Network Admission Control: Agentless Host Support

First Published: February 27, 2006
Last Updated: February 27, 2006

The Network Admission Control: Agentless Host Support feature allows for an exhaustive examination of agentless hosts (hosts that are not running the Cisco Trust Agent software). This examination allows customers to build a robust host or examination functionality by integrating any third-party audit mechanisms into the Network Admission Control architecture.

This feature also allows for Extensible Authentication Protocol over UDP (EAPoUDP) bypass, which speeds up the posture validation of hosts that are not using Cisco Trust Agent.

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 Network Admission Control: Agentless Host Support" section on page 17.

Finding Support Information for Platforms and Cisco IOS Software Images

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.

Contents

CISCO SYSTEMS

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

Prerequisites for Network Admission Control: Agentless Host Support

- You must be running Cisco IOS Release 12.4(6)T or a later release.
- You must be using a Cisco access control server (ACS) version 4.0 or a later version.
- You must have a Cisco or third-party audit server setup.

Information About Network Admission Control: Agentless Host Support

To configure the Network Admission Control: Agentless Host Support feature, you should understand the following concepts:

Network Admission Control

The Cisco Network Admission Control functionality enables the credentials of the endpoint device to be checked for compliance with the security policy before the device is granted access to network resources. This checking requires a security application called Cisco Trust Agent (CTA) to be installed on end devices that gather security state information and communicate it to access servers where policy decisions are made and eventually enforced on Cisco network access devices (such as routers and switches).

Agentless Hosts

End devices that do not run CTA cannot provide credentials when challenged by network access devices (NADs). Such hosts are termed “agentless” or “nonresponsive.” In the Phase 1 release of Network Admission Control, agentless hosts were supported by either a static configuration using exception lists (an identity profile) or by using “clientless” username and password authentication on an ACS. These methods are restrictive and do not convey any specific information about the host while making policy decisions.

EAPoUDP Bypass

You can use the EAPoUDP Bypass feature to reduce latency of the validation of hosts that are not using CTA. If EAPoUDP bypass is enabled, the NAD does not contact the host to request the antivirus condition (the NAD does not try to establish an EAPoUDP association with the host if the EAPoUDP Bypass option is configured). Instead, the NAD sends a request to the Cisco Secure ACS that includes the IP address, MAC address, service type, and EAPoUDP session ID of the host. The Cisco Secure ACS makes the access control decision and sends the policy to the NAD.

If EAPoUDP bypass is enabled, the NAD sends an agentless host request to the Cisco Secure ACS and applies the access policy from the server to the host.

If EAPoUDP bypass is enabled and the host uses the Cisco Trust Agent, the NAD also sends a nonresponsive-host request to the Cisco Secure ACS and applies the access policy from the server to the host.

Vendor-Specific Attributes for This Feature

The following new attributes are supported for various RADIUS message exhanges:

- audit-session-id, page 3
- url-redirect-acl, page 3

audit-session-id

The audit-session-id vendor-specific attribute (VSA) is a 32-byte string that uniquely identifies a host session. This identifier is generated by a NAD when the host is detected, and it remains the same until the session is deleted. Session revalidation or reinitialization does not change this identifier. Every time a session is detected, a new identifier is generated. This attribute is included in access requests to the authentication, authorization, and accounting (AAA) server and in web requests to the audit server. The value of this attribute is displayed in **show eou** command output (using the **ip** keyword).

url-redirect-acl

The url-redirect-acl VSA string specifies the name of the access control list (ACL) for URL redirection. Any ingress HTTP from the host that matches the access list that is specified by this attribute is subjected to redirection to the URL address specified by the url-redirect VSA. The access list specified in this attribute has to be locally configured on the NAD as an “ip access-list extended” named ACL. This attribute is specified only in RADIUS access-accept messages. The value of the url-redirect-acl attribute is displayed using the **show eou** command (with the **ip** keyword).

Note Phase 1 of the Network Admission Control feature introduced the url-redirect VSA that allowed the HTTP sessions of users to be redirected to the address specified by the url-redirect VSA. This redirection is useful if you want to remediate hosts that do not comply to network security policy. However, to determine to which users HTTP requests are to be redirected, Phase 1 of Network Admission Control assumed that any HTTP traffic that was intercepted and denied by the host policy ACL (the access control server ACL) was subjected to redirection. The url-redirect-acl VSA provides an option so that users can customize the redirect criteria. The url-redirect-acl VSA supports backward compatibility. If the url-redirect-acl is specified in the access-accept message for the host, any user HTTP sessions that

match the ACL are subjected to redirection. However, if the url-redirect-acl attribute is not received, the Phase 1 logic to perform redirection is used. The Phase 1 logic to perform redirection applies only to Cisco IOS routers. The url-redirect-acl attribute is mandatory for Cisco IOS switches.

How to Configure Network Admission Control: Agentless Host Support

This section includes the following required and optional tasks.

- Configuring a NAD to Bypass EAPoUDP Communication, page 4 (required)
- Verifying Agentless Host and EAPoUDP Bypass, page 5 (optional)

Configuring a NAD to Bypass EAPoUDP Communication

To configure a NAD to bypass EAPoUDP, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip admission name** *admission-name* **eapoudp bypass**
4. **eou allow clientless**
5. **interface type** *slot/port*
6. **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** **Example:** `Router (config)# ip admission name greentree eapoudp bypass`	The IP network admission control rule bypasses EAPoUDP communication.

	Command or Action	Purpose
Step 4	**eou allow clientless** **Example:** `Router (config)# eou allow clientless`	Allows authentication of clientless hosts (systems that do not run Cisco Trust Agent).
Step 5	**interface type** *slot/port* **Example:** `Router (config)# interface ethernet 2/4`	Configures an interface type and enters interface configuration mode.
Step 6	**end** **Example:** `Router (config-if)# end`	Exits configuration modes.

Verifying Agentless Host and EAPoUDP Bypass

To verify your configuration for Agentless Host and EOUoUDP Bypass, perform the following steps. The **debug** and **show** commands can be used independently of each other.

SUMMARY STEPS

1. **enable**
2. **debug eou**
3. **show eou ip** *ip-address*
4. **show ip admission configuration**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**debug eou** **Example:** `Router# debug eou`	Displays information about EAUoUDP.
Step 3	**show eou ip** *ip-address* **Example:** `Router# show eou ip 10.0.0.0`	Displays information about EAPoUDP global values or EAPoUDP session cache entries.
Step 4	**show ip admission configuration** **Example:** `Router# show ip admission configuration`	Displays information about the agentless and EAPoUDP Bypass configuration.

Configuration Examples for Network Admission Control: Agentless Host Support

This section provides the following configuration examples.

RADIUS Message Exchange url-redirect-acl VSA: Example

ACS Configuration

```
url-redirect=http://audit-server.com/host_session_id=$host_session_id
url-redirect-acl=RedirectACL
```

NAD Configuration

```
Router(config)# ip access-list extended RedirectACL
Router (config-ext-nacl)# permit tcp any 10.0.0.0 0.0.0.255 eq www
Router (config-ext-nacl)# end
```

Show Output Displaying the Value of a Newly Defined VSA

The following **show eou** command output displays EAPoUPD session cache information for a given IP address. The value of the newly defined VSA is also shown.

```
Router# show eou ip 10.0.0.1

Address              : 10.0.0.1
MAC Address          : 0001.027c.f364
Interface            : FastEthernet1/0/3
AuthType             : EAP
Audit Session ID     : 000000001C8A6A330000001812000001
PostureToken         : Infected
Age(min)             : 444
URL Redirect         : http://wwwin.cisco.com
URL Redirect ACL     : RedirectACL
ACL Name             : #ACSACL#-IP-Infected-42835ff7
User Name            : NAC-DEV-PC-3:Administrator
Revalidation Period  : 30000 Seconds
Status Query Period  : 300 Seconds
Current State        : AUTHENTICATED
```

Additional References

The following sections provide references related to Network Admission Control: Agentless Host.

Related Documents

Related Topic	Document Title
Configuring AAA and RADIUS for EAPoUDP	"Configuring AAA for EAPoUDP" section of the *Network Admission Control* feature guide.
Security commands	*Cisco IOS Security Command Reference*
Network Admission Control	*Network Admission Control* feature guide

Standards

Standard	Title
No new or modified standards are supported by this feature.	—

MIBs

MIB	MIBs Link
No new or modified MIBs are supported 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.	—

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, and tools. 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.

eou clientless

Note This command is removed effective with Cisco IOS Release 12.4(6)T.

To set user group credentials for clientless hosts, use the **eou clientless** command in global configuration mode. To remove the user group credentials, use the **no** form of this command.

eou clientless {**password** *password* | **username** *username*}

no eou clientless {**password** | **username**}

Syntax Description

password *password*	Sets a password.
username *username*	Sets a username.

Defaults

Username and password values are clientless.

Command Modes

Global configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.4(6)T	This command is removed effective with Cisco IOS Release 12.4(6)T.

Usage Guidelines

For this command to be effective, the **eou allow** command must also be enabled.

Examples

The following example shows that a clientless host with the username “user1” has been configured:

```
Router (config)# eou clientless username user1
```

The following example shows that a clientless host with the password “user123” has been configured:

```
Router (config)# eou clientless password user123
```

Related Commands

Command	Description
eou allow	Allows additional EAPoUDP options.

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*}]

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

Defaults

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.

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.

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 Is Defined

```
! 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 Can Be Defined As Follows

```
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
```

Access Lists Can Be Defined As Follows

```
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
```

Policy Map That Was Defined Above Is Associated 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.

Related Commands

Command	Description
ip address	Sets a primary or secondary IP address for an interface.

show eou

To display information about Extensible Authentication Protocol over UDP (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.

Defaults

If no keywords are listed, 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.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.

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 as interface specific.

```
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

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.

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.

Feature Information for Network Admission Control: Agentless Host Support

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 Network Admission Control: Agentless Host Support

Feature Name	Releases	Feature Information
Network Admission Control: Agentless Host Support	12.4(6)T	This feature allows for an exhaustive examination of agentless hosts (hosts that are not running Cisco Trust Agent software), allowing customers to build more robust host or examination functionality by integrating any third-party audit mechanisms into the Network Admission Control architecture. The feature also allows for EAPoUDP bypass, which speeds up the posture validation of hosts that are not using Cisco Trust Agent.