aaa accounting command through accounting-server-group Commands

aaa accounting command

To send accounting messages to the TACACS+ accounting server when you enter any command other than **show** commands at the CLI, use the **aaa accounting command** command in global configuration mode. To disable support for command accounting, use the **no** form of this command.

aaa accounting command [**privilege** *level*] *tacacs+-server-tag*

no aaa accounting command [**privilege** *level*] *tacacs+-server-tag*

Syntax Description

privilege *level*	If you customize the command privilege level using the **privilege** command, you can limit which commands the ASA accounts for by specifying a minimum privilege level. The ASA does not account for commands that are below the minimum privilege level. **Note** If you enter a deprecated command and enabled the **privilege** keyword, then the ASA does not send accounting information for the deprecated command. If you want to account for deprecated commands, be sure to disable the **privilege** keyword. Many deprecated commands are still accepted at the CLI, and are often converted into the currently accepted command at the CLI; they are not included in CLI help or this guide.
tacacs+-server-tag	Specifies the server or group of TACACS+ servers to which accounting records are sent, as specified by the **aaa-server protocol** command.

Defaults

The default privilege level is 0.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

When you configure the **aaa accounting command** command, each command other than **show** commands entered by an administrator is recorded and sent to the accounting server or servers.

Examples

The following example specifies that accounting records will be generated for any supported command, and that these records are sent to the server from the group named adminserver:

```
hostname(config)# aaa accounting command adminserver
```

Related Commands

Command	Description
aaa accounting	Enables or disables TACACS+ or RADIUS user accounting (on a server designated by the **aaa-server** command).
clear configure aaa	Removes or resets the configured AAA accounting values.
show running-config aaa	Displays the AAA configuration.

aaa accounting console

To enable support for AAA accounting for administrative access, use the **aaa accounting console** command in global configuration mode. To disable support for aaa accounting for administrative access, use the **no** form of this command.

aaa accounting {**serial | telnet | ssh | enable**} **console** *server-tag*

no aaa accounting {**serial | telnet | ssh | enable**} **console** *server-tag*

Syntax Description

enable	Enables the generation of accounting records to mark the entry to and exit from privileged EXEC mode.
serial	Enables the generation of accounting records to mark the establishment and termination of admin sessions that are established via the serial console interface.
server-tag	Specifies the server group to which accounting records are sent, defined by the **aaa-server protocol** command. Valid server group protocols are RADIUS and TACACS+.
ssh	Enables the generation of accounting records to mark the establishment and termination of admin sessions created over SSH.
telnet	Enables the generation of accounting records to mark the establishment and termination of admin sessions created over Telnet.

Defaults

By default, AAA accounting for administrative access is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**Context**	**System**
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

You must specify the name of the server group, previously specified in the **aaa-server** command.

Examples

The following example specifies that accounting records will be generated for enable access, and that these records are sent to the server named adminserver:

```
hostname(config)# aaa accounting enable console adminserver
```

Related Commands

Command	Description
aaa accounting match	Enables or disables TACACS+ or RADIUS user accounting (on a server designated by the **aaa-server** command),
aaa accounting command	Specifies that each command, or commands of a specified privilege level or higher, entered by an administrator/user is recorded and sent to the accounting server or servers.
clear configure aaa	Removes or resets the configured AAA accounting values.
show running-config aaa	Displays the AAA configuration.

aaa accounting include, exclude

To enable accounting for TCP or UDP connections through the ASA, use the **aaa accounting include** command in global configuration mode. To exclude addresses from accounting, use the **aaa accounting exclude** command. To disable accounting, use the **no** form of this command.

aaa accounting {**include** | **exclude**} *service interface_name inside_ip inside_mask* [*outside_ip outside_mask*] *server_tag*

no aaa accounting {**include** | **exclude**} *service interface_name inside_ip inside_mask* [*outside_ip outside_mask*] *server_tag*

Syntax Description

exclude	Excludes the specified service and address from accounting if it was already specified by an **include** command.
include	Specifies the services and IP addresses that require accounting. Traffic that is not specified by an **include** statement is not processed.
inside_ip	Specifies the IP address on the higher security interface. This address might be the source or the destination address, depending on the interface to which you apply this command. If you apply the command to the lower security interface, then this address is the destination address. If you apply the command to the higher security interface, then this address is the source address. Use 0 to mean all hosts.
inside_mask	Specifies the network mask for the inside IP address. Use 0 if the IP address is 0. Use 255.255.255.255 for a host.
interface_name	Specifies the interface name from which users require accounting.
outside_ip	(Optional) Specifies the IP address on the lower security interface. This address might be the source or the destination address, depending on the interface to which you apply this command. If you apply the command to the lower security interface, then this address is the source address. If you apply the command to the higher security interface, then this address is the destination address. Use 0 to mean all hosts.
outside_mask	(Optional) Specifies the network mask for the outside IP address. Use 0 if the IP address is 0. Use 255.255.255.255 for a host.
server_tag	Specifies the AAA server group defined by the **aaa-server host** command.
service	Specifies the services that require accounting. You can specify one of the following values: • **any** or **tcp/0** (specifies all TCP traffic) • ftp • http • **https** • **ssh** • telnet • **tcp/***port* • **udp/***port*

Defaults

By default, AAA accounting for administrative access is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The ASA can send accounting information to a RADIUS or TACACS+ server about any TCP or UDP traffic that passes through the ASA. If that traffic is also authenticated, then the AAA server can maintain accounting information by username. If the traffic is not authenticated, the AAA server can maintain accounting information by IP address. Accounting information includes when sessions start and stop, username, the number of bytes that pass through the ASA for the session, the service used, and the duration of each session.

Before you can use this command, you must first designate a AAA server with the **aaa-server** command.

To enable accounting for traffic that is specified by an ACL, use the **aaa accounting match** command. You cannot use the **match** command in the same configuration as the **include** and **exclude** commands. We suggest that you use the **match** command instead of the **include** and **exclude** commands; the **include** and **exclude** commands are not supported by ASDM.

You cannot use the **aaa accounting include** and **exclude** commands between same-security interfaces. For that scenario, you must use the **aaa accounting match** command.

Examples

The following example enables accounting on all TCP connections:

```
hostname(config)# aaa-server mygroup protocol tacacs+
hostname(config)# aaa-server mygroup (inside) host 192.168.10.10 thekey timeout 20
hostname(config)# aaa accounting include any inside 0 0 0 0 mygroup
```

Related Commands

Command	Description
aaa accounting match	Enables accounting for traffic specified by an ACL.
aaa accounting command	Enables accounting of administrative access.
aaa-server host	Configures the AAA server.
clear configure aaa	Clears the AAA configuration.
show running-config aaa	Displays the AAA configuration.

aaa accounting match

To enable accounting for TCP and UDP connections through the ASA, use the **aaa accounting match** command in global configuration mode. To disable accounting for traffic, use the **no** form of this command.

aaa accounting match *acl_name interface_name server_tag*

no aaa accounting match *acl_name interface_name server_tag*

Syntax Description

acl_name	Specifies the traffic that requires accounting by matching an ACL name. Permit entries in the ACL are accounted, while deny entries are exempt from accounting. This command is only supported for TCP and UDP traffic. A warning message is displayed if you enter this command and it references an ACL that permits other protocols.
interface_name	Specifies the interface name from which users require accounting.
server_tag	Specifies the AAA server group tag defined by the **aaa-server** command.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The ASA can send accounting information to a RADIUS or TACACS+ server about any TCP or UDP traffic that passes through the ASA. If that traffic is also authenticated, then the AAA server can maintain accounting information by username. If the traffic is not authenticated, the AAA server can maintain accounting information by IP address. Accounting information includes when sessions start and stop, username, the number of bytes that pass through the ASA for the session, the service used, and the duration of each session.

Before you can use this command, you must first designate a AAA server with the **aaa-server** command.

Accounting information is sent only to the active server in a server group unless you enable simultaneous accounting using the **accounting-mode** command in aaa-server protocol configuration mode.

You cannot use the **aaa accounting match** command in the same configuration as the **aaa accounting include** and **exclude** commands. We suggest that you use the **match** command instead of the **include** and **exclude** commands; the **include** and **exclude** commands are not supported by ASDM.

Examples

The following example enables accounting for traffic matching a specific ACL acl2:

```
hostname(config)# access-list acl12 extended permit tcp any any
hostname(config)# aaa accounting match acl2 outside radserver1
```

Related Commands

Command	Description
aaa accounting include, exclude	Enables accounting by specifying the IP addresses directly in the command.
access-list extended	Creates an ACL.
clear configure aaa	Removes AAA configuration.
show running-config aaa	Displays the AAA configuration.

aaa authentication console

To authenticate users who access the ASA CLI over a serial, SSH, HTTPS (ASDM), or Telnet connection, or to authenticate users who access privileged EXEC mode using the **enable** command, use the **aaa authentication console** command in global configuration mode. To disable authentication, use the **no** form of this command.

aaa authentication {**serial | enable | telnet | ssh | http**} **console** {**LOCAL |** *server_group* [**LOCAL**]}

no aaa authentication {**serial | enable | telnet | ssh | http**} **console** {**LOCAL |** *server_group* [**LOCAL**]}

Syntax Description

enable	Authenticates users who access privileged EXEC mode when they use the **enable** command.
http	Authenticates ASDM users who access the ASA over HTTPS. You only need to configure HTTPS authentication if you want to use a RADIUS or TACACS+ server. By default, ASDM uses the local database for authentication even if you do not configure this command.

LOCAL	Uses the local database for authentication. The **LOCAL** keyword is case sensitive. If the local database is empty, the following warning message appears:
	`Warning:local database is empty! Use 'username' command to define local users.`
	If the local database becomes empty when the **LOCAL** keyword is still present in the configuration, the following warning message appears:
	`Warning:Local user database is empty and there are still commands using 'LOCAL' for authentication.`

server-tag [**LOCAL**]	Specifies the AAA server group tag defined by the **aaa-server** command. HTTPS management authentication does not support the SDI protocol for a AAA server group. If you use the **LOCAL** keyword in addition to the *server-tag* argument, you can configure the ASA to use the local database as a fallback method if the AAA server is unavailable. The **LOCAL** keyword is case sensitive. We recommend that you use the same username and password in the local database as the AAA server because the ASA prompt does not give any indication which method is being used.
serial	Authenticates users who access the ASA using the serial console port.
ssh	Authenticates users who access the ASA using SSH.
telnet	Authenticates users who access the ASA using Telnet.

Defaults

By default, fallback to the local database is disabled.

If the **aaa authentication telnet console** command is not defined, you can gain access to the ASA CLI with the ASA login password (set with the **password** command).

If the **aaa authentication http console** command is not defined, you can gain access to the ASA (via ASDM) with no username and the ASA enable password (set with the **enable password** command). If the **aaa** commands are defined, but the HTTPS authentication requests a time out, which implies the AAA servers might be down or not available, you can gain access to the ASA using the default administrator username and the enable password. By default, the enable password is not set.

If the **aaa authentication ssh console** command is not defined, you can gain access to the ASA CLI with the username **pix** and with the ASA enable password (set with the **enable password** command). By default, the enable password is blank. This behavior differs from when you log in to the ASA without AAA configured; in that case, you use the login password (set by the **password** command).

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Before the ASA can authenticate a Telnet or SSH user, you must first configure access to the ASA using the **telnet** or **ssh** commands. These commands identify the IP addresses that are allowed to communicate with the ASA.

Logging in to the Security Appliance

After you connect to the ASA, you log in and access user EXEC mode.

- If you do not enable any authentication for Telnet, you do not enter a username; you enter the login password (set with the **password** command). For SSH, you enter “pix” as the username, and enter the login password.
- If you enable Telnet or SSH authenticationusing this command, you enter the username and password as defined on the AAA server or local user database.

Accessing Privileged EXEC Mode

To enter privileged EXEC mode, enter the **enable** command or the **login** command (if you are using the local database only).

- If you do not configure enable authentication, enter the system enable password when you enter the **enable** command (set by the **enable password** command). However, if you do not use enable authentication, after you enter the **enable** command, you are no longer logged in as a particular user. To maintain your username, use enable authentication.
- If you configure enable authentication, the ASA prompts you for your username and password.

For authentication using the local database, you can use the **login** command, which maintains the username but requires no configuration to turn on authentication.

Accessing ASDM

By default, you can log into ASDM with a blank username and the enable password set by the **enable password** command. However, if you enter a username and password at the login screen (instead of leaving the username blank), ASDM checks the local database for a match.

Although you can configure HTTPS authentication using this command and specify the local database, that functionality is always enabled by default. You should only configure HTTPS authentication if you want to use a AAA server for authentication. HTTPS authentication does not support the SDI protocol for a AAA server group. The maximum username prompt for HTTPS authentication is 30 characters. The maximum password length is 16 characters.

No Support in the System Execution Space for AAA Commands

In multiple context mode, you cannot configure any AAA commands in the system configuration.

Number of Login Attempts Allowed

As the following table shows, the action of the prompts for authenticated access to the ASA CLI differ, depending on the option you choose with the **aaa authentication console** command.

Option	Number of Login Attempts Allowed
enable	Three tries before access is denied
serial	Continual until success
ssh	Three tries before access is denied
telnet	Continual until success
http	Continual until success

Limiting User CLI and ASDM Access

You can configure management authorization with the **aaa authorization exec** command to limit a local user, RADIUS, TACACS+, or LDAP user (if you map LDAP attributes to RADIUS attributes) from accessing the CLI, ASDM, or the **enable** command.

Note Serial access is not included in management authorization, so if you configure **aaa authentication serial console**, then any user who authenticates can access the console port.

To configure the user for management authorization, see the following requirements for each AAA server type or local user:

- RADIUS or LDAP (mapped) users—Configures the Service-Type attribute for one of the following values. (To map LDAP attributes, see the **ldap attribute-map** command.)
  - Service-Type 6 (Administrative)—Allows full access to any services specified by the **aaa authentication console** commands.
  - Service-Type 7 (NAS prompt)—Allows access to the CLI when you configure the **aaa authentication {telnet | ssh} console** command, but denies ASDM configuration access if you configure the **aaa authentication http console** command. ASDM monitoring access is allowed. If you configure **enable** authentication with the **aaa authentication enable console** command, the user cannot access privileged EXEC mode using the **enable** command.

  - Service-Type 5 (Outbound)—Denies management access. The user cannot use any services specified by the **aaa authentication console** commands (excluding the **serial** keyword; serial access is allowed). Remote access (IPSec and SSL) users can still authenticate and terminate their remote access sessions.

- TACACS+ users—Authorization is requested with "service=shell," and the server responds with PASS or FAIL.
  - PASS, privilege level 1—Allows full access to any services specified by the **aaa authentication console** commands.
  - PASS, privilege level 2 and higher—Allows access to the CLI when you configure the **aaa authentication {telnet | ssh} console** command, but denies ASDM configuration access if you configure the **aaa authentication http console** command. ASDM monitoring access is allowed. If you configure enable authentication with the **aaa authentication enable console** command, the user cannot access privileged EXEC mode using the **enable** command.
  - FAIL—Denies management access. The user cannot use any services specified by the **aaa authentication console** commands (excluding the **serial** keyword; serial access is allowed).
- Local users—Set the **service-type** command. By default, the **service-type** is **admin**, which allows full access to any services specified by the **aaa authentication console** commands.

Examples

The following example shows use of the **aaa authentication console** command for a Telnet connection to a RADIUS server with the server tag "radius":

```
hostname(config)# aaa authentication telnet console radius
```

The following example identifies the server group "AuthIn" for enable authentication:

```
hostname(config)# aaa authentication enable console AuthIn
```

The following example shows use of the **aaa authentication console** command with fallback to the LOCAL user database if all the servers in the group "svrgrp1" fail:

```
hostname(config)# aaa-server svrgrp1 protocol tacacs
hostname(config)# aaa authentication ssh console svrgrp1 LOCAL
```

Related Commands

Command	Description
aaa authentication	Enables or disables user authentication.
aaa-server host	Specifies the AAA server to use for user authentication.
clear configure aaa	Remove or resets the configured AAA accounting values.
ldap map-attributes	Maps LDAP attributes to RADIUS attributes that the ASA can understand.
service-type	Limits a local user CLI access.
show running-config aaa	Displays the AAA configuration.

aaa authentication include, exclude

To enable authentication for connections through the ASA, use the **aaa authentication include** command in global configuration mode. To disable authentication, use the **no** form of this command. To exclude addresses from authentication, use the **aaa authentication exclude** command. To not exclude addresses from authentication, use the **no** form of this command.

aaa authentication {include | exclude} *service interface_name inside_ip inside_mask* [*outside_ip outside_mask*] {*server_tag* | **LOCAL**}

no aaa authentication {include | exclude} *service interface_name inside_ip inside_mask* [*outside_ip outside_mask*] {*server_tag* | **LOCAL**}

Syntax Description

exclude	Excludes the specified service and address from authentication if it was already specified by an **include** command.
include	Specifies the services and IP addresses that require authentication. Traffic that is not specified by an **include** statement is not processed.
inside_ip	Specifies the IP address on the higher security interface. This address might be the source or the destination address, depending on the interface to which you apply this command. If you apply the command to the lower security interface, then this address is the destination address. If you apply the command to the higher security interface, then this address is the source address. Use 0 to mean all hosts.
inside_mask	Specifies the network mask for the inside IP address. Use 0 if the IP address is 0. Use 255.255.255.255 for a host.
interface_name	Specifies the interface name from which users require authentication.
LOCAL	Specifies the local user database.
outside_ip	(Optional) Specifies the IP address on the lower security interface. This address might be the source or the destination address, depending on the interface to which you apply this command. If you apply the command to the lower security interface, then this address is the source address. If you apply the command to the higher security interface, then this address is the destination address. Use 0 to mean all hosts.
outside_mask	(Optional) Specifies the network mask for the outside IP address. Use 0 if the IP address is 0. Use 255.255.255.255 for a host.

server_tag	Specifies the AAA server group defined by the **aaa-server** command.
service	Specifies the services that require authentication. You can specify one of the following values: • **any** or **tcp/0** (specifies all TCP traffic) • ftp • http • **https** • **ssh** • telnet • **tcp/***port*[**-***port*] • **udp/***port*[**-***port*] • **icmp/***type* • *protocol*[**/***port*[**-***port*]] Although you can configure the ASA to require authentication for network access to any protocol or service, users can authenticate directly with HTTP, HTTPS, Telnet, or FTP only. A user must first authenticate with one of these services before the ASA allows other traffic requiring authentication. See "Usage Guidelines" for more information.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

To enable authentication for traffic that is specified by an ACL, use the **aaa authentication match** command. You cannot use the **match** command in the same configuration as the **include** and **exclude** commands. We suggest that you use the **match** command instead of the **include** and **exclude** commands; the **include** and **exclude** commands are not supported by ASDM.

You cannot use the **aaa authentication include** and **exclude** commands between same-security interfaces. For that scenario, you must use the **aaa authentication match** command.

TCP sessions might have their sequence numbers randomized even if you disable sequence randomization. This occurs when a AAA server proxies the TCP session to authenticate the user before permitting access.

One-Time Authentication

A user at a given IP address only needs to authenticate one time for all rules and types, until the authentication session expires. (See the **timeout uauth** command for timeout values.) For example, if you configure the ASA to authenticate Telnet and FTP, and a user first successfully authenticates for Telnet, then as long as the authentication session exists, the user does not also have to authenticate for FTP.

For HTTP or HTTPS authentication, once authenticated, a user never has to reauthenticate, no matter how low the **timeout uauth** command is set, because the browser caches the string "Basic=Uuhjksdkfhk==" in every subsequent connection to that particular site. This can be cleared only when the user exits *all* instances of the web browser and restarts. Flushing the cache is of no use.

Applications Required to Receive an Authentication Challenge

Although you can configure the ASA to require authentication for network access to any protocol or service, users can authenticate directly with HTTP, HTTPS, Telnet, or FTP only. A user must first authenticate with one of these services before the ASA allows other traffic requiring authentication.

The authentication ports that the ASA supports for AAA are fixed:

- Port 21 for FTP
- Port 23 for Telnet
- Port 80 for HTTP
- Port 443 for HTTPS

Security Appliance Authentication Prompts

For Telnet and FTP, the ASA generates an authentication prompt.

For HTTP, the ASA uses basic HTTP authentication by default, and provides an authentication prompt. You can optionally configure the ASA to redirect users to an internal web page where they can enter their username and password (configured with the **aaa authentication listener** command).

For HTTPS, the ASA generates a custom login screen. You can optionally configure the ASA to redirect users to an internal web page where they can enter their username and password (configured with the **aaa authentication listener** command).

Redirection is an improvement over the basic method because it provides an improved user experience when authenticating, and an identical user experience for HTTP and HTTPS in both Easy VPN and firewall modes. It also supports authenticating directly with the ASA.

You might want to continue to use basic HTTP authentication if: you do not want the ASA to open listening ports; if you use NAT on a router and you do not want to create a translation rule for the web page served by the ASA; basic HTTP authentication might work better with your network. For example non-browser applications, like when a URL is embedded in email, might be more compatible with basic authentication.

After you authenticate correctly, the ASA redirects you to your original destination. If the destination server also has its own authentication, the user enters another username and password. If you use basic HTTP authentication and need to enter another username and password for the destination server, then you need to configure the **virtual http** command.

Note If you use HTTP authentication without using the **aaa authentication secure-http-client** command, the username and password are sent from the client to the ASA in clear text. We recommend that you use the **aaa authentication secure-http-client** command whenever you enable HTTP authentication.

For FTP, a user has the option of entering the ASA username followed by an at sign (@) and then the FTP username (name1@name2). For the password, the user enters the ASA password followed by an at sign (@) and then the FTP password (password1@password2). For example, enter the following text.

```
name> asa1@partreq
password> letmein@he110
```

This feature is useful when you have cascaded firewalls that require multiple logins. You can separate several names and passwords by multiple at signs (@).

The number of login attempts allowed differs between the supported protocols:

Protocol	Number of Login Attempts Allowed
FTP	Incorrect password causes the connection to be dropped immediately.
HTTP HTTPS	Continual reprompting until successful login.
Telnet	Four tries before dropping the connection.

Static PAT and HTTP

For HTTP authentication, the ASA checks real ports when static PAT is configured. If it detects traffic destined for real port 80, regardless of the mapped port, the ASA intercepts the HTTP connection and enforces authentication.

For example, assume that outside TCP port 889 is translated to port 80 (www) and that any relevant ACLs permit the traffic:

```
static (inside,outside) tcp 10.48.66.155 889 192.168.123.10 www netmask 255.255.255.255
```

Then when users try to access 10.48.66.155 on port 889, the ASA intercepts the traffic and enforces HTTP authentication. Users see the HTTP authentication page in their web browsers before the ASA allows HTTP connection to complete.

If the local port is different than port 80, as in the following example:

```
static (inside,outside) tcp 10.48.66.155 889 192.168.123.10 111 netmask 255.255.255.255
```

Then users do not see the authentication page. Instead, the ASA sends an error message to the web browser indicating that the user must be authenticated before using the requested service.

Authenticating Directly with the ASA

If you do not want to allow HTTP, HTTPS, Telnet, or FTP through the ASA but want to authenticate other types of traffic, you can authenticate with the ASA directly using HTTP or HTTPS by configuring the **aaa authentication listener** command.

You can authenticate directly with the ASA at the following URLs when you enable AAA for the interface:

http://*interface_ip*[**:***port*]**/netaccess/connstatus.html**
https://*interface_ip*[**:***port*]**/netaccess/connstatus.html**

Alternatively, you can configure virtual Telnet (using the **virtual telnet** command). With virtual Telnet, the user Telnets to a given IP address configured on the ASA, and the ASA provides a Telnet prompt.

Examples

The following example includes for authentication TCP traffic on the outside interface, with an inside IP address of 192.168.0.0 and a netmask of 255.255.0.0, with an outside IP address of all hosts, and using a server group named tacacs+. The second command line excludes Telnet traffic on the outside interface with an inside address of 192.168.38.0, with an outside IP address of all hosts:

```
hostname(config)# aaa authentication include tcp/0 outside 192.168.0.0 255.255.0.0 0 0
tacacs+
hostname(config)# aaa authentication exclude telnet outside 192.168.38.0 255.255.255.0 0 0
tacacs+
```

The following examples demonstrate ways to use the *interface-name* parameter. The ASA has an inside network of 192.168.1.0, an outside network of 209.165.201.0 (subnet mask 255.255.255.224), and a perimeter network of 209.165.202.128 (subnet mask 255.255.255.224).

This example enables authentication for connections originated from the inside network to the outside network:

```
hostname(config)# aaa authentication include tcp/0 inside 192.168.1.0 255.255.255.0
209.165.201.0 255.255.255.224 tacacs+
```

This example enables authentication for connections originated from the inside network to the perimeter network:

```
hostname(config)#aaa authentication include tcp/0 inside 192.168.1.0 255.255.255.0
209.165.202.128 255.255.255.224 tacacs+
```

This example enables authentication for connections originated from the outside network to the inside network:

```
hostname(config)# aaa authentication include tcp/0 outside 192.168.1.0 255.255.255.0
209.165.201.0 255.255.255.224 tacacs+
```

This example enables authentication for connections originated from the outside network to the perimeter network:

```
hostname(config)# aaa authentication include tcp/0 outside 209.165.202.128 255.255.255.224
209.165.201.0 255.255.255.224 tacacs+
```

This example enables authentication for connections originated from the perimeter network to the outside network:

```
hostname(config)#aaa authentication include tcp/0 perimeter 209.165.202.128
255.255.255.224 209.165.201.0 255.255.255.224 tacacs+
```

Related Commands

Command	Description
aaa authentication console	Enables authentication for management access.
aaa authentication match	Enables user authentication for through traffic.
aaa authentication secure-http-client	Provides a secure method for user authentication to the ASA before allowing HTTP requests to traverse the ASA.

aaa-server	Configures group-related server attributes.
aaa-server host	Configures host-related attributes.

aaa authentication listener

To enable HTTP(S) listening ports to authenticate network users, use the **aaa authentication listener** command in global configuration mode. When you enable a listening port, the ASA serves an authentication page for direct connections and optionally for through traffic. To disable the listeners, use the **no** form of this command.

aaa authentication listener http[**s**] *interface_name* [**port** *portnum*] [**redirect**]

no aaa authentication listener http[**s**] *interface_name* [**port** *portnum*] [**redirect**]

Syntax Description

http[**s**]	Specifies the protocol that you want to listen for, either HTTP or HTTPS. Enter this command separately for each protocol.
interface_name	Specifies the interface on which you enable listeners.
port *portnum*	Specifies the port number that the ASA listens on for direct or redirected traffic; the defaults are 80 (HTTP) and 443 (HTTPS). You can use any port number and retain the same functionality, but be sure your direct authentication users know the port number; redirected traffic is sent to the correct port number automatically, but direct authenticators must specify the port number manually.
redirect	Redirects through traffic to an authentication web page served by the ASA. Without this keyword, only traffic directed to the ASA interface can access the authentication web pages.

Defaults

By default, no listener services are enabled, and HTTP connections use basic HTTP authentication. If you enable the listeners, the default ports are 80 (HTTP) and 443 (HTTPS).

If you are upgrading from 7.2(1), then the listeners are enabled on ports 1080 (HTTP) and 1443 (HTTPS). The **redirect** option is also enabled.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**Context**	**System**
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.2(2)	This command was introduced.

Usage Guidelines

Without the **aaa authentication listener** command, when HTTP(S) users need to authenticate with the ASA after you configure the **aaa authentication match** or **aaa authentication include** command, the ASA uses basic HTTP authentication. For HTTPS, the ASA generates a custom login screen.

If you configure the **aaa authentication listener** command with the **redirect** keyword, the ASA redirects all HTTP(S) authentication requests to web pages served by the ASA.

Redirection is an improvement over the basic method because it provides an improved user experience when authenticating, and an identical user experience for HTTP and HTTPS in both Easy VPN and firewall modes. It also supports authenticating directly with the ASA.

You might want to continue to use basic HTTP authentication if: you do not want the ASA to open listening ports; if you use NAT on a router and you do not want to create a translation rule for the web page served by the ASA; basic HTTP authentication might work better with your network. For example non-browser applications, like when a URL is embedded in email, might be more compatible with basic authentication.

If you enter the **aaa authentication listener** command *without* the **redirect** option, then you only enable direct authentication with the ASA, while letting through traffic use basic HTTP authentication. The **redirect** option enables both direct and through-traffic authentication. Direct authentication is useful when you want to authenticate traffic types that do not support authentication challenges; you can have each user authenticate directly with the ASA before using any other services.

Note If you enable the **redirect** option, you cannot also configure static PAT for the same interface where you translate the interface IP address and the same port that is used for the listener; NAT succeds, but authentication fails. For example, the following configuration is unsupported:

```
hostname(config)# static (inside,outside) tcp interface www 192.168.0.50 www netmask
255.255.255.255
hostname(config)# aaa authentication listener http outside redirect
```

The following configuration is supported; the listener uses port 1080 instead of the default 80:

```
hostname(config)# static (inside,outside) tcp interface www 192.168.0.50 www netmask
255.255.255.255
hostname(config)# aaa authentication listener http outside port 1080 redirect
```

Examples

The following example configures the ASA to redirect HTTP and HTTPS connections to the default ports:

```
hostname(config)# aaa authentication http redirect
hostname(config)# aaa authentication https redirect
```

The following example allows authentication requests directly to the ASA; through traffic uses basic HTTP authentication:

```
hostname(config)# aaa authentication http
hostname(config)# aaa authentication https
```

The following example configures the ASA to redirect HTTP and HTTPS connections to non-default ports:

```
hostname(config)# aaa authentication http port 1100 redirect
hostname(config)# aaa authentication https port 1400 redirect
```

Related Commands

Command	Description
aaa authentication match	Configures user authentication for through traffic.

aaa authentication secure-http-client	Enables SSL and secure username and password exchange between HTTP clients and the ASA.
clear configure aaa	Removes the configured AAA configuration.
show running-config aaa	Displays the AAA configuration.
virtual http	Supports cascading HTTP authentications with basic HTTP authentication.

aaa authentication match

To enable authentication for connections through the ASA, use the **aaa authentication match** command in global configuration mode. To disable authentication, use the **no** form of this command.

aaa authentication match *acl_name interface_name* {*server_tag* | **LOCAL**} **user-identity**

no aaa authentication match *acl_name interface_name* {*server_tag* | **LOCAL**} **user-identity**

Syntax Description

acl_name	Specifies an extended ACL name.
interface_name	Specifies the interface name from which to authenticate users.
LOCAL	Specifies the local user database.
server_tag	Specifies the AAA server group tag defined by the **aaa-server** command.
user-identity	Specifies the user identity that is mapped to the identity firewall.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.
9.0(1)	The **user-identity** keyword was added.

Usage Guidelines

You cannot use the **aaa authentication match** command in the same configuration as the **include** and **exclude** commands. We suggest that you use the **match** command instead of the **include** and **exclude** commands; the **include** and **exclude** commands are not supported by ASDM.

TCP sessions might have their sequence numbers randomized even if you disable sequence randomization. This occurs when a AAA server proxies the TCP session to authenticate the user before permitting access.

One-Time Authentication

A user at a given IP address only needs to authenticate one time for all rules and types, until the authentication session expires. (See the **timeout uauth** command for timeout values.) For example, if you configure the ASA to authenticate Telnet and FTP, and a user first successfully authenticates for Telnet, then as long as the authentication session exists, the user does not also have to authenticate for FTP.

For HTTP or HTTPS authentication, once authenticated, a user never has to reauthenticate, no matter how low the **timeout uauth** command is set, because the browser caches the string "Basic=Uuhjksdkfhk==" in every subsequent connection to that particular site. This can be cleared only when the user exits *all* instances of the web browser and restarts. Flushing the cache is of no use.

Applications Required to Receive an Authentication Challenge

Although you can configure the ASA to require authentication for network access to any protocol or service, users can authenticate directly with HTTP, HTTPS, Telnet, or FTP only. A user must first authenticate with one of these services before the ASA allows other traffic requiring authentication.

The authentication ports that the ASA supports for AAA are fixed:

- Port 21 for FTP
- Port 23 for Telnet
- Port 80 for HTTP
- Port 443 for HTTPS (requires the **aaa authentication listener** command)

ASA Authentication Prompts

For Telnet and FTP, the ASA generates an authentication prompt.

For HTTP, the ASA uses basic HTTP authentication by default, and provides an authentication prompt. You can optionally configure the ASA to redirect users to an internal web page where they can enter their username and password (configured with the **aaa authentication listener** command).

For HTTPS, the ASA generates a custom login screen. You can optionally configure the ASA to redirect users to an internal web page where they can enter their username and password (configured with the **aaa authentication listener** command).

Redirection is an improvement over the basic method because it provides an improved user experience when authenticating, and an identical user experience for HTTP and HTTPS in both Easy VPN and firewall modes. It also supports authenticating directly with the ASA.

You might want to continue to use basic HTTP authentication if: you do not want the ASA to open listening ports; if you use NAT on a router and you do not want to create a translation rule for the web page served by the ASA; basic HTTP authentication might work better with your network. For example non-browser applications, like when a URL is embedded in email, might be more compatible with basic authentication.

After you authenticate correctly, the ASA redirects you to your original destination. If the destination server also has its own authentication, the user enters another username and password. If you use basic HTTP authentication and need to enter another username and password for the destination server, then you need to configure the **virtual http** command.

Note If you use HTTP authentication without using the **aaa authentication secure-http-client** command, the username and password are sent from the client to the ASA in clear text. We recommend that you use the **aaa authentication secure-http-client** command whenever you enable HTTP authentication.

For FTP, a user has the option of entering the ASA username followed by an at sign (@) and then the FTP username (name1@name2). For the password, the user enters the ASA password followed by an at sign (@) and then the FTP password (password1@password2). For example, enter the following text.

```
name> asa1@partreq
password> letmein@he110
```

This feature is useful when you have cascaded firewalls that require multiple logins. You can separate several names and passwords by multiple at signs (@).

The number of login attempts allowed differs between the supported protocols:

Protocol	Number of Login Attempts Allowed
FTP	Incorrect password causes the connection to be dropped immediately.
HTTP HTTPS	Continual reprompting until successful login.
Telnet	Four tries before dropping the connection.

Static PAT and HTTP

For HTTP authentication, the ASA checks real ports when static PAT is configured. If it detects traffic destined for real port 80, regardless of the mapped port, the ASA intercepts the HTTP connection and enforces authentication.

For example, assume that outside TCP port 889 is translated to port 80 (www) and that any relevant ACLs permit the traffic:

```
static (inside,outside) tcp 10.48.66.155 889 192.168.123.10 www netmask 255.255.255.255
```

Then when users try to access 10.48.66.155 on port 889, the ASA intercepts the traffic and enforces HTTP authentication. Users see the HTTP authentication page in their web browsers before the ASA allows HTTP connection to complete.

If the local port is different than port 80, as in the following example:

```
static (inside,outside) tcp 10.48.66.155 889 192.168.123.10 111 netmask 255.255.255.255
```

Then users do not see the authentication page. Instead, the ASA sends to the web browser an error message indicating that the user must be authenticated before using the requested service.

Authenticating Directly with the ASA

If you do not want to allow HTTP, HTTPS, Telnet, or FTP through the ASA but want to authenticate other types of traffic, you can authenticate with the ASA directly using HTTP or HTTPS by configuring the **aaa authentication listener** command.

You can authenticate directly with the ASA at the following URLs when you enable AAA for the interface:

http://*interface_ip*[**:***port*]**/netaccess/connstatus.html**
https://*interface_ip*[**:***port*]**/netaccess/connstatus.html**

Alternatively, you can configure virtual Telnet (using the **virtual telnet** command). With virtual Telnet, the user Telnets to a given IP address configured on the ASA, and the ASA provides a Telnet prompt.

Examples

The following set of examples illustrates how to use the **aaa authentication match** command:

```
hostname(config)# show access-list
access-list mylist permit tcp 10.0.0.0 255.255.255.0 192.168.2.0 255.255.255.0 (hitcnt=0)
access-list yourlist permit tcp any any (hitcnt=0)

hostname(config)# show running-config aaa
aaa authentication match mylist outbound TACACS+
```

In this context, the following command:

```
hostname(config)# aaa authentication match yourlist outbound tacacs
```

is equivalent to this command:

```
hostname(config)# aaa authentication include TCP/0 outbound 0.0.0.0 0.0.0.0 0.0.0.0
0.0.0.0 tacacs
```

The **aaa** command statement list is order-dependent between **access-list** command statements. If you enter the following command:

```
hostname(config)# aaa authentication match mylist outbound TACACS+
```

before this command:

```
hostname(config)# aaa authentication match yourlist outbound tacacs
```

the ASA tries to find a match in the **mylist access-list** command statement group before it tries to find a match in the **yourlist access-list** command statement group.

To enable authentication for connections through the ASA and match it to the Identity Firewall feature, enter the following command:

```
hostname(config)# aaa authenticate match access_list_name inside user-identity
```

Related Commands

Command	Description
aaa authorization	Enables user authorization services.
access-list extended	Creates an ACL.
clear configure aaa	Removes the configured AAA configuration.
show running-config aaa	Displays the AAA configuration.

aaa authentication secure-http-client

To enable SSL and secure username and password exchange between HTTP clients and the ASA, use the **aaa authentication secure-http-client** command in global configuration mode. To disable this function, use the **no** form of this command.

aaa authentication secure-http-client

no aaa authentication secure-http-client

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The **aaa authentication secure-http-client** command offers a secure method for user authentication to the ASA before allowing user HTTP-based web requests to traverse the ASA. This command is used for HTTP cut-through proxy authentication through SSL.

The **aaa authentication secure-http-client** command has the following limitations:

- At runtime, a maximum of 16 HTTPS authentication processes is allowed. If all 16 HTTPS authentication processes are running, the 17th, new HTTPS connection requiring authentication is not allowed.
- When **uauth timeout 0** is configured (the **uauth timeout** is set to 0), HTTPS authentication might not work. If a browser initiates multiple TCP connections to load a web page after HTTPS authentication, the first connection is let through, but the subsequent connections trigger authentication. As a result, users are continuously presented with an authentication page, even if the correct username and password are entered each time. To work around this, set the **uauth timeout** to 1 second with the **timeout uauth 0:0:1** command. However, this workaround opens a 1-second window of opportunity that might allow non-authenticated users to go through the firewall if they are coming from the same source IP address.

- Because HTTPS authentication occurs on the SSL port 443, users must not configure an **access-list** command statement to block traffic from the HTTP client to HTTP server on port 443. Furthermore, if static PAT is configured for web traffic on port 80, it must also be configured for the SSL port. In the following example, the first line configures static PAT for web traffic and the second line must be added to support the HTTPS authentication configuration:

```
static (inside,outside) tcp 10.132.16.200 www 10.130.16.10 www
static (inside,outside) tcp 10.132.16.200 443 10.130.16.10 443
```

Examples

The following example configures HTTP traffic to be securely authenticated:

```
hostname(config)# aaa authentication secure-http-client
hostname(config)# aaa authentication include http...
```

where "..." represents your values for *authen_service if_name local_ip local_mask* [*foreign_ip foreign_mask*] *server_tag*.

The following command configures HTTPS traffic to be securely authenticated:

```
hostname (config)# aaa authentication include https...
```

where "..." represents your values for *authentication -service interface-name local-ip local-mask* [*foreign-ip foreign-mask*] *server-tag*.

Note The **aaa authentication secure-https-client** command is not needed for HTTPS traffic.

Related Commands

Command	Description
aaa authentication	Enables LOCAL, TACACS+, or RADIUS user authentication, on a server designated by the **aaa-server** command.
virtual telnet	Accesses the ASA virtual server.

aaa authorization command

To enable command authorization, use the **aaa authorization command** command in global configuration mode. To disable command authorization, use the **no** form of this command.

aaa authorization command {**LOCAL** | *tacacs+ server_tag* [**LOCAL**]}

no aaa authorization command {**LOCAL** | *tacacs+ server_tag* [**LOCAL**]}

Syntax Description

LOCAL	Enables local command privilege levels set by the **privilege** command. When a local, RADIUS, or LDAP (if you map LDAP attributes to RADIUS attributes) user authenticates for CLI access, the ASA places that user in the privilege level that is defined by the local database, RADIUS, or LDAP server. The user can access commands at the user privilege level and below. If you specify **LOCAL** after a TACACS+ server group tag, the local user database is used for command authorization only as a fallback when the TACACS+ server group is unavailable.
tacacs+ server_tag	Specifies a predefined server group tag for the TACACS+ authorization server. The AAA server group tag as defined by the **aaa-server** command.

Defaults

Fallback to the local database for authorization is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**Context**	**System**
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	Support added for fallback to LOCAL authorization when a TACACS+ server group is temporarily unavailable.
8.0(2)	Support for privilege levels defined on RADIUS or LDAP servers was added.

Usage Guidelines

The **aaa authorization command** command specifies whether command execution at the CLI is subject to authorization. By default when you log in, you can access user EXEC mode, which offers only a minimal number of commands. When you enter the **enable** command (or the **login** command when you use the local database), you can access privileged EXEC mode and advanced commands, including configuration commands. If you want to control the access to commands, the ASA lets you configure command authorization, where you can determine which commands are available to a user.

Supported Command Authorization Methods

You can use one of two command authorization methods:

- Local privilege levels—Configure the command privilege levels on the ASA. When a local, RADIUS, or LDAP (if you map LDAP attributes to RADIUS attributes) user authenticates for CLI access, the ASA places that user in the privilege level that is defined by the local database, RADIUS, or LDAP server. The user can access commands at the user privilege level and below. Note that all users access user EXEC mode when they first log in (commands at level 0 or 1). The user needs to authenticate again with the **enable** command to access privileged EXEC mode (commands at level 2 or higher), or they can log in with the **login** command (local database only).

Note You can use local command authorization without any users in the local database and without CLI or enable authentication. Instead, when you enter the **enable** command, you enter the system enable password, and the ASA places you in level 15. You can then create enable passwords for every level, so that when you enter **enable** *n* (2 to 15), the ASA places you in level *n*. These levels are not used unless you turn on local command authorization. (See the **enable** command for more information.)

- TACACS+ server privilege levels—On the TACACS+ server, configure the commands that a user or group can use after they authenticate for CLI access. Every command that a user enters at the CLI is checked with the TACACS+ server.

Security Contexts and Command Authorization

The following are important points to consider when implementing command authorization with multiple security contexts:

- AAA settings are discrete per context, not shared between contexts.

  When configuring command authorization, you must configure each security context separately. This provides you the opportunity to enforce different command authorizations for different security contexts.

  When switching between security contexts, administrators should be aware that the commands permitted for the username specified when they login may be different in the new context session or that command authorization may not be configured at all in the new context. Failure to understand that command authorizations may differ between security contexts could confuse an administrator. This behavior is further complicated by the next point.

- New context sessions started with the **changeto** command always use the default “enable_15” username as the administrator identity, regardless of what username was used in the previous context session. This behavior can lead to confusion if command authorization is not configured for the enable_15 user or if authorizations are different for the enable_15 user than for the user in the previous context session.

  This behavior also affects command accounting, which is useful only if you can accurately associate each command that is issued with a particular administrator. Because all administrators with permission to use the **changeto** command can use the enable_15 username in other contexts, command accounting records may not readily identify who was logged in as the enable_15 username. If you use different accounting servers for each context, tracking who was using the enable_15 username requires correlating the data from several servers.

  When configuring command authorization, consider the following:

  – An administrator with permission to use the **changeto** command effectively has permission to use all commands permitted to the enable_15 user in each of the other contexts.

– If you intend to authorize commands differently per context, ensure that in each context the enable_15 username is denied the use of commands that are also denied to administrators who are permitted to use the **changeto** command.

When switching between security contexts, administrators can exit privileged EXEC mode and enter the **enable** command again to use the username they need.

Note The system execution space does not support **aaa** commands; therefore, command authorization is not available in the system execution space.

Local Command Authorization Prerequisites

- Configure enable authentication for local, RADIUS, or LDAP authentication using the **aaa authentication enable console** command.

  Enable authentication is essential to maintain the username after the user accesses the **enable** command.

  Alternatively, you can use the **login** command (which is the same as the **enable** command with authentication), which requires no configuration. We do not recommend this option because it is not as secure as enable authentication.

  You can also use CLI authentication (**aaa authentication** {**ssh** | **telnet** | **serial**} **console**), but it is not required.

- You can use the **aaa authorization exec** command to enable support of administrative user privilege levels from RADIUS if RADIUS is used for authentication, but it is not required. This command also enables management authorization for local, RADIUS, LDAP (mapped), and TACACS+ users.
- See the following prerequisites for each user type:
  - Local database users—Configure each user in the local database at a privilege level from 0 to 15 using the **username** command.
  - RADIUS users—Configure the user with Cisco VSA CVPN3000-Privilege-Level with a value between 0 and 15.
  - LDAP users—Configure the user with a privilege level between 0 and 15, and then map the LDAP attribute to Cisco VAS CVPN3000-Privilege-Level using the **ldap map-attributes** command.
- See the **privilege** command for information about setting command privilege levels.

TACACS+ Command Authorization

If you enable TACACS+ command authorization, and a user enters a command at the CLI, the ASA sends the command and username to the TACACS+ server to determine if the command is authorized.

When configuring command authorization with a TACACS+ server, do not save your configuration until you are sure it works the way you want. If you get locked out because of a mistake, you can usually recover access by restarting the ASA.

Be sure that your TACACS+ system is completely stable and reliable. The necessary level of reliability typically requires that you have a fully redundant TACACS+ server system and fully redundant connectivity to the ASA. For example, in your TACACS+ server pool, include one server connected to interface 1, and another to interface 2. You can also configure local command authorization as a fallback method if the TACACS+ server is unavailable. In this case, you need to configure local users and command privilege levels.

See the CLI configuration guide for information about configuring the TACACS+ server.

TACACS+ Command Authorization Prerequisites

- Configure CLI authentication using the **aaa authentication** {**ssh** | **telnet** | **serial**} **console** command.
- Configure **enable** authentication using the **aaa authentication enable console** command.

Examples

The following example shows how to enable command authorization using a TACACS+ server group named tplus1:

```
hostname(config)# aaa authorization command tplus1
```

The following example shows how to configure administrative authorization to support fallback to the local user database if all servers in the tplus1 server group are unavailable.

```
hostname(config)# aaa authorization command tplus1 LOCAL
```

Related Commands

Command	Description
aaa authentication console	Enables CLI, ASDM, and enable authentication.
aaa authorization exec	Enables support of administrative user privilege levels from RADIUS.
aaa-server host	Configures host-related attributes.
aaa-server	Configures group-related server attributes.
enable	Enters privileged EXEC mode.
ldap map-attributes	Maps LDAP attributes to RADIUS attributes that the ASA can use.
login	Enters privileged EXEC mode using the local database for authentication.
service-type	Limits local database user CLI, ASDM, and enable access.
show running-config aaa	Displays the AAA configuration.

aaa authorization exec

To enable management authorization, use the **aaa authorization exec** command o in global configuration mode. To disable management authorization, use the **no** form of these commands.

aaa authorization exec {**authentication-server** | **LOCAL**}

no aaa authorization exec {**authentication-server** | **LOCAL**}

Syntax Description

authentication-server	Indicates that the authorization attributes will be retrieved from the server that was used to authenticate the user.
LOCAL	Indicates that the authorization attributes will be retrieved from the local user database of the ASA, regardless of how authentication is done.

Defaults

By default, this command is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
8.0(2)	This command was introduced.
8.2(2)	The **LOCAL** option was added.

Usage Guidelines

When using the **aaa authorization exec** command, the service-type credentials of the user are checked before allowing console access.

When you disable management authorization with the **no aaa authorization exec** command, note the following:

- The service-type credentials of the user are not checked before allowing console access.
- If command authorization is configured, privilege-level attributes are still applied if they are found in the AAA server for RADIUS, LDAP, and TACACS+ users.

If you configure **aaa authentication console** commands to authenticate users when they access the CLI, ASDM, or the **enable** command, then the **aaa authorization exec** command can limit management access depending on the user configuration.

Note Serial access is not included in management authorization, so if you configure **aaa authentication serial console**, then any user who authenticates can access the console port.

To configure the user for management authorization, see the following requirements for each AAA server type or local user:

- LDAP mapped users—To map LDAP attributes, see the **ldap attribute-map** command.
- RADIUS users—Use the IETF RADIUS numeric **service-type** attribute, which maps to one of the following values:
  - Service-Type 5 (Outbound) denies management access. The user cannot use any services specified by the **aaa authentication console** commands (excluding the **serial** keyword; serial access is allowed). Remote access (IPsec and SSL) users can still authenticate and terminate their remote access sessions.
  - Service-Type 6 (Administrative) allows full access to any services specified by the **aaa authentication console** commands.
  - Service-Type 7 (NAS prompt) allows access to the CLI when you configure the **aaa authentication {telnet | ssh} console** command, but denies ASDM configuration access if you configure the **aaa authentication http console** command. ASDM monitoring access is allowed. If you configure **enable** authentication with the **aaa authentication enable console** command, the user cannot access privileged EXEC mode using the **enable** command.

Note The only recognized service-types are Login (1), Framed (2), Administrative (6), and NAS-Prompt (7). Using any other service-types results in denied access.

- TACACS+ users—Request authorization with the "service=shell" entry, and the server responds with PASS or FAIL, as follows:
  - PASS, privilege level 1 allows full access to any services specified by the **aaa authentication console** commands.
  - PASS, privilege level 2 and higher allows access to the CLI when you configure the **aaa authentication {telnet | ssh} console** command, but denies ASDM configuration access if you configure the **aaa authentication http console** command. ASDM monitoring access is allowed. If you configure enable authentication with the **aaa authentication enable console** command, the user cannot access privileged EXEC mode using the **enable** command.
  - FAIL denies management access. The user cannot use any services specified by the **aaa authentication console** commands (excluding the **serial** keyword; serial access is allowed).
- Local users—Set the **service-type** command, which is in the username configuration mode of the **username** command. By default, the **service-type** is **admin**, which allows full access to any services specified by the **aaa authentication console** commands.

Examples

The following example enables management authorization using the local database:

```
hostname(config)# aaa authorization exec LOCAL
```

Related Commands

Command	Description
aaa authentication console	Enables console authentication.
ldap attribute-map	Maps LDAP attributes.

service-type	Limits CLI access for a local user .
show running-config aaa	Displays the AAA configuration.

aaa authorization include, exclude

To enable authorization for connections through the ASA, use the **aaa authorization include** command in global configuration mode. To disable authorization, use the **no** form of this command. To exclude addresses from authorization, use the **aaa authorization exclude** command. To not exclude addresses from authorization, use the **no** form of this command.

aaa authorization {include | exclude} *service interface_name inside_ip inside_mask* [*outside_ip outside_mask*] *server_tag*

no aaa authorization {include | exclude} *service interface_name inside_ip inside_mask* [*outside_ip outside_mask*] *server_tag*

Syntax Description

exclude	Excludes the specified service and address from authorization if it was already specified by an **include** command.
include	Specifies the services and IP addresses that require authorization. Traffic that is not specified by an **include** statement is not processed.
inside_ip	Specifies the IP address on the higher security interface. This address might be the source or the destination address, depending on the interface to which you apply this command. If you apply the command to the lower security interface, then this address is the destination address. If you apply the command to the higher security interface, then this address is the source address. Use 0 to mean all hosts.
inside_mask	Specifies the network mask for the inside IP address. Use 0 if the IP address is 0. Use 255.255.255.255 for a host.
interface_name	Specifies the interface name from which users require authorization.
outside_ip	(Optional) Specifies the IP address on the lower security interface. This address might be the source or the destination address, depending on the interface to which you apply this command. If you apply the command to the lower security interface, then this address is the source address. If you apply the command to the higher security interface, then this address is the destination address. Use 0 to mean all hosts.
outside_mask	(Optional) Specifies the network mask for the outside IP address. Use 0 if the IP address is 0. Use 255.255.255.255 for a host.

server_tag	Specifies the AAA server group defined by the **aaa-server** command.
service	Specifies the services that require authorization. You can specify one of the following values: • **any** or **tcp/0** (specifies all TCP traffic) • ftp • http • **https** • **ssh** • telnet • **tcp/***port*[**-***port*] • **udp/***port*[**-***port*] • **icmp/***type* • *protocol*[**/***port*[**-***port*]] **Note** Specifying a port range might produce unexpected results at the authorization server. The ASA sends the port range to the server as a string, with the expectation that the server will parse it out into specific ports. Not all servers do this. In addition, you might want users to be authorized on specific services, which does not occur if a range is accepted.

Defaults

An IP address of **0** means "all hosts." Setting the local IP address to **0** lets the authorization server decide which hosts are authorized.

Fallback to the local database for authorization is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	The **exclude** parameter allows the user to specify a port to exclude to a specific host or hosts.

Usage Guidelines

To enable authorization for traffic that is specified by an ACL, use the **aaa authorization match** command. You cannot use the **match** command in the same configuration as the **include** and **exclude** commands. We suggest that you use the **match** command instead of the **include** and **exclude** commands; the **include** and **exclude** commands are not supported by ASDM.

You cannot use the **aaa authorization include** and **exclude** commands between same-security interfaces. For that scenario, you must use the **aaa authorization match** command.

You can configure the ASA to perform network access authorization with TACACS+. Authentication and authorization statements are independent; however, any unauthenticated traffic matched by an authorization statement will be denied. For authorization to succeed, a user must first authenticate with the ASA. Because a user at a given IP address only needs to authenticate one time for all rules and types, if the authentication session has not expired, authorization can occur even if the traffic is matched by an authentication statement.

After a user authenticates, the ASA checks the authorization rules for matching traffic. If the traffic matches the authorization statement, the ASA sends the username to the TACACS+ server. The TACACS+ server responds to the ASA with a permit or a deny for that traffic, based on the user profile. The ASA enforces the authorization rule in the response.

See the documentation for your TACACS+ server for information about configuring network access authorizations for a user.

For each IP address, one **aaa authorization include** command is permitted.

If the first attempt at authorization fails and a second attempt causes a timeout, use the **service resetinbound** command to reset the client that failed the authorization so that it will not retransmit any connections. An example authorization timeout message in Telnet follows.

```
Unable to connect to remote host: Connection timed out
```

Note Specifying a port range might produce unexpected results at the authorization server. The ASA sends the port range to the server as a string, with the expectation that the server will parse it out into specific ports. Not all servers do this. In addition, you might want users to be authorized on specific services, which does not occur if a range is accepted.

Examples

The following example uses the TACACS+ protocol:

```
hostname(config)# aaa-server tplus1 protocol tacacs+
hostname(config)# aaa-server tplus1 (inside) host 10.1.1.10 thekey timeout 20
hostname(config)# aaa authentication include any inside 0 0 0 0 tplus1
hostname(config)# aaa authorization include any inside 0 0 0 0
hostname(config)# aaa accounting include any inside 0 0 0 0 tplus1
hostname(config)# aaa authentication ssh console tplus1
```

In this example, the first command statement creates a server group named tplus1 and specifies the TACACS+ protocol for use with this group. The second command specifies that the authentication server with the IP address 10.1.1.10 resides on the inside interface and is in the tplus1 server group. The next three command statements specify that any users starting connections through the outside interface to any foreign host will be authenticated using the tplus1 server group, that the users who are successfully authenticated are authorized to use any service, and that all outbound connection information will be logged in the accounting database. The last command statement specifies that SSH access to the ASA console requires authentication from the tplus1 server group.

The following example enables authorization for DNS lookups from the outside interface:

```
hostname(config)# aaa authorization include udp/53 outside 0.0.0.0 0.0.0.0
```

The following example enables authorization of ICMP echo-reply packets arriving at the inside interface from inside hosts:

```
hostname(config)# aaa authorization include 1/0 inside 0.0.0.0 0.0.0.0
```

This means that users cannot ping external hosts if they have not been authenticated using Telnet, HTTP, or FTP.

The following example enables authorization only for ICMP echoes (pings) that arrive at the inside interface from an inside host:

```
hostname(config)# aaa authorization include 1/8 inside 0.0.0.0 0.0.0.0
```

Related Commands

Command	Description
aaa authorization command	Specifies whether or not command execution is subject to authorization, or configures administrative authorization to support fallback to the local user database if all servers in the specified server group are disabled.
aaa authorization match	Enables or disables the LOCAL or TACACS+ user authorization services for a specific access-list command name.
clear configure aaa	Removes or resets the configured AAA accounting values.
show running-config aaa	Displays the AAA configuration.

aaa authorization match

To enable authorization for connections through the ASA, use the **aaa authorization match** command in global configuration mode. To disable authorization, use the **no** form of this command.

aaa authorization match *acl_name interface_name server_tag*

no aaa authorization match *acl_name interface_name server_tag*

Syntax Description

acl_name	Specifies an extended ACL name. See the **access-list extended** command. The **permit** ACEs mark matching traffic for authorization, while **deny** entries exclude matching traffic from authorization.
interface_name	Specifies the interface name from which users require authentication.
server_tag	Specifies the AAA server group tag as defined by the **aaa-server** command.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

You cannot use the **aaa authorization match** command in the same configuration as the **include** and **exclude** commands. We suggest that you use the **match** command instead of the **include** and **exclude** commands; the **include** and **exclude** commands are not supported by ASDM.

You can configure the ASA to perform network access authorization with TACACS+. RADIUS authorization with the **aaa authorization match** command only supports authorization of VPN management connections to the ASA.

Authentication and authorization statements are independent; however, any unauthenticated traffic matched by an authorization statement will be denied. For authorization to succeed, a user must first authenticate with the ASA. Because a user at a given IP address only needs to authenticate one time for all rules and types, if the authentication session has not expired, authorization can occur even if the traffic is matched by an authentication statement.

After a user authenticates, the ASA checks the authorization rules for matching traffic. If the traffic matches the authorization statement, the ASA sends the username to the TACACS+ server. The TACACS+ server responds to the ASA with a permit or a deny for that traffic, based on the user profile. The ASA enforces the authorization rule in the response.

See the documentation for your TACACS+ server for information about configuring network access authorizations for a user.

If the first attempt at authorization fails and a second attempt causes a timeout, use the **service resetinbound** command to reset the client that failed the authorization so that it will not retransmit any connections. An example authorization timeout message in Telnet follows.

```
Unable to connect to remote host: Connection timed out
```

Note Specifying a port range might produce unexpected results at the authorization server. The ASA sends the port range to the server as a string, with the expectation that the server will parse it out into specific ports. Not all servers do this. In addition, you might want users to be authorized on specific services, which does not occur if a range is accepted.

Examples

The following example uses the tplus1 server group with the **aaa** commands:

```
hostname(config)# aaa-server tplus1 protocol tacacs+
hostname(config)# aaa-server tplus1 (inside) host 10.1.1.10 thekey timeout 20
hostname(config)# aaa authentication include any inside 0 0 0 0 tplus1
hostname(config)# aaa accounting include any inside 0 0 0 0 tplus1
hostname(config)# aaa authorization match myacl inside tplus1
```

In this example, the first command statement defines the tplus1 server group as a TACACS+ group. The second command specifies that the authentication server with the IP address 10.1.1.10 resides on the inside interface and is in the tplus1 server group. The next two command statements specify that any connections traversing the inside interface to any foreign host are authenticated using the tplus1 server group, and that all these connections are logged in the accounting database. The last command statement specifies that any connections that match the ACEs in myacl are authorized by the AAA servers in the tplus1 server group.

Related Commands

Command	Description
aaa authorization	Enables or disables user authorization.
clear configure aaa	Resets all aaa configuration parameters to the default values.
clear uauth	Deletes AAA authorization and authentication caches for one user or all users, which forces users to reauthenticate the next time that they create a connection.
show running-config aaa	Displays the AAA configuration.
show uauth	Displays the username provided to the authorization server for authentication and authorization purposes, the IP address to which the username is bound, and whether the user is only authenticated or has cached services.

aaa local authentication attempts max-fail

To limit the number of consecutive failed local login attempts that the ASA allows any given user account (with the exception of users with a privilege level of 15; this feature does not affect level 15 users), use the **aaa local authentication attempts max-fail** command in global configuration mode. To disable this feature and allow an unlimited number of consecutive failed local login attempts, use the **no** form of this command.

aaa local authentication attempts max-fail *number*

Syntax Description

number	The maximum number of times a user can enter a wrong password before being locked out. This number can be in the range 1-16.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

This command only affects authentication with the local user database. If you omit this command, there is no limit on the number of times a user can enter an incorrect password.

After a user makes the configured number of attempts with the wrong password, the user is locked out and cannot log in successfully until the administrator unlocks the username. Locking or unlocking a username results in a syslog message.

Users with a privilege level of 15 are not affected by this command; they cannot be locked out.

The number of failed attempts resets to zero and the lockout status resets to No when the user successfully authenticates or when the ASA reboots.

Examples

The following example shows use of the **aaa local authentication attempts max-limits** command to set the maximum number of failed attempts allowed to 2:

```
hostname(config)# aaa local authentication attempts max-limits 2
```

Related Commands

Command	Description
clear aaa local user lockout	Clears the lockout status of the specified users and set their failed-attempts counter to 0.
clear aaa local user fail-attempts	Resets the number of failed user authentication attempts to zero without modifying the user locked-out status.
show aaa local user	Shows the list of usernames that are currently locked.

aaa mac-exempt

To specify the use of a predefined list of MAC addresses to exempt from authentication and authorization, use the **aaa mac-exempt** command in global configuration mode. To disable the use of a list of MAC addresses, use the **no** form of this command.

aaa mac-exempt match *id*

no aaa mac-exempt match *id*

Syntax Description

id	Specifies a MAC list number configured with the **mac-list** command.

Defaults

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

You can only add one **aaa mac-exempt** command. Configure the MAC list number using the **mac-list** command before using the **aaa mac-exempt** command. Permit entries in the MAC list exempt the MAC addresses from authentication and authorization, while deny entries require authentication and authorization for the MAC address, if enabled. Because you can only add one instance of the **aaa mac-exempt** command, be sure that the MAC list includes all the MAC addresses that you want to exempt.

Examples

The following example bypasses authentication for a single MAC address:

```
hostname(config)# mac-list abc permit 00a0.c95d.0282 ffff.ffff.ffff
hostname(config)# aaa mac-exempt match abc
```

The following entry bypasses authentication for all Cisco IP Phones, which have the hardware ID 0003.E3:

```
hostname(config)# mac-list acd permit 0003.E300.0000 FFFF.FF00.0000
hostname(config)# aaa mac-exempt match acd
```

The following example bypasses authentication for a a group of MAC addresses except for 00a0.c95d.02b2:

```
hostname(config)# mac-list 1 deny 00a0.c95d.0282 ffff.ffff.ffff
hostname(config)# mac-list 1 permit 00a0.c95d.0000 ffff.ffff.0000
hostname(config)# aaa mac-exempt match 1
```

Related Commands

Command	Description
aaa authentication	Enables user authentication.
aaa authorization	Enables user authorization services.
aaa mac-exempt	Exempts a list of MAC addresses from authentication and authorization.
show running-config mac-list	Displays a list of MAC addresses previously specified in the **mac-list** command.
mac-list	Specifies a list of MAC addresses to be used to exempt MAC addresses from authentication and/or authorization.

aaa proxy-limit

To limit the number of concurrent authentication attempts (at the same time) for a given IP address, use the **aaa proxy-limit** command in global configuration mode. To return to the default proxy-limit value, use the **no** form of this command.

aaa proxy-limit *proxy_limit*

aaa proxy-limit disable

no aaa proxy-limit

Syntax Description

disable	Specifies that no proxies are allowed.
proxy_limit	Specifies the number of concurrent proxy connections allowed per user, from 1 to 128.

Defaults

The default proxy-limit value is 16.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**Context**	**System**
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

If a source address is a proxy server, consider excluding this IP address from authentication or increasing the number of allowable outstanding AAA requests.

For example, if two users were at the same IP address (perhaps connected to a terminal server) and both open a browser or connection and try to begin authenticating at exactly the same time, only one would be allowed, and the second would be blocked.

The first session from that IP address will be proxied and sent the auththentication request, while the other session would time out. This has nothing to do with how many connections a single username has.

Examples

The following example shows how to set the maximum number of outstanding authentication attempts (at the same time) for a given IP address:

```
hostname(config)# aaa proxy-limit 6
```

Related Commands

Command	Description
aaa authentication	Enables, disables, or views LOCAL, TACACS+, or RADIUS user authentication, on a server designated by the **aaa-server** command, or ASDM user authentication.
aaa authorization	Enables or disables LOCAL or TACACS+ user authorization services.
aaa-server host	Specifies a AAA server.
clear configure aaa	Removes or resets the configured AAA accounting values.
show running-config aaa	Displays the AAA configuration.

aaa-server

To create a AAA server group and configure AAA server parameters that are group-specific and common to all group hosts, use the **aaa-server** command in global configuration mode. To remove the designated group, use the **no** form of this command.

aaa-server *server-tag* **protocol** *server-protocol*

no aaa-server *server-tag* **protocol** *server-protocol*

Syntax Description

protocol *server-protocol*	Specifies the AAA protocol that the servers in the group support: • **http-form** • **kerberos** • **ldap** • **nt** • **radius** • **sdi** • **tacacs+**
server-tag	Specifies the server group name, which is matched by the name specified by the **aaa-server host** commands. Other AAA commands make reference to the AAA server group name.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**Context**	**System**
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.1(1)	The http-form protocol was added.
8.2(2)	The maximum number of AAA server groups was increased from 15 to 100 for single mode.
8.4(2)	The **ad-agent-mode** option in aaa-server group configuration mode was added.

Usage Guidelines

You can have up to 100 server groups in single mode or 4 server groups per context in multiple mode. Each group can have up to 15 servers in single mode or 4 servers in multiple mode. When a user logs in, the servers are accessed one at a time starting with the first server you specify in the configuration, until a server responds.

You control AAA server configuration by defining a AAA server group protocol with the **aaa-server** command, and then you add servers to the group using the **aaa-server host** command. When you enter the **aaa-server protocol** command, you enter aaa-server group configuration mode.

If you are using the RADIUS protocol and are in the aaa-server group configuration mode, note the following:

- To enable multi-session accounting for clientless SSL and AnyConnect sessions, enter the **interim-accounting-update** option. If you choose this option, interim accounting records are sent to the RADIUS server in addition to the start and stop records.
- To specify the shared secret between the ASA and the AD agent and indicate that a RADIUS server group includes AD agents that are not full-function RADIUS servers, enter the **ad-agent-mode** option. Only a RADIUS server group that has been configured using this option can be associated with user identity. As a result, the **test aaa-server** {**authentication** | **authorization**} *aaa-server-group* command is not available when a RADIUS server group that is not configured using the **ad-agent-mode** option is specified.

Examples

The following example shows the use of the **aaa-server** command to modify details of a TACACS+ server group configuration:

```
hostname(config)# aaa-server svrgrp1 protocol tacacs+
hostname(config-aaa-server-group)# accounting-mode simultaneous
hostname(config-aaa-server-group)# reactivation mode timed
hostname(config-aaa-server-group)# max-failed attempts 2
```

Related Commands

Command	Description
accounting-mode	Indicates whether accounting messages are sent to a single server (single mode) or sent to all servers in the group (simultaneous mode).
reactivation-mode	Specifes the method by which failed servers are reactivated.
max-failed-attempts	Specifies the number of failures that will be tolerated for any given server in the server group before that server is deactivated.
clear configure aaa-server	Removes all AAA server configurations.
show running-config aaa-server	Displays AAA server statistics for all AAA servers, for a particular server group, for a particular server within a particular group, or for a particular protocol.

aaa-server active, fail

To reactivate a AAA server that is marked failed, use the **aaa-server active** command in privileged EXEC mode. To fail an active server, use the **aaa-server fail** command in privileged EXEC mode.

aaa-server *server_tag* [**active | fail**] **host** {*server_ip* | *name*}

Syntax Description

active	Sets the server to an active state.
fail	Sets the server to a failed state.
host	Specifies the host IP address name or IP address.
name	Specifies the name of the server using either a name assigned locally using the **name** command or a DNS name. Maximum characters is 128 for DNS names and 63 characters for names assigned using the **name** command.
server_ip	Specifies the IP address of the AAA server.
server_tag	Specifies a symbolic name of the server group, which is matched by the name specified by the **aaa-server** command.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

Without this command, servers in a group that failed remain in a failed state until all servers in the group fail, after which all are reactivated.

Examples

The following example shows the state for server 192.168.125.60 and manually reactivates it:

```
hostname# show aaa-server group1 host 192.68.125.60
Server Group:  group1
Server Protocol: RADIUS
Server Address:  192.68.125.60
Server port:  1645
Server status: FAILED. Server disabled at 11:10:08 UTC  Fri Aug 22
...
hostname# aaa-server active host 192.168.125.60
```

```
hostname# show aaa-server group1 host 192.68.125.60
Server Group:  group1
Server Protocol: RADIUS
Server Address:  192.68.125.60
Server port:  1645
Server status: ACTIVE (admin initiated). Last Transaction at 11:40:09 UTC  Fri Aug 22
...
```

Related Commands

Command	Description
aaa-server	Creates and modifies AAA server groups.
clear configure aaa-server	Removes all AAA-server configuration.
show running-config aaa-server	Displays AAA server statistics for all AAA servers, for a particular server group, for a particular server within a particular group, or for a particular protocol.

aaa-server host

To configure a AAA server as part of a AAA server group and to configure AAA server parameters that are host-specific, use the **aaa-server host** command in global configuration mode. To remove a host configuration, use the **no** form of this command.

aaa-server *server-tag* [(*interface-name*)] **host** {*server-ip* | *name*} [*key*] [**timeout** *seconds*]

no aaa-server *server-tag* [(*interface-name*)] **host** {*server-ip* | *name*} [*key*] [**timeout** *seconds*]

Syntax Description

(*interface-name*)	(Optional) Specifies the network interface where the authentication server resides. The parentheses are required in this parameter. If you do not specify an interface, the default is **inside**, if available.
key	(Optional) Specifies a case-sensitive, alphanumeric keyword of up to 127 characters that is the same value as the key on the RADIUS or TACACS+ server. Any characters entered past 127 are ignored. The key is used between the ASA and the server for encrypting data between them. the key must be the same on both the ASA and server systems. Spaces are not permitted in the key, but other special characters are allowed. You can add or modify the key using the **key** command in host mode.
name	Specifies the name of the server using either a name assigned locally using the **name** command or a DNS name. Maximum characters is 128 for DNS names and 63 characters for names assigned using the **name** command.
server-ip	Specifies the IP address of the AAA server.
server-tag	Specifies a symbolic name of the server group, which is matched by the name specified by the **aaa-server** command.
timeout *seconds*	(Optional) The timeout interval for the request. This is the time after which the ASA gives up on the request to the primary AAA server. If there is a standby AAA server, the ASA sends the request to the backup server. You can modify the timeout interval using the **timeout** command in host configuration mode.

Defaults

The default timeout value is 10 seconds.

The default interface is inside.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	Support for DNS names was added.
9.0(1)	Support for user identity was added.

Usage Guidelines

You control AAA server configuration by defining a AAA server group with the **aaa-server** command, and then you add servers to the group using the **aaa-server host** command. When you use the **aaa-server host** command, you enter the aaa-server host configuration mode, from which you can specify and manage host-specific AAA server connection data.

You can have up to 15 server groups in single mode or 4 server groups per context in multiple mode. Each group can have up to 16 servers in single mode or 4 servers in multiple mode. When a user logs in, the servers are accessed one at a time starting with the first server that you specify in the configuration, until a server responds.

Examples

The following example configures a Kerberos AAA server group named “watchdogs”, adds a AAA server to the group, and defines the Kerberos realm for the server:

Note Kerberos realm names use numbers and upper-case letters only. Although the ASA accepts lower-case letters for a realm name, it does not translate lower-case letters to upper-case letters. Be sure to use upper-case letters only.

```
hostname(config)# aaa-server watchdogs protocol kerberos
hostname(config-aaa-server-group)# exit
hostname(config)# aaa-server watchdogs host 192.168.3.4
hostname(config-aaa-server-host)# kerberos-realm EXAMPLE.COM
```

The following example configures an SDI AAA server group named “svrgrp1”, and then adds a AAA server to the group, sets the timeout interval to 6 seconds, sets the retry interval to 7 seconds, and configures the SDI version to version 5:

```
hostname(config)# aaa-server svrgrp1 protocol sdi
hostname(config-aaa-server-group)# exit
hostname(config)# aaa-server svrgrp1 host 192.168.3.4
hostname(config-aaa-server-host)# timeout 6
hostname(config-aaa-server-host)# retry-interval 7
hostname(config-aaa-server-host)# sdi-version sdi-5
```

The following example shows how to narrow down the search path to the targeted groups when you use the **aaa-server** *aaa_server_group_tag* command for LDAP search:

```
hostname(config)# aaa-server CISCO_AD_SERVER protocol ldap
hostname(config)# aaa-server CISCO_AD_SERVER host 10.1.1.1
hostname(config-aaa-server-host)# server-port 636
hostname(config-aaa-server-host)# ldap-base-dn DC=cisco,DC=com
hostname(config-aaa-server-host)# ldap-group-base-dn OU=Cisco Groups,DC=cisco,DC=com
hostname(config-aaa-server-host)# ldap-scope subtree
hostname(config-aaa-server-host)# ldap-login-password *
hostname(config-aaa-server-host)# ldap-login-dn CISCO\username1
hostname(config-aaa-server-host)# ldap-over-ssl enable
hostname(config-aaa-server-host)# server-type microsoft
```

Note When the **ldap-group-base-dn** command is specified, all groups must reside under it in the LDAP directory hierarchy and no group can reside outside this path.

The **ldap-group-base-dn** command takes effect only when at least one activated user-identity based policy exists.

The **server-type microsoft** command, which is not the default, must be configured.

The first **aaa-server** *aaa_server_group_tag* **host** command is used for LDAP operations.

Related Commands

Command	Description
aaa-server	Creates and modifies AAA server groups.
clear configure aaa-server	Removes all AAA server configurations.
show running-config aaa-server	Displays AAA server statistics for all AAA servers, for a particular server group, for a particular server within a particular group, or for a particular protocol.

absolute

To define an absolute time when a time range is in effect, use the **absolute** command in time-range configuration mode. To not specify a time for a time range, use the **no** form of this command.

absolute [**end** *time date*] [**start** *time date*]

no absolute

Syntax Description

date	(Optional) Specifies the date in the format, day month year; for example, 1 January 2006. The valid range of years is 1993 through 2035.
end	(Optional) Specifies the end of the time range.
start	(Optional) Specifies the start of the time range.
time	(Optional) Specifies the time in the format HH:MM. For example, 8:00 is 8:00 a.m. and 20:00 is 8:00 p.m.

Defaults

If no start time and date are specified, the permit or deny statement is in effect immediately and always on. Similarly, the maximum end time is 23:59 31 December 2035. If no end time and date are specified, the associated permit or deny statement is in effect indefinitely.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Time-range configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

To implement a time-based ACL, use the **time-range** command to define specific times of the day and week. Then use the **access-list extended time-range** command to bind the time range to an ACL.

Examples

The following example activates an ACL at 8:00 a.m. on 1 January 2006:

```
hostname(config-time-range)# absolute start 8:00 1 January 2006

Because no end time and date are specified, the associated ACL is in effect indefinitely.
```

Related Commands

Command	Description
access-list extended	Configures a policy for permitting or denying IP traffic through the ASA.
default	Restores default settings for the **time-range** command **absolute** and **periodic** keywords.
periodic	Specifies a recurring (weekly) time range for functions that support the time-range feature.
time-range	Defines access control to the ASA based on time.

accept-subordinates

To configure the ASA to accept subordinate CA certificates if delivered during phase one IKE exchange when not previously installed on the device, use the **accept-subordinates** command in crypto ca trustpoint configuration mode. To restore the default setting, use the **no** form of the command.

accept-subordinates

no accept-subordinates

Syntax Description

This command has no arguments or keywords.

Defaults

The default setting is on (subordinate certificates are accepted).

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Crypto ca trustpoint configuration	•	•	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

During phase 1 processing, an IKE peer might pass both a subordinate certificate and an identity certificate. The subordinate certificate might not be installed on the ASA. This command lets an administrator support subordinate CA certificates that are not configured as trustpoints on the device without requiring that all subordinate CA certificates of all established trustpoints be acceptable; in other words, this command lets the device authenticate a certificate chain without installing the entire chain locally.

Examples

The following example enters crypto ca trustpoint configuration mode for trustpoint central, and allows the ASA to accept subordinate certificates for trustpoint central:

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# accept-subordinates
hostname(ca-trustpoint)#
```

Related Commands

Command	Description
crypto ca trustpoint	Enters trustpoint configuration mode.
default enrollment	Returns enrollment parameters to their defaults.

access-group

To bind an ACL to a single interface, use the **access-group** command in global configuration mode. To unbind an ACL from the interface, use the **no** form of this command.

access-group *access-list* {**in | out**} **interface** *interface_name* [***per-user-override*** **|** ***control-plane***]

no access-group *access-list* {**in | out**} **interface** *interface_name*

To apply a single set of global rules to all interfaces with the single command, use the **access-group global** command in global configuration mode. To remove the global rules from all configured interfaces, use the **no** form of this command.

access-group *access-list* [**global**]

no access-group *access-list* **[global**]

Syntax Description

access-list	ACL *id.*
control-plane	(Optional) Specifies whether or not the rule is for to-the-box traffic. For example, you can use this option to block certain remote IP addresses from initiating a VPN session to the ASA by blocking ISAKMP. Access rules for to-the-box management traffic (defined by such commands as **http**, **ssh**, or **telnet**) have higher precedence than an ACL applied with the **control-plane** option. Therefore, such permitted management traffic will be allowed to come in even if explicitly denied by the to-the-box ACL.
global	(Optional) Applies an ACL to all configured interfaces.
in	Filters the inbound packets at the specified interface.
interface *interface-name*	Name of the network interface.
out	Filters the outbound packets at the specified interface.
per-user-override	(Optional) Allows downloadable user ACLs to override the ACL applied to the interface.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**Context**	**System**
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.
8.3(1)	This command was modified to support global policies.

Usage Guidelines

Interface-specific access-group rules have higher priority that global rules, so at the time of packet classification, interface-specific rules are processed before global rules.

Usage Guidelines for Interface-specific Rules

The **access-group** command binds an ACL to an interface. The ACL is applied to traffic inbound to an interface. If you enter the **permit** option in an **access-list** command statement, the ASA continues to process the packet. If you enter the **deny** option in an **access-list** command statement, the ASA discards the packet and generates the following syslog message.

`%ASA-4-106019: IP packet from` *`source_addr`* `to` *`destination_addr`*`, protocol` *`protocol`* `received from interface` *`interface_name`* `deny by access-group` *`id`*

The **per-user-override** option allows downloaded ACLs to override the ACL applied to the interface. If the **per-user-override** option is not present, the ASA preserves the existing filtering behavior. When **per-user-override** is present, the ASA allows the **permit** or **deny** status from the per-user access-list (if one is downloaded) associated to a user to override the permit or deny status from the **access-group** command associated ACL. Additionally, the following rules are observed:

- At the time a packet arrives, if there is no per-user ACL associated with the packet, the interface ACL will be applied.
- The per-user ACL is governed by the timeout value specified by the **uauth** option of the **timeout** command but it can be overridden by the AAA per-user session timeout value.
- Existing ACL log behavior will be the same. For example, if user traffic is denied because of a per-user ACL, syslog message 109025 will be logged. If user traffic is permitted, no syslog message is generated. The log option in the per-user access-list will have no effect.

For VPN remote access traffic, the behavior depends on whether there is a **vpn-filter** applied in the group policy and whether you set the **per-user-override** option:

- No **per-user-override**, no **vpn-filter**—Traffic is matched against the interface ACL (per the default **no sysopt connection permit-vpn** command).
- No **per-user-override**, **vpn-filter**—Traffic is matched first against the interface ACL, then against the VPN filter.
- **per-user-override**, **vpn-filter**—Traffic is matched against the VPN filter only.

Always use the **access-list** command with the **access-group** command.

The **access-group** command binds an ACL to an interface. The **in** keyword applies the ACL to the traffic on the specified interface. The **out** keyword applies the ACL to the outbound traffic.

Note If all of the functional entries (the permit and deny statements) are removed from an ACL that is referenced by one or more **access-group** commands, the **access-group** commands are automatically removed from the configuration. The **access-group** command cannot reference empty ACLs or ACLs that contain only a remark.

Usage Guidelines for Global Rules

The **access-group global** command applies a single set of global rules on all traffic, no matter which interface the traffic arrives at the ASA.

Global rules for the **access-group global** command support extended ACLs only.

All global rules apply only to traffic in the ingress (input) direction. Global rules do not support egress (output) traffic.

Global rules for **access-group global** do not support the **control-plane** nor the **per-user-override** options that are supported in interface-specific access rules.

If global rules are configured in conjunction with interface access rules, then the interface access rule, which is specific, is processed before the global access rule, which is general.

Examples

The following example shows how to use the **access-group global** command to apply an ACL to all configured interfaces:

```
hostname(config)# access-list acl-1 extended permit ip host 10.1.2.2 host 10.2.2.2
hostname(config)# access-list acl-2 extended deny ip any any

hostname(config)# access-group acl-2
hostname(config)# access-group acl-1 in interface outside

hostname(config)# show run access-group acl-2
hostname(config)# access-group acl-1 in interface outside

hostname(config)# access-group acl-2 global
```

The preceding access-group configuration adds the following rules in the classification table (output from the **show asp table classify** command):

```
in  id=0xb1f90068, priority=13, domain=permit, deny=false
        hits=0, user_data=0xaece1ac0, cs_id=0x0, flags=0x0, protocol=0
        src ip=10.1.2.2, mask=255.255.255.255, port=0
        dst ip=10.2.2.2, mask=255.255.255.255, port=0, dscp=0x0
        input_ifc=outside, output_ifc=any
in  id=0xb1f2a250, priority=12, domain=permit, deny=true
        hits=0, user_data=0xaece1b40, cs_id=0x0, flags=0x0, protocol=0
        src ip=0.0.0.0, mask=0.0.0.0, port=0
        dst ip=0.0.0.0, mask=0.0.0.0, port=0, dscp=0x0
        input_ifc=any, output_ifc=any
in  id=0xb1f90100, priority=11, domain=permit, deny=true
        hits=0, user_data=0x5, cs_id=0x0, flags=0x0, protocol=0
        src ip=0.0.0.0, mask=0.0.0.0, port=0
        dst ip=0.0.0.0, mask=0.0.0.0, port=0, dscp=0x0
        input_ifc=outside, output_ifc=any
in  id=0xb1f2a3f8, priority=11, domain=permit, deny=true
        hits=0, user_data=0x5, cs_id=0x0, flags=0x0, protocol=0
        src ip=0.0.0.0, mask=0.0.0.0, port=0
        dst ip=0.0.0.0, mask=0.0.0.0, port=0, dscp=0x0
        input_ifc=any, output_ifc=any
```

The preceding rule passes traffic from 10.1.2.2 to 10.2.2.2 on the output interface and drops traffic from 10.1.1.10 to 10.2.2.20 on the output interface due to the global deny rule.

The following example allows global access to an HTTP server (with the IP address 10.2.2.2) in the DMZ from anywhere:

```
hostname(config)# access-list global_acl permit tcp any host 10.2.2.2 eq 80
hostname(config)# access-group global_acl global
```

The preceding rule permits the HTTP connection from outside host 10.1.2.2 to host 10.2.2.2, and it permits the HTTP connection from the inside host 192.168.0.0 to host 10.2.2.2.

Note If you have no global policy support, the preceding ACL must be applied to all applicable interfaces.

The following example shows how a global policy and an interface policy can be used together. The example allows access to a server (with the IP address 10.2.2.2) from any inside host, but it denies access to the server from any other host. The interface policy takes precedence.

```
hostname(config)# access-list inside_acl permit tcp any host 10.2.2.2 eq 23
hostname(config)# access-list global_acl deny ip any host 10.2.2.2
hostname(config)# access-group inside_acl in interface inside
hostname(config)# access-group global_acl global
```

The preceding rule denies the SSH connection from outside host 10.1.2.2 to host 10.2.2.2, and it permits the SSH connection from the inside host 192.168.0.0 to host 10.2.2..2.

The following example shows how NAT and the global access control policy work together. The example permits one HTTP connection from outside host 10.1.2.2 to host 10.2.2.2, permits another HTTP connection from inside host 192.168.0.0 to host 10.2.2.2, and denies (by implicit rule), one HTTP connection from outside host 10.255.255.255 to host 172.31.255.255.

```
hostname(config)# object network dmz-server host 10.1.1.2
hostname(config)# nat (any, any) static 10.2.2.2
hostname(config)# access-list global_acl permit tcp any host 10.2.2.2 eq 80
hostname(config)# access-group global_acl global
```

The following example shows how NAT and the global access control policy work together. The example permits one HTTP connection from host 10.1.1.1 to host 192.168.0.0, permits another HTTP connection from host 209.165.200.225 to host 172.16.0.0, and denies one HTTP connection from host 10.1.1.1 to host 172.16.0.0.

```
hostname(config)# object network 10.1.1.1 host 10.1.1.1
hostname(config)# object network 172.16.0.0 host 172.16.0.0
hostname(config)# object network 192.168.0.0 host 192.168.0.0
hostname(config)# nat (inside, any) source static 10.1.1.1 10.1.1.1 destination static
                  192.168.0.0 172.16.0.0
hostname(config)# access-list global_acl permit ip object 10.1.1.1 object 172.16.0.0
hostname(config)# access-list global_acl permit ip host 209.165.200.225 object 172.16.0.0
hostname(config)# access-list global_acl deny ip any 172.16.0.0
hostname(config)# access-group global_acl global
```

Related Commands

Command	Description
access-list extended	Creates an ACL or uses a downloadable ACL.
clear configure access-group	Removes access groups from all the interfaces.
show running-config access-group	Displays the current ACL bound to the interfaces.

access-list alert-interval

To specify the time interval between deny flow maximum messages, use the **access-list alert-interval** command in global configuration mode. To return to the default settings, use the **no** form of this command.

access-list alert-interval *secs*

no access-list alert-interval

Syntax Description

secs	Time interval between deny flow maximum message generation; valid values are from 1 to 3600 seconds. The default value is 300 seconds.

Defaults

The default is 300 seconds.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The **access-list alert-interval** command sets the time interval for generating syslog message 106001, which alerts you that the ASA has reached a deny flow maximum. When the deny flow maximum is reached, another syslog message 106001 is generated if at least *secs* seconds have passed since the last syslog message 106001 was generated.

See the **access-list deny-flow-max** command for information about the deny flow maximum message generation.

Examples

The following example shows how to specify the time interval between deny flow maximum messages:

```
hostname(config)# access-list alert-interval 30
```

Related Commands

Command	Description
access-list deny-flow-max	Specifies the maximum number of concurrent deny flows that can be created.
access-list extended	Adds an ACL to the configuration and is used to configure policy for IP traffic through the ASA.
clear access-group	Clears an ACL counter.
clear configure access-list	Clears ACLs from the running configuration.
show access-list	Displays the ACL entries by number.

access-list deny-flow-max

To specify the maximum number of concurrent deny flows that can be created, use the **access-list deny-flow-max** command in global configuration mode. To return to the default settings, use the **no** form of this command.

access-list deny-flow-max

no access-list deny-flow-max

Syntax Description

This command has no arguments or keywords.

Defaults

The default is 4096 concurrent deny flows.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Syslog message 106101 is generated when the ASA has reached the maximum number, *n*, of ACL deny flows.

Examples

The following example shows how to specify the maximum number of concurrent deny flows that can be created:

```
hostname(config)# access-list deny-flow-max 256
```

Related Commands

Command	Description
access-list extended	Adds an ACL to the configuration and is used to configure policy for IP traffic through the ASA.
clear access-group	Clears an ACL counter.
clear configure access-list	Clears ACLs from the running configuration.

Command	Description
show access-list	Displays the ACL entries by number.
show running-config access-list	Displays the current running access list configuration.

access-list ethertype

To configure an ACL that controls traffic based on its EtherType, use the **access-list ethertype** command in global configuration mode. To remove the ACL, use the **no** form of this command.

access-list *id* **ethertype** {**deny** | **permit**} {**ipx** | **is-is** | **bpdu** | **mpls-unicast** | **mpls-multicast** | **any** | *hex_number*}

no access-list *id* **ethertype** {**deny** | **permit**} {**ipx** | **is-is** | **bpdu** | **mpls-unicast** | **mpls-multicast** | **any** | *hex_number*}

Syntax Description

any	Permits or denies all traffic.
bpdu	Permits or denies bridge protocol data units. By default, BPDUs are denied.
deny	Denies traffic.
hex_number	Permits or denies traffic with a particular EtherType, specified as a 16-bit hexadecimal number greater than or equal to 0x600.
id	Specifies the name or number of an ACL.
ipx	Permits or denies IPX.
is-is	Permits or denies IS-IS.
mpls-multicast	Permits or denies MPLS multicast.
mpls-unicast	Permits or denies MPLS unicast.
permit	Permits traffic.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**Context**	**System**
Global configuration	—	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.
8.4(5), 9.1(2)	We added the **is-is** keyword.

Usage Guidelines

An EtherType ACL is made up of one or more Access Control Entries (ACEs) that specify an EtherType. An EtherType rule controls any EtherType identified by a 16-bit hexadecimal number, as well as selected traffic types.

Note For EtherType ACLs, the implicit deny at the end of the ACL does not affect IP traffic or ARPs; for example, if you allow EtherType 8037, the implicit deny at the end of the ACL does not now block any IP traffic that you previously allowed with an extended ACL (or implicitly allowed from a high security interface to a low security interface). However, if you explicitly deny all traffic with an EtherType ACE, then IP and ARP traffic is denied; only physical protocol traffic, such as auto-negotiation, is still allowed.

Supported EtherTypes and Other Traffic

An EtherType rule controls the following:

- EtherType identified by a 16-bit hexadecimal number, including common types IPX and MPLS unicast or multicast.
- Ethernet V2 frames.
- BPDUs, which are permitted by default. BPDUs are SNAP-encapsulated, and the ASA is designed to specifically handle BPDUs.
- Trunk port (Cisco proprietary) BPDUs. Trunk BPDUs have VLAN information inside the payload, so the ASA modifies the payload with the outgoing VLAN if you allow BPDUs.
- IS-IS

The following types of traffic are not supported:

- 802.3-formatted frames—These frames are not handled by the rule because they use a length field as opposed to a type field.

Access Rules for Returning Traffic

Because EtherTypes are connectionless, you need to apply the rule to both interfaces if you want traffic to pass in both directions.

Allowing MPLS

If you allow MPLS, ensure that Label Distribution Protocol and Tag Distribution Protocol TCP connections are established through the ASA by configuring both MPLS routers connected to the ASA to use the IP address on the ASA interface as the router-id for LDP or TDP sessions. (LDP and TDP allow MPLS routers to negotiate the labels (addresses) used to forward packets.)

On Cisco IOS routers, enter the appropriate command for your protocol, LDP or TDP. The interface is the interface connected to the ASA.

```
hostname(config)# mpls ldp router-id interface force
```

Or

```
hostname(config)# tag-switching tdp router-id interface force
```

Examples

The following example shows how to add an EtherType ACL:

```
hostname(config)# access-list ETHER ethertype permit ipx
hostname(config)# access-list ETHER ethertype permit bpdu
hostname(config)# access-list ETHER ethertype permit mpls-unicast
hostname(config)# access-group ETHER in interface inside
```

Related Commands

Command	Description
access-group	Binds the ACL to an interface.
clear access-group	Clears ACL counters.
clear configure access-list	Clears an ACL from the running configuration.
show access-list	Displays the ACL entries by number.
show running-config access-list	Displays the current running access-list configuration.

access-list extended

To add an Access Control Entry (ACE), use the **access-list extended** command in global configuration mode. To remove an ACE, use the **no** form of this command.

For any type of traffic, no ports:

access-list *access_list_name* [**line** *line_number*] **extended** {**deny** | **permit**} *protocol_argument* [*user_argument*] [*security_group_argument*] *source_address_argument* [*security_group_argument*] *dest_address_argument* [**log** [[*level*] [**interval** *secs*] | **disable** | **default**]] [**inactive** | **time-range** *time_range_name*]

no access-list *access_list_name* [**line** *line_number*] **extended** {**deny** | **permit**} *protocol_argument* [*user_argument*] [*security_group_argument*] *source_address_argument* [*security_group_argument*] *dest_address_argument* [**log** [[*level*] [**interval** *secs*] | **disable** | **default**]] [**inactive** | **time-range** *time_range_name*]

For TCP or UDP traffic, with ports:

access-list *access_list_name* [**line** *line_number*] **extended** {**deny** | **permit**} {**tcp** | **udp**} [*user_argument*] [*security_group_argument*] *source_address_argument* [*port_argument*] [*security_group_argument*] *dest_address_argument* [*port_argument*] [**log** [[*level*] [**interval** *secs*] | **disable** | **default**]] [**inactive** | **time-range** *time_range_name*]

no access-list *access_list_name* [**line** *line_number*] **extended** {**deny** | **permit**} {**tcp** | **udp**} [*user_argument*] [*security_group_argument*] *source_address_argument* [*port_argument*] [*security_group_argument*] *dest_address_argument* [*port_argument*] [**log** [[*level*] [**interval** *secs*] | **disable** | **default**]] [**inactive** | **time-range** *time_range_name*]

For ICMP traffic, with ICMP type:

access-list *access_list_name* [**line** *line_number*] **extended** {**deny** | **permit**} **icmp** [*user_argument*] [*security_group_argument*] *source_address_argument* [*security_group_argument*] *dest_address_argument* [*icmp_argument*] [**log** [[*level*] [**interval** *secs*] | **disable** | **default**]] [**inactive** | **time-range** *time_range_name*]

no access-list *access_list_name* [**line** *line_number*] **extended** {**deny** | **permit**} **icmp** [*user_argument*] [*security_group_argument*] *source_address_argument* [*security_group_argument*] *dest_address_argument* [*icmp_argument*] [**log** [[*level*] [**interval** *secs*] | **disable** | **default**]] [**inactive** | **time-range** *time_range_name*]

Syntax Description

access_list_name	Specifies the ACL ID, as a string or integer up to 241 characters in length. The ID is case-sensitive. **Tip** Use all capital letters to see the ACL ID better in your configuration.
default	(Optional) Sets logging to the default method, which is to generate system log message 106023 for each denied packet.

deny	Denies a packet if the conditions are matched. In the case of network access (the **access-group** command), this keyword prevents the packet from passing through the ASA. In the case of applying application inspection to a class map (the **class-map** and **inspect** commands), this keyword exempts the traffic from inspection. Some features do not allow deny ACEs to be used. See the command documentation for each feature that uses an ACL for more information.
dest_address_argument	Specifies the IP address or FQDN to which the packet is being sent. Available arguments include: • **host** *ip_address*—Specifies an IPv4 host address. • *dest_ip_address mask*—Specifies an IPv4 network address and subnet mask. When you specify a network mask, the method is different from the Cisco IOS software **access-list** command. The ASA uses a network mask (for example, 255.255.255.0 for a Class C mask). The Cisco IOS mask uses wildcard bits (for example, 0.0.0.255). • *ipv6-address/prefix-length*—Specifies an IPv6 host or network address and prefix. • **any**, **any4**, and **any6**—**any** specifies both IPv4 and IPv6 traffic; **any4** specifies only IPv4 traffic; and **any6** specifies any6 traffic. • **interface**—Specifies the interface address. You must specify the interface keyword instead of specifying the actual IP address in the ACL when the traffic source is a device interface. For example, you can use this option to block certain remote IP addresses from initiating a VPN session to the ASA by blocking ISAKMP. Any traffic originated from or destined to the ASA, itself, requires that you use the **access-group** command with the **control-plane** optional keyword. • **object** *nw_obj_id*—Specifies a network object created using the **object network** command. • **object-group** *nw_grp_id*—Specifies a network object group created using the **object-group network** command.
disable	(Optional) Disables logging for this ACE.
icmp_argument	(Optional) Specifies the ICMP type and code. • *icmp_type* [*icmp_code*]—Specifies the ICMP type by name or number, and the optional ICMP code for that type. If you do not specify the code, then all codes are used. • **object-group** *icmp_grp_id*—Specifies an ICMP object group created using the **object-group icmp** command.
inactive	(Optional) Disables an ACE. To reenable it, enter the entire ACE without the **inactive** keyword. This feature lets you keep a record of an inactive ACE in your configuration to make reenabling easier.
interval *secs*	(Optional) Specifies the log interval at which to generate system log message 106100. Valid values are from 1 to 600 seconds. The default is 300.
level	(Optional) Sets the system log message 106100 severity level from 0 to 7. The default level is 6 (informational).

line *line-num*	(Optional) Specifies the line number at which to insert the ACE. If you do not specify a line number, the ACE is added to the end of the ACL. The line number is not saved in the configuration; it only specifies where to insert the ACE.
log	(Optional) Sets logging options when a **ACE** matches a packet for network access (an ACL applied with the **access-group** command). If you enter the **log** keyword without any arguments, you enable system log message 106100 at the default level (6) and for the default interval (300 seconds). If you do not enter the **log** keyword, then the default system log message 106023 is generated.
permit	Permits a packet if the conditions are matched. In the case of network access (the **access-group** command), this keyword lets the packet pass through the ASA. In the case of applying application inspection to a class map (the **class-map** and **inspect** commands), this keyword applies inspection to the packet.
port_argument	(Optional) If you set the protocol to TCP or UDP, specifies the source and/or destination port. Available arguments include: • *operator port*—The *operator* can be one of the following: – **lt**—less than – **gt**—greater than – **eq**—equal to – **neq**—not equal to – **range**—an inclusive range of values. When you use this operator, specify two port numbers, for example: `range 100 200` The *port* can be the integer or name of a TCP or UDP port. DNS, Discard, Echo, Ident, NTP, RPC, SUNRPC, and Talk each require one definition for TCP and one for UDP. TACACS+ requires one definition for port 49 on TCP. • **object-group** *service_grp_id*—Specifies a service object group created using the **object-group service** command.
protocol_argument	Specifies the IP protocol. Available arguments include: • *name* or *number*—Specifies the protocol name or number. For example, UDP is 17, TCP is 6, and EGP is 47. Specify **ip** to apply to all protocols. • **object-group** *protocol_grp_id*—Specifies a protocol object group created using the **object-group protocol** command. • **object** *service_obj_id*—Specifies a service object created using the **object service** command. A TCP, UDP, or ICMP service object can include a protocol and a source and/or destination port or ICMP type and code, which are used when matching traffic to the ACE; you do not have to configure the port/type separately in the ACE. • **object-group** *service_grp_id*—Specifies a service object group created using the **object-group service** command.

security_group_argument	For use with the TrustSec feature, specifies the security group for which to match traffic in addition to the source or destination address. Available arguments include: • **object-group-security** *security_obj_grp_id*—Specifies a security object group created using the **object-group security** command. • **security-group** {**name** *security_grp_id* | **tag** *security_grp_tag*}—Specifies a security group name or tag.
source_address_argument	Specifies the IP address or FQDN from which the packet is being sent. Available arguments include: • **host** *ip_address*—Specifies an IPv4 host address. • *dest_ip_address mask*—Specifies an IPv4 network address and subnet mask. When you specify a network mask, the method is different from the Cisco IOS software **access-list** command. The ASA uses a network mask (for example, 255.255.255.0 for a Class C mask). The Cisco IOS mask uses wildcard bits (for example, 0.0.0.255). • *ipv6-address*/*prefix-length*—Specifies an IPv6 host or network address and prefix. • **any**, **any4**, and **any6**—**any** specifies both IPv4 and IPv6 traffic; **any4** specifies only IPv4 traffic; and **any6** specifies any6 traffic. • **interface**—Specifies the interface address. You must specify the interface keyword instead of specifying the actual IP address in the ACL when the traffic source is a device interface. For example, you can use this option to block certain remote IP addresses from initiating a VPN session to the ASA by blocking ISAKMP. Any traffic originated from or destined to the ASA, itself, requires that you use the **access-group** command with the **control-plane** optional keyword. • **object** *nw_obj_id*—Specifies a network object created using the **object network** command. • **object-group** *nw_grp_id*—Specifies a network object group created using the **object-group network** command.
tcp	Sets the protocol to TCP.
time-range *time_range_name*	(Optional) Schedules each ACE to be activated at specific times of the day and week by applying a time range to the ACE. See the **time-range** command for information about defining a time range.

udp	Sets the protocol to UDP.
user_argument	For use with the identity firewall feature, specifies the user or group for which to match traffic in addition to the source address. Available arguments include: • **object-group-user** *user_obj_grp_id*—Specifies a user object group created using the **object-group user** command. • **user** {[*domain_nickname*\]*name* | **any** | **none**}—Specifies a user name. Specify **any** to match all users with user credentials, or **none** to match users without user credentials. These options are especially useful for combining **access-group** and **aaa authentication match** policies. • **user-group** [*domain_nickname*\\]*user_group_name*—Specifies a user group name.

Defaults

- ACE logging generates system log message 106023 for denied packets. A **deny ACE** must be present to log denied packets.
- When the **log** keyword is specified, the default level for system log message 106100 is 6 (informational), and the default interval is 300 seconds.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**Context**	**System**
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.
8.3(1)	When using NAT or PAT, mapped addresses and ports are no longer required in an ACL for several features. You should now always use the real, untranslated addresses and ports for these features. Using the real address and port means that if the NAT configuration changes, you do not need to change the ACLs. See the "Features That Use Real IP Addresses" section on page 1-74 for more information.
8.4(2)	You can now use identity firewall users and groups for the source and destination, in addition to the source or destination IP address. Support for **user**, **user-group**, and **object-group-user** were added for the source and destination.
9.0(1)	You can now use TrustSec security groups for the source and destination, in addition to the source or destination IP address. Support for **security-group** and **object-group-security** were added for the source or destination.

Release	Modification
9.0(1)	Support for IPv6 was added. The **any** keyword was changed to represent IPv4 and IPv6 traffic. The **any4** and **any6** keywords were added to represent IPv4-only and IPv6-only traffic, respectively. You can specify a mix of IPv4 and IPv6 addresses for the source and destination. If you use NAT to translate between IPv4 and IPv6, the actual packet will not include a mix of IPv4 and IPv6 addresses; however, for many features, the ACL always uses the real IP addresses and does not consider the NAT mapped addresses. The IPv6-specific ACLs are deprecated. Existing IPv6 ACLs are migrated to extended ACLs. See the release notes for more information about migration. For information about ACL migration, see the 9.0 release notes.
9.0(1)	Support for the ICMP code was added. When you specify **icmp** as the protocol, you can enter *icmp_type* [*icmp_code*].

Usage Guidelines

An ACL is made up of one or more ACEs with the same ACL ID. ACLs are used to control network access or to specify traffic for many features to act upon. Each ACE that you enter for a given ACL name is appended to the end of the ACL, unless you specify the line number in the ACE. To remove the entire ACL, use the **clear configure access-list** command.

Order of ACEs

The order of ACEs is important. When the ASA decides whether to forward or drop a packet, the ASA tests the packet with each ACE in the order in which the entries are listed. After a match is found, no more ACEs are checked. For example, if you create an ACE at the beginning of an ACL that explicitly permits all traffic, no further statements are ever checked.

Features That Use Real IP Addresses

Note For ACL migration information, see the *Cisco ASA 5500 Migration to Version 8.3 and Later.*

The following commands and features now use real IP addresses in the ACLs:

- **access-group** command
- Modular Policy Framework **match access-list** command
- Botnet Traffic Filter **dynamic-filter enable classify-list** command
- AAA **aaa ... match** commands
- WCCP

Features That Use Mapped IP Addresses

The following features use ACLs, but these ACLs will continue to use the mapped values as seen on an interface:

- IPsec ACLs
- **capture** command ACLs
- Per-user ACLs
- Routing protocol ACLs
- All other feature ACLs

Features That Do Not Support IDFW, FQDN, and TrustSec ACLs

The following features use ACLs, but cannot accept an ACL with IDFW, FQDN, or TrustSec values:

- **route-map** command
- VPN **crypto map** command
- VPN **group-policy** command, except for **vpn-filter**
- WCCP
- DAP

Examples

The following ACL allows all hosts (on the interface to which you apply the ACL) to go through the ASA:

```
hostname(config)# access-list ACL_IN extended permit ip any any
```

The following sample ACL prevents hosts on 192.168.1.0/24 from accessing the 209.165.201.0/27 network. All other addresses are permitted.

```
hostname(config)# access-list ACL_IN extended deny tcp 192.168.1.0 255.255.255.0
209.165.201.0 255.255.255.224
hostname(config)# access-list ACL_IN extended permit ip any any
```

If you want to restrict access to only some hosts, then enter a limited **permit ACE**. By default, all other traffic is denied unless explicitly permitted.

```
hostname(config)# access-list ACL_IN extended permit ip 192.168.1.0 255.255.255.0
209.165.201.0 255.255.255.224
```

The following ACL restricts all hosts (on the interface to which you apply the ACL) from accessing a website at address 209.165.201.29. All other traffic is allowed.

```
hostname(config)# access-list ACL_IN extended deny tcp any host 209.165.201.29 eq www
hostname(config)# access-list ACL_IN extended permit ip any any
```

The following ACL that uses object groups restricts several hosts on the inside network from accessing several web servers. All other traffic is allowed.

```
hostname(config-network)# access-list ACL_IN extended deny tcp object-group denied
object-group web eq www
hostname(config)# access-list ACL_IN extended permit ip any any
hostname(config)# access-group ACL_IN in interface inside
```

To temporarily disable an ACL that permits traffic from one group of network objects (A) to another group of network objects (B):

```
hostname(config)# access-list 104 permit ip host object-group A object-group B inactive
```

To implement a time-based ACL, use the **time-range** command to define specific times of the day and week. Then use the **access-list extended** command to bind the time range to an ACL. The following example binds an ACL named “Sales” to a time range named “New_York_Minute”:

```
hostname(config)# access-list Sales line 1 extended deny tcp host 209.165.200.225 host
209.165.201.1 time-range New_York_Minute
```

See the **time-range** command for more information about how to define a time range.

The following ACL allows any ICMP traffic:

```
hostname(config)# access-list abc extended permit icmp any any
```

The following ACL allows any ICMP traffic for the object group “obj_icmp_1”:

```
hostname(config)# access-list abc extended permit icmp any any object-group obj_icmp_1
```

The following ACL permits ICMP traffic with ICMP type 3 and ICMP code 4 from source host 10.0.0.0 to destination host 10.1.1.1. All other type of ICMP traffic is not be permitted.

```
hostname(config)# access-list abc extended permit icmp host 10.0.0.0 host 10.1.1.1 3 4
```

The following ACL permits ICMP traffic with ICMP type 3 and any ICMP code from source host 10.0.0.0 to destination host 10.1.1.1. All other type of ICMP traffic is not be permitted.

```
hostname(config)# access-list abc extended permit icmp host 10.0.0.0 host 10.1.1.1 3
```

Related Commands

Command	Description
access-group	Binds the ACL to an interface.
clear access-group	Clears an ACL counter.
clear configure access-list	Clears an ACL from the running configuration.
show access-list	Displays ACEs by number.
show running-config access-list	Displays the current running access list configuration.

access-list remark

To specify the text of a remark to add before or after an **access-list extended** command, use the **access-list remark** command in global configuration mode. To delete the remark, use the **no** form of this command.

access-list *id* [**line** *line-num*] **remark** *text*

no access-list *id* [**line** *line-num*] **remark** [*text*]

Syntax Description

id	Name of an ACL.
line *line-num*	(Optional) The line number at which to insert a remark or an access control element (ACE).
remark text	Text of the remark to add before or after an **access-list extended** command.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The remark text must contain at least one non-space character; an empty remark is not allowed. The remark text can be up to 100 characters long, including spaces and punctuation.

You cannot use the **access-group** command on an ACL that includes a remark only.

Examples

The following example shows how to specify the text of a remark to add before or after an **access-list** command:

```
hostname(config)# access-list 77 remark checklist
```

Related Commands

Command	Description
access-list extended	Adds an ACL to the configuration and is used to configure policy for IP traffic through the ASA.
clear access-group	Clears an ACL counter.
clear configure access-list	Clears ACLs from the running configuration.
show access-list	Displays the ACL entries by number.
show running-config access-list	Displays the current running access list configuration.

access-list rename

To rename an ACL, use the **access-list rename** command in global configuration mode.

access-list *id* **rename** *new_acl_id*

Syntax Description

id	Name of an existing ACL.
rename *new_acl_id*	Specifies the new ACL ID, as a string or integer up to 241 characters long. The ID is case-sensitive.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

If the ACL is renamed to the same name, the ASA will silently ignore the command.

Examples

The following example shows how to rename an ACL from TEST to OUTSIDE:

```
hostname(config)# access-list TEST rename OUTSIDE
```

Related Commands

Command	Description
access-list extended	Adds an ACL to the configuration and is used to configure policy for IP traffic through the ASA.
clear access-group	Clears an ACL counter.
clear configure access-list	Clears ACLs from the running configuration.
show access-list	Displays the ACL entries by number.
show running-config access-list	Displays the current running access-list configuration.

access-list standard

To add an ACL to identify the destination IP addresses of OSPF routes, which can be used in a route map for OSPF redistribution, use the **access-list standard** command in global configuration mode. To remove the ACL, use the **no** form of this command.

access-list *id* **standard** [**line** *line-num*] {**deny** | **permit**} {**any4** | **host** *ip_address* | *ip_address subnet_mask*}

no access-list *id* **standard** [**line** *line-num*] {**deny** | **permit**} {**any4** | **host** *ip_address* | *ip_address subnet_mask*}

Syntax Description

any4	Specifies access to anyone.
deny	Denies access if the conditions are matched.
host *ip_address*	(Optional) Specifies access to a host IP address.
id	Name or number of an ACL.
ip_address ip_mask	Specifies access to a specific IP address (optional) and subnet mask.
line *line-num*	(Optional) The line number at which to insert an ACE.
permit	Permits access if the conditions are matched.

Defaults

The defaults are as follows:

- The ASA denies all packets on the originating interface unless you specifically permit access.
- ACL logging generates system log message 106023 for denied packets—deny packets must be present to log denied packets.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

When used with the **access-group** command, the **deny** keyword does not allow a packet to traverse the ASA. By default, the ASA denies all packets on the originating interface unless you specifically permit access.

Use the following guidelines for specifying a source, local, or destination address:

- Use a 32-bit quantity in four-part, dotted-decimal format.

- Use the keyword **any** as an abbreviation for an address and mask of 0.0.0.0 0.0.0.0.
- Use the **host** *ip_address* option as an abbreviation for a mask of 255.255.255.255.

Examples

The following example shows how to deny IP traffic through the ASA:

```
hostname(config)# access-list 77 standard deny
```

The following example shows how to permit IP traffic through the ASA if conditions are matched:

```
hostname(config)# access-list 77 standard permit
```

The following example shows how to specify a destination address:

```
hostname(config)# access-list 77 standard permit host 10.1.10.123
```

Related Commands

Command	Description
access-group	Defines object groups that you can use to optimize your configuration.
clear access-group	Clears an ACL counter.
clear configure access-list	Clears ACLs from the running configuration.
show access-list	Displays the ACL entries by number.
show running-config access-list	Displays the current running access list configuration.

access-list webtype

To add an ACL to the configuration that supports filtering for clientless SSL VPN, use the **access-list webtype** command in global configuration mode. To remove the ACL, use the **no** form of this command.

access-list *id* **webtype** {**deny** | **permit**} **url** {*url_string* | **any**} [**log** {**disable** | **default** | **level**} [**interval** *secs*]] [**time_range** *name*]] [inactive]

no access-list *id* **webtype** {**deny** | **permit**} **url** {*url_string* | **any**} [**log** {**disable** | **default** | **level**} [**interval** *secs*]] [**time_range** *name*]] [inactive]

access-list *id* **webtype** {**deny** | **permit**} **tcp** [**host** *host_address* | *dest_address subnet_mask* | **any**] [*oper port* [*port*]] [**log** {**disable** | **default** | *level*} [**interval** *secs*] [**time_range** *name*]] [inactive]

no **access-list** *id* **webtype** {**deny** | **permit**} **tcp** [**host** *host_address* | *dest_address subnet_mask* | **any**] [*oper port* [*port*]] [**log** {**disable** | **default** | *level*} [**interval** *secs*] [**time_range** *name*]] [inactive]

Syntax Description

any	Specifies all IP addresses.
any	(Optional) Specifies all URLs.
deny	Denies access if the conditions are matched.
dest_address	Specifies a destination IP address.
host_address	Specifies a host IP address.
id	Specifies a name or number of an ACL.
inactive	Disables an ACE.
interval *secs*	(Optional) Specifies the time interval at which to generate system log message 106100; valid values are from 1 to 600 seconds.
log {**disable** | **default** | *level*}	(Optional) Specifies that system log message 106100 is generated for the ACE. See the **log** command for information.
oper	Compares *ip_address* ports. Possible operands include lt (less than), gt (greater than), eq (equal), neq (not equal), and range (inclusive range).
permit	Permits access if the conditions are matched.
port	Specifies the decimal number or name of a TCP or UDP port.
subnet mask	Specifies the subnet mask of the destination IP address.
time_range *name*	(Optional) Specifies a keyword for attaching the time-range option to this ACL element.
url	Specifies that a URL be used for filtering.
url_string	(Optional) Specifies the URL to be filtered.

Defaults

The defaults are as follows:

- The ASA denies all packets on the originating interface unless you specifically permit access.
- ACL logging generates syslog message 106023 for denied packets—deny packets must be present to log denied packets.

- When the **log** optional keyword is specified, the default level for syslog message 106100 is 6 (informational).

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The **access-list webtype** command is used to configure clientless SSL VPN filtering. The URL specified may be full or partial (no file specified), may include wildcards for the server, or may specify a port.

Valid protocol identifiers are: http, https, cifs, imap4, pop3, and smtp. The URL may also contain the keyword **any** to refer to any URL. An asterisk may be used to refer to a subcomponent of a DNS name.

If you disable an ACE with the inactive keyword, you can enable it again by entering the entire ACE without the **inactive** keyword. This feature enables you to keep a record of an inactive ACE in your configuration to make reenabling easier.

Examples

The following example shows how to deny access to a specific company URL:

```
hostname(config)# access-list acl_company webtype deny url http://*.example.com
```

The following example shows how to deny access to a specific file:

```
hostname(config)# access-list acl_file webtype deny url
https://www.example.com/dir/file.html
```

The following example shows how to deny HTTP access to any URL through port 8080:

```
hostname(config)# access-list acl_company webtype deny url http://my-server:8080/*
```

Related Commands

Command	Description
access-group	Defines object groups that you can use to optimize your configuration.
access-list ethertype	Configures an ACL that controls traffic based on its EtherType.
access-list extended	Adds an ACL to the configuration and configures policy for IP traffic through the ASA.
clear access-group	Clears an ACL counter.
show running-config access-list	Displays the access list configuration running on the ASA.

accounting-mode

To indicate whether accounting messages are sent to a single server (single mode) or sent to all servers in the group (simultaneous mode), use the **accounting-mode** command in aaa-server configuration mode. To remove the accounting mode specification, use the **no** form of this command.

accounting-mode {**simultaneous** | **single**}

Syntax Description

simultaneous	Sends accounting messages to all servers in the group.
single	Sends accounting messages to a single server.

Defaults

The default value is single mode.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Aaa-server configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Use the **single** keyword to send accounting messages to a single server. Use the **simultaneous** keyword to send accounting messages to all servers in the server group.

This command is meaningful only when the server group is used for accounting (RADIUS or TACACS+).

Examples

The following example shows the use of the **accounting-mode** command to send accounting messages to all servers in the group:

```
hostname(config)# aaa-server svrgrp1 protocol tacacs+
hostname(config-aaa-server-group)# accounting-mode simultaneous
hostname(config-aaa-server-group)# exit
hostname(config)#
```

Related Commands

Command	Description
aaa accounting	Enables or disables accounting services.

aaa-server protocol	Enters AAA server group configuration mode, so you can configure AAA server parameters that are group-specific and common to all hosts in the group.
clear configure aaa-server	Removes all AAA server configuration.
show running-config aaa-server	Displays AAA server statistics for all AAA servers, for a particular server group, for a particular server within a particular group, or for a particular protocol.

accounting-port

To specify the port number used for RADIUS accounting for this host, use the **accounting-port** command in aaa-server host configuration mode. To remove the authentication port specification, use the **no** form of this command.

accounting-port *port*

no accounting-port

Syntax Description

port	A port number for RADIUS accounting; the range of valid values is 1- 65535.

Defaults

By default, the device listens for RADIUS on port 1646 for accounting (in compliance with RFC 2058). If the port is not specified, the RADIUS accounting default port number (1646) is used.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Aaa-server host configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

This command specifies the destination TCP/UDP port number of the remote RADIUS server hosts to which you want to send accounting records. If your RADIUS accounting server uses a port other than 1646, you must configure the ASA for the appropriate port before starting the RADIUS service with the **aaa-server** command.

This command is valid only for server groups that are configured for RADIUS.

Examples

The following example configures a RADIUS AAA server named “srvgrp1” on host “1.2.3.4”, sets a timeout of 9 seconds, sets a retry-interval of 7 seconds, and configures accounting port 2222.

```
hostname(config)# aaa-server svrgrp1 protocol radius
hostname(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
hostname(config-aaa-server-host)# timeout 9
hostname(config-aaa-server-host)# retry-interval 7
hostname(config-aaa-server-host)# accountinq-port 2222
hostname(config-aaa-server-host)# exit
hostname(config)#
```

Related Commands

Command	Description
aaa accounting	Keeps a record of which network services a user has accessed.
aaa-server host	Enters aaa server host configuration mode, so you can configure AAA server parameters that are host-specific.
clear configure aaa-server	Removes all AAA command statements from the configuration.
show running-config aaa-server	Displays AAA server statistics for all AAA servers, for a particular server group, for a particular server within a particular group, or for a particular protocol.

accounting-server-group

To specify the AAA server group for sending accounting records, use the **accounting-server-group** command in various modes. To remove accounting servers from the configuration, use the **no** form of this command.

accounting-server-group *group_tag*

no accounting-server-group [*group_tag*]

Syntax Description

group_tag	Identifies the previously configured accounting server or group of servers. Use the **aaa-server** command to configure accounting servers.

Defaults

No accounting servers are configured by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Imap4s configuration	•	—	•	—	—
Pop3s configuration	•	—	•	—	—
Smtps configuration	•	—	•	—	—
Tunnel-group general-attributes configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.
7.1(1)	This command is available in tunnel-group general-attributes configuration mode, instead of webvpn configuration mode.

Usage Guidelines

The ASA uses accounting to keep track of the network resources that users access. If you enter this command in webvpn configuration mode, it is transformed to the same command in tunnel-group general-attributes configuration mode.

Examples

The following example entered in tunnel-group-general attributes configuration mode, configures an accounting server group named “aaa-server123” for an IPSec LAN-to-LAN tunnel group “xyz”:

```
hostname(config)# tunnel-group xyz type IPSec_L2L
hostname(config)# tunnel-group xyz general-attributes
hostname(config-tunnel-general)# accounting-server-group aaa-server123
hostname(config-tunnel-general)#
```

The following example shows how to configure POP3S e-mail proxy to use the set of accounting servers named POP3SSVRS:

```
hostname(config)# pop3s
hostname(config-pop3s)# accounting-server-group POP3SSVRS
```

Related Commands

Command	Description
aaa-server	Configures authentication, authorization, and accounting servers.