



Authentication Authorization and Accounting Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3650 Switches)

First Published: February 24, 2013

Last Modified: January 29, 2013

Americas Headquarters

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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <http://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2013 Cisco Systems, Inc. All rights reserved.



CONTENTS

CHAPTER 1

MAC Authentication Bypass 1

- Finding Feature Information 1
- Prerequisites for Configuring MAC Authentication Bypass 2
- Information About Configuring MAC Authentication Bypass 2
 - Overview of the Cisco IOS Auth Manager 2
- How to Configure MAC Authentication Bypass 3
 - Enabling MAC Authentication Bypass 3
 - Enabling Reauthentication on a Port 4
 - Specifying the Security Violation Mode 6
- Configuration Examples for MAC Authentication Bypass 8
 - Example: MAC Authentication Bypass Configuration 8
- Additional References 8
- Feature Information for MAC Authentication Bypass 9

CHAPTER 2

Standalone MAB Support 11

- Finding Feature Information 11
- Information About Configuring Standalone MAB 12
 - Standalone MAB 12
- How to Configure Standalone MAB Support 12
 - Enabling Standalone MAB 12
 - Troubleshooting Tips 14
- Configuration Examples for Standalone MAB Support 14
 - Example: Standalone MAB Configuration 14
- Additional References 15
- Feature Information for Standalone MAB Support 16

CHAPTER 3

Message Banners for AAA Authentication 17

- Finding Feature Information 17

Information About Message Banners for AAA Authentication	17
Login and Failed-Login Banners for AAA Authentication	17
How to Configure Message Banners for AAA Authentication	18
Configuring a Login Banner for AAA Authentication	18
Configuring a Failed-Login Banner for AAA Authentication	19
Configuration Examples for Message Banners for AAA Authentication	20
Example: Configuring Login and Failed-Login Banners for AAA Authentication	20
Additional References for Message Banners for AAA Authentication	21
Feature Information for Message Banners for AAA Authentication	22

CHAPTER 4**RADIUS Change of Authorization 23**

Finding Feature Information	23
Information About RADIUS Change of Authorization	23
About RADIUS Change of Authorization	23
CoA Requests	24
RFC 5176 Compliance	24
CoA Request Response Code	25
Session Identification	26
CoA ACK Response Code	26
CoA NAK Response Code	26
CoA Request Commands	26
Session Reauthentication	27
Session Termination	27
CoA Request Disable Host Port	27
CoA Request Bounce Port	28
How to Configure RADIUS Change of Authorization	28
Configuring RADIUS Change of Authorization	28
Configuring a Device to Ignore Bounce and Disable RADIUS CoA Requests	30
Configuring the Dynamic Authorization Service for RADIUS CoA	31
Monitoring and Troubleshooting RADIUS Change of Authorization	32
Configuration Examples for RADIUS Change of Authorization	33
Example: Configuring RADIUS Change of Authorization	33
Example: Configuring a Device to Ignore Bounce and Disable a RADIUS Requests	33
Example: Configuring the Dynamic Authorization Service for RADIUS CoA	34
Additional References for RADIUS Change of Authorization	34

Feature Information for RADIUS Change of Authorization 35

CHAPTER 5**TACACS+ over IPv6 37**

Finding Feature Information 37

Information About TACACS+ over IPv6 37

AAA over IPv6 38

TACACS+ Over an IPv6 Transport 38

How to Configure TACACS+ over IPv6 38

Configuring the TACACS+ Server over IPv6 38

Specifying the Source Address in TACACS+ Packets 40

Configuring TACACS+ Server Group Options 40

Configuration Examples for TACACS+ over IPv6 41

Example: Configuring TACACS+ Server over IPv6 41

Additional References 42

Feature Information for TACACS+ over IPv6 42



CHAPTER

1

MAC Authentication Bypass

The MAC Authentication Bypass feature is a MAC-address-based authentication mechanism that allows clients in a network to integrate with the Cisco Identity Based Networking Services (IBNS) and Network Admission Control (NAC) strategy using the client MAC address. The MAC Authentication Bypass feature is applicable to the following network environments:

- Network environments in which a supplicant code is not available for a given client platform.
- Network environments in which the end client configuration is not under administrative control, that is, the IEEE 802.1X requests are not supported on these networks.
- [Finding Feature Information, page 1](#)
- [Prerequisites for Configuring MAC Authentication Bypass, page 2](#)
- [Information About Configuring MAC Authentication Bypass, page 2](#)
- [How to Configure MAC Authentication Bypass, page 3](#)
- [Configuration Examples for MAC Authentication Bypass, page 8](#)
- [Additional References, page 8](#)
- [Feature Information for MAC Authentication Bypass, page 9](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see [Bug Search Tool](#) and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

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.

Prerequisites for Configuring MAC Authentication Bypass

IEEE 802.1x—Port-Based Network Access Control

You should understand the concepts of port-based network access control and have an understanding of how to configure port-based network access control on your Cisco platform. For more information, see the *Securing User Services Configuration Guide Library*.

RADIUS and ACLs

You should understand the concepts of the RADIUS protocol and have an understanding of how to create and apply access control lists (ACLs). For more information, see the documentation for your Cisco platform and the *Securing User Services Configuration Guide Library*.

The device must have a RADIUS configuration and be connected to the Cisco secure access control server (ACS). For more information, see the *User Guide for Secure ACS Appliance 3.2*.

Information About Configuring MAC Authentication Bypass

Overview of the Cisco IOS Auth Manager

The capabilities of devices connecting to a given network can be different, thus requiring that the network support different authentication methods and authorization policies. The Cisco IOS Auth Manager handles network authentication requests and enforces authorization policies regardless of authentication method. The Auth Manager maintains operational data for all port-based network connection attempts, authentications, authorizations, and disconnections and, as such, serves as a session manager.

The possible states for Auth Manager sessions are as follows:

- Idle—In the idle state, the authentication session has been initialized, but no methods have yet been run. This is an intermediate state.
- Running—A method is currently running. This is an intermediate state.
- Authc Success—The authentication method has run successfully. This is an intermediate state.
- Authc Failed—The authentication method has failed. This is an intermediate state.
- Authz Success—All features have been successfully applied for this session. This is a terminal state.
- Authz Failed—At least one feature has failed to be applied for this session. This is a terminal state.
- No methods—There were no results for this session. This is a terminal state.

How to Configure MAC Authentication Bypass

Enabling MAC Authentication Bypass

Perform this task to enable the MAC Authentication Bypass feature on an 802.1X port.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type slot / port*
4. **mab**
5. **end**
6. **show authentication sessions interface** *type slot / port details*

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	interface <i>type slot / port</i> Example: Device(config)# interface FastEthernet 2/1	Enters interface configuration mode.
Step 4	mab Example: Device(config-if)# mab	Enables MAB.
Step 5	end Example: Device(config-if)# end	Returns to privileged EXEC mode.

	Command or Action	Purpose
Step 6	show authentication sessions interface <i>type slot / port</i> details Example: <pre>Device# show authentication session interface FastEthernet 2/1 details</pre>	Displays the interface configuration and the authenticator instances on the interface.

Enabling Reauthentication on a Port

By default, ports are not automatically reauthenticated. You can enable automatic reauthentication and specify how often reauthentication attempts are made.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type slot / port*
4. **switchport**
5. **switchport mode access**
6. **authentication port-control auto**
7. **mab** [eap]
8. **authentication periodic**
9. **authentication timer reauthenticate** {*seconds* | **server**}
10. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: <pre>Device> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: <pre>Device# configure terminal</pre>	Enters global configuration mode.

	Command or Action	Purpose
Step 3	interface <i>type slot / port</i> Example: Device(config)# interface FastEthernet2/1	Enters interface configuration mode.
Step 4	switchport Example: Device(config-if)# switchport	Places interface in Layer 2 switched mode.
Step 5	switchport mode access Example: Device(config-if)# switchport mode access	Sets the interface type as a nontrunking, nontagged single VLAN Layer 2 interface.
Step 6	authentication port-control auto Example: Device(config-if)# authentication port-control auto	Configures the authorization state of the port.
Step 7	mab [cap] Example: Device(config-if)# mab	Enables MAB.
Step 8	authentication periodic Example: Device(config-if)# authentication periodic	Enables reauthentication.
Step 9	authentication timer reauthenticate {seconds server} Example: Device(config-if)# authentication timer reauthenticate 900	Configures the time, in seconds, between reauthentication attempts.
Step 10	end Example: Device(config-if)# end	Exits interface configuration mode and returns to privileged EXEC mode.

Specifying the Security Violation Mode

When there is a security violation on a port, the port can be shut down or traffic can be restricted. By default, the port is shut down. You can configure the period of time for which the port is shut down.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type slot / port*
4. **switchport**
5. **switchport mode access**
6. **authentication port-control auto**
7. **mab** [*eap*]
8. **authentication violation** {*restrict* | *shutdown*}
9. **authentication timer restart** *seconds*
10. **end**

DETAILED STEPS

	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	interface <i>type slot / port</i> Example: Device(config)# interface FastEthernet2/1	Enters interface configuration mode.
Step 4	switchport Example: Device(config-if)# switchport	Places interface in Layer 2 switched mode.

	Command or Action	Purpose
Step 5	switchport mode access Example: Device(config-if)# switchport mode access	Sets the interface type as a nontrunking, nontagged single VLAN Layer 2 interface.
Step 6	authentication port-control auto Example: Device(config-if)# authentication port-control auto	Configures the authorization state of the port.
Step 7	mab [eap] Example: Device(config-if)# mab	Enables MAB.
Step 8	authentication violation {restrict shutdown} Example: Device(config-if)# authentication violation shutdown	Configures the action to be taken when a security violation occurs on the port.
Step 9	authentication timer restart seconds Example: Device(config-if)# authentication timer restart 30	Configures the period of time, in seconds, after which an attempt is made to authenticate an unauthorized port.
Step 10	end Example: Device(config-if)# end	Exits interface configuration mode and returns to privileged EXEC mode.

Configuration Examples for MAC Authentication Bypass

Example: MAC Authentication Bypass Configuration

In the following example, the **mab** command has been configured to enable the MAC Authorization Bypass (MAB) feature on the specified interface. The optional **show authentication sessions** command has been enabled to display the interface configuration and the authentication instances on the interface.

```
Device> enable
Device# configure terminal
Device(config)# interface GigabitEthernet2/1
Device(config-if)# mab
Device(config-if)# end
Device# show authentication sessions interface GigabitEthernet2/1 details
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
Authentication commands	<i>Cisco IOS Security Command Reference</i>
IEEE 802.1x—Flexible Authentication	<i>Securing User Services Configuration Library</i>

MIBs

MIB	MIBs Link
<ul style="list-style-type: none"> • CISCO-AUTH-FRAMEWORK-MIB • CISCO-MAC-AUTH-BYPASS-MIB • CISCO-PAE-MIB • IEEE8021-PAE-MIB 	To locate and download MIBs for selected platforms, Cisco IOS software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 3580	<i>IEEE 802.1x Remote Authentication Dial In User Service (RADIUS)</i>

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 MAC Authentication Bypass

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 1: Feature Information for MAC Authentication Bypass

Feature Name	Releases	Feature Information
MAC Authentication Bypass (MAB)	Cisco IOS XE Release 3.2SE	<p>The MAC Authentication Bypass feature is a MAC-address-based authentication mechanism that allows clients in a network to integrate with the Cisco IBNS and NAC strategy using the client MAC address.</p> <p>The following commands were introduced or modified: dot1x mac-auth-bypass, show dot1x interface.</p>



CHAPTER 2

Standalone MAB Support

Standalone MAC Authentication Bypass (MAB) is an authentication method that grants network access to specific MAC addresses regardless of 802.1X capability or credentials. As a result, devices such as cash registers, fax machines, and printers can be readily authenticated, and network features that are based on authorization policies can be made available.

Before standalone MAB support was available, MAB could be configured only as a failover method for 802.1x authentication. Standalone MAB is independent of 802.1x authentication.

- [Finding Feature Information, page 11](#)
- [Information About Configuring Standalone MAB, page 12](#)
- [How to Configure Standalone MAB Support, page 12](#)
- [Configuration Examples for Standalone MAB Support, page 14](#)
- [Additional References, page 15](#)
- [Feature Information for Standalone MAB Support, page 16](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see [Bug Search Tool](#) and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

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.

Information About Configuring Standalone MAB

Standalone MAB

MAC Authentication Bypass (MAB) uses the MAC address of the connecting device to grant or deny network access. To support MAB, the RADIUS authentication server maintains a database of MAC addresses for devices that require access to the network. MAB generates a RADIUS request with a MAC address in the Calling-Station-Id (attribute 31) and with a Service-Type (attribute 6) 10. After a successful authentication, the Auth Manager enables various authorization features specified by the authorization policy, such as ACL assignment and VLAN assignment.

How to Configure Standalone MAB Support

Enabling Standalone MAB

Ports enabled with the Standalone MAB feature can use the MAC address of connecting devices to grant or deny network access. Perform the steps described in this section to enable standalone MAB on individual ports.

Before You Begin

Before you can configure standalone MAB, the device must be connected to a Cisco Secure ACS server and RADIUS authentication, authorization, and accounting (AAA) must be configured.

**Note**

Standalone MAB can be configured on devices with switched ports only; it cannot be configured on devices with routed ports.

**Note**

If you are unsure whether MAB or MAB Extensible Authentication Protocol (EAP) is enabled or disabled on the switched port, use the **default mab** or **default mab eap** commands in interface configuration mode to configure MAB or MAB EAP.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type slot / port*
4. **switchport**
5. **switchport mode access**
6. **authentication port-control auto**
7. **mab**
8. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	interface <i>type slot / port</i> Example: Device(config)# interface FastEthernet2/1	Enters interface configuration mode.
Step 4	switchport Example: Switch(config-if)# switchport	Places interface in Layer 2 switched mode.
Step 5	switchport mode access Example: Device(config-if)# switchport mode access	Sets the interface type a as nontrunking, nontagged single VLAN Layer 2 interface.
Step 6	authentication port-control auto Example: Device(config-if)# authentication port-control auto	Configures the authorization state of the port.

	Command or Action	Purpose
Step 7	mab Example: Device(config-if)# mab	Enables MAB.
Step 8	end Example: Device(config-if)# end	Exits interface configuration mode and returns to privileged EXEC mode.

Troubleshooting Tips

The following commands can help troubleshoot standalone MAB:

- **debug authentication**
- **debug mab all**
- **show authentication registrations**
- **show authentication sessions**
- **show mab**

Configuration Examples for Standalone MAB Support

Example: Standalone MAB Configuration

The following example shows how to configure standalone MAB on a port. In this example, the client is reauthenticated every 1200 seconds and the connection is dropped after 600 seconds of inactivity.

```

Device> enable
Device# configure terminal
Device(config)# interface GigabitEthernet2/1
Device(config-if)# switchport
Device(config-if)# switchport mode access
Device(config-if)# switchport access vlan 2
Device(config-if)# authentication port-control auto
Device(config-if)# mab
Device(config-if)# authentication violation shutdown
Device(config-if)# authentication timer restart 30
Device(config-if)# authentication periodic
Device(config-if)# authentication timer reauthenticate 1200
Device(config-if)# authentication timer inactivity 600

```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
Authentication commands	<i>Cisco IOS Security Command Reference</i>
IEEE 802.1x—Flexible Authentication	<i>Securing User Services Configuration Library</i>

MIBs

MIB	MIBs Link
<ul style="list-style-type: none"> • CISCO-AUTH-FRAMEWORK-MIB • CISCO-MAC-AUTH-BYPASS-MIB • CISCO-PAE-MIB • IEEE8021-PAE-MIB 	<p>To locate and download MIBs for selected platforms, Cisco IOS software releases, and feature sets, use Cisco MIB Locator found at the following URL:</p> <p>http://www.cisco.com/go/mibs</p>

RFCs

RFC	Title
RFC 3580	<i>IEEE 802.1x Remote Authentication Dial In User Service (RADIUS)</i>

Technical Assistance

Description	Link
<p>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.</p>	<p>http://www.cisco.com/cisco/web/support/index.html</p>

Feature Information for Standalone MAB Support

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 2: Feature Information for Standalone MAB Support

Feature Name	Releases	Feature Information
Standalone MAB Support	Cisco IOS XE Release 3.2SE	<p>This feature grants network access to devices based on MAC address regardless of 802.1x capability or credentials.</p> <p>The following commands were introduced or modified: authentication periodic, authentication port-control, authentication timer inactivity, authentication timer reauthenticate, authentication timer restart, authentication violation, debug authentication, mab, show authentication interface, show authentication registrations, show authentication sessions, and show mab.</p>



Message Banners for AAA Authentication

The Message Banners for AAA authentication feature is used to configure personalized login and failed-login banners for user authentication. The message banners are displayed when a user logs in to the system to be authenticated using authentication, authorization, and accounting (AAA) and when an authentication fails.

- [Finding Feature Information, page 17](#)
- [Information About Message Banners for AAA Authentication, page 17](#)
- [How to Configure Message Banners for AAA Authentication, page 18](#)
- [Configuration Examples for Message Banners for AAA Authentication, page 20](#)
- [Additional References for Message Banners for AAA Authentication, page 21](#)
- [Feature Information for Message Banners for AAA Authentication, page 22](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see [Bug Search Tool](#) and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

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.

Information About Message Banners for AAA Authentication

Login and Failed-Login Banners for AAA Authentication

Login and failed-login banners use a delimiting character that notifies the system of the exact text string that must be displayed as the banner for authorization, authentication, and accounting (AAA) authentication. The delimiting character is repeated at the end of the text string to signify the end of the login or failed-login

banner. The delimiting character can be any single character in the extended ASCII character set, but once defined as the delimiter, that character cannot be used in the text string for the banner.

You can display a maximum of 2996 characters in a login or failed-login banner.

How to Configure Message Banners for AAA Authentication

Configuring a Login Banner for AAA Authentication

Perform this task to configure a banner that is displayed when a user logs in (replacing the default message for login). Use the **no aaa authentication banner** command to disable a login banner.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa authentication banner *delimiter-string delimiter***
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • 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 authentication banner <i>delimiter-string delimiter</i> Example: Device(config)# aaa authentication banner *Unauthorized Access Prohibited*	Creates a personalized login banner.

	Command or Action	Purpose
Step 5	<p>end</p> <p>Example: Device(config)# end</p>	Returns to privileged EXEC mode.

Configuring a Failed-Login Banner for AAA Authentication

Perform this task to configure a failed-login banner that is displayed when a user login fails (replacing the default message for failed login). Use the **no aaa authentication fail-message** command to disable a failed-login banner.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa authentication banner** *delimiter-string delimiter*
5. **aaa authentication fail-message** *delimiter-string delimiter*
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p>enable</p> <p>Example: Device> enable</p>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	<p>configure terminal</p> <p>Example: Device# configure terminal</p>	Enters global configuration mode.
Step 3	<p>aaa new-model</p> <p>Example: Device(config)# aaa new-model</p>	Enters AAA globally.

	Command or Action	Purpose
Step 4	aaa authentication banner <i>delimiter-string delimiter</i> Example: Device(config)# aaa authentication banner *Unauthorized Access Prohibited*	Creates a personalized login banner.
Step 5	aaa authentication fail-message <i>delimiter-string delimiter</i> Example: Device(config)# aaa authentication fail-message *Failed login. Try again*	Creates a message to be displayed when a user login fails.
Step 6	end Example: Device(config)# end	Returns to privileged EXEC mode.

Configuration Examples for Message Banners for AAA Authentication

Example: Configuring Login and Failed-Login Banners for AAA Authentication

The following example shows how to configure a login banner that is displayed when a user logs in to the system, (in this case, the phrase “Unauthorized Access Prohibited”). The asterisk (*) is used as the delimiting character. RADIUS is specified as the default login authentication method.

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa authentication banner *Unauthorized Access Prohibited*
Device(config)# aaa authentication login default group radius
```

This configuration displays the following login banner:

```
Unauthorized Access Prohibited
Username:
```

The following example shows how to configure a failed-login banner that is displayed when a user tries to log in to the system and fails, (in this case, the phrase “Failed login. Try again”). The asterisk (*) is used as the delimiting character. RADIUS is specified as the default login authentication method.

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
```

```
Device(config)# aaa authentication banner *Unauthorized Access Prohibited*
Device(config)# aaa authentication fail-message *Failed login. Try again.*
Device(config)# aaa authentication login default group radius
This configuration displays the following login and failed-login banner:
```

```
Unauthorized Access Prohibited
Username:
Password:
Failed login. Try again.
```

Additional References for Message Banners for AAA Authentication

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
Security commands	<ul style="list-style-type: none"> • 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	<i>Authentication, Authorization, and Accounting Configuration Guide</i>

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 Message Banners for AAA Authentication

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 3: Feature Information for Message Banners for AAA Authentication

Feature Name	Releases	Feature Information
Message Banners for AAA Authentication	Cisco IOS XE Release 3.2SE	The Message Banners for AAA Authentication feature enables you to configure personalized login and failed-login banners for user authentication. The message banners are displayed when a user logs in to the system to be authenticated using authentication, authorization, and accounting (AAA) and when an authentication fails. The following commands were introduced or modified: aaa authentication banner , aaa authentication fail-message , aaa new-model .



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.

- [Finding Feature Information, page 23](#)
- [Information About RADIUS Change of Authorization, page 23](#)
- [How to Configure RADIUS Change of Authorization, page 28](#)
- [Configuration Examples for RADIUS Change of Authorization, page 33](#)
- [Additional References for RADIUS Change of Authorization, page 34](#)
- [Feature Information for RADIUS Change of Authorization, page 35](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see [Bug Search Tool](#) and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

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.

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 4: 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 5: 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
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 6: 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 802.1x, 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

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

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.

	Command or Action	Purpose
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 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

	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.

	Command or Action	Purpose
Step 5	authentication command disable-port ignore Example: <pre>Device(config)# authentication command disable-port ignore</pre>	(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. <ul style="list-style-type: none"> • The shutting down of the port causes session termination.
Step 6	end Example: <pre>Device(config)# end</pre>	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

	Command or Action	Purpose
Step 1	enable Example: <pre>Device> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: <pre>Device# configure terminal</pre>	Enters global configuration mode.

	Command or Action	Purpose
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. <ul style="list-style-type: none"> In this mode, the RADIUS application commands are configured.
Step 5	client { <i>ip-addr</i> <i>hostname</i> } [server-key [0 7] <i>string</i>] 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. <ul style="list-style-type: none"> Use the optional server-key keyword and <i>string</i> 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 { <i>delimiter character</i> stripping right-to-left } Example: Device(config-locsvr-da-radius)# domain stripping right-to-left	(Optional) Configures username domain options for the RADIUS application. <ul style="list-style-type: none"> The delimiter keyword specifies the domain delimiter. One of the following options can be specified for the <i>character</i> argument: @, /, \$, %, \, #, or -. 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 <i>port-num</i> 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 7: 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	<ul style="list-style-type: none"> • 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	<i>Authentication, Authorization, and Accounting Configuration Guide</i>

Standards and RFCs

Standard/RFC	Title
RFC 2903	<i>Generic AAA Architecture</i>

Standard/RFC	Title
RFC 5176	<i>Dynamic Authorization Extensions to Remote Authentication Dial In User Service(RADIUS)</i>

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 8: Feature Information for RADIUS Change of Authorization

Feature Name	Releases	Feature Information
RADIUS Change of Authorization	Cisco IOS XE Release 3.2SE	<p>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.</p> <p>The following commands were introduced or modified: aaa server radius dynamic-author, authentication command bounce-port ignore, and authentication command disable-port ignore.</p>



TACACS+ over IPv6

An IPv6 server can be configured to be used with TACACS+.

- [Finding Feature Information, page 37](#)
- [Information About TACACS+ over IPv6, page 37](#)
- [How to Configure TACACS+ over IPv6, page 38](#)
- [Configuration Examples for TACACS+ over IPv6, page 41](#)
- [Additional References, page 42](#)
- [Feature Information for TACACS+ over IPv6, page 42](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see [Bug Search Tool](#) and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

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.

Information About TACACS+ over IPv6

The Terminal Access Controller Access-Control System (TACACS+) security protocol provides centralized validation of users. TACACS+ services are maintained in a database on a TACACS+ daemon typically running on a UNIX or Windows NT workstation. You must have access to and must configure a TACACS+ server before the configured TACACS+ features on your devices are available.

TACACS+ provides for separate authentication, authorization, and accounting facilities. TACACS+ allows for a single access control server (the TACACS+ daemon) to provide each service (authentication, authorization, and accounting) independently. Each service is associated with its own database to take advantage of other services available on that server or on the network, depending on the capabilities of the daemon.

AAA over IPv6

Vendor-specific attributes (VSAs) are used to support Authentication, Authorization and Accounting(AAA) over IPv6. Cisco VSAs are `inacl`, `outacl`, `prefix`, and `route`.

You can configure prefix pools and pool names by using the AAA protocol. Customers can deploy an IPv6 RADIUS server or a TACACS+ server to communicate with Cisco devices.

TACACS+ Over an IPv6 Transport

An IPv6 server can be configured to use TACACS+. Both IPv6 and IPv4 servers can be configured to use TACACS+ using a name instead of an IPv4 or IPv6 address.

How to Configure TACACS+ over IPv6

Configuring the TACACS+ Server over IPv6

SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `tacacs server name`
4. `address ipv6 ipv6-address`
5. `key [0 | 7] key-string`
6. `port [number]`
7. `send-nat-address`
8. `single-connection`
9. `timeout seconds`

DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code> Example: Router> <code>enable</code>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	<code>configure terminal</code> Example: Router# <code>configure terminal</code>	Enters global configuration mode.

	Command or Action	Purpose
Step 3	tacacs server <i>name</i> Example: Router(config)# tacacs server server1	Configures the TACACS+ server for IPv6 and enters TACACS+ server configuration mode.
Step 4	address ipv6 <i>ipv6-address</i> Example: Router(config-server-tacacs)# address ipv6 2001:DB8:3333:4::5	Configures the IPv6 address of the TACACS+ server.
Step 5	key [0 7] <i>key-string</i> Example: Router(config-server-tacacs)# key 0 key1	Configures the per-server encryption key on the TACACS+ server.
Step 6	port [<i>number</i>] Example: Router(config-server-tacacs)# port 12	Specifies the TCP port to be used for TACACS+ connections.
Step 7	send-nat-address Example: Router(config-server-tacacs)# send-nat-address	Sends a client's post-NAT address to the TACACS+ server.
Step 8	single-connection Example: Router(config-server-tacacs)# single-connection	Enables all TACACS packets to be sent to the same server using a single TCP connection.
Step 9	timeout <i>seconds</i> Example: Router(config-server-tacacs)# timeout 10	Configures the time to wait for a reply from the specified TACACS server.

Specifying the Source Address in TACACS+ Packets

SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `ipv6 tacacs source-interface type number`

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p><code>enable</code></p> <p>Example:</p> <pre>Router> enable</pre>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	<p><code>configure terminal</code></p> <p>Example:</p> <pre>Router# configure terminal</pre>	<p>Enters global configuration mode.</p>
Step 3	<p><code>ipv6 tacacs source-interface type number</code></p> <p>Example:</p> <pre>Router(config)# ipv6 tacacs source-interface Ethernet 0/0</pre>	<p>Specifies an interface to use for the source address in TACACS+ packets.</p>

Configuring TACACS+ Server Group Options

SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `aaa group server tacacs+ group-name`
4. `server name server-name`
5. `server-private {ip-address | name | ipv6-address} [nat] [single-connection] [port port-number] [timeout seconds] [key [0 | 7] string]`

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	aaa group server tacacs+ group-name Example: Router(config)# aaa group server tacacs+ group1	Groups different TACACS+ server hosts into distinct lists and distinct methods.
Step 4	server name server-name Example: Router(config-sg-tacacs)# server name server1	Specifies an IPv6 TACACS+ server.
Step 5	server-private {ip-address name ipv6-address} [nat] [single-connection] [port port-number] [timeout seconds] [key [0 7] string] Example: Router(config-sg-tacacs)# server-private 2001:DB8:3333:4::5 port 19 key key1	Configures the IPv6 address of the private TACACS+ server for the group server.

Configuration Examples for TACACS+ over IPv6

Example: Configuring TACACS+ Server over IPv6

```

Device# show tacacs

Tacacs+ Server:          server1
Server Address:         FE80::200:F8FF:FE21:67CF
Socket opens:           0
Socket closes:          0
Socket aborts:          0
Socket errors:          0
Socket Timeouts:        0
Failed Connect Attempts: 0

```

```
Total Packets Sent:      0
Total Packets Recv:     0
```

Additional References

Related Documents

Related Topic	Document Title
IPv6 addressing and connectivity	<i>IPv6 Configuration Guide</i>
Commands	Cisco IOS Master Command List, All Releases
IPv6 commands	Cisco IOS IPv6 Command Reference
IPv6 features	CiscoIOS_IPv6_Feature_Mapping

Standards and RFCs

Standard/RFC	Title
RFCs for IPv6	<i>IPv6 RFCs</i>

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 TACACS+ over IPv6

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 9: Feature Information for TACACS+ over IPv6

Feature Name	Releases	Feature Information
TACACS+ over IPv6	Cisco IOS XE Release 3.2SE	The TACACS+ over IPv6 feature allows you to configure an IPv6 server to use the TACACS+ security protocol. The following commands were introduced or modified: aaa group server tacacs+ , address ipv6 (TACACS+) , ipv6 tacacs source-interface , key (TACACS+) , port (TACACS+) , send-nat-address , server name (IPv6 TACACS+) , server-private (TACACS+) , single-connection , tacacs server , timeout (TACACS+) .

