NAC—Auth Fail Open

First Published: November 17, 2006
Last Updated: November 17, 2006

In network admission control (NAC) deployments, authentication, authorization, and accounting (AAA) servers validate the antivirus status of clients before granting network access. This process is called posture validation. If the AAA server is unreachable, clients will not have access to the network. The NAC—Auth Fail Open feature enables the administrator to apply a policy that allows users to have network access when the AAA server is unreachable. The administrator can configure a global policy that applies to a device, or a rule-based policy that applies to a specific interface.

When the AAA server returns to a reachable status, the posture validation process resumes for clients that are using the NAC—Auth Fail Open policy.

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the "Feature Information for NAC—Auth Fail Open" section on page 29.

Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

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

Contents

Corporate Headquarters
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Prerequisites for NAC—Auth Fail Open

You can configure this feature in networks using NAC and an AAA server for security. NAC is implemented on Cisco IOS routers running Cisco IOS Release 12.3(8)T or a later release.

Restrictions for NAC—Auth Fail Open

To apply local policies to a device or an interface when the AAA server is unreachable, you must configure the **aaa authorization network default local** command.

Information About Network Admission Control

You should understand the following concepts:

Controlling Admission to a Network

NAC protects networks from endpoint devices or clients (such as PCs or servers) that are infected with viruses by enforcing access control policies that prevent infected devices from adversely affecting the network. It checks the antivirus condition (called *posture*) of endpoint systems or clients before granting the devices network access. NAC keeps insecure nodes from infecting the network by denying access to noncompliant devices, placing them in a quarantined network segment or giving them restricted access to computing resources.

NAC enables network access devices (NADs) to permit or deny network hosts access to the network based on the state of the antivirus software on the host. This process is called posture validation.

Posture validation consists of the following actions:

- Checking the antivirus condition or credentials of the client.
- Evaluating the security posture credentials from the network client.
- Providing the appropriate network access policy to the NAD based on the system posture.

Network Admission Control When the AAA Server Is Unreachable

Typical deployments of NAC use a AAA server to validate the client posture and to pass policies to the NAD. If the AAA server is not reachable when the posture validation occurs, the typical response is to deny network access. Using NAC—Auth Fail Open, an administrator can configure a default policy that allows the host at least limited network access while the AAA server is unreachable.

This policy offers these two advantages:

- While AAA is unavailable, the host will still have connectivity to the network, although it may be restricted.

- When the AAA server is once again reachable, users can be revalidated, and their policies can be downloaded from the access control server (ACS).

Note When the AAA server is unreachable, the NAC—Auth Fail Open policy is applied only when there is no existing policy associated with the host. Typically, when the AAA server becomes unreachable during revalidation, the policies already in effect for the host are retained.

How to Configure NAC—Auth Fail Open

You can configure NAC—Auth Fail Open policies per interface, or globally for a device. Configuring NAC—Auth Fail Open is optional, and includes the following tasks:

Configuring a NAC Rule-Associated Policy Globally for a Device

This task creates a NAC rule and associates a policy to be applied while the AAA server is unreachable. You can apply a policy globally to all interfaces on a network access device, if you want to provide the same level of network access to all users who access that device.

Prerequisites

An AAA server must be configured and NAC must be implemented on the NAD.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip admission name** *admission-name* [**eapoudp** [**bypass**] | **proxy** {**ftp** | **http** | **telnet**} | **service-policy type tag** {*service-policy-name*}] [**list** {*acl* | *acl-name*}] [**event**] [**timeout aaa**] [**policy identity** {*identity-policy-name*}]
4. **ip admission** *admission-name* [**event timeout aaa policy identity** *identity-policy-name*]
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip admission name** *admission-name* [**eapoudp** [**bypass**] | **proxy** {**ftp** | **http** | **telnet**} | **service-policy type tag** {*service-policy-name*}] [**list** {*acl* | *acl-name*}] [**event**] [**timeout aaa**] [**policy identity** {*identity-policy-name*}] Example: `Router (config)# ip admission name greentree event timeout aaa policy identity aaa-down`	(Optional) Configures a rule-specific policy globally for the device. If a rule is configured, it will be applied instead of any other global event timeout policy configured on the device. To remove a rule that was applied globally to the device, use the **no** form of the command.
Step 4	**ip admission** *admission-name* [**event timeout aaa policy identity** *identity-policy-name*] **Example:** `Router (config)# ip admission event timeout aaa policy identity AAA_DOWN`	(Optional) Configures the specified IP NAC policy globally for the device. To remove IP NAC policy that was applied to the device, use the **no** form of the command. **Note** This policy will apply only if no rule-specific policy is configured.
Step 5	**end** **Example:** `Router (config)# end`	Exits the global configuration mode.

Applying a NAC Policy to a Specific Interface

An IP admission rule with NAC—Auth Fail Open policies can be attached to an interface. This task attaches a NAC—Auth Fail Open policy to a rule, and applies the rule to a specified interface on a device.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *interface-id*
4. **ip access-group** {*access-list-number* | *name*} **in**
5. **ip admission** *admission-name*
6. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *interface-id* **Example:** `Router (config)# interface fastEthernet 2/1`	Enters interface configuration mode.
Step 4	**ip access-group** {*access-list-number* | *name*} **in** **Example:** `Router (config-if)# ip access-group ACL15 in`	Controls access to the specified interface.
Step 5	**ip admission** *admission-name* **Example:** `Router (config-if)# ip admission AAA_DOWN`	Attaches the globally configured IP admission rule to the specified interface(s). To remove the rule on the interface, use the **no** form of the command.
Step 6	**exit** **Example:** `Router (config)# exit`	Returns to global configuration mode.

Configuring Authentication and Authorization Methods

This task configures the authentication and authorization methods for the device. The access granted using these methods will remain in effect for users who attempt reauthorization while the AAA server is unavailable. These methods must be configured before you configure any policy to be applied to users who try to access the network when the AAA server is unreachable.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa authentication eou default group radius**
5. **aaa authorization network default local**

DETAILED STEPS

	Command or Action	Purpose

Step 1	`enable`
	
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		• Enter your password if prompted.

Step 2	`configure terminal`
	
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

Step 3	`aaa new-model`
	
	Example:
	`Router (config)# aaa new-model`
		Enables AAA.

Step 4	`aaa authentication eou default group radius`
	
	Example:
	`Router (config)# aaa authentication eou default group radius`
		Sets authentication methods for Extensible Authorization Protocol over User Datagram Protocol (EAPoUDP).
		To remove the EAPoUDP authentication methods, use the use the **no** form of the command.

Step 5	`aaa authorization network default local`
	
	Example:
	`Router (config)# aaa authorization network default local`
		Sets the authorization method to local. To remove the authorization method, use the **no** form of the command.

Configuring RADIUS Server Parameters

This task configures the identity and parameters of the RADIUS server that provides AAA services to the network access device. To configure RADIUS server parameters, you should understand the following concepts:

- Identifying the RADIUS Server, page 6
- Determining When the RADIUS Server Is Unavailable, page 7

Identifying the RADIUS Server

A RADIUS server can be identified by:

- hostname
- IP address
- hostname and a specific UDP port number
- IP address and a specific UDP port number

The combination of the RADIUS server IP address and a specific UDP port number creates a unique identifier, which enables RADIUS requests to be sent to multiple UDP ports on a server at the same IP address. If two different host entries on the same RADIUS server are configured for the same service—for example, authentication—the second host entry configured acts as the backup to the first one. The RADIUS host entries are tried in the order that they were configured.

Determining When the RADIUS Server Is Unavailable

Because the NAC—Auth Fail Open feature applies a local policy when the RADIUS server is unavailable, you should configure "dead criteria" that identify when the RADIUS server is unavailable. There are two configurable dead criteria:

- time—the interval (in seconds) without a response to a request for AAA service
- tries—the number of consecutive AAA service requests without a response

If you do not configure the dead criteria, they will be calculated dynamically, based on the server configuration and the number of requests being sent to the server.

You can also configure the number of minutes to wait before attempting to resume communication with a RADIUS server after it has been defined as unavailable.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. r**adius-server dead-criteria** [**time** *seconds*] [**tries** *number-of-tries*]
4. **radius-server deadtime** *minutes*
5. **radius-server host** {*hostname* | *ip-address*} [**test username** *user-name*] [**auth-port** *port-number*] [**ignore-auth-port**] [**acct-port** *port-number*] [**ignore-acct-port**] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*] [**alias** {*hostname* | *ip-address*}] [**idle-time** *seconds*]
6. **radius-server attribute 8 include-in-access-req**
7. **radius-server vsa send** [**accounting** | **authentication**]
8. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**radius-server dead-criteria** [**time** *seconds*] [**tries** *number-of-tries*] **Example:** `Router (config)# radius-server dead-criteria time 30 tries 20`	(Optional) Sets the conditions that are used to decide when a RADIUS server is considered unavailable or *dead*. • The range for *seconds* is from 1 to 120 seconds. The default is that the NAD dynamically determines the *seconds* value within a range from 10 to 60 seconds. • The range for *number-of-tries* is from 1 to 100. The default is that the NAD dynamically determines the *number-of-tries* parameter within a range from 10 to 100.
Step 4	**radius-server deadtime** *minutes* **Example:** `Router (config)# radius-server deadtime 60`	(Optional) Sets the number of minutes that a RADIUS server is not sent requests after it is found to be dead. The range is from 0 to 1440 minutes (24 hours). The default is 0 minutes.

	Command or Action	Purpose
Step 5	**radius-server host** *ip-address* **[acct-port** *udp-port*] [**auth-port** *udp-port*] [**key** *string*] [**test username** *name* [**idle-time** *time*] **Example:** `Router (config)# radius-server host 10.0.0.2 acct-port 1550 auth-port 1560 test username user1 idle-time 30 key abc1234`	(Optional) Configures the RADIUS server parameters by using these keywords: • **acct-port** *udp-port*—Specifies the UDP port for the RADIUS accounting server. The range for the UDP port number is from 0 to 65536. The default is 1646. If the port number is set to 0, the host is not used for accounting. • **auth-port** *udp-port*—Specifies the UDP port for the RADIUS authentication server. The range for the UDP port number is from 0 to 65536. The default is 1645. If the port number is set to 0, the host is not used for authentication. **Note** You should configure the UDP port for the RADIUS accounting server and the UDP port for the RADIUS authentication server to nondefault values. • **key** *string*—Specifies the authentication and encryption key for all RADIUS communication between the NAD and the RADIUS daemon. **Note** Always configure the key as the last item in the **radius-server host** command syntax because leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in the key, do not enclose the key in quotation marks unless the quotation marks are part of the key. This key must match the encryption used on the RADIUS daemon. • **test username** *name*—Enables automated testing of the RADIUS server status, and specify the username to be used. • **idle-time** *time*—Sets the interval of time in minutes after which the NAD sends test packets to the server. The range is from 1 to 35791 minutes. The default is 60 minutes (1 hour). To configure multiple RADIUS servers, reenter this command.
Step 6	`radius-server attribute 8 include-in-access-req` **Example:** `Router (config)# radius-server attribute 8 include-in-access-req`	If the device is connected to nonresponsive hosts, configures the device to send the Framed-IP-Address RADIUS attribute (attribute[8]) in access-request or accounting-request packets. To configure the device to not send the Framed-IP-Address attribute, use the **no radius-server attribute 8 include-in-access-req** global configuration command.

	Command or Action	Purpose
Step 7	**radius-server vsa send authentication** **Example:** `Router (config)# radius-server vsa send authentication`	Configures the network access server to recognize and use vendor-specific attributes (VSAs).
Step 8	**end** **Example:** `Router (config)# end`	Returns to privileged EXEC mode.

Displaying the Status of the Configured AAA Servers

This task displays the status of the AAA servers you have configured for the device.

SUMMARY STEPS

1. **enable**
2. **show aaa servers**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show aaa servers** **Example:** `Router# show aaa servers`	Displays the status of the AAA servers configured for the device.

Displaying the NAC Configuration

This task displays the current NAC configuration for the device.

SUMMARY STEPS

1. **enable**
2. **show ip admission** {[**cacke**] [**configuration**] [**eapoudp**]}

DETAILED STEPS

	Command or Action	Purpose

Step 1	`enable`
	
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		• Enter your password if prompted.

Step 2	`show ip admission configuration`
	
	Example:
	`Router# show ip admission configuration`
		Displays all the IP admission control rules configured for the device.

Displaying the EAPoUDP Configuration

This task displays information about the current EAPoUDP configuration for the device, including any NAC—Auth Fail Open policies in effect.

SUMMARY STEPS

1. **enable**
2. **show eou** {**all** | **authentication** {**clientless** | **eap** | **static**} | **interface** {*interface-type*} | **ip** {*ip-address*} | **mac** {*mac-address*} | **posturetoken** {*name*}} [{**begin** | **exclude** | **include**} *expression*]

DETAILED STEPS

	Command or Action	Purpose

Step 1	`enable`
	
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		• Enter your password if prompted.

Step 2	`show eou ip 10.0.0.1`
	
	Example:
	`Router# show eou ip 10.0.0.1`
		Displays information about the EAPoUDP configuration for the specified interface.

Enabling EOU Logging

A set of new system logs is included in Cisco IOS Release 12.4(11)T. These new logs track the status of the servers defined by the methodlist, and the NAC Auth Fail policy configuration. You should enable EOU logging to generate syslog messages that notify you when the AAA servers defined by the methodlist are unavailable, and display the configuration of the NAC—Auth Fail Open policy. The display shows whether a global or rule-specific policy is configured for the NAD or interface. If no policy is configured, the existing policy is retained.

This task enables EOU logging.

SUMMARY STEPS

1. **configure terminal**
2. **eou logging**

DETAILED STEPS

	Command or Action	Purpose

Step 1	`configure terminal`
	
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

Step 2	`eou logging`
	
	Example:
	`Router (config) # eou logging`
		Enables EOU logging.

Configuration Examples for NAC—Auth Fail Open

This section contains the following examples:

Sample NAC—Auth Fail Open Configuration: Example

The example below shows how to configure the NAC—Auth Fail Open feature:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# ip admission name AAA_DOWN eapoudp event timeout aaa policy identity
global_policy
Switch(config)# aaa new-model
Switch(config)# aaa authorization network default local
Switch(config)# aaa authentication eou default group radius
Switch(config)# identity policy global_policy
Switch(config-identity-policy)# ac
Switch(config-identity-policy)# access-group global_acl
Switch(config)# ip access-list extended global_acl
Switch(config-ext-nacl)# permit ip any any
Switch(config-ext-nacl)# exit
```

Sample RADIUS Server Configuration: Example

The example below shows that the RADIUS server will be considered unreachable after 3 unsuccessful tries:

```
Switch(config)# radius-server host 10.0.0.4 test username administrator idle-time 1 key
sample
Switch(config)# radius-server dead-criteria tries 3
Switch(config)# radius-server deadtime 30
Switch(config)# radius-server vsa send authentication
Switch(config)# radius-server attribute 8 include-in-access-req
Switch(config)# int fastEthernet 2/13
Switch(config-if)# ip admission AAA_DOWN
Switch(config-if)# exit
```

show ip admission configuration Output: Example

The following example shows that a policy called “global policy” has been configured for use when the AAA server is unreachable:

```
Switch# show ip admission configuration

Authentication global cache time is 60 minutes Authentication global absolute time is 0
minutes Authentication global init state time is 2 minutes Authentication Proxy Watch-list
is disabled


Authentication Proxy Rule Configuration

 Auth-proxy name AAA_DOWN

    eapoudp list not specified auth-cache-time 60 minutes

    Identity policy name global_policy for AAA fail policy
```

show eou Output: Example

The example below shows the configuration of the AAA servers defined for a NAC—Auth Fail policy configuration:

```
Router# show eou ip 10.0.0.1

Address : 10.0.0.1
MAC Address : 0001.027c.f364
Interface : Vlan333
! Authtype is show as AAA DOWN when in AAA is not reachable.
AuthType : AAA DOWN
! AAA Down policy name:
AAA Down policy : rule_policy
Audit Session ID : 00000000011C11830000000311000001
PostureToken : -------
Age(min) : 0
URL Redirect : NO URL REDIRECT
URL Redirect ACL : NO URL REDIRECT ACL
ACL Name : rule_acl
Tag Name : NO TAG NAME
User Name : UNKNOWN USER
```

```
Revalidation Period : 500 Seconds
Status Query Period : 300 Seconds
Current State : AAA DOWN
```

show aaa servers Output: Example

The example below shows sample status information for a configured AAA server:

```
Switch# show aaa servers

RADIUS: id 1, priority 1, host 10.0.0.4, auth-port 1645, acct-port 1646

     State: current UP, duration 5122s, previous duration 9s

     Dead: total time 79s, count 3

     Authen: request 158, timeouts 14

             Response: unexpected 1, server error 0, incorrect 0, time 180ms

             Transaction: success 144, failure 1

     Author: request 0, timeouts 0

             Response: unexpected 0, server error 0, incorrect 0, time 0ms

             Transaction: success 0, failure 0

     Account: request 0, timeouts 0

             Response: unexpected 0, server error 0, incorrect 0, time 0ms

             Transaction: success 0, failure 0

     Elapsed time since counters last cleared: 2h13mS
```

EOU Logging Output: Example

The example below shows the display when EOU logging is enabled:

```
Router (config)# eou logging
EOU-5-AAA_DOWN: AAA unreachable.
METHODLIST=Default| HOST=17.0.0.1| POLICY=Existing policy retained.
EOU-5-AAA_DOWN: AAA unreachable.
METHODLIST=Default| HOST=17.0.0.1| POLICY=aaa_unreachable_policy
```

Additional References

The following sections provide references related to the NAC—Auth Fail Open feature.

Related Documents

Related Topic	Document Title
Configuring NAC	*Network Admission Control Software Configuration Guide*
Security commands	*Cisco IOS Security Command Reference*, Release 12.4

Standards

Standard	Title
IEEE 802.1x	IEEE Standard 802.1X - 2004 Port-Based Network Access Control

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	—

Technical Assistance

Description	Link
The Cisco Technical Support & Documentation website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, tools, and technical documentation. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

Command Reference

This section documents modified commands only.

- **ip admission**
- **ip admission name**
- **show eou**
- **show ip admission**

ip admission

To create a Layer 3 network admission control rule to be applied to the interface, or to create a policy that can be applied on an interface when the authentication, authorization and accounting (AAA) server is unreachable, use the **ip admission** command in interface configuration mode. To create a global policy that can be applied on a network access device, use the **ip admission** command with the optional keywords and argument in global configuration mode. To remove the admission control rule, use the **no** form of this command.

ip admission *admission-name* [**event timeout aaa policy identity** *identity-policy-name*]

no ip admission *admission-name* [**event timeout aaa policy identity** *identity-policy-name*]

Syntax Description

admission-name	Authentication or admission rule name.
event timeout aaa policy identity	Specifies an authentication policy to be applied when the AAA server is unreachable.
identity-policy-name	Authentication or admission rule name to be applied when the AAA server is unreachable.

Command Default

A network admission control rule is not applied to the interface.

Command Modes

Interface configuration
Global configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.4(11)T	This command was modified to include the **event timeout aaa policy identity** keywords and the *identity-policy-name* argument.

Usage Guidelines

The admission rule defines how you apply admission control.

The optional keywords and argument define the network admission policy to be applied to a network access device or an interface when no AAA server is reachable. The command can be used to associate a default identity policy with Extensible Authentication Protocol over User Datagram Protocol (EAPoUDP) sessions.

Examples

The following example shows how to apply a network admission control rule named “nacrule1” to the interface:

```
Router (config-if)# ip admission nacrule1
```

The following example shows how to apply an identity policy named “example” to the device when the AAA server is unreachable:

```
Router (config)# ip admission event timeout aaa policy identity example
```

Related Commands

Command	Description
interface	Defines an interface.

ip admission name

To create an IP network admission control rule, use the **ip admission name** command in global configuration mode. To remove the network admission control rule, use the **no** form of this command.

ip admission name *admission-name* [**eapoudp** [**bypass**] | **proxy** {**ftp** | **http** | **telnet**} | **service-policy type tag** {*service-policy-name*}] [**list** {*acl* | *acl-name*}] [**event] [timeout aaa]** [**policy identity** {*identity-policy-name*}]

no ip admission name *admission-name* [**eapoudp** [**bypass**] | **proxy** {**ftp** | **http** | **telnet**} | **service-policy type tag** {*service-policy-name*}] [**list** {*acl* | *acl-name*}] [**event] [timeout aaa]** [**policy identity** {*identity-policy-name*}]

Syntax Description

admission-name	Name of network admission control rule.
eapoudp	(Optional) Specifies IP network admission control using EAPoUDP.
bypass	(Optional) Admission rule bypasses Extensible Authentication Protocol over UDP (EAPoUDP) communication.
proxy	(Optional) Specifies authentication proxy.
ftp	Specifies that FTP is to be used to trigger the authentication proxy.
http	Specifies that HTTP is to be used to trigger authentication proxy.
telnet	Specified that Telnet is to be used to trigger authentication proxy.
service-policy type tag	(Optional) A control plane service policy is to be configured.
service-policy-name	Control plane tag service policy that is configured using the **policy-map type control tag** {*policy name*} command, keyword, and argument. This policy map is used to apply the actions on the host when a tag is received.
list	(Optional) Associates the named rule with an access control list (ACL).
acl	Applies a standard, extended list to a named admission control rule. The value ranges from 1 through 199.
acl-name	Applies a named access list to a named admission control rule.
event	Identifies the condition that triggered the application of the policy.
timeout aaa	(Optional) Specifies that the AAA server is unreachable.
policy identity	Configures the application of an identity policy to be used while the AAA server is unreachable.
identity-policy-name	Specifies the identity policy to apply.

Command Default

An IP network admission control rule is not created.

Command Modes

Global configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.4(6)T	The **bypass** and **service-policy type tag** keywords and *service-policy-name* argument were added.
12.4 (11)T	The **event**, **timeout aaa**, and **policy identity** keywords and the *identity-policy-name* argument were added.

Usage Guidelines

The admission rule defines how you apply admission control.

You can associate the named rule with an ACL, providing control over which hosts use the admission control feature. If no standard access list is defined, the named admission rule intercepts IP traffic from all hosts whose connection-initiating packets are received at the configured interface.

The **bypass** keyword allows an administrator the choice of not having to use the EAPoUDP-based posture validation for the hosts that are trying to connect on the port. The bypass can be used if an administrator knows that the hosts that are connected on the port do not have the Cisco Trust Agent client installed.

The **service-policy type tag** {*service-policy-name*} keywords and argument allow you to associate the service policy of the type tag with the IP admission rule. On the network access device (NAD), a set of policies can be associated with an arbitrary tag string, and if the AAA server sends the same tag in response to the posture validation or authentication response, the policies that are associated with the tag can be applied on the host. The **service-policy** keyword is an optional keyword, and if the service policy is not associated with the IP admission name, the policies that are received from the AAA server are applied on the host.

The **list** keyword option allows you to apply a standard, extended (1 through 199) or named access list to a named admission control rule. IP connections that are initiated by hosts in the access list are intercepted by the admission control feature.

The **event** keyword option allows you to specify the condition that triggered application of an identity policy.

The **timeout aaa** keyword option specifies that the AAA server is unreachable, and this condition is triggering the application of an identity policy.

The **policy identity** keyword and the *identity-policy-name* argument allow you to configure application of an identity policy and specify the policy type to be applied while the AAA server is unreachable.

Examples

"Tag and Template" Feature Examples:

The following example shows that an IP admission control rule is named "greentree" and that it is associated with ACL "101." Any IP traffic that is destined to a previously configured network (using the **access-list** command) will be subjected to antivirus state validation using EAPoUDP.

```
Router (config)# ip admission name greentree eapoudp list 101
```

The following example shows that EAPoUDP bypass has been configured:

```
Router (config)# ip admission name greentree eapoudp bypass list 101
```

In the following service policy example, tags named "healthy" and "non_healthy" can be received from an AAA server, the policy map is defined on the NAD, and the tag policy type is associated with the IP admission name "greentree."

Class Map Definition for the “healthy class” Type Tag

```
Router (config)# class-map type tag healthy_class
Router(config-cmap)# match tag healthy
Router(config-cmap)# end
```

Class Map Definition for the “non_healthy_class” Type Tag

```
Router (config)# class-map type tag non_healthy_class
Router (config-cmap)# match tag non_healthy
Router (config-cmap)# end
```

Policy Map Definition

```
! The following line will be associated with the IP admission name.
Router (config)# policy-map type control tag global_class
! The following line refers to the healthy class map that was defined above.
Router (config-pmap)# class healthy_class
Router (config-pmap-c)# identity policy healthy_policy
Router(config-pmap-c)# exit
The following line refers to the non_healthy class that was defined above.
Router (config-pmap)# class non_healthy_class
Router(config-pmap-c)# identity policy non_healthy_policy
Router (config-pmap-c)# end
```

Identity Policy Definition

```
Router (config)# identity policy healthy_policy
! The following line is the IP access list for healthy users.
Router (config-identity-policy)# access-group healthy
Router (config-identity-policy)# end
Router (config)# identity policy non_healthy_policy
Router (config-identity-policy)# access-group non_healthy
Router (config-identity-policy)# end
```

Defining Access Lists

```
Router (config)# ip access-list extended healthy_class
! The following line can be anything, but as an example, traffic is being allowed.
Router (config-ext-nacl)# permit ip any any
Router (config-ext-nac)# end
Router (config)# ip access-list extended non_healthy_class
! The following line is only an example. In practical cases, you could prevent a user from
accessing specific networks.
Router (config-ext-nacl)# deny ip any any
Router (config-ext-nac)# end
```

Associating the Policy Map with the IP Admission Name

```
Router (config)# ip admission name greentree service-policy type tag global_class
! In the next line, the admission name can be associated with the interface.
Router (config)# interface fastethernet 1/0
Router (config-if)# ip admission greentree
```

In the above configuration, if the AAA server sends a tag named "healthy" or "non_healthy" for any host, the policies that are associated with the appropriate identity policy will be applied on the host.

NAC Auth Fail Open Feature Examples

The following example shows how to define an IP admission control rule named “samplerule” and attach it to a specific interface:

```
Router (config)# ip admission name samplerule eapoudp list 101 event timeout aaa policy
identity aaa_fail_policy
Router (config)# interface fastethernet 1/1
```

```
Router (config-if)# ip admission samplerule
Router (config-if)# end
```

In the above configuration, if the specified interface is not already authorized when the AAA server becomes unreachable, it will operate under the specified policy until revalidation is possible.

Related Commands

Command	Description
ip address	Sets a primary or secondary IP address for an interface.
ip admission event timeout aaa policy identity	Defines a policy to be applied when the AAA server is unreachable.

show eou

To display information about Extensible Authentication Protocol over User Datagram Protocol (EAPoUDP) global values or EAPoUDP session cache entries, use the **show eou** command in privileged EXEC mode.

show eou {**all** | **authentication** {**clientless** | **eap** | **static**} | **interface** {*interface-type*} | **ip** {*ip-address*} | **mac** {*mac-address*} | **posturetoken** {*name*}} [{**begin** | **exclude** | **include**} *expression*]

Syntax Description

all	Displays EAPoUDP information about all clients.
authentication	Authentication type.
clientless	Authentication type is clientless, that is, the endpoint system is not running Cisco Trust Agent (CTA) software.
eap	Authentication type is EAP.
static	Authentication type is statically configured.
interface	Provides information about the interface.
interface-type	Type of interface (see Table 1 for the interface types that may be shown).
ip	Specifies an IP address.
ip-address	IP address of the client device.
mac	Specifies a MAC address.
mac-address	The 48-bit address of the client device.
posturetoken	Displays information about a posture token name.
name	Name of the posture token.
begin	(Optional) Display begins with the line that matches the *expression* argument.
exclude	(Optional) Display excludes lines that match the *expression* argument.
include	(Optional) Display includes lines that match the specified *expression* argument.
expression	(Optional) Expression in the output to use as a reference point.

Command Default

All global EAPoUDP global values are displayed.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.2(18)SXF	This command was integrated into Cisco IOS Release 12.2(18)SXF.
12.2(25)SED	This command was integrated into Cisco IOS Release 12.2(25)SED.

Release	Modification
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.4(11)T	The output of this command was enhanced to display information about whether the session is using the AAA timeout policy.

Usage Guidelines

If you do not specify a port, global parameters and a summary appear. If you specify a port, details for that port appear.

Expressions are case sensitive. For example, if you enter "**exclude output**," the lines that contain "output" are not displayed, but the lines that contain "Output" appear.

Table 1 lists the interface types that may be used for the *interface-type* argument.

Table 1 Description of Interface Types

Interface Type	Description
Async	Asynchronous interface
BVI	Bridge-Group Virtual Interface
CDMA-Ix	Code division multiple access Internet exchange (CDMA Ix) interface
CTunnel	Connectionless Network Protocol (CLNS) tunnel (Ctunnel) interface
Dialer	Dialer interface
Ethernet	IEEE 802.3 standard interface
Lex	Lex interface
Loopback	Loopback interface
MFR	Multilink frame relay bundle interface
Multilink	Multilink-group interface
Null	Null interface
Serial	Serial interface
Tunnel	Tunnel interface
Vif	Pragmatic General Multicast (PGM) Multicase Host interface
Virtual-PPP	Virtual PPP interface
Virtual-Template	Virtual template interface
Virtual-TokenRing	Virtual TokenRing interface

Examples

The following output displays information about a global EAPoUDP configuration. The default values can be changed or customized using the **eou default**, **eou max-retry**, **eou revalidate**, or **eou timeout** commands, depending on whether you configure them globally or on a specific interface.

```
Router# show eou

Global EAPoUDP Configuration

---------------------------

EAPoUDP Version     = 1
```

```
EAPoUDP Port        = 0x5566

Clientless Hosts    = Disabled

IP Station ID       = Disabled

Revalidation        = Enabled

Revalidation Period = 36000 Seconds

ReTransmit Period   = 3 Seconds

StatusQuery Period  = 300 Seconds

Hold Period         = 180 Seconds

AAA Timeout         = 60 Seconds

Max Retries         = 3

EAPoUDP Logging     = Disabled

Clientless Host Username = clientless

Clientless Host Password = clientless


Interface Specific EAPoUDP Configurations

----------------------------------------

Interface Ethernet2/1

  No interface specific configuration
```

Table 2 describes the significant fields shown in the display.

The following output displays information about a global EAPoUDP configuration that includes a NAC Auth Fail Open policy for use when the AAA server is unavailable.

```
Router# show eou ip 10.0.0.1

Address : 10.0.0.1
MAC Address : 0001.027c.f364
Interface : Vlan333
AuthType : AAA DOWN
AAA Down policy : rule_policy
Audit Session ID : 00000000011C11830000000311000001
PostureToken : -------
Age(min) : 0
URL Redirect : NO URL REDIRECT
URL Redirect ACL : NO URL REDIRECT ACL
ACL Name : rule_acl
Tag Name : NO TAG NAME
User Name : UNKNOWN USER
Revalidation Period : 500 Seconds
Status Query Period : 300 Seconds
Current State : AAA DOWN
```

Table 2 describes the significant fields shown in the display.

Table 2 show eou Field Descriptions

Field	Description
EAPoUDP Version	EAPoUDP protocol version.
EAPoUDP Port	EAPoUDP port number.
Clientless Hosts	Clientless hosts are enabled or disabled.
IP Station ID	Specifies whether the IP address is allowed in the AAA station-id field. By default, it is disabled.
Revalidation	Revalidation is enabled or disabled.
Revalidation Period	Specifies whether revalidation of hosts is enabled. By default, it is disabled.
ReTransmit Period	Specifies the EAPoUDP packet retransmission interval. The default is 3 seconds.
StatusQuery Period	Specifies the EAPoUDP status query interval for validated hosts. The default is 300 seconds.
Hold Period	Hold period following a failed authentication.
AAA Timeout	AAA timeout period.
Max Retries	Maximum number of allowable retransmissions.
EAPoUDP Logging	Logging is enabled or disabled.
AAA Down policy	Name of policy to be applied when the AAA server is unreachable. (This is the NAC Auth Fail Open policy.)

Related Commands

Command	Description
eou default	Sets global EAPoUDP parameters to the default values.
eou max-retry	Sets the number of maximum retry attempts for EAPoUDP.
eou rate-limit	Sets the number of simultaneous posture validations for EAPoUDP.
eou timeout	Sets the EAPoUDP timeout values.

show ip admission

To display the network admission control cache entries or the running network admission control configuration, use the **show ip admission** command in privileged EXEC mode.

show ip admission {[**cache**] [**configuration**] [**eapoudp**]}

Syntax Description

cache	Displays the current list of network admission entries.
configuration	Displays the running network admission control configuration.
eapoudp	Displays the Extensible Authentication Protocol over User Datagram Protocol (EAPoUDP) network admission control entries.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.4(11)T	The output of this command was enhanced to display whether the AAA timeout policy is configured.

Usage Guidelines

Use this command to display either the IP admission control entries or the running IP admission control configuration. Use **show ip admission cache eapoudp** to list the host IP addresses, the session timeout, and the posture state. If the posture statue is POSTURE ESTAB, the host validation was successful.

Examples

The following output displays all the IP admission control rules that are configured on the router:

```
Router# show ip admission configuration

Authentication global cache time is 60 minutes
Authentication global absolute time is 0 minutes
Authentication Proxy Watch-list is disabled

Authentication Proxy Rule Configuration
 Auth-proxy name avrule
    eapoudp list not specified auth-cache-time 60 minutes
```

The following output displays the host IP addresses, the session timeout, and the posture states:

```
Router# show ip admission cache eapoudp

Posture Validation Proxy Cache
Total Sessions: 3 Init Sessions: 1
 Client IP 10.0.0.112, timeout 60, posture state POSTURE ESTAB
 Client IP 10.0.0.142, timeout 60, posture state POSTURE INIT
 Client IP 10.0.0.205, timeout 60, posture state POSTURE ESTAB
```

The following output displays a configuration that includes both a global and a rule-specific NAC Auth Fail Open policy:

```
Router# show ip admission configuration

Authentication global cache time is 60 minutes
Authentication global absolute time is 0 minutes
Authentication global init state time is 2 minutes
Authentication Proxy Watch-list is enabled
Watch-list expiry timeout is 1 minutes
! The line below shows the global policy:
Authentication global AAA fail identity policy aaa_fail_policy
Authentication Proxy Rule Configuration Auth-proxy name greentree
    eapoudp list 101 specified auth-cache-time 60 minutes
! The line below shows the rule-specific AAA fail policy; the name changes based on what
the user configured.
    Identity policy name aaa_fail_policy for AAA fail policy
```

The field descriptions in the display are self-explanatory.

Related Commands

Command	Description
clear ip admission cache	Clears IP admission cache entries from the router.
ip admission name	Creates a Layer 3 network admission control rule.

Feature Information for NAC—Auth Fail Open

Table 3 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Cisco IOS software images are specific to a Cisco IOS software release, a feature set, and a platform. Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Note Table 3 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 3 Feature Information for NAC—Auth Fail Open

Feature Name	Releases	Feature Information
NAC—Auth Fail Open	12.2(25)SEE 12.2(31)SG 12.4(11)T	This feature enables the administrator to apply a policy for the host, allowing users to have network access when the AAA server is unreachable. In Cisco IOS Release 12.2(25)SEE, this feature was introduced on the Cisco Catalyst 3750 switch. In Cisco IOS Release 12.2(31)SG, support was added for the Cisco Catalyst 4500 switch. In Cisco IOS Release 124.(11)T, support was added for Cisco routers.