

RADIUS Change of Authorization

The RADIUS Change of Authorization (CoA) feature provides a mechanism to change the attributes of an authentication, authorization, and accounting (AAA) session after it is authenticated. When a policy changes for a user or user group in AAA, administrators can send the RADIUS CoA packets from the AAA server such as a Cisco Secure Access Control Server (ACS) to reinitialize authentication and apply the new policy.

- Information About RADIUS Change of Authorization, on page 1
- How to Configure RADIUS Change of Authorization, on page 5
- Configuration Examples for RADIUS Change of Authorization, on page 11
- Additional References for RADIUS Change of Authorization, on page 12
- Feature Information for RADIUS Change of Authorization, on page 13

Information About RADIUS Change of Authorization

About RADIUS Change of Authorization

A standard RADIUS interface is typically used in a pulled model, in which the request originates from a device attached to a network and the response is sent from the queried servers. The Cisco software supports the RADIUS CoA request defined in RFC 5176 that is used in a pushed model, in which the request originates from the external server to the device attached to the network, and enables the dynamic reconfiguring of sessions from external authentication, authorization, and accounting (AAA) or policy servers.

Use the following per-session CoA requests:

- Session reauthentication
- Session termination
- Session termination with port shutdown
- Session termination with port bounce
- Security and Password
- Accounting

CoA Requests

CoA requests, as described in RFC 5176, are used in a pushed model to allow for session identification, host reauthentication, and session termination. The model comprises one request (CoA-Request) and two possible response codes:

- CoA acknowledgment (ACK) [CoA-ACK]
- CoA non-acknowledgment (NAK) [CoA-NAK]

The request is initiated from a CoA client (typically a RADIUS or policy server) and directed to the device that acts as a listener.

RFC 5176 Compliance

The Disconnect Request message, which is also referred to as Packet of Disconnect (POD), is supported by the device for a session termination.

The following table shows the IETF attributes that are supported for the RADIUS Change of Authorization (CoA) feature.

Table 1: Supported IETF Attributes

Attribute Number	Attribute Name
24	State
31	Calling-Station-ID
44	Acct-Session-ID
80	Message-Authenticator
101	Error-Cause

The following table shows the possible values for the Error-Cause attribute.

Table 2: Error-Cause Values

Value	Explanation
201	Residual Session Context Removed
202	Invalid EAP Packet (Ignored)
401	Unsupported Attribute
402	Missing Attribute
403	NAS Identification Mismatch
404	Invalid Request
405	Unsupported Service
406	Unsupported Extension

Value	Explanation
407	Invalid Attribute Value
501	Administratively Prohibited
502	Request Not Routable (Proxy)
503	Session Context Not Found
504	Session Context Not Removable
505	Other Proxy Processing Error
506	Resources Unavailable
507	Request Initiated
508	Multiple Session Selection Unsupported

CoA Request Response Code

The CoA Request Response code can be used to issue a command to the device. The supported commands are listed in the "CoA Request Commands" section.

The packet format for a CoA Request Response code as defined in RFC 5176 consists of the following fields: Code, Identifier, Length, Authenticator, and Attributes in the Type:Length:Value (TLV) format.

The Attributes field is used to carry Cisco VSAs.

Session Identification

For disconnect and CoA requests targeted at a particular session, the device locates the session based on one or more of the following attributes:

- Acct-Session-Id (IETF attribute #44)
- Audit-Session-Id (Cisco vendor-specific attribute (VSA))
- Calling-Station-Id (IETF attribute #31, which contains the host MAC address)

Unless all session identification attributes included in the CoA message match the session, the device returns a Disconnect-NAK or CoA-NAK with the "Invalid Attribute Value" error-code attribute.

Note A CoA NAK message is not sent for all CoA requests with a key mismatch. The message is sent only for the first three requests for a client. After that, all the packets from that client are dropped. When there is a key mismatch, the response authenticator sent with the CoA NAK message is calculated from a dummy key value.

CoA ACK Response Code

If an authorization state is changed successfully, a positive acknowledgment (ACK) is sent. The attributes returned within a CoA ACK can vary based on the CoA Request.

CoA NAK Response Code

A negative acknowledgment (NAK) indicates a failure to change the authorization state and can include attributes that indicate the reason for the failure.

CoA Request Commands

The commands supported on the device are shown in the table below. All CoA commands must include the session identifier between the device and the CoA client.

Table 3: CoA Request Commands Supported on the Device

Command	Cisco VSA
Bounce host port	Cisco:Avpair="subscriber:command=bounce-host-port"
Disable host port	Cisco:Avpair="subscriber:command=disable-host-port"
Reauthenticate host	Cisco:Avpair="subscriber:command=reauthenticate"
Terminate session	This is a standard disconnect request that does not require a VSA

Session Reauthentication

To initiate session reauthentication, the authentication, authorization, and accounting (AAA) server sends a standard CoA-Request message that contains a Cisco VSA and one or more session identification attributes. The Cisco VSA is in the form of Cisco:Avpair="subscriber:command=reauthenticate".

The current session state determines the device's response to the message in the following scenarios:

- If the session is currently authenticated by IEEE 802.1*x*, the device responds by sending an Extensible Authentication Protocol over LAN (EAPoL)-RequestId message to the server.
- If the session is currently authenticated by MAC authentication bypass (MAB), the device sends an access request to the server, passing the same identity attributes used for the initial successful authentication.
- If session authentication is in progress when the device receives the command, the device terminates the process and restarts the authentication sequence, starting with the method configured to be attempted first.

Session Termination

A CoA Disconnect-Request terminates the session without disabling the host port. CoA Disconnect-Request termination causes reinitialization of the authenticator state machine for the specified host, but does not restrict the host's access to the network. If the session cannot be located, the device returns a Disconnect-NAK message with the "Session Context Not Found" error-code attribute. If the session is located, the device terminates the session. After the session has been completely removed, the device returns a Disconnect-ACK message.

To restrict a host's access to the network, use a CoA Request with the Cisco:Avpair="subscriber:command=disable-host-port" VSA. This command is useful when a host is known to cause problems on the network and network access needs to be immediately blocked for the host. If you want to restore network access on the port, reenable it using a non-RADIUS mechanism.

CoA Request Disable Host Port

The RADIUS server CoA disable port command administratively shuts down the authentication port that is hosting a session, resulting in session termination. This command is useful when a host is known to cause problems on the network and network access needs to be immediately blocked for the host. If you want to restore network access on the port, reenable it using a non-RADIUS mechanism. This command is carried in a standard CoA-Request message that has the following VSA:

Cisco:Avpair="subscriber:command=disable-host-port"

Because this command is session-oriented, it must be accompanied by one or more of the session identification attributes described in the "Session Identification" section. If the device cannot locate the session, it returns a CoA-NAK message with the "Session Context Not Found" error-code attribute. If the device locates the session, it disables the hosting port and returns a CoA-ACK message.

If the device fails before returning a CoA-ACK to the client, the process is repeated on the new active device when the request is re-sent from the client. If the device fails after returning a CoA-ACK message to the client but before the operation is complete, the operation is restarted on the new active device.

To ignore the RADIUS server CoA disable port command, see the "Configuring the Device to Ignore Bounce and Disable RADIUS CoA Requests" section.

CoA Request Bounce Port

A RADIUS server CoA bounce port sent from a RADIUS server can cause a link flap on an authentication port, which triggers DHCP renegotiation from one or more hosts connected to this port. This incident can occur when there is a VLAN change and the endpoint is a device (such as a printer) that does not have a mechanism to detect a change on this authentication port. The CoA bounce port is carried in a standard CoA-Request message that contains the following VSA:

Cisco:Avpair="subscriber:command=bounce-host-port"

Because this command is session-oriented, it must be accompanied by one or more of the session identification attributes described in the Session Identification. If the session cannot be located, the device returns a CoA-NAK message with the "Session Context Not Found" error-code attribute. If the session is located, the device disables the hosting port for a period of 10 seconds, reenables it (port-bounce), and returns a CoA-ACK.

To ignore the RADIUS server CoA bounce port, see the "Configuring the Device to Ignore Bounce and Disable RADIUS CoA Requests" section.

How to Configure RADIUS Change of Authorization



Note Some configurations and protocols are identified as insecure and is a security risk for Cisco devices. Existing deployments continue to function, but new installations require intentional enablement. For more information on remediation, refer to Resilient Infrastructure: Cisco Catalyst SD-WAN and Routing

Configuring RADIUS Change of Authorization

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa server radius dynamic-author**
5. **client** {*ip-address* | *name* [**vrf** *vrf-name*]} **server-key** [**0** | **7**] *string*
6. **port** *port-number*
7. **auth-type** {**any** | **all** | **session-key**}
8. **ignore session-key**
9. **ignore server-key**
10. **exit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**aaa new-model** **Example:** `Device(config)# aaa new-model`	Enables authentication, authorization, and accounting (AAA) globally.
Step 4	**aaa server radius dynamic-author** **Example:** `Device(config)# aaa server radius dynamic-author`	Enters dynamic authorization local server configuration mode and specifies a RADIUS client from which a device accepts Change of Authorization (CoA) and disconnect requests. Configures the device as a AAA server to facilitate interaction with an external policy server.
Step 5	**client** {*ip-address* | *name* [**vrf** *vrf-name*]} **server-key** [**0** | **7**] *string* **Example:** `Device(config-locsvr-da-radius)# client 10.0.0.1`	Configures the RADIUS key to be shared between a device and RADIUS clients.
Step 6	**port** *port-number* **Example:** `Device(config-locsvr-da-radius)# port 3799`	Specifies the port on which a device listens for RADIUS requests from configured RADIUS clients. **Note**

	Command or Action	Purpose
		The default port for packet of disconnect is 1700. Port 3799 is required to interoperate with ACS 5.1.
Step 7	**auth-type** {**any** | **all** | **session-key**} **Example:** `Device(config-locsvr-da-radius)# auth-type all`	Specifies the type of authorization that the device must use for RADIUS clients. The client must match the configured attributes for authorization.
Step 8	**ignore session-key** **Example:** `Device(config-locsvr-da-radius)# ignore session-key`	(Optional) Configures the device to ignore the session key.
Step 9	**ignore server-key** **Example:** `Device(config-locsvr-da-radius)# ignore server-key`	(Optional) Configures the device to ignore the server key.
Step 10	**exit** **Example:** `Device(config-locsvr-da-radius)# exit`	Returns to global configuration mode.

Configuring a Device to Ignore Bounce and Disable RADIUS CoA Requests

When an authentication port is authenticated with multiple hosts and there is a Change of Authorization (CoA) request for one host to flap on this port or one host session to be terminated on this port, the other hosts on this port are also affected. Thus, an authenticated port with multiple hosts can trigger a DHCP renegotiation from one or more hosts in the case of a flap, or it can administratively shut down the authentication port that is hosting the session for one or more hosts.

Perform the following steps to configure the device to ignore RADIUS server Change of Authorization (CoA) requests in the form of a bounce port command or disable port command.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **authentication command bounce-port ignore**
5. **authentication command disable-port ignore**
6. **end**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**aaa new-model** **Example:** `Device(config)# aaa new-model`	Enables authentication, authorization, and accounting (AAA) globally.
Step 4	**authentication command bounce-port ignore** **Example:** `Device(config)# authentication command bounce-port ignore`	(Optional) Configures the device to ignore a RADIUS server bounce port command that causes a host to link flap on an authentication port, which causes DHCP renegotiation from one or more hosts connected to this port.
Step 5	**authentication command disable-port ignore** **Example:** `Device(config)# authentication command disable-port ignore`	(Optional) Configures the device to ignore a RADIUS server CoA disable port command that administratively shuts down the authentication port that hosts one or more host sessions. • The shutting down of the port causes session termination.
Step 6	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.

Configuring the Dynamic Authorization Service for RADIUS CoA

Perform the following steps to enable the device as an authentication, authorization, and accounting (AAA) server for the dynamic authorization service. This service supports the Change of Authorization (CoA) functionality that pushes the policy map in an input and output direction.

SUMMARY STEPS

1. **enable**
2. **configure terminal**

3. **aaa new-model**
4. **aaa server radius dynamic-author**
5. **client** {*ip-addr* | *hostname*} [**server-key** [**0** | **7**] *string*]
6. **domain** {**delimiter** *character* | **stripping** | [**right-to-left**]}
7. **port** *port-num*
8. **end**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**aaa new-model** **Example:** `Device(config)# aaa new-model`	Enables AAA globally.
Step 4	**aaa server radius dynamic-author** **Example:** `Device(config)# aaa server radius dynamic-author`	Sets up the local AAA server for the dynamic authorization service, which must be enabled to support the CoA functionality to push the policy map in an input and output direction, and enters dynamic authorization local server configuration mode. • In this mode, the RADIUS application commands are configured.
Step 5	**client** {*ip-addr*	*hostname*} [**server-key** [**0**	**7**] *string*] **Example:** `Device(config-locsvr-da-radius)# client 192.168.0.5 server-key cisco1`	Configures the IP address or hostname of the AAA server client. • Use the optional **server-key** keyword and *string* argument to configure the server key at the client level. **Note** Configuring the server key at the client level overrides the server key configured at the global level.
Step 6	**domain** {**delimiter** *character*	**stripping**	[**right-to-left**]} **Example:** `Device(config-locsvr-da-radius)# domain stripping right-to-left`	(Optional) Configures username domain options for the RADIUS application. • The **delimiter** keyword specifies the domain delimiter. One of the following options can be specified for the *character* argument: **@**, /, **$**, **%**, \, **#**, or **-**.

	Command or Action	Purpose
		• The **stripping** keyword compares the incoming username with the names oriented to the left of the **@** domain delimiter. • The **right-to-left** keyword terminates the string at the first delimiter going from right to left.
Step 7	**port** *port-num* **Example:** `Device(config-locsvr-da-radius)# port 3799`	Configures the UDP port for CoA requests.
Step 8	**end** **Example:** `Device(config-locsvr-da-radius)# end`	Returns to privileged EXEC mode.

Monitoring and Troubleshooting RADIUS Change of Authorization

The following commands can be used to monitor and troubleshoot the RADIUS Change of Authorization feature:

Table 4: Monitoring and Troubleshooting RADIUS Change of Authorization

Command	Purpose
debug aaa coa	Displays debug information for CoA processing.
debug aaa pod	Displays debug messages related to packet of disconnect (POD) packets.
debug radius	Displays information associated with RADIUS.
show aaa attributes protocol radius	Displays the mapping between an authentication, authorization, and accounting (AAA) attribute number and the corresponding AAA attribute name.

Configuration Examples for RADIUS Change of Authorization

Example: Configuring RADIUS Change of Authorization

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa server radius dynamic-author
Device(config-locsvr-da-radius)# client 10.0.0.1
Device(config-locsvr-da-radius)# server-key cisco123
Device(config-locsvr-da-radius)# port 3799
Device(config-locsvr-da-radius)# auth-type all
Device(config-locsvr-da-radius)# ignore session-key
Device(config-locsvr-da-radius)# ignore server-key
Device(config-locsvr-da-radius)# end
```

Example: Configuring a Device to Ignore Bounce and Disable a RADIUS Requests

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# authentication command bounce-port ignore
Device(config)# authentication command disable-port ignore
Device(config)# end
```

Example: Configuring the Dynamic Authorization Service for RADIUS CoA

The following example shows how to configure the device as a authentication, authorization, and accounting (AAA) server to support Change of Authorization (CoA) functionality that pushes the policy map in an input and output direction:

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa server radius dynamic-author
Device(config-locsvr-da-radius)# client 192.168.0.5 server-key cisco1
Device(config-locsvr-da-radius)# domain delimiter @
Device(config-locsvr-da-radius)# port 3799
Device(config-locsvr-da-radius)# end
```

Additional References for RADIUS Change of Authorization

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
Security commands	• Security Command Reference: Commands A to C • Security Command Reference: Commands D to L • Security Command Reference: Commands M to R • Security Command Reference: Commands S to Z
Configuring AAA	*Authentication, Authorization, and Accounting Configuration Guide*

Standards and RFCs

Standard/RFC	Title
RFC 2903	*Generic AAA Architecture*
RFC 5176	*Dynamic Authorization Extensions to Remote Authentication Dial In User Service(RADIUS)*

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for RADIUS Change of Authorization

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 5: Feature Information for RADIUS Change of Authorization

Feature Name	Releases	Feature Information
RADIUS Change of Authorization		The RADIUS Change of Authorization (CoA) feature provides a mechanism to change the attributes of an AAA session after it is authenticated. When policy changes for a user or user group in AAA, administrators can send the RADIUS CoA packets from the AAA server, such as the Cisco Secure Access Control Server (ACS), to reinitialize authentication and apply the new policy. The following commands were introduced or modified: **aaa server radius dynamic-author**, **authentication command bounce-port ignore**, and **authentication command disable-port ignore**.