile)# show running-config current-context
fault-monitor profile noisy-ports
    excessive-broadcasts
    excessive-broadcasts threshold pps 10000
    excessive-broadcasts action notify-and-disable auto-enable 2000
    excessive-multicasts
    excessive-multicasts threshold pps 10000
    excessive-link-flaps
    excessive-link-flaps action notify-and-disable auto-enable 2000
```

Showing all running configuration:

```
switch# show running-config all
...
fault-monitor profile noisy-ports
    excessive-broadcasts
    excessive-broadcasts threshold pps 10000
```

```

excessive-broadcasts action notify-and-disable auto-enable 2000
excessive-multicasts
excessive-multicasts threshold pps 10000
excessive-multicasts action notify
excessive-link-flaps
excessive-link-flaps threshold count 7
excessive-link-flaps action notify-and-disable auto-enable 2000
no excessive-oversize-packets
excessive-oversize-packets threshold value 25
excessive-oversize-packets action notify
no excessive-jabbers
excessive-jabbers threshold value 25
excessive-jabbers action notify
no excessive-fragments
excessive-fragments threshold value 25
excessive-fragments action notify
no excessive-crc-errors
excessive-crc-errors threshold value 25
excessive-crc-errors action notify
no excessive-tx-drops
excessive-tx-drops threshold value 25
excessive-tx-drops action notify
...
interface 1/1/1
...
  apply fault-monitor profile noisy-ports
...

```

Command History

Release	Modification
10.11.1000	Command introduced on the 8320, 8325, 8360, 9300 and 10000.

Command Information

Platforms	Command context	Authority
All platforms	Manager (#)	Administrators or local user group members with execution rights for this command.

threshold

```

<FAULT> threshold value <VALUE>
no <FAULT> threshold [value <VALUE>]

excessive-link-flaps threshold count <COUNT>
no excessive-link-flaps threshold [count <COUNT>]

excessive-fc-watchdog-triggers threshold count <COUNT>
no excessive-fc-watchdog-triggers threshold [count <COUNT>]

{excessive-broadcasts | excessive-multicasts}
  threshold {percent <BW-PERCENT> | pps <PPS>}
no {excessive-broadcasts | excessive-multicasts}
  threshold [{percent <BW-PERCENT> | pps <PPS>}]

no all threshold

```

Description

Within the selected fault monitor profile context, sets the specified fault threshold.

The **no** form of this command resets the threshold to its default value.

Parameter	Description
<code><FAULT> threshold value <VALUE></code> With <code><FAULT></code> set to any of these names: excessive-oversize-packets excessive-jabbers excessive-fragments excessive-crc-errors excessive-tx-drops	Sets the threshold number of bad frames per 10000 good frames received or per 10000 good frames sent (depending on the fault), to be considered a fault. Range: 1 to 10000. Default: 25.
<code>excessive-link-flaps threshold count <COUNT></code>	Sets the threshold count of interface link flaps, during a 10 second sampling interval, to be considered a fault. Range: 1 to 100. Default: 7.
<code>{excessive-broadcasts excessive-multicasts} threshold percent <BW-PERCENT></code>	Sets the fault threshold as a percentage of port bandwidth for minimum sized packets that is considered to be a fault. Range: 1 to 100. Default 5.
<code>{excessive-broadcasts excessive-multicasts} threshold pps <PPS></code>	Sets the fault threshold in packets per second. Range: 1 to 195312500.

If excessive-broadcast or excessive-multicast faults are configured with the threshold higher than the `rate-limit` threshold, the following occurs:



- Fault reporting still happens as the port has actually received packets at a rate that violated its threshold.
- Traffic gets shaped as per `rate-limit` configuration and any packet exceeding the `rate-limit` threshold gets dropped.

Examples

Setting thresholds:

```
switch(config-fault-monitor-profile)# excessive-oversize-packets threshold value 40
switch(config-fault-monitor-profile)# excessive-jabbers threshold value 30
switch(config-fault-monitor-profile)# excessive-fragments threshold value 50
switch(config-fault-monitor-profile)# excessive-crc-errors threshold value 35
switch(config-fault-monitor-profile)# excessive-tx-drops threshold value 20

switch(config-fault-monitor-profile)# excessive-link-flaps threshold count 14
switch(config-fault-monitor-profile)# excessive-broadcasts threshold percent 40
switch(config-fault-monitor-profile)# excessive-multicasts threshold pps 7500
```

Resetting all thresholds to their defaults:

```
switch(config-fault-monitor-profile)# no all threshold
```

Resetting individual thresholds to their defaults:

```

switch(config-fault-monitor-profile) # no excessive-oversize-packets threshold
switch(config-fault-monitor-profile) # no excessive-jabbers threshold
switch(config-fault-monitor-profile) # no excessive-fragments threshold
switch(config-fault-monitor-profile) # no excessive-crc-errors threshold
switch(config-fault-monitor-profile) # no excessive-tx-drops threshold

switch(config-fault-monitor-profile) # no excessive-link-flaps threshold

switch(config-fault-monitor-profile) # no excessive-broadcasts threshold
switch(config-fault-monitor-profile) # no excessive-multicasts threshold

```

Command History

Release	Modification
10.11.1000	Command introduced on the 8320, 8325, 8360, 9300 and 10000.

Command Information

Platforms	Command context	Authority
All platforms	config-fault-monitor-profile	Administrators or local user group members with execution rights for this command.

vsx-sync (fault monitor)

```

vsx-sync
no vsx-sync

```

Description

Within the selected fault monitor profile context, configures VSX synchronization for the selected fault monitoring profile.

The **no** form of this command removes the VSX synchronization for a fault monitoring profile.

Example

Configuring VSX synchronization for a fault monitoring profile:

```

switch(config-fault-monitor-profile) # vsx-sync

```

Command History

Release	Modification
10.11.1000	Command introduced on the 8320, 8325, 8360, 9300 and 10000.

Command Information

Platforms	Command context	Authority
8100 8360	config-fault-monitor-profile	Administrators or local user group members with execution rights for this command.



The 8360 Switch Series supports the core and edge for relaying the GBP tag. Access is not supported. For core and edge to support GBP relay, you must enable GBP with command `gbp enable`.

Group Based Policies (GBP) are used to segment user traffic in a network by grouping the users into roles based on user authentication at the source or ingress VXLAN tunnel endpoint (VTEP). Source-based roles will remain effective even if a device authenticates at a different location, or if the device is assigned a different IP address. Users can be local authenticated, MAC authenticated, or 802.1X authenticated clients. After authentication a Group Policy ID is mapped based on the role applied.

Dynamic Segmentation or Virtual Network Based Tunneling (VNBT) helps in segmentation of user traffic over a VXLAN overlay based network and GBP helps by providing segmentation of user traffic in the same domain based on user role (determined during authentication). Segmentation using GBP feature performs the following actions:

- Allows micro-segmentation of the user traffic on the same VLAN by classifying the user traffic based on user role. The role is then converted into Group Policy IDs and carried in the VXLAN header.
- At egress, the switch determines if the traffic from the source role (as carried in the Group Policy ID) is permitted to the destination role (as determined from the destination MAC) and accordingly either forwards or drops the traffic.
- In a gateway scenario, the traffic on a VXLAN tunnel may get terminated and enter another VXLAN tunnel. In such scenarios, the Group Policy ID must be transported to the new tunnel for the final destination to enforce role-based policies.
- Since 6200 Switch Series connected leaf uses only static vxlan , the traffic on a VXLAN tunnel may get terminated and enter another VXLAN tunnel. In such scenarios, the Group Policy ID must be transported to the new tunnel for the final destination to enforce role-based policies.
- GBP tag is transmitted from one tunnel to another on the leaf connected to the 6200 Switch Series and you must enable `inter-vxlan-bridging-mode ( deny | static-evpn | static-all )` command on leaf to support this.



Enabling inter-VXLAN bridging with the `inter-vxlan-bridging-mode {deny | static-evpn | static-all}` command under the VXLAN interface is a prerequisite for GBP on edge and wherever 6200 is connected to leaf. This applies to 6300, 6400 and 8360 Switch Series.

The port-access group-based policies support GBP-MAC, GBP-IPv4 and GBP-IPv6 based classes. These classes cannot be configured under classifier or port-access policies as match criteria. All the destination roles in the class entries match condition should be the same role.

Group based port-access policies (GBP) are configured and applied globally via local user roles (LUR) to the clients. GBP does not support downloadable user roles (DUR). Classes in group based policies should have a destination role that is the same as the associated user role. If the associated role is not the same, the clients will not be onboarded.

Limitations and considerations

- CPU-generated packets are assigned the **infra** role as source role, but packets re-forwarded by the CPU (such as CPU tx-to-port packets) are assigned the **default** role as the source role.
- The following applications) re-forward packets, so GBP policies for the default role are required to egress the packet: DHCP Snooping (both IPv4 and IPv6), Captive Portal, ND snooping, RA Guard, IGMP, MLD and mDNS.
- When a GBP is updated while the port-access daemon is not running, all the clients associated with the GBP will be logged off when the daemon restarts.
- New system roles **internet(3)**, **intranet(4)**, and **isl(5)** are introduced in 10.13. If you upgrade from a release earlier than 10.14, make sure that reserved system role id's are be available. Any user defined role names conflicting with newly introduced system role names should be removed. If any existing user defined or system roles using role id's 3,4,5 should be re-configured with different role-id.
- Data packets can get an **Intranet** role assigned as a source role based on an Intranet role object group mapping, where the object group contains list of IPv4/IPv6 prefixes. Data packets have the **Intranet** role assigned as the source role as intranet role if the source IPv4/IPv6 address of the packet matches any of IPv4/IPv6 prefixes specified in the object group that is mapped to the **intranet** role. Traffic destined to subnets associated with intranet role object groups are permitted unless explicitly denied.



Host prefixes /32 or /128 configured in the object group are not included in matching prefix list to match against source IPV4/IPv6 address of the packet while assigning the role.

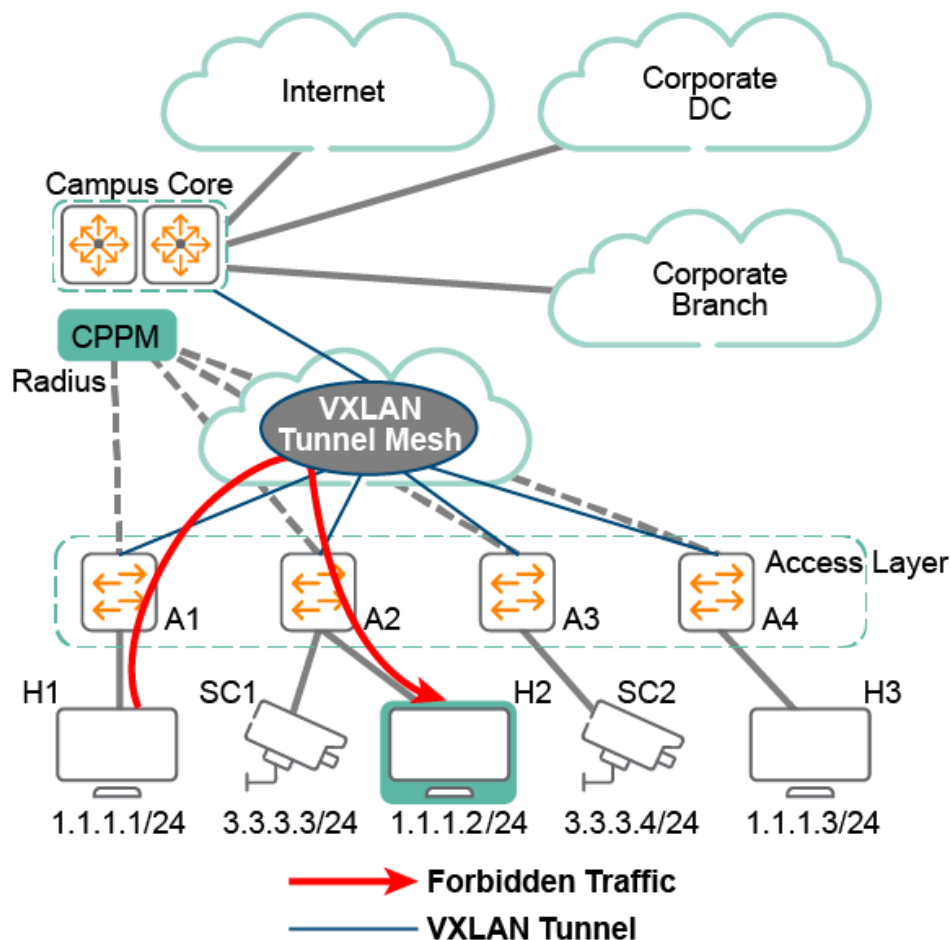
GBP scenarios

Group Policy ID-based segmentation in the wired network

The following figure depicts a distributed routing scenario. Consider the following for traffic segmentation:

- Macro segmentation—Disallow all traffic from the security cameras to guests.
- Micro segmentation—Disallow all traffic from guests to the admin.

Example for Group Policy ID-based segmentation



Client	MAC	VLAN/Subnet	L2-VNI	Role
H1	M1	100/1.1.1.0/24	1000	Guest
H2	M2	100/1.1.1.0/24	1000	Admin
H3	M3	100/1.1.1.0/24	1000	Guest
SC1	M4	300/3.3.3.0/24	3000	Security Camera
SC2	M5	300/3.3.3.0/24	3000	Security Camera

The access clients are assigned the respective roles and each switch knows the roles of the clients directly connected to them.

Macro segmentation

A simple subnet ACL having a destination prefix of 3.3.3.0/24 can be associated with the guest role and help in enforcing prohibition of any traffic from security cameras towards guests. Switches A1 and A4 enforce this ACL on such traffic originating from H1 and H3 respectively.

Micro segmentation

A subnet ACL cannot enforce similar prohibition of traffic from guests to the admin as guest and admin clients are on the same subnet. Consider a packet originated from H1 flowing towards H2:

1. Switch A1 identifies the source role (guest) based on source MAC and inserts an integer ID (Group Policy ID) that represents the guest role into the VXLAN-GBP bits and forwards the packet over VXLAN to switch A2. The forwarding mechanism is regular VXLAN bridging.
2. When the packet arrives at A2, it determines the destination role (admin) from the destination MAC (M2). Now A2 has information about both roles, the source role tag arriving over VXLAN and the locally-determined destination role. It can now enforce the guest to admin traffic prohibition.

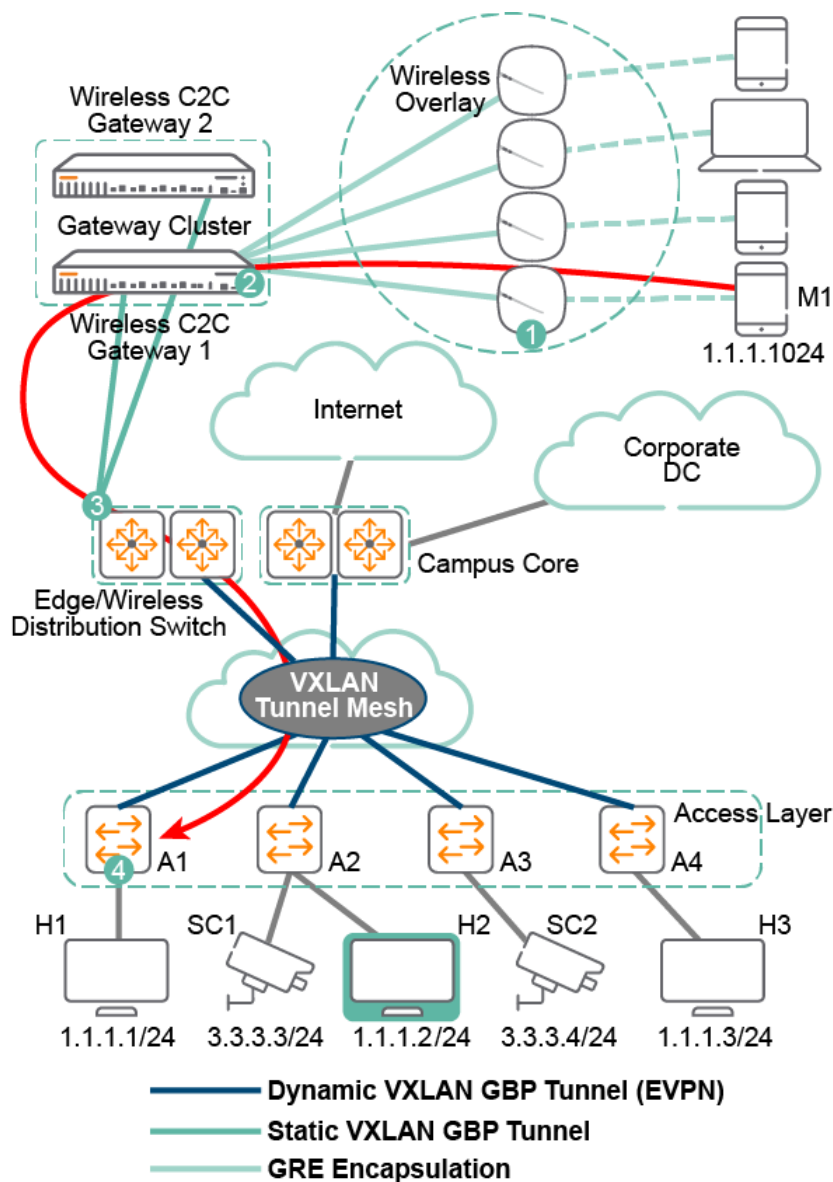
TCAM size

Platform	TCAM Size
6300	16K
6400	16K
8360	16K
6200	4K
8100	4K

Group Policy ID-based segmentation between wired and wireless clients

The Group Policy ID-based segmentation can also be implemented between a wired and wireless network using micro segmentation between wired and wireless clients.

Micro segmentation between wired and wireless clients



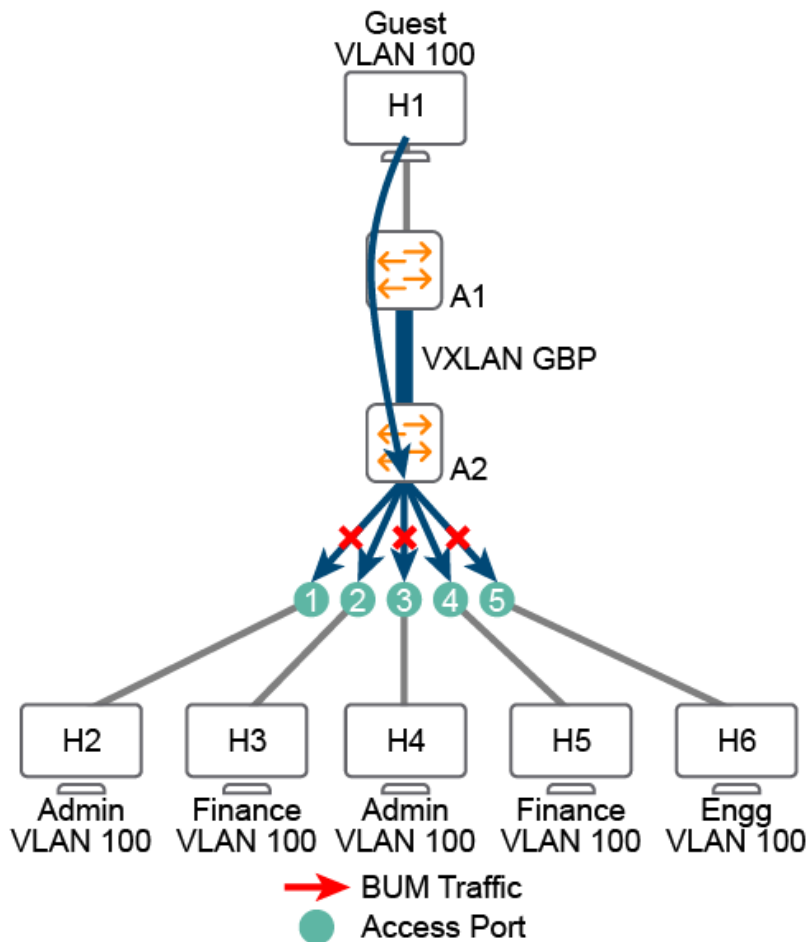
The following actions occur when a role-to-role ACL must be applied on the traffic from role of mobile device M1 to the role of H2.

1. The AP forwards the packet from M1 to gateway 1.
2. Gateway 1 forwards the traffic over the static VXLAN tunnel to the edge switch (8360). This packet carries the Group Policy ID corresponding to the role of M1.
3. The edge switch acts as the intermediate node and transfers the Group Policy ID over a static VXLAN to a dynamic VXLAN tunnel and forwards the packet to switch A1.
4. Switch A1 determines the destination role based on destination MAC or destination IP, and enforces role-to-role ACLs. This is similar to the case of wired network segmentation described earlier.

Group Policy ID-based segmentation for multicast traffic

Role-to-role ACLs must be enforced on multicast traffic, including broadcast, unknown unicast, and multicast (BUM) traffic. This is crucial for micro segmentation use cases where multiple roles are configured on the same VLAN. This scenario has all clients placed on a single VLAN.

Role-to-role ACL enforcement on multicast traffic



Source	Destination	Ethtype	Action
Guest	Admin	Any	Deny
Guest	Finance	Any	Permit
Guest	Engg	Any	Deny

In the above scenario all clients are placed on VLAN 100. The clients on A2 are connected over different access ports. When an ARP request packet originated from H1 arrives at A2 over VXLAN, the natural VLAN multicast mechanism is to send a copy of the packet out of all the five ports. However, given the role-to-role ACL configurations, the packet is sent out only to the finance clients out of ports 2 and 4. Consider that A2 implements IGMP snooping, and multicast group joins are received from ports 1, 2, and 5. As per the role-to-role ACL configuration, the allowed port list is 2 and 4. Therefore, when the multicast stream for the group arrives from H1 at A2, it is sent out of the intersection of the two sets of ports, that is, port 2 only.

Multicast traffic limitations

If both permitted clients and denied clients are connected to the same exit port, the switch lets the traffic out of the port, ignoring the presence of denied clients. The downstream hub or non-learning switch broadcasts the packets to both the clients.

In the above scenario, if H2 and H3 both are connected to port 1 on A2, and the role-to-role ACL configuration prohibits H1 to H2 multicast traffic where as H1 to H3 traffic is allowed, the permit action takes precedence at the port and the traffic is sent to both H2 and H3.

GBP limitations

- Only local user roles (LUR) are supported for GBP.
- Source roles must be created at the ingress VTEP.
- Source and destination roles must be created at the egress VTEP.
- Authentication is required to assign roles to devices and implement role-based policies.
- Reauthentication will fail If you configure a GBP MAC policy to allow only ARP using the **class gbp-mac** command. You must allow reauthentication traffic for reauthentication to be successful.

Group based policy commands

apply gbp role-access-list

```
[no] apply gbp role-access-list {ip|ipv6} <GBP_ACL_NAME>
```

Description

Applies the GBP role access list at the system level. When a new IPv4 or IPv6 GBP ACL is applied, the previously applied IPv4 or IPv6 GBP ACL is replaced with the new ACL.

This command is supported only on profile: Core-Spine.

The **no** form of this command removes the applied GBP role access list.

Parameter	Description
<i>ip ipv6</i>	Specifies the GBP role access list type, ip for IPv4, or ipv6 for IPv6.
<i><GBP_ACL_NAME></i>	Specifies the name of the GBP ACL. The maximum number of supported characters is 64.

Examples

Applying a GBP ACL:

```
switch(config)# apply gbp role-access-list ip gbp-inet
```

Command History

Release	Modification
10.13	Command introduced

Command Information

Platforms	Command context	Authority
8360	config	Administrators or local user group members with execution rights for this command.

gbp enable

```
gbp enable
no gbp enable
```

Description

Enables group based policy (GBP).

The **no** form of this command disables group based policy (GBP).

Examples

Enabling group based policy:

```
switch(config)# gbp enable
```

Disabling group based policy:

```
switch(config)# no gbp enable
```

Command History

Release	Modification
10.12	Added support for the 8100 Switch Series.
10.10	Added support for the 8360 Switch Series.
10.08	Command introduced.

Command Information

Platforms	Command context	Authority
8360 8100	config config-class- <i><CLASS-TYPE></i>	Administrators or local user group members with execution rights for this command.

gbp role

```
gbp role <ROLE_NAME> <ROLE_ID> object-group {ip|ipv6} <OBJECT_GROUP_NAME>
no gbp role <ROLE_NAME> <ROLE_ID> object-group {ip|ipv6} <OBJECT_GROUP_NAME>
```

Description

Starting from 10.13, for 8360 switch series, new default roles, internet, intranet, and ISL are introduced to differentiate traffic from different fabrics or networks. It is necessary to ensure that the reserved system role names are available before upgrading to AOS-CX 10.13. Any existing user defined system roles that use the role names, internet, intranet, and ISL should be removed and reconfigured with a different role name.

This command maps the role name to the role ID. This command also maps an existing object group (VRF) to an intranet role to differentiate internet traffic from other traffic that comes from different fabrics or networks. The mapping of an object group to a role is currently supported only for the intranet role. For example, if the traffic from DHCP server is part of an object group that is mapped to intranet, then the packets from the DHCP server will have the intranet tag. Similarly, traffic from the multicast source will have the internet or intranet tags based on the object group mapping

configuration. The object group mapping for VRFs is supported only on profile: Core-Spine. The **no** form of this command removes the intranet role mapping to the object group.



The new default roles, internet, intranet are also supported on 8100 switch series.

Parameter	Description
<ROLE_NAME>	Specifies the role name to be mapped.
<ROLE_ID>	Specifies the role ID. Range: 100 to 8191. The <ROLE_ID> parameter is supported only on 8100 switch series.
object-group {ip ipv6}	Specifies the object group type. ip for IPv4, or ipv6 for IPv6. The object-group parameter is supported only on 8360 switch series.
<OBJECT_GROUP_NAME>	Specifies the name of the object group.

Examples

Mapping the **employee** role to the role ID **130**:

```
switch(config)# gbp role employee 130
```

The following error message is displayed when user attempts to delete a GBP role which is used inside a policy:

```
switch(config)# no gbp role finance
Role 'finance' is present inside a class. Deletion of role mapping will impact the
traffic flow.
Do you want to continue (y/n)? y
```

Mapping the **intranet** role to object group **net_group**:

```
switch(config)# gbp role intranet object-group ip net_group
```

Command History

Release	Modification
10.13	The object-group parameter was introduced for 8360 switch series.
10.12	Added support for the 8100 Switch series
10.10	Added support for the 8360 Switch series
10.08	Command introduced

Command Information

Platforms	Command context	Authority
8360 8100	config config-class- <i><CLASS-TYPE></i>	Administrators or local user group members with execution rights for this command.

gbp role infra

```
gbp role infra <TAG-VALUE>
no gbp role infra [<TAG-VALUE>]
```

Description

Sets the GBP infra (infrastructure) role tag value for CPU-generated packets. Prior to AOS-CX 10.09, CPU generated traffic and non-secure port traffic was tagged with a default tag of 0.

This does not apply to CPU re-forwarded packets (DHCP snooping (v4, v6), ND snooping, RA guard, IGMP, MLD, and mDNS).

The **no** form of this command resets the GBP infra tag value to its default of 2.



The same GBP infra role tag value must be used across the VXLAN network fabric.

Parameter	Description
<i><TAG-VALUE></i>	Specifies the infra tag value to use for CPU-generated packets. Range: 1 to 8191. Default: 2.

Examples

Setting the GBP infra tag value to 10:

```
switch(config)# gbp role infra 10
```

Resetting the GBP infra tag value to its default of 2:

```
switch(config)# no gbp role infra
```

Command History

Release	Modification
10.12	Added support for the 8100 Switch series
10.10	Added support for the 8360 Switch series.
10.08	Command introduced.

Command Information

Platforms	Command context	Authority
8100 8360	config	Administrators or local user group members with execution rights for this command.

gbp role-access-list

```
gbp role-access-list
  ip|ipv6 <GBP_ACL_NAME>
    <SEQUENCE-NUMBER>
    permit | deny
    <SRC-ROLE-NAME>
    any|{<DEST_IP_ADDRESS>[/(<PREFIX_LENGTH>|<SUBNET_MASK>)]}
    vrf <VRF_NAME>}
    count
    no...
<GBP_ACL_NAME>
  copy <destination-gbp-acl>
  resequence <STARTING_SEQUENCE_NUMBER> <RE_SEQUENCE_INCREMENT>
  no...
```

Description

Configures a Group-Based Policy (GBP) access list entry. This command is supported only on profile: Core-Spine.

The **no** form of this command removes the GBP access list entry.

Parameter	Description
<code>ip ipv6</code>	Specifies the GBP role access list type, ip for IPv4, or ipv6 for IPv6.
<code><GBP_ACL_NAME></code>	Specifies the name of the GBP Access Control List (ACL). The maximum number of supported characters is 64.
<code><SEQUENCE-NUMBER></code>	Specifies the GBP role Access Control Entry (ACE) sequence number. Range: 1 to 4294967295 .
<code>{permit deny}</code>	Specifies whether to permit or deny traffic matching this ACE.
<code>{any <DEST_IP_ADDRESS>[/(<PREFIX_LENGTH> <SUBNET_MASK>)]}</code>	Specifies the destination IP address. ▪ any - specifies any destination IP address. ▪ <DST-IP-ADDRESS> - specifies the destination IP host address. ◦ <PREFIX-LENGTH> - specifies the address bits to mask (CIDR subnet mask notation). Range: 1 to 32. ◦ <SUBNET-MASK> - specifies the address bits to mask (dotted decimal notation).
<code>vrf <VRF_NAME></code>	Specifies the VRF name.
<code>count</code>	Keeps the hit counts of the number of packets matching this ACE.
<code>copy <destination-gbp-acl></code>	Copies the GBP ACL to the specified destination GBP ACL.
<code>resequence</code>	Resequencing increment number for the GBP ACE.

Parameter	Description
<STARTING_SEQUENCE_NUMBER>	Specifies the starting sequence number for GBP ACE.
<RE_SEQUENCE_INCREMENT>	Specifies the resequence increment number for GBP ACE.

Examples

Creating a GBP ACL:

```
switch(config)# gbp role-access-list ip gbp-inet
switch(config-gbp-acl)# 10 permit printer 100.100.100.100 vrf red
switch(config-gbp-acl)# 20 deny finance 100.100.100.100 vrf blue count
```

Enabling VSX synchronization:

```
gbp role-access-list ip acl1
vsx-sync
!
10 permit Role1 101.101.101.0/255.255.255.0 vrf VRF_1 count
20 permit Role1 101.101.102.0/255.255.255.0 vrf VRF_1 count
30 permit Role2 101.101.101.0/255.255.255.0 vrf VRF_1 count
40 permit Role2 101.101.102.0/255.255.255.0 vrf VRF_1 count
50 permit Role3 101.101.101.0/255.255.255.0 vrf VRF_1 count
60 permit Role3 101.101.102.0/255.255.255.0 vrf VRF_1 count
```

Command History

Release	Modification
10.13	Command introduced.

Command Information

Platforms	Command context	Authority
8360	config	Administrators or local user group members with execution rights for this command.

class gbp-ip

```
[no] class gbp-ip <CLASS-NAME>
```

```
[no] [<SEQUENCE-NUMBER>]
    {match | ignore}
    {any | <SRC-ROLE-NAME> | default}
    {any | <DST-ROLE-NAME>}
    [count]
```

```
[no] [<SEQUENCE-NUMBER>]
    {match | ignore}
    {sctp | tcp | udp}
    {any | <SRC-ROLE-NAME> | default}
```

```

    [{eq | gt | lt} <PORT-NUMBER> | range <MIN-PORT> <MAX-PORT>]
    {any | <DST-ROLE-NAME>}
    [{eq | gt | lt} <PORT-NUMBER> | range <MIN-PORT> <MAX-PORT>]
    [count]

[no] [<SEQUENCE-NUMBER>]
    {match | ignore}
    {icmp}
    {any | <SRC-ROLE-NAME> | default}
    {any | <DST-ROLE-NAME>}
    [icmp-type {echo | echo-reply | <ICMP-TYPE-VALUE>}] [icmp-code <ICMP-CODE-VALUE>]
    [count]

[no] [<SEQUENCE-NUMBER>] comment <TEXT-STRING>

[no] class gbp-ip <CLASS-NAME> resequence <STARTING-SEQUENCE-NUMBER> <INCREMENT>

[no] class gbp-ip <CLASS-NAME> copy <DESTINATION-CLASS>

```

Description

Creates, deletes, or modifies an IPv4 Group-Based Policy (GBP) class to match specified protocol packets. A class consists of one or more class entries ordered and prioritized by sequence numbers. Each class can classify traffic based on IPv4 protocol header information.

The **no** keyword deletes either a class or an individual class entry.

Usage

- Entering an existing **<CLASS-NAME>** value modifies the existing class.
- Any new **<SEQUENCE-NUMBER>** value creates an additional class entry.
- Any existing **<SEQUENCE-NUMBER>** value replaces the existing class entry with the same sequence number.
- If no sequence number is specified, a new class entry will be appended with a sequence number equal to the highest policy entry currently in the list plus 10.
- Copying a class to an existing class overwrites the existing entries with new entries.
- Removing a GBP class with entries removes all its entries as well. If a GBP class, that is currently associated with a GBP policy, is attempted to be removed, then a warning message is presented to remove the association before removing the class.
- You can reorder the sequence numbers with the **class resequence** command.
- You can also create redundant class entries in a class that have the same match criteria and action. However, each redundant copy of the class entry will consume additional resources.

Parameter	Description
<CLASS-NAME>	Specifies the class name.
<SEQUENCE-NUMBER>	Specifies the class entry sequence number. Range: 1 to 4294967295.
{match ignore}	Creates a rule to ignore or match specified IPv4 packets.
<SRC-ROLE-NAME>	Specifies the source role name.

Parameter	Description
<DST-ROLE-NAME>	Specifies the destination role name.
<PORT-NUMBER>	Specifies the layer 4 port number. Range: 0 to 65535.
<MIN-PORT>	Specifies the start port number in the range. Range: 0 to 65535.
<MAX-PORT>	Specifies the end port number in the range. Range: 0 to 65535.
<ICMP-TYPE-VALUE>	Specifies a valid ICMP type number. Range: 0 to 255.
<ICMP-CODE-VALUE>	Specifies a valid ICMP code number. Range: 0 to 255.

Examples

Creating a group based policy IPv4 class with three entries:

```
switch(config)# class gbp-ip my_gbp_ip_class
switch(config-class-gbp-ip)# 1 match icmp any any
switch(config-class-gbp-ip)# 2 ignore udp default any
switch(config-class-gbp-ip)# 3 match tcp guest admin
switch(config-class-gbp-ip)# 4 count
```

Adding a comment to an existing GBP IPv4 class entry:

```
switch(config)# class gbp-ip my_gbp_ip_class
switch(config-class-gbp-ip)# 3 comment mygbpipClass
```

Removing a comment from an existing class entry:

```
switch(config)# class gbp-ip my_gbp_ip_class
switch(config-class-gbp-ip)# no 3 comment
```

Replacing an IPv4 class entry in an existing GBP IPv4 class:

```
switch(config)# class gbp-ip my_gbp_ip_class
switch(config-class-gbp-ip)# 1 match igmp any any
```

Resequencing a GBP IPv4 class:

```
switch(config)# class gbp-ip my_gbp_ip_class resequence 1 10
```

Removing a GBP IPv4 class entry:

```
switch(config)# class gbp-ip my_gbp_ip_class
switch(config-class-gbp-ip)# no 1
```

Copying a GBP class entries from the source to the destination:

```
switch(config)# class gbp-ip my_gbp_ip_class copy my_gbp_ip_class2
```

Removing a GBP IPv4 class:

```
switch(config)# no class gbp-ip my_gbp_ip_class
```

Command History

Release	Modification
10.12	Added support for the 8100 Switch series
10.10	Added support for the 8360 Switch series
10.08	Command introduced

Command Information

Platforms	Command context	Authority
8360 8100	config config-class-<CLASS-TYPE>	Administrators or local user group members with execution rights for this command.

class gbp-ipv6

```
class gbp-ipv6 <CLASS-NAME>
```

```
  [no] [<SEQUENCE-NUMBER>]
```

```
    {match | ignore}
```

```
    {any | <SRC-ROLE-NAME> | default}
```

```
    {any | <DST-ROLE-NAME>}
```

```
  [count]
```

```
  [no] [<SEQUENCE-NUMBER>]
```

```
    {match | ignore}
```

```
    {sctp | tcp | udp}
```

```
    {any | <SRC-ROLE-NAME> | default}
```

```
    [{eq | gt | lt} <PORT-NUMBER> | range <MIN-PORT> <MAX-PORT>]
```

```
    {any | <DST-ROLE-NAME>}
```

```
    [{eq | gt | lt} <PORT-NUMBER> | range <MIN-PORT> <MAX-PORT>]
```

```
  [count]
```

```
  [no] [<SEQUENCE-NUMBER>]
```

```
    {match | ignore}
```

```
    {icmpv6}
```

```
    {any | <SRC-ROLE-NAME> | default}
```

```
    {any | <DST-ROLE-NAME>}
```

```
    [icmp-type {echo | echo-reply | <ICMP-TYPE-VALUE>}] [icmp-code <ICMP-CODE-VALUE>]
```

```
  [count]
```

```
[no]class gbp-ipv6 <CLASS-NAME> resequence <STARTING-SEQUENCE-NUMBER> <INCREMENT>
```

```
[no] class gbp-ipv6 <CLASS-NAME> copy <DESTINATION-CLASS>
```

Description

Creates, deletes, or modifies an IPv6 Group-Based Policy (GBP) class to match specified protocol packets.. A class consists of one or more class entries ordered and prioritized by sequence numbers. Each class can classify traffic based on IPv6 protocol header information.

The **no** keyword deletes either a class or an individual class entry.

Usage

- Entering an existing **<CLASS-NAME>** value modifies the existing class.
- Any new **<SEQUENCE-NUMBER>** value creates an additional class entry.
- Any existing **<SEQUENCE-NUMBER>** value replaces the existing class entry with the same sequence number.
- If no sequence number is specified, a new class entry will be appended with a sequence number equal to the highest policy entry currently in the list plus 10.
- Copying a class to an existing class overwrites the existing entries with new entries.
- Removing a GBP class with entries removes all its entries as well. If a GBP class, that is currently associated with a GBP policy, is attempted to be removed, then a warning message is presented to remove the association before removing the class.
- You can reorder the sequence numbers with the **class resequence** command.
- You can also create redundant class entries in a class that have the same match criteria and action. However, each redundant copy of the class entry will consume additional resources.

Parameter	Description
<CLASS-NAME>	Specifies the class name.
<SEQUENCE-NUMBER>	Specifies the class entry sequence number. Range: 1 to 4294967295.
{match ignore}	Creates a rule to ignore or match specified IPv6 packets.
<SRC-ROLE-NAME>	Specifies the source role name.
<DST-ROLE-NAME>	Specifies the destination role name.
<PORT-NUMBER>	Specifies the layer 4 port number. Range: 0 to 65535.
<MIN-PORT>	Specifies the start port number in the range. Range: 0 to 65535.
<MAX-PORT>	Specifies the end port number in the range. Range: 0 to 65535.
<ICMP-TYPE-VALUE>	Specifies a valid ICMP type number. Range: 0 to 255.
<ICMP-CODE-VALUE>	Specifies a valid ICMP code number. Range: 0 to 255.

Examples

Creating a group based policy IPv6 class with three entries:

```
switch(config)# class gbp-ipv6 my_gbp_ipv6_class
switch(config-class-gbp-ipv6)# 10 match icmpv6 any any
```



```
switch(config-class-gbp-ipv6)# 20 ignore udp default any
```

Adding a comment to an existing GBP IPv6 class entry:

```
switch(config)# class gbp-ipv6 my_gbp_ipv6_class
switch(config-class-gbp-ipv6)# 10 match icmpv6 any any
switch(config-class-gbp-ipv6)# 20 ignore udp default any
switch(config-class-gbp-ipv6)# 20 comment myipv6Class
```

Removing a comment from an existing class entry:

```
switch(config)# class gbp-ipv6 my_gbp_ipv6_class
switch(config-class-gbp-ipv6)# no 20 comment
```

Replacing an IPv6 class entry in an existing GBP IPv6 class:

```
switch(config)# class gbp-ipv6 my_gbp_ipv6_class
switch(config-class-gbp-ipv6)# 10 match any any admin
```

Resequencing a GBP IPv6 class:

```
switch(config)# class gbp-ipv6 my_gbp_ipv6_class resequence 1 1
```

Removing a GBP IPv6 class entry:

```
switch(config)# class gbp-ipv6 my_gbp_ipv6_class
switch(config-class-gbp-ipv6)# no 1
```

Copying a GBP class entries from the source to the destination:

```
switch(config)# class gbp-ipv6 my_gbp_ipv6_class copy my_gbp_ipv6_class2
```

Removing a GBP IPv6 class:

```
switch(config)# no class gbp-ipv6 my_gbp_ipv6_class
```

Command History

Release	Modification
10.12	Added support for the 8100 Switch series
10.10	Added support for the 8360 Switch series
10.08	Command introduced

Command Information

Platforms	Command context	Authority
8360 8100	config config-class-<CLASS-TYPE>	Administrators or local user group members with execution rights for this command.

class gbp-mac

```

class gbp-mac <CLASS-NAME>
    [<SEQUENCE-NUMBER>]
    {match | ignore}
    {any | <SRC-ROLE-NAME> | default}
    {any | <DST-ROLE-NAME>}
    {any | aarp | appletalk | arp | fcoe | fcoe-init | ip | ipv6 | ipx-arp | ipx-non-
    arp | is-is | lldp | mpls-multicast | mpls-unicast | q-in-q | rbridge | trill | wake-
    on-lan | <NUMERIC-ETHERTYPE>}
    [count]

[<SEQUENCE-NUMBER>] comment <TEXT-STRING>

class gbp-mac <CLASS-NAME> resequence <STARTING-SEQUENCE-NUMBER> <INCREMENT>

class gbp-mac <CLASS-NAME> copy <DESTINATION-CLASS>

no class gbp-mac <CLASS-NAME>
    no [<SEQUENCE-NUMBER>]
    {match | ignore}
    {any | <SRC-ROLE-NAME> | default}
    {any | <DST-ROLE-NAME>}
    {any | aarp | appletalk | arp | fcoe | fcoe-init | ip | ipv6 | ipx-arp | ipx-non-
    arp | is-is | lldp | mpls-multicast | mpls-unicast | q-in-q | rbridge | trill | wake-
    on-lan | <NUMERIC-ETHERTYPE>} [
    count]
    no [<SEQUENCE-NUMBER>] comment <TEXT-STRING>

```

Description

Creates, deletes, or modifies class to match specified protocol packets. A class consists of one or more class entries ordered and prioritized by sequence numbers. Each class can classify traffic based on MAC information.

The **no** keyword deletes either a class or an individual class entry.

Usage

- Entering an existing **<CLASS-NAME>** value modifies the existing class.
- Any new **<SEQUENCE-NUMBER>** value creates an additional class entry.
- Any existing **<SEQUENCE-NUMBER>** value replaces the existing class entry with the same sequence number.
- If no sequence number is specified, a new class entry will be appended with a sequence number equal to the highest policy entry currently in the list plus 10.
- Copying a class to an existing class overwrites the existing entries with new entries.
- Removing a GBP class with entries removes all its entries as well. If a GBP class, that is currently associated with a GBP policy, is attempted to be removed, then a warning message is presented to remove the association before removing the class.
- You can reorder the sequence numbers with the **class resequence** command.

- You can also create redundant class entries in a class that have the same match criteria and action. However, each redundant copy of the class entry will consume additional resources.

Parameter	Description
<CLASS-NAME>	Specifies the class name.
<SEQUENCE-NUMBER>	Specifies the class entry sequence number. Range: 1 to 4294967295.
{match ignore}	Creates a rule to ignore or match specified packets.
<SRC-ROLE-NAME>	Specifies the source role name.
<DST-ROLE-NAME>	Specifies the destination role name.
<NUMERIC-ETHERTYPE>	Specifies the EtherType number. Range: 0x600 to 0xffff.

Examples

Creating a GBP MAC class with three entries:

```
switch(config)# class gbp-mac my_gbp_mac_class
switch(config-class-gbp-mac)# 1 match any any lldp
switch(config-class-gbp-mac)# 2 ignore default any arp
```

Adding a comment to an existing GBP MAC class entry:

```
switch(config)# class gbp-mac my_gbp_mac_class
switch(config-class-gbp-mac)# 10 comment myGbpMacClass
```

Removing a comment from an existing class entry:

```
switch(config)# class gbp-mac my_gbp_mac_class
switch(config-class-gbp-mac)# no 10 comment myGbpMacClass
```

Replacing a MAC class entry in an existing GBP MAC class:

```
switch(config)# class gbp-mac my_gbp_mac_class
switch(config-class-gbp-mac)# 10 match any any any
```

Resequencing a GBP MAC class:

```
switch(config)# class gbp-mac my_gbp_mac_class resequence 1 1
```

Removing a GBP MAC class entry:

```
switch(config)# class gbp-mac my_gbp_mac_class
switch(config-class-gbp-mac)# no 1
```

Copying a GBP class entries from the source to the destination:

```
switch(config)# class gbp-mac my_gbp_mac_class copy my_gbp_mac_class2
```

Removing a GBP MAC class:

```
switch(config)# no class gbp-mac my_gbp_mac_class
```

Command History

Release	Modification
10.12	Added support for the 8100 Switch series
10.10	Added support for the 8360 Switch series
10.08	Command introduced

Command Information

Platforms	Command context	Authority
8360 8100	config config-class-<CLASS-TYPE>	Administrators or local user group members with execution rights for this command.

port-access gbp

```
port-access gbp <POLICY-NAME>
    [<SEQUENCE-NUMBER>]
    class {gbp-ip | gbp-ipv6 | gbp-mac} <CLASS-NAME> [action {drop | reflect}]
    [<SEQUENCE-NUMBER>] comment <TEXT-STRING>
```

```
port-access gbp <POLICY-NAME> resequence <STARTING-SEQUENCE-NUMBER> <INCREMENT>
port-access gbp <POLICY-NAME> copy <DESTINATION-POLICY>
port-access gbp <POLICY-NAME> reset
```

```
[no] [<SEQUENCE-NUMBER>]
    class {gbp-ip | gbp-ipv6 | gbp-mac} <CLASS-NAME> [action {drop | reflect}]
[no] [<SEQUENCE-NUMBER>] comment <TEXT-STRING>
```

Description

Creates, deletes, or modifies a group based policy and its entries. Group based policy consists of one or more policy entries that are ordered and prioritized by sequence numbers. Each entry has a GBP-IPv4, GBP-IPv6, or a GBP-MAC class, and corresponding drop or permit policy actions associated with it. A group-based policy has an implicit permit rule to allow any traffic originating from the source role **infra**. The **no** form of the command deletes either a group based policy or an individual policy entry.

When configuring GBP-MAC class along with other classes, you must configure the GBP-MAC class entry at the end. For example, if you configure as shown below:

```
port-access gbp gbp1
    class gbp-mac class1
    class gbp-ip class2 action drop
```

Although, you would want to drop GBP-IPv4 traffic, it will be allowed because traffic will be allowed because of the MAC rule. In order to drop traffic, you must configure as show below:

```
port-access gbp gbp1
    class gbp-ip class2 action drop
    class gbp-mac class1
```

Usage

To use a GBP, you must associate the policy with a role using the **associate gbp** command.

- A group based policy that is in use cannot be removed from the configuration. To remove, the policy must be unassociated with the roles currently using the policy.
- Entering an existing *<POLICY-NAME>* value modifies the existing policy, with any new sequence number creating an additional policy entry, and any existing sequence number replacing the existing policy entry with the same sequence number.
- If no sequence number is specified, a new policy entry will be appended with a sequence number equal to the highest policy entry currently in the list plus 10.
- You can reorder the sequence numbers with the **class resequence** command.

Parameter	Description
<i><POLICY-NAME></i>	Specifies the class name.
<i><SEQUENCE-NUMBER></i>	Specifies the policy entry sequence number. Range: 1 to 4294967295 .
class-type	Specifies the type of class to associate with the policy.
<i><CLASS-NAME></i>	Specifies the class name.
action	Specifies the action for the class. The default action is to permit all traffic, if the action is not specified as drop explicitly. Other available actions are: drop Selects drop of all traffic.

Examples

Creating a policy and associating it with GBP IPv4 class to permit all traffic:

```
switch(config)# port-access gbp policy01
switch(config-pa-role)# 10 class my_gbp_ip_class
```

Creating a policy and associating it with GBP MAC class to deny all traffic:

```
switch(config)# port-access gbp policy01
switch(config-pa-role)# 10 class my_gbp_mac_class action drop
```

Command History

Release	Modification
10.12	Added support for the 8100 Switch series
10.10	Added support for the 8360 Switch series
10.08	Command introduced

Command Information

Platforms	Command context	Authority
8360 8100	config config-class-<CLASS-TYPE>	Administrators or local user group members with execution rights for this command.

port-access role associate gbp

```
port-access role <ROLE-NAME>
    associate gbp <POLICY-NAME>
no port-access role <ROLE-NAME>
    no associate gbp <POLICY-NAME>
```

Description

Associates a group based policy with a role.

The **no** form of this command dissociates the policy from the role.

Parameter	Description
<ROLE-NAME>	Specifies the role name.
<POLICY-NAME>	Specifies the group based policy name to associate with the role.

Examples

Associating a policy with a role:

```
switch(config)# port-access role EMPLOYEE
switch(config-pa-role)# associate gbp GROUPPOLICY
```

Dissociating a policy from the role:

```
switch(config)# port-access role EMPLOYEE
switch(config-pa-role)# no associate GBP
```

Command History

Release	Modification
10.12	Added support for the 8100 Switch series

Release	Modification
10.10	Added support for the 8360 Switch series
10.08	Command introduced

Command Information

Platforms	Command context	Authority
8360 8100	config config-class-<CLASS-TYPE>	Administrators or local user group members with execution rights for this command.

clear port-access gbp hitcounts

```
clear port-access gbp [<POLICY-NAME>] hitcounts {client}
```

Description

Clears the statistics of the group based policy applied on the client.

Parameter	Description
<TLV-NUMBER>	Specifies the CDP TLV number. Supported values are 1 to 6, 10, and 11.

Examples

Clearing statistics of GBP applied on the client:

```
switch(config)# clear port-access gbp policy01 hitcounts {client}
```

Command History

Release	Modification
10.12	Added support for the 8100 Switch series
10.10	Added support for the 8360 Switch series
10.08	Command introduced

Command Information

Platforms	Command context	Authority
8360 8100	config config-class-<CLASS-TYPE>	Administrators or local user group members with execution rights for this command.

show gbp role-mapping

```
show gbp role-mapping
```

Description

Shows the list of default and configured mappings between role name and role ID.

Examples

Showing details of role name to role ID mapping:

```
switch (config)# show gbp role-mapping
GBP status : Enabled
GBP_ROLE           GBP_ROLE_ID
-----
default            0
infra              2
```

Command History

Release	Modification
10.12	Added support for the 8100 Switch series
10.10	Added support for the 8360 Switch Series.
10.08	Command introduced

Command Informations

Platforms	Command context	Authority
8100 8360	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show class

```
show class {gbp-ip | gbp-ipv6 | gbp-mac} <CLASS-NAME> [commands] [configuration]
```

Description

Shows details of class configuration and its entries. Displays the active configuration providing the list of classes that have been configured and accepted by the system.

Usage

The **show class** command along with the **configuration** option displays the classes that are configured. The output of this command may not be the same as what is active due to unsupported command parameters or if the class was modified after the GBP policy was applied and might have been unsuccessful due to a lack of hardware resources. To determine if there is a discrepancy between what was configured and what is active, compare the output of the **show class** and the **show class configuration** commands. If the active class configuration and the configured class is not the same, a warning message is displayed to help troubleshoot the difference.

Parameter	Description
<CLASS-NAME>	Specifies the class name.

Examples

Showing configured GBP classes:

```
switch# show classshow class gbp-ip my_gbp_ip_class
Type      Name
Sequence  Comment
          Action
          Source Role Name
          Destination Role Name
          Additional Parameters
-----
GBP-IPv4  my_gbp_ip_class
1 match
  any
  admin
2 ignore
  default
  admin
3 match
  guest
  admin
4 match
  guest
  admin
```

Command History

Release	Modification
10.12	Added support for the 8100 Switch series
10.10	Added support for the 8360 Switch series
10.08	Command introduced

Command Information

Platforms	Command context	Authority
8360 8100	config config-class-<CLASS-TYPE>	Administrators or local user group members with execution rights for this command.

show port-access gbp

```
show port-access gbp [<POLICY-NAME>]
```

Description

Shows details of the group based policies and its current usage.

Parameter	Description
<POLICY-NAME>	Specifies the GBP policy name.

Examples

Showing details of group based policy:

```
switch (config)# show port-access gbp
```

```
Port Access GBP Details:  
=====
```

```
GBP Name   : plcy  
GBP Type   : Local  
GBP Status : Rejected
```

SEQUENCE	CLASS	TYPE	ACTION
--			
10	cs	gbp-ipv4	drop
20	cls6	gbp-ipv6	permit

Command History

Release	Modification
10.12	Added support for the 8100 Switch series
10.10	Added support for the 8360 Switch series
10.08	Command introduced

Command Information

Platforms	Command context	Authority
8360 8100	config config-class-<CLASS-TYPE>	Administrators or local user group members with execution rights for this command.

show port-access gbp hitcounts

```
show port-access gbp [<POLICY-NAME>] hitcounts {client}
```

Description

Shows statistics of the group based policy applied on the client. The output of this command helps to identify the group based policy entries that are currently matched.

Parameter	Description
<POLICY-NAME>	Specifies the GBP policy name.

Examples

Showing GBP statistics:

```
switch (config)# show port-access gbp gbp2000 hitcounts
```

```
Port Access GBP Hit-Counts Details:
```

```

=====

GBP Name : gbp2000
GBP Type : Local
GBP Status : Applied

SEQUENCE      CLASS                                TYPE      ACTION
-----
10            class2000                                gbp-ipv4  permit
15            classinfra                               gbp-ipv4  permit
30            classmacinfra                           gbp-mac   permit

Class Name : class2000
Class Type : gbp-ipv4

SEQUENCE      CLASS-ENTRY                                HIT-COUNT
-----
10            match tcp Role6 Role1 count                10
20            match udp default Role1 count              0

Class Name : classinfra
Class Type : gbp-ipv4

SEQUENCE      CLASS-ENTRY                                HIT-COUNT
-----
10            match udp infra Role1 count                 4
20            match icmp infra Role1 count               5

Class Name : classmacinfra
Class Type : gbp-mac

SEQUENCE      CLASS-ENTRY                                HIT-COUNT
-----
10            match arp infra Role1 count                 0

```

Command History

Release	Modification
10.12	Added support for the 8100 Switch series
10.10	Added support for the 8360 Switch series
10.08	Command introduced

Command Information

Platforms	Command context	Authority
	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

Several measures can be taken to enhance switch security, including setting secure mode to enhanced in the Service OS. For maximum security, perform all the configuration described in this chapter.

Configuring enhanced security

Prerequisites

If you have switch configuration that you want to retain, create a backup. This procedure erases all configuration, including the current running configuration, the startup configuration, and all historical configuration checkpoints.

Procedure

1. Set enhanced security mode:
 - a. Reboot the switch into the Service OS with command `boot system serviceos`. If on an 8400 Switch with both Management Modules:
 - i. Issue the **boot** command only on the active Management Module. This command ensures that both Management Modules are booted into the Service OS.
 - ii. Perform steps b to e on both modules starting with the active module.
 - b. Log in to the Service OS as **admin**.
 - c. Enter command **secure-mode enhanced**.
 - d. When prompted about the mode change, respond with **y** for "yes."
 - e. Wait for the reboot and zeroization to complete. The switch firmware boots automatically.
2. Ensure adequate password requirements:
 - a. Before adding users, enable and configure password complexity as described in [password complexity](#). To maintain enhanced security, configure the **password complexity** subcommand settings no smaller than their defaults.
 - b. Configure passwords for all users, including **admin**. To make your password complexity settings applicable to the default admin user, change the admin password after enabling password complexity. The new admin password must respect your password complexity settings.
3. Ensure proper login management as follows:
 - a. Configure local user session management as described in [CLI user session management commands](#) using **cli-session** and its subcommands **max-per-user**, **timeout**, and **tracking-range** to achieve the wanted configuration. To maintain enhanced security, configure **cli-session** subcommand settings no smaller than their defaults.
 - b. Restrict remote SSH connections to only use certified crypto algorithms using **ssh certified-algorithms-only**.
 - c. Configure pre- and post-login banners using respectively, **banner motd**, and **banner exec**.

4. Ensure that the switch date and time is accurately set using `clock datetime <DATE> <TIME>`.
5. When logging to a remote syslog server is required, ensure that the connection to the server is cryptographically secure. See [Configuring remote logging using SSH reverse tunnel](#).

To ensure that enhanced security is maintained, also respect these requirements:

- Do not configure remote logging with a remote server directly without setting up an SSH tunnel.
- Do not configure passwords and secret keys using the plaintext option.



When in enhanced security mode, the switch (Product OS) `start-shell` command is disabled for security purpose. If you attempt to use this command while in enhanced security mode, it is rejected and the following error message is displayed:

```
The start-shell command is not available in enhanced secure mode.
```



When in enhanced security mode, the following Service OS commands are disabled for security purposes: **config-clear**, **password**, **sh**, and **update**. If you attempt to use any of these Service OS commands while in enhanced security mode, the command is rejected and an error message is displayed.

Configuring remote logging using SSH reverse tunnel

Logging to a remote syslog server can be made cryptographically secure by using SSH reverse tunnel. The `syslog` daemon on the switch forwards log messages to the SSH tunnel, and the SSH tunnel endpoint on the remote server host forwards messages to the listening `syslog` server.



This procedure includes sample configuration commands for a user-supplied syslog server based on Ubuntu 14.04.5 LTS with `rsyslog`. It is up to the user to check their server documentation and adjust the sample commands as required. Optionally see your server documentation for information on how to use the `systemd` and `autossh` services to automatically restore the SSH tunnel after system reboot.

Prerequisites

The user-supplied remote syslog server must be on a network that can reach the switch management interface.

Procedure

1. Configure SSH server on the switch.
 - a. Enter these commands (although this example uses the `mgmt` VRF, other VRFs can be used):

```
switch(config)# interface mgmt
switch(config-if-mgmt)# no shutdown
switch(config-if-mgmt)# ip address <switch_mgmt_IP>
switch(config-if-mgmt)# exit
switch(config)# ssh server vrf mgmt
```

- b. If public key authentication is desired for remote SSH users, configure it on the switch:

```
switch(config)# user admin authorized-key <PUBKEY>
```

2. Configure logging on the switch to forward to localhost:

```
switch(config)# logging localhost tcp <switch_tcp_port> vrf mgmtinclude-auditable-events
```

3. Configure the **rsyslog** server on the remote host:
 - a. Make **rsyslog** accept TCP connections and specify the log file, by adding the following to **/etc/rsyslog.conf**:

```
$ModLoad imtcp
$InputTCPServerRun <server_tcp_port>
$template RemoteLogs, "/var/log/remote.log"
*. * ?RemoteLogs
```

- b. To activate the added configuration, restart the **rsyslog** server

```
root@Ubuntu4479:~#sudo service rsyslog restart
```

4. Establish an SSH reverse tunnel from the remote host to the switch:

```
root@Ubuntu4479:~#ssh -nNTx -R
<switch_tcp_port>:127.0.0.1:<server_tcp_port>
admin@<switch_mgmt_IP>
```

CLI user session management commands

cli-session

```
cli-session
no cli-session
```

Description

Enters the CLI session context (shown in the switch prompt as **config-cli-session**) for the purpose of configuring CLI user session management. Session management enhances security by enforcing specific CLI user session requirements. The following information is provided at time of successful login:

- When applicable, the number of failed login attempts since the most recent successful login.
- The date, time, and location (console or IP address or hostname) of the most recent previous successful login.
- The count of successful logins within the past (configurable) time period.

For example:

```
switch login: admin
Password:
```

```
There were 3 failed login attempts since the last successful login
Last login: 2019-04-20 08:51:33 from the console
User "admin" has logged in 73 times in the past 30 days
```

The no form of this command disables concurrent CLI user session restrictions and reverts **timeout** and **tracking-range** to their default values.



To ensure that enhanced security is maintained, it is recommended that you keep CLI user session management fully enabled by setting **max-per-user** to a nondefault value.



The **cli-session** command applies only to SSH/console login connection types. It does not apply to other connection types such as REST.

Subcommands

These subcommands are available within the CLI session context.

[no] **max-per-user** <SESSIONS>

Specifies the maximum number of concurrent CLI sessions per user. The no form of this subcommand disables concurrent CLI user session restrictions. Default: Disabled (no value). Range: 1 to 5.



When the same user name is configured for both local and remote authentication, both users, regardless of privilege level, are considered to be the same user for the purpose of counting concurrent CLI sessions. For example, with **max-per-user** set to 1 and user **admin1** configured for local and remote authentication, only the local user **admin1** or the remote user **admin1** can be logged in at any given moment. Both **admin1** users cannot be logged in simultaneously unless **max-per-user** is increased to at least 2.

[no] **timeout** <MINUTES>

Specifies the number of minutes a CLI session can be idle before the session is automatically terminated and the user is logged out. A value of 0 minutes disables the session timeout. The no form of this subcommand sets the timeout value to the default. Default 30: Range 0 to 4320.



This subcommand is the recommended replacement for the **session-timeout** command.

[no] **tracking-range** <DAYS>

Specifies the maximum number of days to track CLI user session logins. The no form of this subcommand resets the value to its default. Default 30: Range 1 to 30.

exit

Exits the CLI session context.

end

Exits the CLI session context and then the config context.

Examples

Configuring CLI user session settings for a maximum of one concurrent session, a 20-minute timeout, and tracking for a maximum of 25 days.

```
switch(config)# cli-session
switch(config-cli-session)# max-per-user 1
switch(config-cli-session)# timeout 20
switch(config-cli-session)# tracking-range 25
switch# exit
```

After successful earlier logins, logging in from the console without any intervening unsuccessful logins.

```
switch login: admin1
Password:

Last login: 2019-04-15 14:10:21 from the console
User 'admin1' has logged in 65 times in the past 25 days
```

Attempting to log in as `admin1` when already logged in as **admin1** from elsewhere.

```
switch login: admin1
Password:
Too many logins for 'admin1'
```

After successful earlier logins, attempting to log in twice with an invalid password, followed by a successful login.

```
switch login: admin1
Password:

Login incorrect
switch login: admin1
Password:

Login incorrect
switch login: admin1
Password:

There were 2 failed login attempts since the last successful login
Last login: 2019-04-15 17:22:45 from 192.168.1.1
User 'admin1' has logged in 72 times in the past 25 days
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	<code>config</code>	Administrators or local user group members with execution rights for this command.

The **auditors** group enables administrators to create users that can perform auditing tasks without allowing those users the authority to view or change the switch configuration.

As is the case for other users, auditors can access the switch using the Web UI, REST API, or the CLI.

Auditing tasks (CLI)

When you log on to the switch CLI as a user with auditor rights, you have access to the auditor command context only.

```
auditor>
```

The tasks that can be performed by auditors are as follows. The commands listed are the only commands auditors can execute other than session commands like `print`, `list`, and `exit`. However, auditors can use all command options except as noted. See the command description for each command for complete information about the command.

Task	Command name	Example
Show event log contents	<code>show events</code>	<code>show events -a -r</code>
Show local accounting log contents	<code>show accounting log</code>	<code>show accounting log last 10</code>
Copy command output to a remote server or to a local USB drive.	<code>copy command-output</code>	<code>copy command-output "show events -a -r" tftp://10.100.0.12/file</code>

When using the `copy command-output` command, users with auditor rights can specify the following commands only:

```
show accounting log
show events
```

Auditing tasks (Web UI)

Auditors have access to the Log page only. When you log on to the switch Web UI as a user with auditor rights, the Log page is displayed.

From the Log page, you can view and export event log entries.

The Web UI does not provide access to the accounting logs.

REST requests and accounting logs

All REST requests—including GET requests—are logged to the accounting (audit) log.

The URI of the REST API resource for accounting logs is the following:

`/rest/v10.04/logs/audit`

In an accounting log entry for a REST request:

- `service=https-server` indicates that the log entry is a result of a REST API request or a Web UI action.
- The string value of `data` identifies the REST API request that was executed.

For more information about accounting log entries, see the description of the `show accounting log` CLI command.

Accessing HPE Aruba Networking Support

HPE Aruba Networking Support Services	https://www.arubanetworks.com/support-services/
AOS-CX Switch Software Documentation Portal	https://www.arubanetworks.com/techdocs/AOS-CX/help_portal/Content/home.htm
HPE Aruba Networking Support Portal	https://networkingsupport.hpe.com/home
North America telephone	1-800-943-4526 (US & Canada Toll-Free Number) +1-408-754-1200 (Primary - Toll Number) +1-650-385-6582 (Backup - Toll Number - Use only when all other numbers are not working)
International telephone	https://www.arubanetworks.com/support-services/contact-support/

Be sure to collect the following information before contacting Support:

- Technical support registration number (if applicable)
- Product name, model or version, and serial number
- Operating system name and version
- Firmware version
- Error messages
- Product-specific reports and logs
- Add-on products or components
- Third-party products or components

Other useful sites

Other websites that can be used to find information:

Airheads social forums and Knowledge Base	https://community.arubanetworks.com/
HPE Aruba Networking Hardware Documentation and Translations Portal	https://www.arubanetworks.com/techdocs/hardware/DocumentationPortal/Content/home.htm

HPE Aruba Networking software	https://networkingsupport.hpe.com/downloads
Software licensing and Feature Packs	https://lms.arubanetworks.com/
End-of-Life information	https://www.arubanetworks.com/support-services/end-of-life/
HPE Aruba Networking Developer Hub	https://developer.arubanetworks.com/

Accessing Updates

You can access updates from the HPE Aruba Networking Support Portal at <https://networkingsupport.hpe.com>.

Some software products provide a mechanism for accessing software updates through the product interface. Review your product documentation to identify the recommended software update method.

To subscribe to eNewsletters and alerts:

<https://networkingsupport.hpe.com/notifications/subscriptions> (requires an active HPE Aruba Networking Support Portal account to manage subscriptions). Security notices are viewable without an HPE Aruba Networking Support Portal account.

Warranty Information

To view warranty information for your product, go to <https://www.arubanetworks.com/support-services/product-warranties/>.

Regulatory Information

To view the regulatory information for your product, view the *Safety and Compliance Information for Server, Storage, Power, Networking, and Rack Products*, available at <https://www.hpe.com/support/Safety-Compliance-EnterpriseProducts>

Additional regulatory information

HPE Aruba Networking is committed to providing our customers with information about the chemical substances in our products as needed to comply with legal requirements, environmental data (company programs, product recycling, energy efficiency), and safety information and compliance data, (RoHS and WEEE). For more information, see <https://www.arubanetworks.com/company/about-us/environmental-citizenship/>.

Documentation Feedback

HPE Aruba Networking is committed to providing documentation that meets your needs. To help us improve the documentation, send any errors, suggestions, or comments to Documentation Feedback (docsfeedback-switching@hpe.com). When submitting your feedback, include the document title, part number, edition, and publication date located on the front cover of the document. For online help

content, include the product name, product version, help edition, and publication date located on the legal notices page.