



Network Admission Control

First Published: May 27, 2004

Last Updated: July 19, 2007

The Network Admission Control feature addresses the increased threat and impact of worms and viruses to networked businesses. This feature is part of the Cisco Self-Defending Network Initiative that helps customers identify, prevent, and adapt to security threats.

In its initial phase, the Cisco Network Admission Control (NAC) functionality enables Cisco routers to enforce access privileges when an endpoint attempts to connect to a network. This access decision can be on the basis of information about the endpoint device, such as its current antivirus state. The antivirus state includes information such as version of antivirus software, virus definitions, and version of scan engine.

Network admission control systems allow noncompliant devices to be denied access, placed in a quarantined area, or given restricted access to computing resources, thus keeping insecure nodes from infecting the network.

The key component of the Cisco Network Admission Control program is the Cisco Trust Agent, which resides on an endpoint system and communicates with Cisco routers on the network. The Cisco Trust Agent collects security state information, such as what antivirus software is being used, and communicates this information to Cisco routers. The information is then relayed to a Cisco Secure Access Control Server (ACS) where access control decisions are made. The ACS directs the Cisco router to perform enforcement against the endpoint.

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](#)” section on page 73.

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.



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

© 2006–2007 Cisco Systems, Inc. All rights reserved.

Contents

- [Prerequisites for Network Admission Control, page 2](#)
- [Restrictions for Network Admission Control, page 2](#)
- [Information About Network Admission Control, page 2](#)
- [How to Configure Network Admission Control, page 7](#)
- [Configuration Examples for Network Admission Control, page 22](#)
- [Additional References, page 25](#)
- [Command Reference, page 26](#)
- [Feature Information for Network Admission Control, page 73](#)
- [Glossary, page 75](#)

Prerequisites for Network Admission Control

- You must have a Cisco IOS router that is running Cisco IOS software, Release 12.3(8)T or later.
- You must have Cisco Trust Agent installed on the endpoint devices (for example, on PCs and laptops).
- You must have a Cisco Secure ACS for authentication, authorization, and accounting (AAA).
- You must be familiar with configuring access control lists (ACLs).
- You should be familiar with configuring AAA.

Restrictions for Network Admission Control

- This feature is available only on Cisco IOS firewall feature sets.

Information About Network Admission Control

Before configuring the Network Admission Control feature, you should understand the following concepts:

- [Virus Infections and Their Effect on Networks, page 3](#)
- [How Network Admission Control Works, page 3](#)
- [Network Access Device, page 3](#)
- [Cisco Trust Agent, page 4](#)
- [Cisco Secure ACS, page 4](#)
- [Remediation, page 5](#)
- [Network Admission Control and Authentication Proxy, page 5](#)
- [NAC MIB, page 5](#)

Virus Infections and Their Effect on Networks

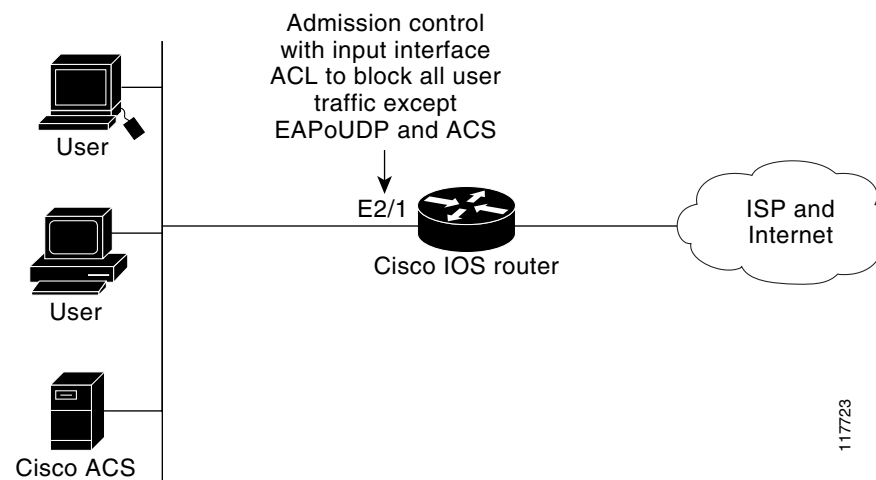
Virus infections are the single largest cause of serious security breaches for networks and often result in huge financial losses. Sources of virus infections are insecure endpoints (for example, PCs, laptops, and servers). Although the endpoints may have antivirus software installed, the software is often disabled. Even if the software is enabled, the endpoints may not have the latest virus definitions and scan engines. A larger security risk is from devices that do not have any antivirus software installed. Although antivirus vendors today are making it more difficult to disable the antivirus software, they are not addressing the risk of outdated virus definitions and scan engines.

How Network Admission Control Works

Endpoint systems, or clients, are normally hosts on the network, such as PCs, laptops, workstations, and servers. The endpoint systems are a potential source of virus infections, and their antivirus states have to be validated before they are granted network access. When an endpoint attempts an IP connection to a network through an upstream Cisco network access device (typically a Cisco IOS router), the router challenges the endpoint for its antivirus state. The endpoint systems run a client called Cisco Trust Agent, which collects antivirus state information from the end device and transports the information to the Cisco network access device. This information is then communicated to a Cisco Secure ACS where the antivirus state of the endpoint is validated and access control decisions are made and returned to Cisco network access devices. The network devices either permit, deny, or quarantine the end device. The Cisco Secure ACS may in turn use back-end antivirus vendor-specific servers for evaluating the antivirus state of the endpoint.

Figure 1 illustrates how Cisco Network Admission Control works.

Figure 1 Cisco IOS Network Admission Control System



Network Access Device

A network access device (NAD) is typically a Cisco IOS router (a Layer 3 Extensible Authentication Protocol over User Datagram Protocol [EAPoUDP] access point) that provides connectivity to external networks, such as the Internet or remote enterprise networks. Cisco Network Admission Control

functionality may have an Intercept ACL, which determines connections that are intercepted for network admission. Connections from endpoints that match the access list are intercepted by Network Admission Control and are challenged for their antivirus states over a Layer 3 association before they are granted network access.

Cisco Trust Agent

Cisco Trust Agent is a specialized software that runs on endpoint systems. Cisco Trust Agent responds to challenges from the router about the antivirus state of an endpoint system. If an endpoint system is not running the Cisco Trust Agent, the network access device (router) classifies the endpoint system as “clientless.” The network access device uses the EOU clientless username and EOU clientless password that are configured on the network access device as the credentials of the endpoint system for validation with Cisco Secure ACS. The policy attributes that are associated with this username are enforced against the endpoint system.

Cisco Secure ACS

Cisco Secure ACS provides authentication, authorization, and accounting services for network admission control using industry-standard RADIUS authentication protocol. Cisco Secure ACS returns access control decisions to the network access device on the basis of the antivirus credentials of the endpoint system.

Using RADIUS `cisco_av_pair` vendor-specific attributes (VSAs), you can set the following attribute-value pairs (AV pairs) on the Cisco Secure ACS. These AV pairs will be sent to the network access device along with other access-control attributes.

- `url-redirect`—Enables the AAA client to intercept an HTTP request and redirect it to a new URL. This redirection is especially useful if the result of posture validation indicates that the network access control endpoint requires an update or patch that you have made available on a remediation web server. For example, a user can be redirected to a remediation web server to download and apply a new virus Directory Administration Tool (DAT) file or an operating system patch. (See the following example.)

```
url-redirect=http://10.1.1.1
```

- `posture-token`—Enables Cisco Secure ACS to send a text version of a system posture token (SPT) that is derived by posture validation. The SPT is always sent in numeric format, and using the `posture-token` AV pair makes it easier to view the result of a posture validation request on the AAA client. (See the following example.)

```
posture-token=Healthy
```

Valid SPTs, in order of best to worst, are as follows:

- Healthy
 - Checkup
 - Quarantine
 - Infected
 - Unknown
- `status-query-timeout`—Overrides the `status-query` default value of the AAA client with the value you specify, in seconds. (See the following example.)

```
status-query-timeout=150
```

For more information about AV pairs that are supported by Cisco IOS software, see the documentation for the releases of Cisco IOS software that are implemented on your AAA clients.

Remediation

Network Admission Control supports HTTP redirection that redirects any HTTP request from the endpoint device to a specified redirect address. This support mechanism redirects all HTTP requests from a source to a specified web page (URL) to which the latest antivirus files can be downloaded. For the HTTP redirection to work, you have to set the value of the “url-redirect” VSA on the ACS and, correspondingly, associate an access control entry in the downloadable ACL that permits the access of the endpoint system to the redirect URL address. After the value of the url-redirect VSA has been set and the access control entry has been associated, any HTTP request that matches the IP admission Intercept ACL will be redirected to the specified redirect URL address.

Network Admission Control and Authentication Proxy

It is possible that network admission control and authentication proxy can be configured for the same set of hosts on a given interface. In each case, the Intercept ACL should be the same for IP admission EAPoUDP and authentication proxy. IP admission proxy with proxy authentication should be configured first, followed by IP admission control.

NAC MIB

The NAC MIB feature adds Simple Network Management Protocol (SNMP) support for the NAC subsystem. Using SNMP commands (get and set operations), an administrator can monitor and control NAC sessions on the network access device (NAD).

For more information about SNMP get and set operations, see the subsection “[Related Documents](#)” in the section “[Additional References](#).”

Correlation Between SNMP Get and Set Operations and the Cisco CLI

Most of the objects in the object tables in the NAC MIB (CISCO-NAC-NAD-MIB.my) describe various EAPoUDP and session parameters that are applicable to the setup of a NAD. These properties can be viewed and modified by performing various SNMP get and set operations. Many of the values of the table objects can also be viewed or modified by configuring corresponding command-line interface (CLI) commands on a router. For example, you can perform an SNMP get operation on the `cnnEOUGlobalObjectsGroup` table or you can configure the `show eou` command on a router. The parameter information obtained from the SNMP get operation is the same as the output from the `show eou` command. Similarly, performing an SNMP get operation on the table `cnnEouIfConfigTable` provides interface-specific parameters that can also be viewed in output from the `show eou` command.

SNMP set operations are allowed for table objects that have corresponding CLI commands, which can be used to modify table object values. For example, to change the value range for the `cnnEouHostValidateAction` object in the `cnnEouHostValidateAction` MIB table to 2, you can either perform the SNMP set operation or configure the `eou initialize all` command on a router.

For examples of NAC MIB output, see the subsection “[NAC MIB Output: Examples](#)” in the section “[Configuration Examples for Network Admission Control](#).”

Initializing and Revalidating Sessions

NAC allows administrators to initialize and revalidate sessions using the following CLI commands:

- **euo initialize all**
- **euo initialize authentication clientless**
- **euo initialize authentication eap**
- **euo initialize authentication static**
- **euo initialize ip** {*ip-address*}
- **euo initialize mac** {*mac-address*}
- **euo initialize posturetoken** {*string*}
- **euo revalidate all**
- **euo revalidate authentication clientless**
- **euo revalidate authentication eap**
- **euo revalidate authentication static**
- **euo revalidate ip** {*ip-address*}
- **euo revalidate mac** {*mac-address*}
- **euo revalidate posturetoken** {*string*}

The initialization and revalidation actions can also be accomplished by performing SNMP set operations on the objects of the `cnnEuoHostValidateAction` table. For more information about initializing and revalidating sessions, see the section [“CLI Commands That Correlate to `cnnEuoHostValidateAction` Table Objects.”](#)

For examples of CLI commands that correlate to changes that can be made to `cnnEuoHostValidateAction` table objects, see the subsection [“NAC MIB Output: Examples”](#) in the section [“Configuration Examples for Network Admission Control.”](#)

Session-Specific Information

The NAC MIB provides a way to view session-specific details using the `cnnEuoHostQueryTable` and `cnnEuoHostResultTable`. The `cnnEuoHostQueryTable` is used to build the query. The query is the same format as the **show euo ip** {*ip-address*} command (that is, the IP address would be shown as in the **show euo ip** command—for example, 10.1.1.1). Administrators must use the SNMP set operation on the objects of the `cnnEuoHostQueryTable` to create the query. The results of the query are stored as a row in the `cnnEuoHostResultTable`. For more information about viewing session-specific details, see the section [“Viewing MIB Query Results.”](#)

Using show Commands to View MIB Object Information

The CLI commands **show euo**, **show euo all**, **show euo authentication**, **show euo initialize**, **show euo ip**, **show euo mac**, **show euo posturetoken**, **show euo revalidate**, and **show ip device tracking all** provide the same output information as that in the CISCO-NAC-NAD-MIB tables using SNMP get operations.

For examples of **show** command output information that can also be viewed in MIB object tables, see the subsection [“NAC MIB Output: Examples”](#) in the section [“Configuration Examples for Network Admission Control.”](#)

How to Configure Network Admission Control

This section contains the following procedures:

- [Configuring the ACL and Admission Control, page 7](#) (required)
- [Configuring Global EAPoUDP Values, page 9](#) (optional)
- [Configuring an Interface-Specific EAPoUDP Association, page 10](#) (optional)
- [Configuring AAA for EAPoUDP, page 11](#) (optional)
- [Configuring the Identity Profile and Policy, page 12](#) (required)
- [Clearing EAPoUDP Sessions That Are Associated with an Interface, page 14](#) (optional)
- [Verifying Network Admission Control, page 15](#) (optional)
- [Troubleshooting Network Admission Control, page 15](#) (optional)
- [Monitoring and Controlling NAC with the CISCO-NAC-NAD-MIB, page 16](#) (optional)

Configuring the ACL and Admission Control

Network admission control is applied in the inbound direction at any interface. Applying network admission control inbound at an interface causes network admission control to intercept the initial IP connections of the intercept end system through the router.

[Figure 1](#) shows that IP admission control is applied at the LAN interface. All network devices must be validated for their antivirus states upon their initial IP connections through the router. Until then, all traffic from endpoint systems (except for EAPoUDP and Cisco Secure ACS traffic) is blocked at the interface.

The endpoint system is then challenged for its antivirus state over an EAPoUDP association. The endpoint system gains access to the network if it complies with the network admission control policy as evaluated by the Cisco Secure ACS. If the endpoint system does not comply, the device is either denied access or quarantined.

To configure an intercept ACL, perform the DETAILED STEPS below.

In this configuration, an intercept ACL is defined as “101,” and the Intercept ACL is associated with the IP admission control rule “greentree.” Any IP traffic that is destined to the 192.50.0.0 network will be subjected to validation. In addition, beginning with Step 5, an intercept ACL is applied inbound to the interface that is associated with network admission control. This ACL typically blocks access to endpoint systems until they are validated. This ACL is referred to as the default access list.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **access-list** *access-list-number* {**permit** | **deny**} *protocol source destination*
4. **ip admission name** *admission-name* [**eapoudp** | **proxy** {**ftp** | **http** | **telnet**}] [**list** {*acl* | *acl-name*}]
5. **interface** *type slot/port*
6. **ip address** *ip-address mask*
7. **ip admission** *admission-name*
8. **exit**

9. **access-list** *access-list-number* {**permit** | **deny**} *protocol source destination*
10. **ip access-group** {*access-list-number* | *access-list-name*} **in**

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p>enable</p> <p>Example: Router> 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: Router# configure terminal</p>	<p>Enters global configuration mode.</p>
Step 3	<p>access-list <i>access-list-number</i> {permit deny} <i>protocol source destination</i></p> <p>Example: Router (config)# access-list 101 permit ip any 192.50.0.0 0.0.0.255</p>	<p>Defines a numbered access list.</p>
Step 4	<p>ip admission name <i>admission-name</i> [eapoudp proxy {ftp http telnet}] [list {<i>acl</i> <i>acl-name</i>}]</p> <p>Example: Router (config)# ip admission name greentree eapoudp list 101</p>	<p>Creates IP network admission control rules. The rules define how you apply admission control. The rules are as follows:</p> <ul style="list-style-type: none"> • eapoudp—Specifies IP network admission control using EAPoUDP. • proxy ftp—Specifies FTP to trigger authentication proxy. • proxy http—Specifies HTTP to trigger authentication proxy. • proxy telnet—Specifies Telnet to trigger authentication proxy. <p>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.</p> <p>The list 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.</p>
Step 5	<p>interface <i>type slot/port</i></p> <p>Example: Router (config)# interface ethernet 2/1</p>	<p>Defines an interface and enters interface configuration mode.</p>

	Command or Action	Purpose
Step 6	<p>ip address <i>ip-address mask</i></p> <p>Example: Router (config-if)# ip address 192.0.0.1 255.255.255.0</p>	Sets a primary or secondary IP address for an interface.
Step 7	<p>ip admission <i>admission-name</i></p> <p>Example: Router (config-if)# ip admission greentree</p>	Applies the named admission control rule at the interface.
Step 8	<p>exit</p> <p>Example: Router (config-if)# exit</p>	Exits interface configuration mode.
Step 9	<p>access-list <i>access-list-number {permit deny}</i> <i>protocol source destination</i></p> <p>Example: Router (config)# access-list 105 permit udp any any or Router (config)# access-list 105 permit ip host 192.168.0.2 any or Router (config)# access-list 105 deny ip any any</p>	<p>Defines a numbered access list.</p> <p>Note In the first two examples (under “Command or Action”), ACL “105” denies all IP traffic except UDP and access to 192.168.0.2 (Cisco Secure ACS).</p> <p>Note In the third example (under “Command or Action,” ACL “105” will be applied on the interface that is configured for network admission control, and access to endpoint systems (except for EAPoUDP traffic and access to Cisco Secure ACS [192.168.0.2 in the example] is blocked until their antivirus states are validated. This ACL (“105”) is referred to as “Interface ACL.”</p>
Step 10	<p>ip access-group <i>{access-list-number access-list-name}</i> in</p> <p>Example: Router (config)# ip access-group 105 in</p>	Controls access to an interface.

Configuring Global EAPoUDP Values

To configure global EAPoUDP values, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **eou {allow | clientless | default | initialize | logging | max-retry | port | rate-limit | revalidate | timeout}**

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	eou { allow clientless default initialize logging max-retry port rate-limit revalidate timeout } Example: Router (config)# eou initialize	Specifies EAPoUDP values. <ul style="list-style-type: none"> For a breakout of available keywords and arguments for the eou command, see the following commands: <ul style="list-style-type: none"> eou allow eou clientless eou default eou initialize eou logging eou max-retry eou port eou rate-limit eou revalidate eou timeout

Configuring an Interface-Specific EAPoUDP Association

To configure an EAPoUDP association that can be changed or customized for a specific interface that is associated with network admission control, perform the following steps.

SUMMARY STEPS

- enable**
- configure terminal**
- interface** *type slot/port*
- eou** [**default** | **max-retry** | **revalidate** | **timeout**]

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 <i>type slot/port</i> Example: Router (config)# interface ethernet 2/1	Defines an interface and enters interface configuration mode.
Step 4	eou [default max-retry revalidate timeout] Example: Router (config-if)# eou revalidate	Enables an EAPoUDP association for a specific interface. • For a breakout of available keywords and arguments for the eou command, see the following commands: – eou default – eou max-retry – eou revalidate – eou timeout

Configuring AAA for EAPoUDP

To set up AAA for EAPoUDP, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa authentication eou default enable group radius**
5. **aaa authorization network default group radius**
6. **radius-server host** {*hostname* | *ip-address*}
7. **radius-server key** {*0 string* | *7 string* | *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 new-model Example: Router (config)# aaa new-model	Enables the AAA access control model.
Step 4	aaa authentication eou default enable group radius Example: Router (config)# aaa authentication eou default enable group radius	Sets authentication lists for an EAPoUDP association.
Step 5	aaa authorization network default group radius Example: Router (config)# aaa authorization network default group radius	Uses the list of all RADIUS servers for authentication.
Step 6	radius-server host {hostname ip-address} Example: Router (config)# radius-server host 192.0.0.40	Specifies a RADIUS server host.
Step 7	radius-server key {0 string 7 string string} Example: Router (config)# radius-server key cisco	Sets the authentication and encryption key for all RADIUS communications between the router and the RADIUS daemon.

Configuring the Identity Profile and Policy

Identity is a common infrastructure that is used to specify local profile and policy configurations. The identity profile allows you to statically authorize or validate individual devices on the basis of IP address, MAC address, or device type. Each statically authenticated device can be associated with a local policy that specifies the network access control attributes. Hosts are added to this “exception list” using the **identity profile** command, and corresponding policies are associated with these hosts using the **identity policy** command.

If the client is part of the identity (that is, the client is on the exception list), the status of the client is set on the basis of the identity configuration. The client does not have to go through the posture validation process, and the associated identity policy is applied for the client.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **identity profile eapoudp**
4. **device {authorize {ip address *ip-address* {policy *policy-name*} | mac-address *mac-address* | type {cisco | ip | phone}} | not-authorize}**
5. **exit**
6. **identity policy *policy-name* [access-group *group-name* | description *line-of-description* | redirect *url* | template [virtual-template *interface-name*]]**
7. **access-group *group-name***
8. **exit**
9. **exit**
10. **ip access-list extended *access-list-name***
11. **{permit | deny} *source source-wildcard destination destination-wildcard***

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	identity profile eapoudp Example: Router (config)# identity profile eapoudp	Creates an identity profile and enters identity profile configuration mode.
Step 4	device {authorize {ip address <i>ip-address</i> {policy <i>policy-name</i>} mac-address <i>mac-address</i> type {cisco ip phone}} not-authorize} Example: Router (config-identity-prof)# device authorize ip address 10.10.142.25 policy bluemoon	Statically authorizes an IP device and applies an associated policy to the device.
Step 5	exit Example: Router (config-identity-prof)# exit	Exits identity profile configuration mode.

	Command or Action	Purpose
Step 6	identity policy <i>policy-name</i> [access-group <i>group-name</i> description <i>line-of-description</i> redirect <i>url</i> template [virtual-template <i>interface-name</i>]] Example: Router (config-identity-prof)# identity policy bluemoon	Creates an identity policy and enters identity policy configuration mode.
Step 7	access-group <i>group-name</i> Example: Router (config-identity-policy)# access-group exempt-acl	Defines network access attributes for the identity policy.
Step 8	exit Example: Router (config-identity-policy)# exit	Exits identity policy configuration mode.
Step 9	exit Example: Router (config-identity-prof)# exit	Exits identity profile configuration mode.
Step 10	ip access-list extended <i>access-list-name</i> Example: Router (config)# ip access-list extended exempt-acl	Defines access control for statically authenticated devices (and enters network access control configuration mode).
Step 11	{permit deny} <i>source source-wildcard</i> <i>destination destination-wildcard</i> Example: Router (config-ext-nacl)# permit ip any 192.50.0.0. 0.0.0.255	Set conditions to allow a packet to pass a named IP access list.

Clearing EAPoUDP Sessions That Are Associated with an Interface

To clear EAPoUDP sessions that are associated with a particular interface or that are on the NAD, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **clear eou all**

DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code> Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	<code>clear eou all</code> Example: Router# clear eou all	Clears all EAPoUDP sessions on the NAD.

Verifying Network Admission Control

To verify EAP and EAPoUDP messages or sessions, perform the following steps. The **show** commands may be used in any order or independent of the other **show** command.

SUMMARY STEPS

1. `enable`
2. `show eou all`
3. `show ip admission eapoudp`

DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code> Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	<code>show eou all</code> Example: Router# show eou all	Displays information about EAPoUDP sessions on the network access device.
Step 3	<code>show ip admission eapoudp</code> Example: Router# show ip admission eapoudp	Displays the network admission control configuration or network admission cache entries.

Troubleshooting Network Admission Control

The following commands may be used to display information about EAP and EAPoUDP messages or sessions. The **debug** commands may be used in any order or independent of the other **debug** commands.

SUMMARY STEPS

1. `enable`
2. `debug eap {all | errors | packets | sm}`
3. `debug eou {all | eap | errors | packets | sm}`
4. `debug ip admission eapoudp`

DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code> Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	<code>debug eap {all errors packets sm}</code> Example: Router# debug eap all	Displays information about EAP messages.
Step 3	<code>debug eou {all eap errors packets sm}</code> Example: Router# debug eou all	Displays information about EAPoUDP messages.
Step 4	<code>debug ip admission eapoudp</code> Example: Router# debug ip admission eapoudp	Displays information about IP admission events.

Monitoring and Controlling NAC with the CISCO-NAC-NAD-MIB

This section includes the following tasks:

- [CLI Commands That Correlate to cnnEouHostValidateAction Table Objects, page 17](#)
- [CLI Commands That Correlate to cnnEouIfConfigTable Objects, page 17](#)
- [CLI Commands That Correlate to cnnEouHostValidateAction Table Objects, page 17](#)
- [Creating MIB Query Tables, page 18](#)
- [Viewing MIB Query Results, page 21](#)

CLI Commands That Correlate to cnnEouGlobalObjectsGroup Table Objects

An SNMP get or set operation can be performed to obtain or change information about value ranges for objects in the `cnnEouGlobalObjectsGroup` table. The same information can be viewed in output from the `show eou` command. [Table 1](#) displays examples of some global configuration objects and the SNMP get and set operations required to obtain or change their values.

For an example of `show eou` command output, see the section “[show eou](#)” [section on page 24](#).

Table 1 *Obtaining and Changing Global Configuration Values Using SNMP Get and Set Operations*

Global Configuration Objects	SNMP Operation
EAPoUDP version	Performs a get operation on the <code>cnnEouVersion</code> object. (The object value will be “1.”)
EAPoUDP port	Performs a get operation on the <code>cnnEouPort</code> object.
Enabling logging (enable EOU logging)	Sets the <code>cnnEouLoggingEnable</code> object. (The object value will be “true.”)

CLI Commands That Correlate to `cnnEouIfConfigTable` Objects

An SNMP get operation is performed to obtain information about value ranges for objects in the `cnnEouIfConfigTable`. The same information can be viewed in output from the `show eou` command. [Table 2](#) displays examples of some interface-specific configuration objects and the SNMP get operations required to obtain their values.

Table 2 *Obtaining Interface-Specific Configuration Values Using SNMP Get Operations*

Interface-Specific Object	SNMP Operation
AAA timeout	Performs a get operation on the <code>cnnEouIfTimeoutAAA</code> object. <ul style="list-style-type: none"> Format: GET <code>cnnEouIfTimeoutAAA.IfIndex</code> You must specify the corresponding index number of the specific interface.
Maximum retries	Performs a get operation on the <code>cnnEouIfMaxRetry</code> object. <ul style="list-style-type: none"> Format: GET <code>cnnEouIfMaxRetry.IfIndex</code>

CLI Commands That Correlate to `cnnEouHostValidateAction` Table Objects

EOU sessions can be initialized or revalidated by the CLI or by using the SNMP set operation on the table `cnnEouHostValidateAction`.

Following are some examples (listed by CLI command) that correlate to MIB objects.

eou initialize all

EOU initialization can be accomplished for all sessions by using the `eou initialize all` command or by using an SNMP set operation on the object `cnnEouHostValidateAction`. This object must be set to the numeric value 2.

eou initialize authentication clientless

EOU initialization can be accomplished for sessions having an authentication type “clientless” using the `eou initialize authentication clientless` command or an SNMP set operation on the object `cnnEouHostValidateAction`. This object must be set to the numeric value 3.

eou initialize ip

EOU initialization can be accomplished for a particular session using the `eou initialize ip {ip-address}` command.

To achieve the same result using an SNMP operation, three objects have to be set in the `cnnEouHostValidateAction` MIB table:

- `cnnEouHostValidateAction`—The value range must be set.
- `cnnEouHostValidateIpAddrType`—The IP address type must be set. This value must be set to IPv4 because IPv4 is currently the only address type supported by NAC. (This value is the type of address being set for the `cnnEouHostValidateIPAddr` object.)
- `cnnEouHostValidateIPAddr`—The IP address must be set.



Note The three MIB objects should be set in a single SNMP set operation.

eou initialize posturetoken

All sessions having a particular posturetoken can be initialized using the **eou initialize posturetoken** {*string*} command. The default value range for this command is 8.

To achieve the same result using an SNMP set operation, you must set the following objects:

- `cnnEouHostValidateAction`—Set this value to 8.
- `cnnEouHostValidatePostureTokenStr`—Set the string value.



Note The two MIB objects should be set in a single SNMP set operation.

Creating MIB Query Tables

The MIB table `cnnEouHostQueryTable` is used to create, or build, MIB queries.

MIB Query Correlating to the CLI `show eou all` Command

To build a query that provides the same results as using the **show eou all** command, perform the following SNMP get operation.

The object `cnnEouHostQueryMask` in the table `cnnEouHostQueryTable` indicates the kind of query. The corresponding value of the `cnnEouHostQueryMask` object in output from the **show eou all** command is 8 (the integer value).

SUMMARY STEPS

1. Set the `cnnEouHostQueryStatus` object to `createandgo`.
2. Set the `cnnEouHostQueryMask` object to 8.
3. Set the `cnnEouHostQueryStatus` object to `active` to indicate that query creation is complete.

DETAILED STEPS

	Command or Action	Purpose
Step 1	Set the <code>cnnEouHostQueryStatus</code> object to <code>createandgo</code> .	Creates a query row.
Step 2	Set the <code>cnnEouHostQueryMask</code> object to 8.	Corresponds in value to the show eou all command.
Step 3	Set the <code>cnnEouHostQueryStatus</code> object to <code>active</code> .	Indicates that you have finished building the query.

**Note**

Examples are not shown in the previous table because the format differs depending on the software you are using.

What to Do Next

View the results. See the section “[Viewing MIB Query Results Correlating to the show eou all Command.](#)”

Viewing MIB Query Results Correlating to the show eou all Command

After the MIB query has been built and you have indicated that you are finished (with the “active” status), the results can be viewed. A query in the `cnnEouHostQueryTable` is represented by a row. The row number is the Query Index. Similarly, the `cnnEouHostResultTable` is composed of result rows. Each row in the `cnnEouHostResultTable` is uniquely identified by a combination of Query Index and Result Index. The results of the `cnnEouHostQueryTable` index and the `cnnEouHostResultTable` have to be matched. Match one row in the Query table to one of the rows in the Result table. For example, if a query that corresponds to a **show** command results in ten sessions, the Result table has ten rows, each row corresponding to a particular session. The first row in the Result table is R1.1. The second row is R1.2, and so on to R1.10. If another query is created in the Query table, and it results in five sessions, five rows are created in the Result table (R2.1, R2.2, R2.3, R2.4, and R2.5).

[Table 3](#) illustrates how the above Query table sessions are mapped to Result table rows.

Table 3 Query Table-to-Result Table Mapping

Query Table	Result Table Rows
Q1 (10 sessions)	R1.1, R1.2, R1.3, R1.4, R1.5, R1.6, R1.7, R1.8, R1.9, R1.10
Q2 (5 sessions)	R2.1, R2.2, R2.3, R2.4, R2.5

Creating the SNMP Query

To create an SNMP query that provides the same information as output from the **show eou ip {ip-address}** command, perform the following steps.

SUMMARY STEPS

1. Set `cnnEouHostQueryStatus` to `createandgo`.
2. Set `cnnEouHostQueryIpAddrType` to `IPv4` and the IP address (for example, `10.2.3.4`).
3. Set `cnnEouHostQueryStatus` to `active`.

DETAILED STEPS

	Command or Action	Purpose
Step 1	Set <code>cnnEouHostQueryStatus</code> to <code>createandgo</code> .	Creates a query row.
Step 2	Set <code>cnnEouHostQueryIpAddrType</code> to <code>IPv4</code> and the IP address (for example, 10.2.3.4).	Sets the address type. <ul style="list-style-type: none"> The only address type currently supported by NAC is IPv4.
Step 3	Set <code>cnnEouHostQueryStatus</code> to <code>active</code> .	Indicates you have finished building the query.



Note

Examples are not shown in the previous table because the format differs depending on the software you are using.

Viewing the Results

To view the results in the `cnnEouHostResultTable`, perform the following steps.

SUMMARY STEPS

1. Perform a get operation on `cnnEouHostQueryRows`.
2. Perform a get operation on the `cnnEouHostResultTable` objects in the format `resultTableObjectName.QueryIndex.ResultIndex`.

DETAILED STEPS

	Command or Action	Purpose
Step 1	Perform a get operation on <code>cnnEouHostQueryRows</code> .	Finds how many rows will be created in a Result table for a particular query. <ul style="list-style-type: none"> If a query row is a negative number, the query is still being processed.
Step 2	Perform a get operation on the <code>cnnEouHostResultTable</code> objects in the format <code>resultTableObjectName.QueryIndex.ResultIndex</code> .	Finds the value of a particular object in a Result table that matches a particular query. <ul style="list-style-type: none"> For multiple rows in the Result table for a single query, the <code>ResultIndex</code> ranges from 1 to the value of <code>cnnEouHostQueryRows</code>.



Note

Examples are not shown in the above table because the format differs depending on the software you are using.

MIB Query Correlating to the `show eou ip` Command

To build a MIB query that provides the same results as the `show eou ip {ip-address}` command, perform the following SNMP get operation.

SUMMARY STEPS

1. Set the `cnnEouHostQueryStatus` object to `createandgo`.
2. Set the `cnnEouHostQueryIpAddrType` object to “IPv4”.
3. Set the `cnnEouHostQueryIpAddr` object to IP address (for example, 10.2.3.4).
4. Set the `cnnEouHostQueryStatus` object to `active`.

DETAILED STEPS

	Command or Action	Purpose
Step 1	Set the <code>cnnEouHostQueryStatus</code> object to <code>createandgo</code> .	Sets the query status.
Step 2	Set the <code>cnnEouHostQueryIpAddrType</code> object to “IPv4”.	Sets the address type. Note The only address type currently supported by NAC is IPv4.
Step 3	Set the <code>cnnEouHostQueryIpAddr</code> object to IP address (for example, 10.2.3.4).	Sets the IP address.
Step 4	Set the <code>cnnEouHostQueryStatus</code> object to <code>active</code> .	Indicates that you have finished building the query.



Note

Examples are not shown in the previous table because the format differs depending on the software you are using.

Viewing MIB Query Results

After the MIB query has been built, the results can be viewed in `cnnEouHostResultTable`. For information about how to review the results, see the subsection “[Viewing MIB Query Results Correlating to the `show eou all` Command](#)” in the previous section “[Creating MIB Query Tables](#).”

Splitting a Query into Subqueries

If you are doing a MIB query that correlates to the `show eou all` command, there could possibly be as many as 2,000 rows of output. To ensure that you can view all the information in a MIB query, you can split the query into subqueries. For example, for a query having 2,000 rows of output, you could split the query into four subqueries to view the results in a page-by-page format. The first subquery would include rows 1 through 500 (the first 500 sessions); the second subquery would include rows 501 through 1,000; the third subquery would include rows 1,001 through 1,500; and the fourth subquery would include rows 1,501 through 2,000.



Note

The `cnnEouHostQueryTotalHosts` object provides the total number of hosts (number of rows) that match a query criterion. By looking at this number, you can determine how many subqueries are necessary. However, you cannot get the `cnnEouHostQueryTotalHosts` object number until you have built your first query.

Build your query by performing the following steps.

SUMMARY STEPS

1. Set the `cnnEouHostQueryStatus` object to `createandgo`.
2. Set the `cnnEouHostQueryMask` object to 8.
3. Set `cnnEouHostQueryRows` to 500.
4. Set `cnnEouHostQuerySkipNHosts` to 0.
5. Set the `cnnEouHostQueryStatus` object to `active`.

DETAILED STEPS

	Command or Action	Purpose
Step 1	Set the <code>cnnEouHostQueryStatus</code> object to <code>createandgo</code> .	Sets the query status.
Step 2	Set the <code>cnnEouHostQueryMask</code> object to 8.	Correlates to the default of the show eou all command.
Step 3	Set <code>cnnEouHostQueryRows</code> to 500.	Identifies the maximum number of rows to be built in the result table for this query.
Step 4	Set <code>cnnEouHostQuerySkipNHosts</code> to 0.	Corresponds to the result rows to be created.
Step 5	Set the <code>cnnEouHostQueryStatus</code> object to <code>active</code> .	Indicates that you have finished building the query.



Note

Examples are not shown in the previous table because the format differs depending on the software you are using. The table is on the basis of a query having 2,000 sessions (rows).

What to Do Next

After you have performed the above task, you will have query information for the first 500 hosts (rows). To view query information for the next 500 hosts (rows), you have to perform the same five steps, but you must change the Step 4 (`cnnEouHostQuerySkipNHosts` object) value to 500. This task will result in query information for rows 501 through 1000. In the same way, to obtain query information for the remaining hosts (through 2000), you have to perform the same five steps again but with `cnnEouHostQuerySkipNHosts` object values of 1000 and 1500, respectively.

Configuration Examples for Network Admission Control

This section includes the following example.

- [Network Admission Control: Example, page 22](#)
- [NAC MIB Output: Examples, page 24](#)

Network Admission Control: Example

The following output example shows that IP admission control has been configured on a Cisco IOS router:

```
Router# show running-config
```

```
Building configuration...

Current configuration: 1240 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
boot-start-marker
boot-end-marker
!
aaa new-model
!
!
aaa authentication eou default group radius
aaa session-id common
ip subnet-zero
ip cef
!
! The following line creates a network admission rule. A list is not specified; therefore,
! the rule intercepts all traffic on the applied interface.
ip admission name avrule eapoudp
!
eou logging
!
!
interface FastEthernet0/0
 ip address 10.13.11.106 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 10.0.0.1 255.255.255.0
 ip access-group 102 in
! The following line configures an IP admission control interface.
 ip admission avrule
 duplex auto
 speed auto
!
ip http server
no ip http secure-server
ip classless
!
!
! The following lines configure an interface access list that allows EAPoUDP traffic
! and blocks the rest of the traffic until it is validated.
access-list 102 permit udp any any eq 21862
access-list 102 deny ip any any
!
!
! The following line configures RADIUS.
radius-server host 10.13.11.105 auth-port 1645 acct-port 1646 key cisco
!
control-plane
!
!
!
line con 0
 exec-timeout 0 0
line aux 0
```

```

line vty 0 4
!
!
end

```

NAC MIB Output: Examples

The following are examples of **show** command output displaying MIB object information.

show eou

The **show eou** command provides output for information that can also be viewed in various CISCO-NAC-NAD-MIB tables. The information that follows the **show eou** command can also be found in the `cnnEouGlobalObjectsGroup` table and the information that follows the **show eou all** command can be found in the `cnnEouIfConfigTable`.

```
Router# show eou
```

```

Global EAPoUDP Configuration
-----
EAPoUDP Version      = 1
EAPoUDP Port         = 0x5566
Clientless Hosts     = Enabled
IP Station ID        = Disabled
Revalidation         = Enabled
Revalidation Period  = 36000 Seconds
ReTransmit Period    = 3 Seconds
StatusQuery Period   = 300 Seconds
Hold Period          = 30 Seconds
AAA Timeout          = 60 Seconds
Max Retries          = 3
EAP Rate Limit       = 20
EAPoUDP Logging      = Enabled
Clientless Host Username = clientless
Clientless Host Password = clientless

```

```
Router# show eou all
```

```

Interface Specific EAPoUDP Configurations
-----
Interface Vlan333
AAA Timeout          = 60 Seconds
Max Retries          = 3
eou initialize interface {interface-name}
eou revalidate interface {interface-name}

```

show ip device tracking all

The **show ip device tracking all** command provides output for information that can also be found in the `cnnIpDeviceTrackingObjectsGroup` MIB table. The following is an example of such **show** command output:

```

Router# show ip device tracking all

IP Device Tracking = Enabled
Probe Count: 2
Probe Interval: 10

```

Additional References

The following sections provide references related to Network Admission Control.

Related Documents

Related Topic	Document Title
Configuring ACLs	“ Access Control Lists: Overview and Guidelines ” chapter of the “Traffic Filtering and Firewalls” section of the <i>Cisco IOS Security Configuration Guide</i> , Release 12.3.
Authentication, authorization, and accounting	“ Authentication, Authorization, and Accounting ” section of <i>Cisco IOS Security Configuration Guide</i> , Release 12.3.
Interfaces, configuring	<i>Cisco IOS Interface and Hardware Component Configuration Guide</i> , Release 12.3.
SNMP and SNMP get and set operations	<ul style="list-style-type: none"> “Simple Network Management Protocol” section of the <i>Internetworking Technology Handbook</i> “Configuring SNMP Support” section of the <i>Cisco IOS Configuring Fundamentals Configuration Guide</i>, Release 12.4.

Standards

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

MIBs

MIBs	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

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

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register on Cisco.com.</p>	<p>http://www.cisco.com/techsupport</p>

Command Reference

This section documents only commands that are new or modified:

New

- [aaa authentication eou default enable group radius](#)
- [access-group \(identity policy\)](#)
- [auth-type](#)
- [clear eou](#)
- [clear ip admission cache](#)
- [debug eap](#)
- [debug eou](#)
- [debug ip admission eapoudp](#)
- [description \(identity policy\)](#)
- [eou allow](#)
- [eou clientless](#)
- [eou default](#)
- [eou initialize](#)
- [eou logging](#)
- [eou max-retry](#)
- [eou port](#)
- [eou rate-limit](#)
- [eou revalidate](#)
- [eou timeout](#)
- [identity policy](#)
- [identity profile eapoudp](#)
- [ip admission](#)
- [ip admission name](#)

- [redirect \(identity policy\)](#)
- [show eou](#)
- [show ip admission](#)
- [show ip device tracking](#)
- [template \(identity policy\)](#)

Modified

- [description \(identity profile\)](#)
- [device \(identity profile\)](#)

aaa authentication eou default enable group radius

To set authentication lists for Extensible Authentication Protocol over UDP (EAPoUDP), use the **aaa authentication eou default enable group radius** command in global configuration mode. To remove the authentication lists, use the **no** form of this command.

aaa authentication eou default enable group radius

no aaa authentication eou default enable group radius

Syntax Description This command has no arguments or keywords.

Defaults Authentication lists for EAPoUDP are not set.

Command Modes Global configuration

Command History	Release	Modification
	12.3(8)T	This command was introduced.

Examples The following example shows that authentication lists have been set for EAPoUDP:

```
Router (config)# aaa new-model
Router (config)# aaa authentication eou default enable group radius
```

Related Commands	Command	Description
	eou	Provides information about EAPoUDP.
	ip admission	Creates a Layer 3 network admission control rule to be applied to the interface.

access-group (identity policy)

To specify an access group to be applied to an identity policy, use the **access-group** command in identity policy configuration mode. To remove the access group, use the **no** form of this command.

```
access-group group-name
```

```
no access-group group-name
```

Syntax Description

<i>group-name</i>	Access list name.
-------------------	-------------------

Defaults

An access group is not specified.

Command Modes

Identity policy configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

Using this command, you can access only named access lists.

Examples

The following example shows that access group “exempt-acl” is to be applied to the identity policy “bluemoon”:

```
Router (config)# identity policy bluemoon  
Router (config-identity-policy)# access-group exempt-acl
```

Related Commands

Command	Description
identity profile	Creates an identity profile.

auth-type

To set policy for devices that are dynamically authenticated or unauthenticated, use the **auth-type** command in identity profile configuration mode. To remove the policy that was specified, use the **no** form of this command.

auth-type {**authorize** | **not-authorize**} **policy** *policy-name*

no auth-type {**authorize** | **not-authorize**} **policy** *policy-name*

Syntax Description

authorize	Policy is specified for all authorized devices.
not-authorize	Policy is specified for all unauthorized devices.
policy <i>policy-name</i>	Specifies the name of the identity policy to apply for the associated authentication result.

Defaults

A policy is not set for authorized or unauthorized devices.

Command Modes

Identity profile configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

This command is used when a device is dynamically authenticated or unauthenticated by the network access device, and the device requires the name of the policy that should be applied for that authentication result.

Examples

The following example shows that 802.1x authentication applies to the identity policy “grant” for all dynamically authenticated hosts:

```
Router (config)# ip access-list extended allow-acl
Router (config-ext-nacl)# permit ip any any
Router (config-ext-nacl)# exit

Router (config)# identity policy grant
Router (config-identity-policy)# access-group allow-acl
Router (config-identity-policy)# exit

Router (config)# identity profile dot1x
Router (config-identity-prof)# auth-type authorize policy grant
```

Related Commands	Command	Description
	identity policy	Creates an identity policy.
	identity profile dot1x	Creates an 802.1x identity profile.

clear eou

To clear all client device entries that are associated with a particular interface or that are on the network access device (NAD), use the **clear eou** command in privileged EXEC mode.

```
clear eou {all | authentication {clientless | eap | static} | interface {interface-type} | ip
  {ip-address} | mac {mac-address} | posturetoken {name}}
```

Syntax Description

all	Clears all client device entries.
authentication	Authentication type.
clientless	Authentication type is clientless.
eap	Authentication type is Extensible Authentication Protocol (EAP).
static	Authentication type is static.
interface	Provides information about the interface.
<i>interface-type</i>	Type of interface (see Table 4 for a list of interface types).
ip	Specifies an IP address.
<i>ip-address</i>	IP address of the client device.
mac	Specifies a MAC address.
<i>mac-address</i>	The 48-bit address of the client device.
posturetoken	Posture token name.
<i>name</i>	Name of the posture token.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

[Table 4](#) lists the interface types that may be used for the *interface-type* argument.

Table 4 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

Table 4 *Description of Interface Types (continued)*

Interface Type	Description
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) Multicast Host interface
Virtual-PPP	Virtual PPP interface
Virtual-Template	Virtual template interface
Virtual-TokenRing	Virtual TokenRing interface

Examples

The following example shows that all client device entries are to be cleared:

```
Router# clear eou all
```

Related Commands

Command	Description
eou	Displays information about EAPoUDP.

clear ip admission cache

To clear IP admission cache entries from the router, use the **clear ip admission cache** command in privileged EXEC mode.

```
clear ip admission cache {* | host ip address}
```

Syntax Description		
*		Clears all IP admission cache entries and associated dynamic access lists.
host ip address		Clears all IP admission cache entries and associated dynamic access lists for the specified host.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.3(8)T	This command was introduced.

Usage Guidelines Use this command to clear entries from the admission control cache before they time out.

Examples The following example shows that all admission entries are to be deleted:

```
Router# clear ip admission cache *
```

The following example shows that the authentication proxy entry for the host with the IP address 192.168.4.5 is to be deleted:

```
Router# clear ip admission cache 192.168.4.5
```

Related Commands	Command	Description
	show ip admission cache	Displays the admission control entries or the running admission control configuration.

debug eap

To display information about Extensible Authentication Protocol (EAP), use the **debug eap** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

```
debug eap [all | method] [authenticator | peer ] {all | errors | events | packets | sm}
```

```
no debug eap [all | method] [authenticator | peer ] {all | errors | events | packets | sm}
```

Syntax Description

all <i>method</i>	(Optional) Specifies the method to which the debug command refers. <ul style="list-style-type: none"> The all keyword turns on debugging for all EAP methods, including the EAP framework. The <i>method</i> argument turns on debugging for specific methods. This keyword or argument is dynamically linked into the parse chain and is present only if the method itself is present. If this keyword or argument is omitted, the debug command is applied to the EAP framework.
authenticator	(Optional) Limits the scope of the output to only authenticator contexts.
peer	(Optional) Limits the scope of the output to only peer contexts.
all	Debugging is turned on for all debug types.
errors	Displays information about EAP packet errors.
events	Displays information about EAP events.
packets	Turns on packet debugging for the specified method or methods.
sm	Turns on state machine debugging for the specified method or methods.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.4(6)T	The <i>method</i> argument and authenticator and peer keywords were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

The following sample output from the **debug eap all** command shows all EAP information:

```
Router# debug eap all

*Nov 7 13:05:58.512: EAP-EVENT: Received get canned status from lower layer (0x00000000)
*Nov 7 13:05:59.460: EAP-EVENT: Received context create from lower layer (0x00000009)
*Nov 7 13:05:59.460: eap_authen : initial state eap_auth_initialize has enter
*Nov 7 13:05:59.460: EAP-EVENT: Started 'Authenticator Start' timer (1s) for EAP session
handle 0xD6000008
*Nov 7 13:05:59.460: EAP-EVENT: Allocated new EAP context (handle = 0xD6000008)
*Nov 7 13:05:59.464: EAP-EVENT: Started EAP tick timer
```

debug eap

```
*Nov 7 13:06:00.488: EAP-EVENT: 'Authenticator Start' timer expired for EAP sesion handle
0xD6000008
*Nov 7 13:06:00.488:      eap_authen : during state eap_auth_initialize, got event
21(eapStartTmo)
*Nov 7 13:06:00.488: @@@ eap_authen : eap_auth_initialize -> eap_auth_select_action
*Nov 7 13:06:00.488:      eap_authen : during state eap_auth_select_action, got event
17(eapDecisionPropose)
*Nov 7 13:06:00.488: @@@ eap_authen : eap_auth_select_action -> eap_auth_propose_method
```

Related Commands

Command	Description
debug eou	Displays information about EAPoUDP.

debug eou

To display information about Extensible Authentication Protocol over User Datagram Protocol (UDP) (EAPoUDP), use the **debug eou** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

```
debug eou {all | eap | errors | events | packets | ratelimit | sm}
```

```
no debug eou {all | eap | errors | events | packets | ratelimit | sm}
```

Syntax Description

all	Displays all EAPoUDP information.
eap	Displays EAPoUDP packets.
errors	Displays information about EAPoUDP packet errors.
events	Displays information about EAPoUDP events.
packets	Displays EAPoUDP packet-related information.
ratelimit	Displays EAPoUDP posture-validation information.
sm	Displays EAPoUDP state machine transitions.

Defaults

If you do not enter any keywords, debugging is turned on for all EAPoUDP messages.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

The following sample output from the **debug eou all** command shows all EAPoUDP information:

```
Router# debug eou all

*Apr  9 19:30:40.782: eou-ev:EOU Init Validation for idb= FastEthernet0/0.420 src_mac=
0001.027c.f364 src_ip= 10.0.0.1
*Apr  9 19:30:40.786:      eou_auth 10.0.0.1: initial state eou_initialize has enter
*Apr  9 19:30:40.786: @@@ eou_auth 10.0.0.1: eou_initialize -> eou_hello
*Apr  9 19:30:40.786: eou-ev:eou_send_hello_request: Send Hello Request host= 10.0.0.15
eou_port= 5566 (hex)

*Apr  9 19:30:40.790: EAPoUDP (tx) Flags:0 Ver=1 opcode=2 Len=8 MsgId=3839857370 Assoc
ID=0
*Apr  9 19:30:40.790: Dumping TLV contents
*Apr  9 19:30:40.790: TLV M:1 R:0 Type=ASSOCIATION ID Length=4 Association=-1994800267
*Apr  9 19:30:40.999: EAPoUDP (rx) Flags:128 Ver=1 opcode=2 Len=24 MsgId=3839857370 Assoc
ID=2300167029
*Apr  9 19:30:40.999: Dumping TLV contents
```

■ debug eou

```

*Apr  9 19:30:40.999: TLV M:1 R:0 Type=COOKIE PAYLOAD Length=12
07167CE0:          8919C375 259B6D41 5FEA5D27      ..Cu%.mA_j]'
07167CF0:
*Apr  9 19:30:40.999: TLV M:1 R:0 Type=ASSOCIATION ID Length=4 Association=1016688999

*Apr  9 19:31:50.048: @@@ eou_auth 10.0.0.1: eou_eap -> eou_eap
*Apr  9 19:31:50.048: eou-ev:10.0.0.1: msg = 24(eventEouEapSuccess)
*Apr  9 19:31:50.048:      eou_auth 10.0.0.1: during state eou_eap, got event
14(eouEapSuccess)
*Apr  9 19:31:50.048: @@@ eou_auth 10.0.0.1: eou_eap -> eou_result
*Apr  9 19:31:50.052: eou-ev:Starting RESULT timer 3(10.0.0.1)

```

Related Commands

Command	Description
debug eap	Displays information about EAP messages.
debug ip admission eapudp	Displays information about EAPoUDP network admission control events.

debug ip admission eapoudp

To display information about Extensible Authentication Protocol over User Datagram Protocol (UDP) (EAPoUDP) network admission control events, use the **debug ip admission eapoudp** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug ip admission eapoudp

no debug ip admission eapoudp

Syntax Description This command has no arguments or keywords.

Defaults Debugging is not enabled.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.3(8)T	This command was introduced.

Examples The following sample output from the **debug ip admission eapoudp** command shows information about network admission control using EAPoUDP. In the command output, the term “posture” refers to the credentials (for example, antivirus state or version of Cisco IOS software) of the host system.

```
Router# debug ip admission eapoudp

Posture validation session created for client mac= 0001.027c.f364 ip= 10.0.0.1
Total Posture sessions= 1 Total Posture Init sessions= 1
*Apr  9 19:39:45.684: %AP-6-POSTURE_START_VALIDATION: IP=10.0.0.1|
Interface=FastEthernet0/0.420
*Apr  9 19:40:42.292: %AP-6-POSTURE_STATE_CHANGE: IP=10.0.0.1| STATE=POSTURE ESTAB
*Apr  9 19:40:42.292: auth_proxy_posture_parse_aaa_attributes:
CiscoDefined-ACL name= #ACSACL#-IP-HealthyACL-40921e54
Apr  9 19:40:42.957: %AP-6-POSTURE_POLICY: Apply access control list
(xACSACLx-IP-HealthyACL-40921e54) policy for host (10.0.0.1)
```

The fields in the display are self-explanatory.

Related Commands	Command	Description
	show ip admission	Displays IP admission control cache entries or the running admission control configuration.

description (identity policy)

To enter a description for an identity policy, use the **description** command in identity policy configuration mode. To remove the description, use the **no** form of this command.

description *line-of-description*

no description *line-of-description*

Syntax Description	<i>line-of-description</i>	Description of the identity policy.
--------------------	----------------------------	-------------------------------------

Defaults	A description is not entered for the identity policy.
----------	-------------------------------------------------------

Command Modes	Identity policy configuration
---------------	-------------------------------

Command History	Release	Modification
	12.3(8)T	This command was introduced.

Examples	The following example shows that a default identity policy and its description (“bluemoon”) have been specified:
----------	------------------------------------------------------------------------------------------------------------------

```
Router (config)# identity policy bluemoon
Router (config-identity-policy)# description policyABC
```

Related Commands	Command	Description
	description (identity profile)	Enters a description for an identity profile.

description (identity profile)

To enter a description for an identity profile, use the **description** command in identity profile configuration mode. To remove the description of the identity profile, use the **no** form of this command.

description *line-of-description*

no description *line-of-description*

Syntax Description

<i>line-of-description</i>	Description of the identity profile.
----------------------------	--------------------------------------

Defaults

A description is not entered for the identity profile.

Command Modes

Identity profile configuration

Command History

Release	Modification
12.3(2)XA	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.3(8)T	This command was previously configured in dot1x configuration mode.

Usage Guidelines

The **identity profile** command and one of its keywords (**default**, **dot1x**, or **eapoudp**) must be entered in global configuration mode before the **description** command can be used.

Examples

The following example shows that a default identity profile and its description (“ourdefaultpolicy”) have been specified:

```
Router (config)# identity profile default
Router (config-identity-prof)# description ourdefaultpolicy
```

Related Commands

Command	Description
description (identity policy)	Enters a description for an identity policy.
identity profile	Creates an identity profile and enters identity profile configuration mode.

device (identity profile)

To statically authorize or reject individual devices, use the **device** command in identity profile configuration mode. To disable the authorization or rejection, use the **no** form of this command.

```
device {authorize {ip address ip-address policy policy-name | mac-address mac-address | type
{cisco | ip | phone}} | not-authorize}
```

```
no device {authorize {ip address ip-address policy policy-name | mac-address mac-address | type
{cisco | ip | phone}} | not-authorize}
```

Syntax Description

authorize	Configures an authorized device.
ip address	Specifies a device by its IP address.
<i>ip-address</i>	The IP address.
policy	Applies an associated policy with the device.
<i>policy-name</i>	Name of the policy.
mac-address	Specifies a device by its MAC address.
<i>mac-address</i>	The MAC address.
type	Specifies a device by its type.
cisco	Specifies a Cisco device.
ip	Specifies an IP device.
phone	Specifies a Cisco IP phone.
not-authorize	Configures an unauthorized device.

Defaults

A device is not statically authorized or rejected.

Command Modes

Identity profile configuration

Command History

Release	Modification
12.3(2)XA	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.3(8)T	The unauthorize keyword was changed to not authorize . The <i>cisco-device</i> argument was deleted. The ip address keyword and <i>ip-address</i> argument were added. The ip and phone keywords were added.

Usage Guidelines

The **identity profile** command and **default**, **dot1x**, or **eapoudp** keywords must be entered in global configuration mode before the **device** command can be used.

Examples

The following configuration example defines an identity profile for Extensible Authentication Protocol over User Datagram Protocol (EAPoUDP) to statically authorize host 192.168.1.3 with “greentree” as the associated identity policy:

```
Router(config)# identity profile eapoudp  
Router(config-identity-prof)# device authorize ip-address 192.168.1.3 policy greentree
```

Related Commands

Command	Description
identity profile	Creates an identity profile.
eapoudp	

eou allow

To allow additional Extensible Authentication Protocol over UDP (EAPoUDP) options, use the **eou allow** command in global configuration mode. To disable the options that have been set, use the **no** form of this command.

```
eou allow { clientless | ip-station-id }
```

```
no eou allow { clientless | ip-station-id }
```

Syntax Description

clientless	Allows authentication of clientless hosts (systems that do not run Cisco Trust Agent).
ip-station-id	Allows an IP address in the station-id field.

Defaults

No additional EAPoUDP options are allowed.

Command Modes

Global configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

The **eou allow** command used with the **clientless** keyword requires that a user group be configured on the Cisco Access Control Server (ACS) using the same username and password that are specified using the **eou clientless** command.

Examples

The following example shows that clientless hosts are allowed:

```
Router (config)# eou allow clientless
```

Related Commands

Command	Description
eou clientless	Sets user group credentials for clientless hosts.

eou clientless

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 <i>password</i>	Sets a password.
username <i>username</i>	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.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.

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.

eou default

To set global Extensible Authentication Protocol over UDP (EAPoUDP) parameters to the default values, use the **eou default** command in global or interface configuration mode.

eou default

Syntax Description This command has no arguments or keywords.

Defaults The EAPoUDP parameters are set to their default values.

Command Modes Global configuration
Interface configuration

Command History	Release	Modification
	12.3(8)T	This command was introduced.

Usage Guidelines You can configure this command globally by using global configuration mode or for a specific interface by using interface configuration mode.

Using this command, you can reset existing values to their default values.

Examples The following configuration example shows that EAPoUDP parameters have been set to their default values:

```
Router (config)# eou default
```

eou initialize

To manually initialize Extensible Authentication Protocol over UDP (EAPoUDP) state machines, use the **eou initialize** command in global configuration mode. This command has no **no** form.

```
eou initialize { all | authentication { clientless | eap | static } | interface interface-name | ip
ip-address | mac mac-address | posturetoken string }
```

Syntax Description		
all		Initiates reauthentication of all EAPoUDP clients. This keyword is the default.
authentication		Specifies the authentication type.
clientless		Clientless authentication type.
eap		EAP authentication type.
static		Static authentication type.
interface		Specifies a specific interface.
<i>interface-name</i>		
ip	<i>ip-address</i>	Specifies a specific IP address.
mac	<i>mac-address</i>	Specifies a specific MAC address.
posturetoken	<i>string</i>	Specifies a specific posture token.

Defaults No default behaviour or values

Command Modes Global configuration

Command History	Release	Modification
	12.3(8)T	This command was introduced.

Usage Guidelines If this command is used, existing EAPoUDP state machines will be reset.

Examples The following example shows that all EAPoUDP state machines have been reauthenticated:

```
Router (config)# eou initialize
```

Related Commands	Command	Description
	eou revalidate	Revalidates an EAPoUDP association.

eou logging

To enable Extensible Authentication Protocol over UDP (EAPoUDP) system logging events, use the **eou logging** command in global configuration mode. To remove EAPoUDP logging, use the **no** form of this command.

eou logging

no eou logging

Syntax Description This command has no arguments or keywords.

Defaults Logging is disabled.

Command Modes Global configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Examples

The following example shows that EAPoUDP logging has been enabled:

```
Router (config)# eou logging
```

The following is sample EAPoUDP logging output:

```
Apr  9 10:04:09.824: %EOU-6-SESSION: IP=10.0.0.1| HOST=DETECTED| Interface=FastEthernet0/0
*Apr  9 10:04:09.900: %EOU-6-CTA: IP=10.0.0.1| CiscoTrustAgent=DETECTED
*Apr  9 10:06:19.576: %EOU-6-POLICY: IP=10.0.0.1| TOKEN=Healthy
*Apr  9 10:06:19.576: %EOU-6-POLICY: IP=10.0.0.1| ACLNAME=#ACSACL#-IP-HealthyACL-40921e54
*Apr  9 10:06:19.576: %EOU-6-POSTURE: IP=10.0.0.1| HOST=AUTHORIZED|
Interface=FastEthernet0/0.420
*Apr  9 10:06:19.580: %EOU-6-AUTHTYPE: IP=10.0.0.1| AuthType=EAP
*Apr  9 10:06:04.424: %EOU-6-SESSION: IP=192.168.2.1| HOST=REMOVED|
Interface=FastEthernet0/0.420
```

eou max-retry

To set the number of maximum retry attempts for Extensible Authentication Protocol over UDP (EAPoUDP), use the **eou max-retry** command in global or interface configuration mode. To remove the number of retries that were entered, use the **no** form of this command.

eou max-retry *number-of-retries*

no eou max-retry *number-of-retries*

Syntax Description	<i>number-of-retries</i>	Number of maximum retries that may be attempted. The value ranges from 1 through 10. The default is 3.
---------------------------	--------------------------	--------------------------------------------------------------------------------------------------------

Defaults	The default number of retries is 3.
-----------------	-------------------------------------

Command Modes	Global configuration Interface Configuration
----------------------	-------------------------------------------------

Command History	Release	Modification
	12.3(8)T	This command was introduced.
	12.4	The value range was changed from 1 through 3 to 1 through 10.

Usage Guidelines	You can configure this command globally by using global configuration mode or for a specific interface by using interface configuration mode.
-------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------

Examples	The following example shows that the maximum number of retries for an EAPoUDP session has been set for 2:
-----------------	-----------------------------------------------------------------------------------------------------------

```
Router (config)# eou max-retry 2
```

Related Commands	Command	Description
	show eou	Displays information about EAPoUDP global values or EAPoUDP session cache entries.

eou port

To set the UDP port for Extensible Authentication Protocol over UDP (EAPoUDP), use the **eou port** command in global configuration mode. This command has no **no** form.

eou port *port-number*

Syntax Description	<i>port-number</i>	Number of the port. The value ranges from 1 through 65535. The default value is 27186.
--------------------	--------------------	----------------------------------------------------------------------------------------

Defaults The default *port-number* value is 27186.

Command Modes Global configuration

Command History	Release	Modification
	12.3(8)T	This command was introduced.

Usage Guidelines Ensure that the port you set does not conflict with other UDP applications.

Examples The following example shows that the port for an EAPoUDP session has been set to 200:

```
Router (config)# eou port 200
```

Related Commands	Command	Description
	show eou	Displays information about EAPoUDP.

eou rate-limit

To set the number of simultaneous posture validations for Extensible Authentication Protocol over UDP (EAPoUDP), use the **eou rate-limit** command in global configuration mode. This command has no **no** form.

eou rate-limit *number-of-validations*

Syntax Description

<i>number-of-validations</i>	Number of clients that can be simultaneously validated. The value ranges from 1 through 200. The default value is 20.
------------------------------	-----------------------------------------------------------------------------------------------------------------------

Defaults

No default behaviors or values

Command Modes

Global configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

If you set the rate limit to 0 (zero), rate limiting will be turned off.

If the rate limit is set to 100 and there are 101 clients, validation will not occur until one drops off.

To return to the default value, use the **eou default** command.

Examples

The following example shows that the number of posture validations has been set to 100:

```
Router (config)# eou rate-limit 100
```

Related Commands

Command	Description
eou default	Sets global EAPoUDP parameters to the default values.
show eou	Displays information about EAPoUDP.

eou revalidate

To revalidate an Extensible Authentication Protocol over User Datagram Protocol (EAPoUDP) association, use the **eou revalidate** command in privileged EXEC mode. To disable the revalidation, use the **no** form of this command.

```
eou revalidate { all | authentication { clientless | eap | static } | interface interface-name | ip
ip-address | mac mac-address | posturetoken string }
```

```
no eou revalidate { all | authentication { clientless | eap | static } | interface interface-name | ip
ip-address | mac mac-address | posturetoken string }
```

Syntax	Description
all	Enables revalidation of all EAPoUDP clients. This keyword option is the default.
authentication	Specifies the authentication type.
clientless	Clientless authentication type.
eap	EAP authentication type.
static	Static authentication type.
interface <i>interface-name</i>	Name of the interface. (See Table 5 for the types of interface that may be shown.)
ip <i>ip-address</i>	IP address of the client.
mac <i>mac-address</i>	The 48-bit hardware address of the client.
posturetoken <i>string</i>	Name of the posture token.

Command Default No default behavior or values

Command Modes Privileged EXEC

Command	Release	Modification
	12.3(8)T	This command was introduced.

Usage Guidelines If you use this command, existing EAPoUDP sessions will be revalidated. [Table 5](#) lists the interface types that may be used with the **interface** keyword.

Table 5 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

Table 5 Description of Interface Types

Interface Type	Description
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) Multicast Host interface
Virtual-PPP	Virtual PPP interface
Virtual-Template	Virtual template interface
Virtual-TokenRing	Virtual TokenRing interface

Examples

The following example shows that all EAPoUDP clients are to be revalidated:

```
Router# eou revalidate all
```

Related Commands

Command	Description
eou initialize	Manually initializes EAPoUDP state machines.

eou timeout

To set the Extensible Authentication Protocol over UDP (EAPoUDP) timeout values, use the **eou timeout** command in global or interface configuration mode. To remove the value that was set, use the **no** form of this command.

```
eou timeout {aaa seconds | hold-period seconds | retransmit seconds | revalidation seconds | status query seconds}
```

```
no timeout {aaa seconds | hold-period seconds | retransmit seconds | revalidation seconds | status query seconds}
```

Syntax Description

aaa <i>seconds</i>	Authentication, authorization, and accounting (AAA) timeout period, in seconds. The value range is from 1 through 60. Default=60.
hold-period <i>seconds</i>	Hold period following failed authentication, in seconds. The value range is from 60 through 86400. Default=180.
retransmit <i>seconds</i>	Retransmit period, in seconds. The value range is from 1 through 60. Default=3.
revalidation <i>seconds</i>	Revalidation period, in seconds. The value range is from 300 through 86400. Default=36000.
status query <i>seconds</i>	Status query period after revalidation, in seconds. The value range is from 30 through 1800. Default=300.

Defaults

No default behavior or values

Command Modes

Global configuration
Interface configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

You can configure this command globally by using global configuration mode or for a specific interface by using interface configuration mode.

Examples

The following example shows that the status query period after revalidation is set to 30:

```
Router (config)# eou timeout status query 30
```

Related Commands

Command	Description
show eou	Displays information about EAPoUDP global values.

identity policy

To create an identity policy and to enter identity policy configuration mode, use the **identity policy** command in global configuration mode. To remove the policy, use the **no** form of this command.

```
identity policy policy-name [access-group group-name | description line-of-description | redirect url | template [virtual-template interface-number]]
```

```
no identity policy policy-name [access-group name | description line-of-description | redirect url | template [virtual-template interface-number]]
```

Syntax Description		
policy-name		Name of the policy.
access-group <i>group-name</i>		(Optional) Access list to be applied.
description <i>line-of-description</i>		(Optional) Description of the policy.
redirect url		(Optional) Redirects clients to a particular URL.
template		(Optional) Virtual template interface from which commands may be cloned.
virtual-template <i>interface-number</i>		(Optional) Virtual template number. The values range from 1 through 200.

Defaults

An identity policy is not created.

Command Modes

Global configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

An identity policy has to be associated with an identity profile.

Examples

The following example shows that an access policy named “greentree” is being created. The access-group attribute is set to “allow-access.” The redirect URL is set to “http://remediate-url.com.” This access policy will be associated with a statically authorized device in the identity profile.

```
Router (config)# identity policy greentree
Router (config-identity-policy)# access-group allow-access
Router (config-identity-policy)# redirect url http://remediate-url.com
```

Related Commands

Command	Description
identity profile	Creates an identity profile.

identity profile eapoudp

To create an identity profile and to enter Extensible Authentication Protocol over UDP (EAPoUDP) profile configuration mode, use the **identity profile eapoudp** command in global configuration mode. To remove the policy, use the **no** form of this command.

identity profile eapoudp

no identity profile eapoudp

Syntax Description This command has no arguments or keywords.

Defaults No EAPoUDP identity profile exists.

Command Modes Global configuration

Command History	Release	Modification
	12.3(8)T	This command was introduced.

Usage Guidelines Using this command, you can statically authenticate or unauthenticate a device either on the basis of the device IP address or MAC address or on the type, and the corresponding network access policy can be specified using the **identity policy** command.

Examples The following example shows that an EAPoUDP identity profile has been created:

```
Router (config)# identity profile eapoudp
```

Related Commands	Command	Description
	identity policy	Creates an identity policy.

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		
	<i>admission-name</i>	Authentication or admission rule name.
	event timeout aaa policy identity	Specifies an authentication policy to be applied when the AAA server is unreachable.
	<i>identity-policy-name</i>	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 <i>identity-policy-name</i> 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	
<i>admission-name</i>	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.
<i>service-policy-name</i>	Control plane tag service policy that is configured using the policy-map type control tag { <i>policy name</i> } 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).
<i>acl</i>	Applies a standard, extended list to a named admission control rule. The value ranges from 1 through 199.
<i>acl-name</i>	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.
<i>identity-policy-name</i>	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 <i>service-policy-name</i> argument were added.
12.4(11)T	The event , timeout aaa , and policy identity keywords and the <i>identity-policy-name</i> 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.

redirect (identity policy)

To redirect clients to a particular URL, use the **redirect** command in identity policy configuration mode. To remove the URL, use the **no** form of this command.

redirect url *url*

no redirect url *url*

Syntax Description	url	URL to which clients should be redirected.
	<i>url</i>	Valid URL.

Defaults No default behavior or values

Command Modes Identity policy configuration

Command History	Release	Modification
	12.3(8)T	This command was introduced.

Usage Guidelines When you use this command, an identity policy has to be associated with an Extensible Authentication Protocol over UDP (EAPoUDP) identity profile.

Examples The following example shows the URL to which clients will be redirected:

```
Router (config)# identity policy p1
Router (config-identity-policy)# redirect url http://www.cisco.com
```

Related Commands	Command	Description
	identity policy	Creates an identity policy.

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.
<i>interface-type</i>	Type of interface (see Table 6 for the interface types that may be shown).
ip	Specifies an IP address.
<i>ip-address</i>	IP address of the client device.
mac	Specifies a MAC address.
<i>mac-address</i>	The 48-bit address of the client device.
posturetoken	Displays information about a posture token name.
<i>name</i>	Name of the posture token.
begin	(Optional) Display begins with the line that matches the <i>expression</i> argument.
exclude	(Optional) Display excludes lines that match the <i>expression</i> argument.
include	(Optional) Display includes lines that match the specified <i>expression</i> argument.
<i>expression</i>	(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.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.

Release	Modification
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.(33)SRA.
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 6 lists the interface types that may be used for the *interface-type* argument.

Table 6 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) Multicast 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

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 7 describes the significant fields shown in the display

Table 7 *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.

show ip device tracking

To display information about entries in the IP device tracking table, use the **show ip device tracking** command in privileged EXEC mode.

```
show ip device tracking {all count | interface type-of-interface | ip ip-address | mac mac-address}
```

Syntax Description	all count	Displays a count of all IP tracking host entries.
	interface <i>type-of-interface</i>	Displays interface information. See Table 8 for a list of valid interfaces.
	ip <i>ip-address</i>	Displays the IP address of the client.
	mac <i>mac-address</i>	Displays the 48-bit hardware MAC address.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2SX	This command was introduced.
	12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T.

Usage Guidelines [Table 8](#) displays valid interfaces that may be shown as the *type-of-interface* argument with the **interface** keyword.

Table 8 Interfaces That Can Be Tracked

Interface	Description
Async	Asynchronous interface
BVI	Bridge-Group Virtual Interface
CDMA-Ix	CDMA Ix interface
CTunnel	CTunnel interface
Dialer	Dialer interface
FastEthernet	FastEthernet IEEE 802.3
Lex	Lex interface
Loopback	Loopback interface
MFR	Multilink Frame Relay bundle intrface
Multilink	Multilink-group interface
Null	Null interface
Port-channel	Ethernet channel of interfaces
Serial	Serial
Tunnel	Tunnel interface

Table 8 *Interfaces That Can Be Tracked (continued)*

Interface	Description
vif	Pragmatic General Multicast (PGM) multicast host interface
virtual	Virtual interface
virtual-PPP	Virtual PPP interface
virtual-Template	Virtual template interface
virtual-TokenRing	Virtual TokenRing
XTagATM	Extended Tag ATM interface

Examples

The following example shows that all host entries are to be tracked:

```
Router# show ip device tracking all count
```

```
IP Device Tracking = Enabled  
Probe Count: 2  
Probe Interval: 10
```

The fields in the above display are self-explanatory.

template (identity policy)

To specify a virtual template from which commands may be cloned, use the **template** command in identity policy configuration mode. To disable the virtual template, use the **no** form of this command.

```
template { virtual-template template-number }
```

```
no template { virtual-template template-number }
```

Syntax Description

virtual-template	Specifies the virtual template interface that will serve as the configuration clone source for the virtual interface that is dynamically created for authenticated users.
<i>template-number</i>	Template interface number. The value ranges from 1 through 200.

Defaults

A virtual template from which commands may be cloned is not specified.

Command Modes

Identity policy configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

The **identity policy** command must be entered in global configuration mode before the **template** command can be used.

Examples

The following example shows that an identity policy and a template have been specified:

```
Router (config)# identity policy mypolicy
Router (config-identity-policy)# template virtual-template 1
```

Related Commands

Command	Description
identity policy	Creates an identity policy.

Feature Information for Network Admission Control

Table 9 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.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



Note

Table 9 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 9 Feature Information for Network Admission Control

Feature Name	Releases	Feature Information
Network Admission Control	12.3(8)T	<p>The Network Admission Control feature addresses the increased threat and impact of worms and viruses to networked businesses. This feature is part of the Cisco Self-Defending Network Initiative that helps customers identify, prevent, and adapt to security threats.</p> <p>In its initial phase, the Cisco Network Admission Control functionality enables Cisco routers to enforce access privileges when an endpoint attempts to connect to a network.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> • Prerequisites for Network Admission Control, page 2 • Restrictions for Network Admission Control, page 2 • Information About Network Admission Control, page 2 • How to Configure Network Admission Control, page 7 • Configuration Examples for Network Admission Control, page 22 <p>The following commands were introduced or modified by this feature: <code>aaa authentication eou default enable group radius</code>, <code>access-group (identity policy)</code>, <code>auth-type</code>, <code>clear eou</code>, <code>clear ip admission cache</code>, <code>debug eap</code>, <code>debug eou</code>, <code>debug ip admission eapoudp</code>, <code>description (identity policy)</code>, <code>description (identity profile)</code>, <code>device (identity profile)</code>, <code>eou allow</code>, <code>eou clientless</code>, <code>eou default</code>, <code>eou initialize</code>, <code>eou logging</code>, <code>eou max-retry</code>, <code>eou port</code>, <code>eou rate-limit</code>, <code>eou revalidate</code>, <code>eou timeout</code>, <code>identity policy</code>, <code>identity profile eapoudp</code>, <code>ip admission</code>, <code>ip admission name</code>, <code>redirect (identity policy)</code>, <code>show eou</code>, <code>show ip admission</code>, <code>template (identity policy)</code>.</p>

Table 9 *Feature Information for Network Admission Control (continued)*

Feature Name	Releases	Feature Information
NAC MIB	12.4(15)T	<p>Support was added for the CISCO-NAC-NAD-MIB. This MIB module is used to monitor and configure the NAD on the Cisco NAC system.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> • “NAC MIB” section on page 5 • “Monitoring and Controlling NAC with the CISCO-NAC-NAD-MIB” section on page 16 <p>The following commands were introduced or modified by this feature: show ip device tracking.</p>

Glossary

default access policy—Set of ACLs that are applied to a client device until its credentials are validated by the AAA server.

EAPoUDP—Extensible Authentication Protocol over User Datagram Protocol. EAP is a framework that supports multiple, optional authentication mechanisms for PPP, including clear-text passwords, challenge-response, and arbitrary dialogue sequences. UDP is a connectionless transport layer protocol in the TCP/IP protocol stack. UDP is a simple protocol that exchanges datagrams without acknowledgments or guaranteed delivery, and it requires that error processing and retransmission be handled by other protocols. UDP is defined in RFC 768.

ip admission rule—Named rule that defines how IP admission control is applied. The IP admission rule is associated with an Intercept ACL and provides control over which hosts can use the IP admission feature. To create an IP admission control rule, use the **ip admission name** command.

posture token—Status that is used to convey the result of the evaluation of posture credentials. The AAA server maps the posture token (its status can be Healthy, Checkup, Quarantine, Infected, or Unknown) to a network access policy (ACL, URL, redirect, or status query timer) for the peer that the client wants to reach.

**Note**

See [Internetworking Terms and Acronyms](#) for terms not included in this glossary.

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website 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. (0711R)

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

© 2004–2007 Cisco Systems, Inc. All rights reserved.

