R Commands

This chapter describes the Cisco NX-OS security commands that begin with R.

radius abort

To discard a RADIUS Cisco Fabric Services distribution session in progress, use the **radius abort** command.

radius abort

Syntax Description

This command has no other arguments or keywords.

Defaults

None

Command Modes

Global configuration

SupportedUserRoles

network-admin
vdc-admin

Command History

Release	Modification
4.1(2)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to discard a RADIUS Cisco Fabric Services distribution session in progress:

```
switch# configure terminal
switch(config)# radius abort
```

Related Commands

Command	Description
show radius	Displays the RADIUS Cisco Fabric Services distribution status and other details.

radius commit

To apply the pending configuration pertaining to the RADIUS Cisco Fabric Services (CFS) distribution session in progress in the fabric, use the **radius commit** command.

radius commit

Syntax Description

This command has no other arguments or keywords.

Defaults

None

Command Modes

Global configuration

SupportedUserRoles

network-admin
vdc-admin

Command History

Release	Modification
4.1(2)	This command was introduced.

Usage Guidelines

Before committing the RADIUS configuration to the fabric, all switches in the fabric must have distribution enabled using the **radius distribute** command.

CFS does not distribute the RADIUS server group configurations, periodic RADIUS server testing configurations, or server and global keys. The keys are unique to the Cisco NX-OS device and are not shared with other Cisco NX-OS devices.

This command does not require a license.

Examples

This example shows how to initiate distribution of a RADIUS configuration to the switches in the fabric:

```
switch# configure terminal
switch(config)# radius commit
```

Related Commands

Command	Description
radius distribute	Enables Cisco Fabric Services distribution for RADIUS.
show radius	Displays the RADIUS Cisco Fabric Services distribution status and other details.

radius distribute

To enable Cisco Fabric Services distribution for RADIUS, use the **radius distribute** command. To disable this feature, use the **no** form of the command.

radius distribute

no radius distribute

Syntax Description

This command has no other arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration

SupportedUserRoles

network-admin
vdc-admin

Command History

Release	Modification
4.1(2)	This command was introduced.

Usage Guidelines

CFS does not distribute the RADIUS server group configurations, periodic RADIUS server testing configurations, or server and global keys. The keys are unique to the Cisco NX-OS device and are not shared with other Cisco NX-OS devices.

This command does not require a license.

Examples

This example shows how to enable RADIUS fabric distribution:

```
switch# configure terminal
switch(config)# radius distribute
```

This example shows how to disable RADIUS fabric distribution:

```
switch# configure terminal
switch(config)# no radius distribute
```

Related Commands

Command	Description
show radius distribution status	Displays the RADIUS Cisco Fabric Services distribution status.

radius-server deadtime

To configure the dead-time interval for all RADIUS servers on a Cisco NX-OS device, use the **radius-server deadtime** command. To revert to the default, use the **no** form of this command.

radius-server deadtime *minutes*

no radius-server deadtime *minutes*

Syntax Description

minutes	Number of minutes for the dead-time interval. The range is from 1 to 1440 minutes.

Defaults

0 minutes

Command Modes

Global configuration

SupportedUserRoles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

The dead-time interval is the number of minutes before the Cisco NX-OS device checks a RADIUS server that was previously unresponsive.

Note The default idle timer value is 0 minutes. When the idle time interval is 0 minutes, periodic RADIUS server monitoring is not performed.

The command does not require a license.

Examples

This example shows how to configure the global dead-time interval for all RADIUS servers to perform periodic monitoring:

```
switch# configure terminal
switch(config)# radius-server deadtime 5
```

This example shows how to revert to the default for the global dead-time interval for all RADIUS servers and disable periodic server monitoring:

```
switch# configure terminal
switch(config)# no radius-server deadtime 5
```

Related Commands

Command	Description
show radius-server	Displays RADIUS server information.

radius-server directed-request

To allow users to send authentication requests to a specific RADIUS server when logging in, use the **radius-server directed request** command. To revert to the default, use the **no** form of this command.

radius-server directed-request

no radius-server directed-request

Syntax Description

This command has no arguments or keywords.

Defaults

Sends the authentication request to the configured RADIUS server group

Command Modes

Global configuration

SupportedUserRoles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

You can specify the *username@vrfname:hostname* during login, where *vrfname* is the virtual routing and forwarding (VRF) instance to use and *hostname* is the name of a configured RADIUS server. The username is sent to the RADIUS server for authentication.

This command does not require a license.

Examples

This example shows how to allow users to send authentication requests to a specific RADIUS serve when logging in:

```
switch# configure terminal
switch(config)# radius-server directed-request
```

This example shows how to disallow users to send authentication requests to a specific RADIUS server when logging in:

```
switch# configure terminal
switch(config)# no radius-server directed-request
```

Related Commands

Command	Description
show radius-server directed-request	Displays the directed request RADIUS server configuration.

radius-server host

To configure RADIUS server parameters, use the **radius-server host** command. To revert to the default, use the **no** form of this command.

radius-server host {*hostname* | *ipv4-address* | *ipv6-address*}
[**key** [**0** | **7**] *shared-secret* [**pac**]] [**accounting**]
[**acct-port** *port-number*] [**auth-port** *port-number*] [**authentication**] [**retransmit** *count*]
[**test** {**idle-time** *time* | **password** *password* | **username** *name*}]
[**timeout** *seconds* [**retransmit** *count*]]

no radius-server host {*hostname* | *ipv4-address* | *ipv6-address*}
[**key** [**0** | **7**] *shared-secret* [**pac**]] [**accounting**]
[**acct-port** *port-number*] [**auth-port** *port-number*] [**authentication**] [**retransmit** *count*]
[**test** {**idle-time** *time* | **password** *password* | **username** *name*}]
[**timeout** *seconds* [**retransmit** *count*]]

Syntax Description

hostname	RADIUS server Domain Name Server (DNS) name. The name is alphanumeric, case sensitive, and has a maximum of 256 characters.
ipv4-address	RADIUS server IPv4 address in the *A.B.C.D* format.
ipv6-address	RADIUS server IPv6 address in the *X:X:X::X* format.
key	(Optional) Configures the RADIUS server preshared secret key.
0	(Optional) Configures a preshared key specified in clear text to authenticate communication between the RADIUS client and server. This is the default.
7	(Optional) Configures a preshared key specified in encrypted text (indicated by 7) to authenticate communication between the RADIUS client and server.
shared-secret	Preshared key to authenticate communication between the RADIUS client and server. The preshared key can include any printable ASCII characters (white spaces are not allowed), is case sensitive, and has a maximum of 63 characters.
pac	(Optional) Enables the generation of Protected Access Credentials (PAC) on the RADIUS Cisco Access Control Server (ACS) for use with Cisco TrustSec.
accounting	(Optional) Configures accounting.
acct-port *port-number*	(Optional) Configures the RADIUS server port for accounting. The range is from 0 to 65535.
auth-port *port-number*	(Optional) Configures the RADIUS server port for authentication. The range is from 0 to 65535.
authentication	(Optional) Configures authentication.
retransmit *count*	(Optional) Configures the number of times that the device tries to connect to a RADIUS server(s) before reverting to local authentication. The range is from 1 to 5 times and the default is 1 time.
test	(Optional) Configures parameters to send test packets to the RADIUS server.
idle-time *time*	Specifies the time interval (in minutes) for monitoring the server. The range is from 1 to 1440 minutes.
password *password*	Specifies a user password in the test packets. The password is alphanumeric, case sensitive, and has a maximum of 32 characters.

username *name*	Specifies a username in the test packets. The name is alphanumeric, not case sensitive, and has a maximum of 32 characters.
timeout *seconds*	Specifies the timeout (in seconds) between retransmissions to the RADIUS server. The default is 5 seconds and the range is from 1 to 60 seconds.

Defaults

Accounting port: 1813

Authentication port: 1812

Accounting: enabled

Authentication: enabled

Retransmission count: 1

Idle-time: none

Server monitoring: disabled

Timeout: 5 seconds

Test username: test

Test password: test

Command Modes

Global configuration

SupportedUserRoles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

When the idle time interval is 0 minutes, periodic RADIUS server monitoring is not performed.

This command does not require a license.

Examples

This example shows how to configure RADIUS server authentication and accounting parameters:

```
switch# configure terminal
switch(config)# radius-server host 10.10.2.3 key HostKey
switch(config)# radius-server host 10.10.2.3 auth-port 2003
switch(config)# radius-server host 10.10.2.3 acct-port 2004
switch(config)# radius-server host 10.10.2.3 accounting
switch(config)# radius-server host radius2 key 0 abcd
switch(config)# radius-server host radius3 key 7 1234
switch(config)# radius-server host 10.10.2.3 test idle-time 10
switch(config)# radius-server host 10.10.2.3 test username tester
switch(config)# radius-server host 10.10.2.3 test password 2B9ka5
```

Related Commands

Command	Description
show radius-server	Displays RADIUS server information.

radius-server key

To configure a RADIUS shared secret key, use the **radius-server key** command. To remove a configured shared secret, use the **no** form of this command.

radius-server key [**0** | **6** | **7**] *shared-secret*

no radius-server key [**0** | **6** | **7**] *shared-secret*

Syntax Description

0	(Optional) Configures a preshared key specified in clear text to authenticate communication between the RADIUS client and server.
6	(Optional) Configures a preshared key specified in type6 encrypted text to authenticate communication between the RADIUS client and server.
7	(Optional) Configures a preshared key specified in encrypted text to authenticate communication between the RADIUS client and server.
shared-secret	Preshared key used to authenticate communication between the RADIUS client and server. The preshared key can include any printable ASCII characters (white spaces are not allowed), is case sensitive, and has a maximum of 63 characters.

Defaults

Clear text

Command Modes

Global configuration

SupportedUserRoles

network-admin
vdc-admin

Command History

Release	Modification
5.2(1)	Added the
4.0(1)	This command was introduced.

Usage Guidelines

You must configure the RADIUS preshared key to authenticate the switch to the RADIUS server. The length of the key is restricted to 63 characters and can include any printable ASCII characters (white spaces are not allowed). You can configure a global key to be used for all RADIUS server configurations on the switch. You can override this global key assignment by using the **key** keyword in the **radius-server host** command.

This command does not require a license.

Examples

This example shows how to provide various scenarios to configure RADIUS authentication:

```
switch# configure terminal
switch(config)# radius-server key AnyWord
switch(config)# radius-server key 0 AnyWord
switch(config)# radius-server key 7 public pac
```

Related Commands

Command	Description
show radius-server	Displays RADIUS server information.

radius-server retransmit

To specify the number of times that the device should try a request with a RADIUS server, use the **radius-server retransmit** command. To revert to the default, use the **no** form of this command.

radius-server retransmit *count*

no radius-server retransmit *count*

Syntax Description

count	Number of times that the device tries to connect to a RADIUS server(s) before reverting to local authentication. The range is from 1 to 5 times.

Defaults

1 retransmission

Command Modes

Global configuration

SupportedUserRoles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to configure the number of retransmissions to RADIUS servers:

```
switch# configure terminal
switch(config)# radius-server retransmit 3
```

This example shows how to revert to the default number of retransmissions to RADIUS servers:

```
switch# configure terminal
switch(config)# no radius-server retransmit 3
```

Related Commands

Command	Description
show radius-server	Displays RADIUS server information.

radius-server test

To monitor the availability of all RADIUS servers without having to configure the test parameters for each server individually, use the **radius-server test** command. To disable this configuration, use the **no** form of this command.

radius-server test {**idle-time** *time* | **password** *password* | **username** *name*}

no radius-server test {**idle-time** *time* | **password** *password* | **username** *name*}

Syntax Description

test	Configures parameters to send test packets to the RADIUS server.
idle-time *time*	Specifies the time interval (in minutes) for monitoring the server. The range is from 1 to 1440 minutes. **Note** When the idle time interval is 0 minutes, periodic RADIUS server monitoring is not performed.
password *password*	Specifies a user password in the test packets. The password is alphanumeric, case sensitive, and has a maximum of 32 characters.
username *name*	Specifies a username in the test packets. The name is alphanumeric, not case sensitive, and has a maximum of 32 characters. **Note** To protect network security, we recommend that you use a username that is not the same as an existing username in the RADIUS database.

Defaults

Server monitoring: Disabled
Idle time: 0 minutes
Test username: test
Test password: test

Command Modes

Global configuration

SupportedUserRoles

network-admin
vdc-admin

Command History

Release	Modification
5.0(2)	This command was introduced.

Usage Guidelines

To use this command, you must enable RADIUS authentication.

Any servers for which test parameters are not configured are monitored using the global level parameters.

Test parameters that are configured for individual servers take precedence over global test parameters.

When the idle time interval is 0 minutes, periodic RADIUS server monitoring is not performed.

This command does not require a license.

Examples

This example shows how to configure the parameters for global RADIUS server monitoring:

```
switch# configure terminal
switch(config)# radius-server test username user1 password Ur2Gd2BH idle-time 3
```

Related Commands

Command	Description
show radius-server	Displays RADIUS server information.

radius-server timeout

To specify the time between retransmissions to the RADIUS servers, use the **radius-server timeout** command. To revert to the default, use the **no** form of this command.

radius-server timeout *seconds*

no radius-server timeout *seconds*

Syntax Description

seconds	Number of seconds between retransmissions to the RADIUS server. The range is from 1 to 60 seconds.

Defaults

1 second

Command Modes

Global configuration

SupportedUserRoles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to configure the timeout interval:

```
switch# configure terminal
switch(config)# radius-server timeout 30
```

This example shows how to revert to the default interval:

```
switch# configure terminal
switch(config)# no radius-server timeout 30
```

Related Commands

Command	Description
show radius-server	Displays RADIUS server information.

range

To specify a range of ports as a group member in an IP port object group, use the **range** command. To remove a port range group member from port object group, use the **no** form of this command.

[*sequence-number*] **range** *starting-port-number ending-port-number*

no {*sequence-number* | **range** *starting-port-number ending-port-number*}

Syntax Description

sequence-number	(Optional) Sequence number for this group member. Sequence numbers maintain the order of group members within an object group. Valid sequence numbers are from 1 to 4294967295. If you do not specify a sequence number, the device assigns a number that is 10 greater than the largest sequence number in the current object group.
starting-port-number	Lowest port number that this group member matches. Valid values are from 0 to 65535.
ending-port-number	Highest port number that this group member matches. Valid values are from 0 to 65535.

Defaults

None

Command Modes

IP port object group configuration

SupportedUserRoles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

IP port object groups are not directional. Whether a **range** command matches a source or destination port or whether it applies to inbound or outbound traffic depends upon how you use the object group in an ACL.

This command does not require a license.

Examples

This example shows how to configure an IP port object group named port-group-05 with a group member that matches traffic sent to or from port 137 through port 139:

```
switch# configure terminal
switch(config)# object-group ip port port-group-05
switch(config-port-ogroup)# range 137 139
```

Related Commands

Command	Description
eq	Specifies an equal-to group member in an IP port object group.
gt	Specifies a greater-than group member in an IP port object group.
lt	Specifies a less-than group member in an IP port object group.
neq	Specifies a not-equal-to group member in an IP port object group.
object-group ip port	Configures an IP port object group.
show object-group	Displays object groups.

rate-limit cpu direction

To configure rate limits globally on the device for packets that reach the supervisor module, use the **rate-limit cpu direction** command. To remove the rate limit configuration, use the **no** form of this command.

rate-limit cpu direction {**input** | **output** | **both**} **pps** *packets* **action log**

no rate-limit cpu direction {**input** | **output** | **both**} **pps** *packets* **action log**

Syntax Description

input	Specifies the maximum incoming packet rate.
output	Specifies the maximum outgoing packet rate.
both	Specifies the maximum incoming and outgoing packet rate.
pps	Specifies packets per second.
packets	Packets that reach the supervisor module. The range is from 1 to 100000.
action	Specifies the action to be taken when the rate of incoming or outgoing packets exceeds the configured rate limit.
log	Logs a system message when the rate of incoming or outgoing packets exceeds the configured rate limit.

Defaults

10000 packets per second

Command Modes

Global configuration

SupportedUserRoles

network-admin
network-operator

Command History

Release	Modification
5.1(1)	This command was introduced.

Usage Guidelines

If the rate of incoming or outgoing packets exceeds the configured rate limit, the device logs a system message but does not drop any packets.

F1 Series modules support up to five rate limiters shared among all control traffic sent to the Supervisor module.

This command does not require a license.

Examples

This example shows how to configure rate limits globally on the device for packets that reach the supervisor module:

```
switch# configure terminal
```

```
switch(config)# rate-limit cpu direction both pps 10000 action log
switch(config)#
```

This example shows how to remove the global rate limit configuration:

```
witch# configure terminal
switch(config)# no rate-limit cpu direction both pps 10000 action log
switch(config)#
```

Related Commands

Command	Description
show system internal pktmgr internal control sw-rate-limit	Displays the inband and outband global rate limit configuration for packets that reach the supervisor module.

remark

To enter a comment into an IPv4, IPv6, or MAC access control list (ACL), use the **remark** command. To remove a **remark** command, use the **no** form of this command.

[*sequence-number*] **remark** *remark*

no {*sequence-number* | **remark** *remark*}

Syntax Description

sequence-number	(Optional) Sequence number of the **remark** command, which causes the device to insert the command in that numbered position in the access list. Sequence numbers maintain the order of rules within an ACL. A sequence number can be any integer between 1 and 4294967295. By default, the first rule in an ACL has a sequence number of 10. If you do not specify a sequence number, the device adds the rule to the end of the ACL and assigns to it a sequence number that is 10 greater than the sequence number of the preceding rule. Use the **resequence** command to reassign sequence numbers to remarks and rules.
remark	Text of the remark. This argument can be up to 100 alphanumeric, case-sensitive characters.

Defaults

No ACL contains a remark by default.

Command Modes

IP access-list configuration
IPv6 access-list configuration
MAC access-list configuration

SupportedUserRoles

network-admin
vdc-admin

Command History

Release	Modification
4.1(2)	Support for the IPv6 access-list configuration mode was added.
4.0(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

The *remark* argument can be up to 100 characters. If you enter more than 100 characters for the *remark* argument, the device accepts the first 100 characters and drops any additional characters.

Examples

This example shows how to create a remark in an IPv4 ACL and display the results:

```
switch# configure terminal
switch(config)# ip access-list acl-ipv4-01
switch(config-acl)# 100 remark this ACL denies the marketing department access to the lab
switch(config-acl)# show access-list acl-ipv4-01

IP access list acl-ipv4-01
        100 remark this ACL denies the marketing department access to the lab
ciscobox(config-acl)#
```

Related Commands

Command	Description
ip access-list	Configures an IPv4 ACL.
mac access-list	Configures a MAC ACL.
show access-list	Displays all ACLs or one ACL.
statistics per-entry	Enables collection of statistics for each entry in an ACL.

replay-protection

To enable the data-path replay protection feature for Cisco TrustSec authentication on an interface, use the **replay-protection** command. To disable the data-path replay protection feature, use the **no** form of this command.

replay-protection

no replay-protection

Syntax Description

This command has no arguments or keywords.

Defaults

Enabled

Command Modes

Cisco TrustSec 802.1X configuration

SupportedUserRoles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command is not supported for F1 Series modules.

To use this command, you must enable the Cisco TrustSec feature using the **feature cts** command.

After using this command, you must enable and disable the interface using the **shutdown/no shutdown** command sequence for the configuration to take effect.

This command requires the Advanced Services license.

Examples

This example shows how to enable data-path protect for Cisco TrustSec authentication on an interface:

```
switch# configure terminal
switch(config)# interface ethernet 2/3
switch(config-if)# cts dot1x
switch(config-if-cts-dot1x)# replay-protection
switch(config-if-cts-dot1x)# exit
switch(config-if)# shutdown
switch(config-if)# no shutdown
```

This example shows how to disable data-path protect for Cisco TrustSec authentication on an interface:

```
switch# configure terminal
switch(config)# interface ethernet 2/3
switch(config-if)# cts dot1x
switch(config-if-cts-dot1x)# no replay-protection
switch(config-if-cts-dot1x)# exit
switch(config-if)# shutdown
switch(config-if)# no shutdown
```

Related Commands

Command	Description
cts dot1x	Enters Cisco TrustSec 802.1X configuration mode for an interface.
feature cts	Enables the Cisco TrustSec feature.
show cts interface	Displays the Cisco TrustSec configuration for interfaces.

resequence

To reassign sequence numbers to all rules in an access control list (ACL) or a time range, use the **resequence** command.

resequence *access-list-type* **access-list** *access-list-name starting-sequence-number increment*

resequence time-range *time-range-name starting-sequence-number increment*

Syntax Description

access-list-type	Type of the ACL. Valid values for this argument are the following keywords: • **arp** • **ip** • **ipv6** • **mac**
access-list *access-list-name*	Specifies the name of the ACL, which can be up to 64 alphanumeric, case-sensitive characters.
time-range *time-range-name*	Specifies the name of the time range, which can be up to 64 alphanumeric, case-sensitive characters.
starting-sequence-number	Sequence number for the first rule in the ACL or time range.
increment	Number that the device adds to each subsequent sequence number.

Defaults

None

Command Modes

Global configuration

SupportedUserRoles

network-admin
vdc-admin

Command History

Release	Modification
4.1(2)	Support for IPv6 ACLs was added.
4.0(1)	This command was introduced.

Usage Guidelines

The **resequence** command allows you to reassign sequence numbers to the rules of an ACL or time range. The new sequence number for the first rule is determined by the *starting-sequence-number* argument. Each additional rule receives a new sequence number determined by the *increment* argument. If the highest sequence number would exceed the maximum possible sequence number, then no sequencing occurs and the following message appears:

```
ERROR: Exceeded maximum sequence number.
```

The maximum sequence number is 4294967295.

This command does not require a license.

Examples

This example shows how to resequence an IPv4 ACL named ip-acl-01 with a starting sequence number of 100 and an increment of 10, using the **show ip access-lists** command to verify sequence numbering before and after the use of the **resequence** command:

```
switch# configure terminal
switch(config)# show ip access-lists ip-acl-01

IP access list ip-acl-01
        7 permit tcp addrgroup lab-machines any
        10 permit udp addrgroup lab-machines any
        13 permit icmp addrgroup lab-machines any
        17 deny igmp any any
switch(config)# resequence ip access-list ip-acl-01 100 10
switch(config)# show ip access-lists ip-acl-01

IP access list ip-acl-01
        100 permit tcp addrgroup lab-machines any
        110 permit udp addrgroup lab-machines any
        120 permit icmp addrgroup lab-machines any
        130 deny igmp any any
```

Related Commands

Command	Description
arp access-list	Configures an ARP ACL.
ip access-list	Configures an IPv4 ACL.
mac access-list	Configures a MAC ACL.
show access-lists	Displays all ACLs or a specific ACL.

revocation-check

To configure trustpoint revocation check methods, use the **revocation-check** command. To discard the revocation check configuration, use the **no** form of this command.

revocation-check {**crl** [**none**] | **none**}

no revocation-check {**crl** [**none**] | **none**}

Syntax Description

crl	Specifies the locally stored certificate revocation list (CRL) as the place to check for revoked certificates.
none	(Optional) Specifies that no checking is performed for revoked certificates.

Defaults

By default, the revocation checking method for a trustpoint is CRL.

Command Modes

Trustpoint configuration

Command History

Release	Modification
4.1(2)	This command was introduced.

Usage Guidelines

A revocation check can perform one or more of the methods which you specify as an ordered list. During peer certificate verification, each method is tried in the specified order until one method succeeds by providing the revocation status. When you specify **none** as the method, it means that there is no need to check the revocation status, and the peer certificate is not revoked. If **none** is the first method that you specify in the method list, you cannot specify subsequent methods because checking is not required.

This command does not require a license.

Examples

This example shows how to check for revoked certificates in the locally stored CRL:

```
switch(config-trustpoint)# revocation-check crl
```

This example shows how to do no checking for revoked certificates:

```
switch(config-trustpoint)# revocation-check none
```

Related Commands

Command	Description
crypto ca crl-request	Configures a CRL or overwrites the existing one for the trustpoint CA.
show crypto ca crl	Displays configured CRLs.

role abort

To discard a user role Cisco Fabric Services distribution session in progress, use the **role abort** command.

role abort

Syntax Description

This command has no other arguments or keywords.

Defaults

None

Command Modes

Global configuration

SupportedUserRoles

network-admin
vdc-admin

Command History

Release	Modification
4.1(2)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to discard a user role Cisco Fabric Services distribution session in progress:

```
switch# configure terminal
switch(config)# role abort
```

Related Commands

Command	Description
show role	Displays the user role Cisco Fabric Services distribution status and other details.

role commit

To apply the pending configuration pertaining to the user role Cisco Fabric Services distribution session in progress in the fabric, use the **role commit** command.

role commit

Syntax Description

This command has no other arguments or keywords.

Defaults

None

Command Modes

Global configuration

SupportedUserRoles

network-admin
vdc-admin

Command History

Release	Modification
4.1(2)	This command was introduced.

Usage Guidelines

Before committing the user role configuration to the fabric, all switches in the fabric must have distribution enabled using the **role distribute** command.

This command does not require a license.

Examples

This example shows how to initiate distribution of a user role configuration to the switches in the fabric:

```
switch# configure terminal
switch(config)# role commit
```

Related Commands

Command	Description
role distribute	Enables Cisco Fabric Services distribution for user roles.
show role	Displays the user role Cisco Fabric Services distribution status and other details.

role distribute

To enable Cisco Fabric Services distribution for user roles, use the **role distribute** command. To disable this feature, use the **no** form of the command.

role distribute

no role distribute

Syntax Description

This command has no other arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration

SupportedUserRoles

network-admin
vdc-admin

Command History

Release	Modification
4.1(2)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to enable role fabric distribution:

```
switch# configure terminal
switch(config)# role distribute
```

This example shows how to disable role fabric distribution:

```
switch# configure terminal
switch(config)# no role distribute
```

Related Commands

Command	Description
show role distribution status	Displays role Cisco Fabric Services distribution status.

role feature-group name

To create or specify a user role feature group and enter user role feature group configuration mode, use the **role feature-group name** command. To delete a user role feature group, use the **no** form of this command.

role feature-group name *group-name*

no role feature-group name *group-name*

Syntax Description

group-name	User role feature group name. The *group-name* has a maximum length of 32 characters and is a case-sensitive, alphanumeric character string.

Defaults

None

Command Modes

Global configuration

SupportedUserRoles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

The Cisco NX-OS software provides the default user role feature group L3 for Layer 3 features. You cannot modify or delete the L3 user role feature group.

This command does not require a license.

Examples

This example shows how to create a user role feature group and enter user role feature group configuration mode:

```
switch# configure terminal
switch(config)# role feature-group name MyGroup
switch(config-role-featuregrp)#
```

This example shows how to remove a user role feature group:

```
switch# configure terminal
switch(config)# no role feature-group name MyGroup
```

Related Commands

Command	Description
feature-group name	Specifies or creates a user role feature group and enters user role feature group configuration mode.
show role feature-group	Displays the user role feature groups.

role name

To create or modify a user role or privilege role and enter user role configuration mode, use the **role name** command. To delete a user role, use the **no** form of this command.

role name {*role-name* | **priv-***n*}

no role name {*role-name* | **priv-***n*}

Syntax Description

role-name	User role name. The *role-name* argument has a maximum length of 16 characters and is a case-sensitive, alphanumeric character string.
priv-*n*	Specifies the privilege level. The *n* argument is a number between 0 and 13.

Defaults

None

Command Modes

Global configuration

SupportedUserRoles

network-admin
vdc-admin

Command History

Release	Modification
5.0(2)	The **priv-***n* keyword was added.
4.0(1)	This command was introduced.

Usage Guidelines

The Cisco NX-OS software provides four default user roles:

- network-admin—Complete read-and-write access to the entire Cisco NX-OS device (only available in the default VDC)
- network-operator—Complete read access to the entire Cisco NX-OS device (only available in the default VDC)
- vdc-admin—Read-and-write access limited to a VDC
- vdc-operator—Read access limited to a VDC

You cannot change or remove the default user roles.

You must follow these guidelines when changing the rules of privilege roles:

- You cannot modify the priv-14 and priv-15 roles.
- You can add deny rules only to the priv-0 role.
- These commands are always permitted for the priv-0 role: **configure**, **copy**, **dir**, **enable**, **ping**, **show**, **ssh**, **telnet**, **terminal**, **traceroute**, **end**, and **exit**.

This command does not require a license.

Examples

This example shows how to create a user role and enter user role configuration mode:

```
switch# configure terminal
switch(config)# role name MyRole
switch(config-role)#
```

This example shows how to remove a user role:

```
switch# configure terminal
switch(config)# no role name MyRole
```

This example shows how to enable privilege level 5 for users:

```
switch# configure terminal
switch(config)# role name priv-5
switch(config-role)#
```

Related Commands

Command	Description
rule	Configure rules for a user role or for users of privilege roles.
show role	Displays the user roles.

rsakeypair

To configure and associate the RSA key pair details to a trustpoint, use the **rsakeypair** command. To disassociate the RSA key pair from the trustpoint, use the **no** form of this command.

rsakeypair *key-pair-label* [*key-pair-size*]

no rsakeypair *key-pair-label* [*key-pair-size*]

Syntax Description

key-pair-label	Name for the RSA key pair. The name is alphanumeric, case sensitive, and has a maximum of 64 characters.
key-pair-size	(Optional) Size for the RSA key pair. The size values are 512, 768, 1024, 1536, and 2048 bits.

Defaults

The default key pair size is 512 if the key pair is not already generated.

Command Modes

Trustpoint configuration

Command History

Release	Modification
4.1(2)	This command was introduced.

Usage Guidelines

You can associate only one RSA key pair with a trustpoint CA, even though you can associate the same key pair with many trustpoint CAs. This association must occur before you enroll with the CA to obtain an identity certificate. If the key pair was previously generated (using the **crypto key generate** command), then the key pair size, if specified, should be the same size as that was used during the generation. If the specified key pair is not yet generated, you can enter the **crypto ca enroll** command to generated the RSA key pair during the enrollment.

Note The **no** form of the **rsakeypair** command disassociates the key pair from the trustpoint. Before you enter the **no rsakeypair** command, first remove the identity certificate, if present, from the trustpoint CA to ensure that the association between the identity certificate and the key pair for a trustpoint is consistent.

This command does not require a license.

Examples

This example shows how to associate an RSA key pair to a trustpoint:

```
switch# configure terminal
switch(config)# crypto ca trustpoint admin-ca
switch(config-trustpoint)# rsakeypair adminid-key
```

This example shows how to disassociate an RSA key pair from a trustpoint:

```
switch(config-trustpoint)# no rsakeypair adminid-key
```

Related Commands

Command	Description
crypto ca enroll	Requests certificates for the switch's RSA key pair created for the trustpoint CA.
crypto key generate rsa	Configures RSA key pair information.
show crypto key mypubkey rsa	Displays information about configured RSA key pairs.

rule

To configure rules for a user role or for users of privilege roles, use the **rule** command. To delete a rule, use the **no** form of this command.

rule *number* {**deny** | **permit**} {**command** *command-string* | {**read** | **read-write**} [**feature** *feature-name* | **feature-group** *group-name*]}

no rule *number*

Syntax Description

number	Sequence number for the rule. The Cisco NX-OS software applies the rule with the highest value first and then the rest in descending order. The range is 1 to 256.
deny	Denies access to commands or features.
permit	Permits access to commands or features.
command *command-string*	Specifies a command string.
read	Specifies read access.
read-write	Specifies read and write access.
feature *feature-name*	(Optional) Specifies a feature name. Use the **show role feature** command to list the Cisco NX-OS feature names.
feature-group *group-name*	(Optional) Specifies a feature group.

Defaults

None

Command Modes

User role configuration

SupportedUserRoles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

You can configure up to 256 rules for each role.

The rule number that you specify determines the order in which the rules are applied. Rules are applied in descending order. For example, if a role has three rules, rule 3 is applied before rule 2, which is applied before rule 1.

This command does not require a license.

Examples

This example shows how to add rules to a user role:

```
switch# configure terminal
switch(config)# role MyRole
switch(config-role)# rule 1 deny command clear users
switch(config-role)# rule 1 permit read-write feature-group L3
```

This example shows how to remove rule from a user role:

```
switch# configure terminal
switch(config)# role MyRole
switch(config-role)# no rule 10
```

Related Commands

Command	Description
role name	Creates or specifies a user role name and enters user role configuration mode.
show role	Displays the user roles.