aa - ac

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.

Command Default

The default privilege level is 0.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.

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:

```
ciscoasa(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.

Command Default

By default, AAA accounting for administrative access is disabled.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.

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:

```
ciscoasa(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

Command Default

By default, AAA accounting for administrative access is disabled.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.

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 Adaptive Security Device Manager (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:

```
ciscoasa(config)# aaa-server mygroup protocol tacacs+
ciscoasa(config)# aaa-server mygroup (inside) host 192.168.10.10 thekey timeout 20
ciscoasa(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.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.

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:

```
ciscoasa(config)# access-list acl12 extended permit tcp any any
ciscoasa(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. By default, ASDM accepts a blank username and the enable password, and can also use the local database for authentication even if you do not configure this command. This command disallows the blank username/enable password login. 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 a blank username and the enable password. By default, the enable password is not set.

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 with passwords who access the ASA using SSH. For a local **username**, you can enable public key authentication instead of password authentication using the **ssh authentication** command. In Version 9.6(2) and 9.7(1), the **aaa authentication ssh console LOCAL** command is required for **ssh authentication**. For 9.6(1) and earlier and for 9.6(3)/9.8(1) and later, you do not have to configure the **aaa authentication ssh console LOCAL** command for public key authentication; this command only applies to users with passwords, and you can specify any server type, not just LOCAL. For example, some users can use public key authentication using the local database, and other users can use passwords with RADIUS.
telnet	Authenticates users who access the ASA using Telnet. 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).

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.
8.4(2)	You can no longer connect to the ASA using SSH with the **pix** or **asa** username and the login password. To use SSH, you must configure AAA authentication using the **aaa authentication ssh console LOCAL** command (CLI) or **Configuration > Device Management > Users/AAA > AAA Access > Authentication** (ASDM); then define a local user by entering the **username** command (CLI) or choosing **Configuration > Device Management > Users/AAA > User Accounts** (ASDM). If you want to use a AAA server for authentication instead of the local database, we recommend also configuring local authentication as a backup method.
9.6(2)	The **aaa authentication ssh console LOCAL** command is required for **ssh authentication**. In Version 9.6(2) and later, you can create a **username** without any password defined, so you can require public key authentication only.
9.6(3)/9.8(1)	Separate authentication for users with SSH public key authentication and users with passwords. You no longer have to explicitly enable AAA SSH authentication (**aaa authentication ssh console)**; when you configure the **ssh authentication** command for a user, local authentication is enabled by default for users with this type of authentication. Moreover, when you explicitly configure AAA SSH authentication, this configuration only applies for usernames with passwords, and you can use any AAA server type.

Usage Guidelines

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

Logging in to the ASA

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

- If you do not enable any authentication for serial access, you do not enter a username or password.
- 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).
- If you enable Telnet or SSH authentication using 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.

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

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”:

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

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

```
ciscoasa(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:

```
ciscoasa
(config)# aaa-server svrgrp1 protocol tacacs
ciscoasa(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 the "Usage Guidelines" section for more information.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.

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

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 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:

```
ciscoasa(config)# aaa authentication include tcp/0 outside 192.168.0.0 255.255.0.0 0 0
tacacs+
ciscoasa(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:

```
ciscoasa(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:

```
ciscoasa(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:

```
ciscoasa(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:

```
ciscoasa(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:

```
ciscoasa(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.

Command	Description
aaa-server host	Configures host-related attributes.

aaa authentication listener

To enable HTTP/HTTPS 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** | **https** } *interface_name* [**port** *portnum*] [**redirect**]
no aaa authentication listener { **http** | **https** } *interface_name* [**port** *portnum*] [**redirect**]

Syntax Description

{**http** | **https**}	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.

Command Default

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:

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

Command History

Release	Modification
7.2(2)	This command was added.

Usage Guidelines

Without the **aaa authentication listener** command, when HTTP/HTTPS 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/HTTPS 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 For cut-through proxy, when the user logs out from the authentication page, the connection stays active. The user must also log out of the SSH session to completely clear the connection.

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:

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

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

```
ciscoasa(config)# static (inside,outside) tcp interface www 192.168.0.50 www netmask
255.255.255.255
ciscoasa(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:

```
ciscoasa(config)# aaa authentication listener http inside redirect
ciscoasa(config)# aaa authentication listener https inside redirect
```

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

```
ciscoasa(config)# aaa authentication listener http inside
ciscoasa(config)# aaa authentication listener https inside
```

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

```
ciscoasa(config)# aaa authentication listener http inside port 1100 redirect
ciscoasa(config)# aaa authentication listener https inside port 1400 redirect
```

Related Commands

Command	Description
aaa authentication listener no-logout-button	Remove the logout button from the cut-through proxy login page.
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 listener no-logout-button

To remove the logout button from the cut-through proxy portal page, use the **aaa authentication listener no-logout-button** command in global configuration mode. To restore the logout button, use the **no** form of this command.

aaa authentication listener no-logout-button *interface_name*
no aaa authentication listener no-logout-button *interface_name*

Syntax Description

interface_name	Specifies the interface on which you enabled the authentication listener.

Command Default

By default, the portal page has a logout button.

Command Modes

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

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

Command History

Release	Modification
9.10(1)	This command was added.

Usage Guidelines

By default, the cut-through proxy portal page (/netaccess/connstatus.html) presents session information and a logout button if it is accessed when a cut-through-proxy session is already active for the connecting host. You can use this command to remove the logout button.

This is useful in case where users connect from behind a NAT device and cannot be distinguished by IP address. When one user logs out, it logs out all users of the IP address.

Examples

The following example enables the HTTP and HTTPS listeners on the inside interface and configures the ASA to redirect all HTTP/HTTPS traffic that requires authentication.

```
ciscoasa(config)# aaa authentication listener http inside redirect
ciscoasa(config)# aaa authentication listener https inside redirect
ciscoasa(config)# aaa authentication listener no-logout-button inside
```

Related Commands

Command	Description
aaa authentication listener http/https	Enables HTTP/HTTPS listening ports to authenticate network users

aaa authentication login-history

To set the login history duration, use the **aaa authentication login-history** command in global configuration mode. To disable the login history, use the **no** form of this command.

aaa authentication login-history duration *days*
no aaa authentication login-history [**duration** *days*]

Syntax Description

duration *days*	Sets the days between 1 and 365. The default is 90.

Command Default

The default is 90 days.

Command Modes

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

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

Command History

Release	Modification
9.8(1)	We introduced this command.

Usage Guidelines

This feature applies to usernames in the local database or from a AAA server when you enable local AAA authentication for one or more of the CLI management methods (SSH, Telnet, serial console).

ASDM logins are not saved in the history.

The login history is only saved per unit; in failover and clustering environments, each unit maintains its own login history only.

Login history data is not maintained over reloads.

To view the login history, use the **show aaa login-history** command.

Examples

The following example sets the login history to 365 days:

```
ciscoasa(config)# aaa authentication login-history duration 365
```

When a user logs in, they see their own login history, such as this SSH example:

```
cugel@10.86.194.108's password:
User cugel logged in to ciscoasa at 21:04:10 UTC Dec 14 2016
Last login: 21:01:44 UTC Dec 14 2016 from ciscoasa console
Successful logins over the last 90 days: 6
```

```
Authentication failures since the last login: 0
Type help or '?' for a list of available commands.
ciscoasa>
```

Related Commands

Command	Description
aaa authentication login-history	Saves the local **username** login history.
password-history	Stores previous **username** passwords. This command is not user-configurable.
password-policy reuse-interval	Prohibits the reuse of a **username** password.
password-policy username-check	Prohibits a password that matches a **username** name.
show aaa login-history	Shows the local **username** login history.
username	Configures a local user.

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.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.
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:

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

In this context, the following command:

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

is equivalent to this command:

```
ciscoasa(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:

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

before this command:

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

the ASA tries to find a match in the **mylist acc**ess-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:

```
ciscoasa(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.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.

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 64 HTTPS authentication processes is allowed. If all 64 HTTPS authentication processes are running, the 65th, 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:

```
ciscoasa(config)# aaa authentication secure-http-client
ciscoasa(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:

```
ciscoasa (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** [*server-tag + tacacs* | **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.

Command Default

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:

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

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:
- 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:

```
ciscoasa(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.

```
ciscoasa(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** } [**auto-enable**]
no aaa authorization exec { **authentication-server** | **LOCAL** } [**auto-enable**]

Syntax Description

authentication-server	Indicates that the authorization attributes will be retrieved from the server that was used to authenticate the user.
auto-enable	Enables administrators who have sufficient authorization privileges to enter privileged EXEC mode by entering their authentication credentials once.
LOCAL	Indicates that the authorization attributes will be retrieved from the local user database of the ASA, regardless of how authentication is done.

Command Default

By default, this command is disabled.

Command Modes

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

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

Command History

Release	Modification
8.0(2)	This command was added.
8.2(2)	The **LOCAL** option was added.
9.2(1)	The **auto-enable** option was added.
9.4(1)	This CLI will only apply to management sessions other than HTTP.

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. If you configure *command* authorization, then console users are still subject to command usage limits.

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:

```
ciscoasa(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 http

To enable authorization for ASDM, use the **aaa authorization http** command. To disable authorization of username for ASDM, use the no form of the command:

aaa authorization http console LOCAL | <aaa-server-group>

[no] aaa authorization http console LOCAL | <aaa-server-group>

Syntax Description

aaa-server-group	Defined already, and the protocol configured for the aaa-server-group must be LDAP, RADIUS, or TACACS+. The command will have no effect if the protocol is not LDAP, RADIUS, or TACACS+.
console	Specify this keyword to identify a server group for administrative authorization.
LOCAL	Predefined server tag for AAA protocol 'local'

Command Default

Authorization of username for ASDM is disabled by default.

Command Modes

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

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

Command History

Release	Modification
9.4(1)	This command was added.

Usage Guidelines

This command is not available on platforms that do no support webvpn (ASA 1000v) and platforms with No Payload Encryption (NPE) enabled.

Examples

```
5520-1(config)# aaa ?
configure mode commands/options:
  accounting      Configure user accounting parameters
  authentication  Configure user authentication parameters
  authorization   Configure user authorization parameters
  local           AAA Local method options
  mac-exempt      Configure MAC Exempt parameters
  proxy-limit     Configure number of concurrent proxy connections allowed per
                  user
5520-1(config)# aaa authorization ?
configure mode commands/options:
  command  Specify this keyword to allow command authorization to be configured
           for all administrators on all consoles
```

```
  exclude  Exclude the service, local and foreign network which needs to be
           authenticated, authorized, and accounted
  exec     Perform administrative authorization for console connections(ssh,
           telnet and enable) configured for authentication to RADIUS,
           LDAP, TACACS or LOCAL authentication servers.
  include  Include the service, local and foreign network which needs to be
           authenticated, authorized, and accounted
  match    Specify this keyword to configure an ACL to match
  http     Perform administrative authorization for http connections

5520-1(config)# aaa authorization http ?
configure mode commands/options:
  console  Specify this keyword to identify a server group for administrative
           authorization
5520-1(config)# aaa authorization http console ?
configure mode commands/options:
  LOCAL  Predefined server tag for AAA protocol 'local'
  WORD   Name of RADIUS,LDAP or TACACS+ aaa-server group for administrative
         authorization
```

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.

Command Default

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:

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

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:

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

```
ciscoasa(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:

```
ciscoasa(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:

```
ciscoasa(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.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.

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:

```
ciscoasa(config)# aaa-server tplus1 protocol tacacs+
ciscoasa(config)# aaa-server tplus1 (inside) host 10.1.1.10 thekey timeout 20
ciscoasa(config)# aaa authentication include any inside 0 0 0 0 tplus1
ciscoasa(config)# aaa accounting include any inside 0 0 0 0 tplus1
ciscoasa(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 kerberos import-keytab

To import a Kerberos keytab file so that it can be used to authenticate the Kerberos server, use the **aaa kerberos import-keytab** command in global configuration mode. To remove an imported keytab file, use the **clear aaa kerberos keytab** command.

aaa kerberos import-keytab *file*

Syntax Description

url The location or URL of the file to be imported. Supported locations for importing the file are the following; include the complete path and file name as appropriate for the location.

- disk0:
- disk1:
- flash:
- ftp://
- http://
- https://
- scp://
- smb://
- tftp://

Command Default

No default values.

Command Modes

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

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

Command History

Release	Modification
9.8(4)	This command was added.

Usage Guidelines

You can configure a Kerberos AAA server group to authenticate the servers in the group using the **validate-kdc** command. To accomplish the authentication, you must also import a keytab file that you exported from the Kerberos Key Distribution Center (KDC). By validating the KDC, you can prevent an attack where the attacker spoofs the KDC so that user credentials are authenticated against the attacker's Kerberos server.

When you enable KDC validation, after obtaining the ticket-granting ticket (TGT) and validating the user, the system also requests a service ticket on behalf of the user for **host**/*ASA_hostname*. The system then validates the returned service ticket against the secret key for the KDC, which is stored in a keytab file that you generated from the KDC and then uploaded to the ASA. If KDC authentication fails, the server is considered untrusted and the user is not authenticated.

To accomplish KDC authentication, you must do the following:

1. (On the KDC.) Create a user account in the Microsoft Active Directory for the ASA (go to **Start > Programs > Administrative Tools > Active Directory Users and Computers**). For example, if the fully-qualified domain name (FQDN) of the ASA is asahost.example.com, create a user named asahost.
2. (On the KDC.) Create a host service principal name (SPN) for the ASA using the FQDN and user account:

```
C:> setspn -A HOST/asahost.example.com asahost
```

3. (On the KDC.) Create a keytab file for the ASA (line feeds added for clarity):

```
C:\Users\Administrator> ktpass /out new.keytab +rndPass
/princ host/asahost@EXAMPLE.COM
/mapuser asahost@example.com
/ptype KRB5_NT_SRV_HST
/mapop set
```

4. (On the ASA.) Import the keytab (in this example, new.keytab) to the ASA using the **aaa kerberos import-keytab** command.
5. (On the ASA.) Add the **validate-kdc** command to the Kerberos AAA server group configuration. The keytab file is used only by server groups that contain this command.

Note You cannot use KDC validation in conjunction with Kerberos Constrained Delegation (KCD). The **validate-kdc** command will be ignored if the server group is used for KCD.

Examples

The following example shows how to import a keytab named new.keytab that resides on an FTP server, and enable KDC validation in a Kerberos AAA server group.

```
ciscoasa(config)# aaa kerberos import-keytab ftp://ftpserver.example.com/new.keytab

ftp://ftpserver.example.com/new.keytab imported successfully
ciscoasa(config)# aaa-server svrgrp1 protocol kerberos

ciscoasa(config-aaa-server-group)# validate-kdc
```

Related Commands

Command	Description
clear aaa kerberos keytab	Clears the imported Kerberos keytab file.
show aaa kerberos keytab	Shows information about the Kerberos keytab file.

Command	Description
validate-kdc	Configures a Kerberos AAA server group to perform Kerberos Key Distribution Center (KDC) validation.

aaa local authentication attempts max-fail

To limit the number of consecutive failed local login attempts that the ASA allows any given user account, 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.

Command Default

This command is disabled by default.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.
9.17(1)	Users will be unlocked after 10 minutes and privilege level 15 users are also now affected.

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, or until 10 minutes passes. Locking or unlocking a username results in a syslog message.

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:

```
ciscoasa(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.

Command Default

No default behaviors or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.

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:

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

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

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

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

```
ciscoasa(config)# mac-list 1 deny 00a0.c95d.0282 ffff.ffff.ffff
ciscoasa(config)# mac-list 1 permit 00a0.c95d.0000 ffff.ffff.0000
ciscoasa(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.

Command Default

The default proxy-limit value is 16.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.

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:

```
ciscoasa(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 sdi import-node-secret

To import a node secret file that you exported from an RSA Authentication Manager for use with an SDI AAA server group, use the **aaa sdi import-node-secret** command in global configuration mode. To remove an imported node secret file, use the **clear aaa sdi node-secret** command.

aaa sdi import-node-secret *filepath rsa_server_address password*

Syntax Description

filepath	The complete path to the unzipped node secret file that was exported from the RSA Authentication Manager. Supported locations for importing the file are the following; include the complete path and file name as appropriate for the location. • disk0: • disk1: • flash: • ftp:// • http:// • https:// • scp:// • smb:// • tftp://
rsa_server_address	The IP address or fully-qualified hostname of the RSA Authentication Manager server to which the node secret belongs.
password	The password used to protect the file when you exported it.

Command Default

No default values.

Command Modes

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

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

Command History

Release	Modification
9.15(1)	This command was added.

Usage Guidelines

You can manually import the node-secret file that is generated by the RSA Authentication Manager (SecurID) server.

You must export the node secret file from the RSA Authentication Manager server. For details, see the RSA Authentication Manager documentation. Then, either upload the unzipped file to the ASA, or place it on a server from which you can import it using this command.

Examples

The following example shows how to import the nodesecret.rec file for the rsaam.example.com server, using mysecret as the password.

```
ciscoasa# aaa sdi import-node-secret nodesecret.rec rsaam.example.com mysecret

nodesecret.rec imported successfully
ciscoasa#
```

Related Commands

Command	Description
clear aaa sdi node-secret	Clears an imported SDI node secret file.
show aaa sdi node-secrets	Shows information about SecurID servers that have an imported node secret file.

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** (Note that this option is no longer available as of the 9.3(1) release.) • **radius** • **sdi** (RSA SecurID using the authentication and server management protocol (ACE)) • **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.

Command Default

No default behavior or values.

Command Modes

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

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

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.

Release	Modification
9.3(1)	The **nt** option is no longer available. Windows NT domain authentication support has been deprecated.
9.13(1)	The limit on the number of allowed server groups was increase from 100 to 200 for single mode, and from 4 to 8 in multiple mode. In addition, the limit for the number of servers in a group was increased from 4 to 8 in multiple mode. The per-group server limit in single mode remains unchanged at 16.

Usage Guidelines

You can have up to 100 server groups in single mode or 4 server groups per context in multiple mode. Starting with 9.13(1), the limits are increased to 200 groups in single mode, 8 groups in multiple mode.

Each group can have up to 16 servers in single mode or 4 servers in multiple mode. Starting with 9.13(1), the limit for multiple mode is 8 servers per group. 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 Secure Client 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:

```
ciscoasa
(config)#
aaa-server svrgrp1 protocol tacacs+
ciscoasa(config-aaa-server-group)# accounting-mode simultaneous
ciscoasa(config-aaa-server-group)# reactivation mode timed
ciscoasa(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	Specifies 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.

Command	Description
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.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
8.0(2)	This command was added.

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:

```
ciscoasa
#
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
...
ciscoasa
#
aaa-server active host 192.168.125.60
ciscoasa
#
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. **Note** After you configure the host with an interface, if you need to change the interface, you must first remove the host command using the **no** form. You can then add a new host entry with the correct interface. If you simply try to change the interface without first removing the command, your change is accepted but ignored.
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. If you use a DNS name, the name is resolved to an IP address only when the server transitions to active, either when you initially create it or it returns to active state from failed state. The name is not resolved just because the time-to-live (TTL) for the name expired.
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.

Command Default

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:

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

Command History

Release	Modification
7.2(1)	Support for DNS names was added.
9.0(1)	Support for user identity was added.
9.9(2)	Support for IPv6 addressing of and connectivity to Radius servers added.
9.13(1)	The limit on the number of allowed server groups was increase from 100 to 200 for single mode, and from 4 to 8 in multiple mode. In addition, the limit for the number of servers in a group was increased from 4 to 8 in multiple mode. The per-group server limit in single mode remains unchanged at 16.

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.

Each group can have up to 16 servers in single mode or 4 servers in multiple mode. Starting with 9.13(1), the limit for multiple mode is 8 servers per group. 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.

```
ciscoasa
(config)#
aaa-server watchdogs protocol kerberos
ciscoasa
(config-aaa-server-group)#
exit
ciscoasa
(config)#
aaa-server watchdogs host 192.168.3.4
ciscoasa
(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:

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

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

Command	Description
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.

Command Default

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:

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

Command History

Release	Modification
7.0(1)	This command was added.

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:

```
ciscoasa(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.

Command Default

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

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.

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:

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

Related Commands

Command	Description
crypto ca trustpoint	Enters trustpoint configuration mode.

Command	Description
default enrollment	Returns enrollment parameters to their defaults.

access-group

To bind an extended or Ethertype 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 extended 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	The name of an extended ACL. For bridge group member interfaces, you can also specify an Ethertype ACL.
control-plane	(Optional) Specifies whether or not the ACL 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. This option is available for the **in** direction only.
global	Applies an ACL to all traffic on all interfaces.
in	Applies the ACL in the inbound direction at the specified interface.
interface *interface_name*	Name of the network interface. In routed mode, you can apply an extended ACL to both a Bridge Virtual Interface (BVI) and its member interfaces. In transparent mode, you can apply an extended ACL to the member interfaces only. In both modes, you can apply Ethertype ACLs to member interfaces only.
out	Applies the ACL in the outbound direction at the specified interface.
per-user-override	(Optional) Allows downloadable user ACLs to override the ACL applied to the interface. This option is available for the **in** direction only.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.
8.3(1)	This command was modified to support global policies.
9.7(1)	This command was modified to allow applying extended access groups to a BVI, and Ethertype ACLs to bridge group member interfaces, in routed mode.

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.

In routed mode, if you apply access groups to both a BVI and its member interfaces, the precedence depends on direction. Inbound, the member interface access group is checked first, then the BVI access group, and finally the global group. Outbound, the BVI access group is checked first, then the member interface access group.

Usage Guidelines for Interface-specific Rules

The **access-group** command binds an extended ACL to an interface. You must use the **access-list extended** command first to create the ACL.

You can apply the ACL to traffic inbound to an interface or outbound from 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 syslog message 106023 (or 106100 for ACEs that use non-default logging).

For inbound ACLs, 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.

By default, VPN remote access traffic is not matched against interface ACLs. However, if you use the **no sysopt connection permit-vpn** command to turn off this bypass, 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.
- 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.

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.

All global rules apply only to traffic in the ingress (inbound) direction. Global rules are not applied to egress (outbound) traffic. If global rules are configured in conjunction with inbound 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:

```
ciscoasa(config)# access-list acl-1 extended permit ip host 10.1.2.2 host 10.2.2.2
ciscoasa(config)# access-list acl-2 extended deny ip any any
ciscoasa(config)# access-group acl-1 in interface outside
ciscoasa(config)# access-group acl-2 global
```

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

```
ciscoasa(config)# access-list global_acl permit tcp any host 10.2.2.2 eq 80
ciscoasa(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.

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.

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

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

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

Related Commands

Command	Description
access-list extended	Creates an extended ACL.

Command	Description
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.

Command Default

The default is 300 seconds.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

If you configure the **log** option for an ACL deny statement, and a traffic flow matches the ACL statement, the appliance caches the flow information. To prevent cache overload, there is a maximum number of cached deny flows that will be kept for the statistics shown in syslog message 106100. If the maximum is reached before issuing 106100 and resetting the cache, syslog message 106101 is issued to indicate that the deny flow maximum was exceeded.

The **access-list alert-interval** command sets the time interval for generating syslog message 106101. When the deny flow maximum is reached, another syslog message 106101 is generated if at least *secs* seconds have passed since the last syslog message 106101 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:

```
ciscoasa(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 cached for calculating statistics for message 106100, 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 *number*
no access-list deny-flow-max *number*

Syntax Description

number	The maximum number of deny flows that should be cached to calculate statistics for syslog message 106100, between 1 and 4096. The default is 4096.

Command Default

The default is 4096.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

Syslog message 106101 is generated when the ASA has reached the maximum number of cached deny flows.

Examples

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

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

Related Commands

Command	Description
access-list alert-interval	Sets the time between issuing message 106101.
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** } { **any** | **bpdu** | **dsap** { *hex_address* | **bpdu** | **ipx** | **isis** | **raw-ipx** } | **eii-ipx** | **ipx** | **isis** | **mpls-unicast** | **mpls-multicast** | *hex_number* }
no access-list *id* **ethertype** { **deny** | **permit** } { **any** | **bpdu** | **dsap** { *hex_address* | **bpdu** | **ipx** | **isis** | **raw-ipx** } | **eii-ipx** | **ipx** | **isis** | **mpls-unicast** | **mpls-multicast** | *hex_number* }

Syntax Description

any	Permits or denies all traffic.
bpdu	Permits or denies bridge protocol data units. Starting with 9.6(2), this keyword no longer provides the intended result. Instead, write rules for **dsap 0x42**. In 9.9(1) and 9.6+ maintenance releases with the requisite support, **bpdu** and **dsap 0x42** are converted to **dsap bpdu** rules.
deny	Denies traffic.
dsap {*hex_address* | **bpdu** | **ipx** | **isis** | **raw-ipx**}	The IEEE 802.2 Logical Link Control packet's Destination Service Access Point address. Include the address you want to permit or deny in hexadecimal, from 0x01 to 0xff. You can also use these keywords for common values: • **bpdu** for 0x42, bridge protocol data units. • **ipx** for 0xe0, Internet Packet Exchange (IPX) 802.2 LLC. • **isis** for 0xfe, Intermediate System to Intermediate System (IS-IS). • **raw-ipx** for 0xff, raw IPX 802.3 format.
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.
eii-ipx	Permits or denies Ethernet II IPX format, EtherType 0x8137.
ipx	Permits or denies IPX. In 9.9(1) and 9.6+ maintenance releases with the requisite support, **ipx** is a shortcut for configuring three separate rules, for **dsap ipx**, **dsap raw-ipx**, and **eii-ipx**.
isis	Permits or denies Intermediate System to Intermediate System (IS-IS). In 9.9(1) and 9.6+ maintenance releases with the requisite support, **isis** is converted to **dsap isis** rules.
mpls-multicast	Permits or denies MPLS multicast.

mpls-unicast	Permits or denies MPLS unicast.
permit	Permits traffic.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.
8.4(5), 9.1(2)	The **isis** keyword was added.
9.6(2)	The **dsap** *hex_address* keyword was added. The **bpdu** keyword no longer matches the intended traffic; use **dsap 0x42** instead.
9.7(1)	You can now configure Ethertype ACLs for bridge group member interfaces in routed mode.
9.9(1)	The following changes were made: • Keywords for common protocols were added to the **dsap** keyword: **dsap** {**bpdu** | **ipx** | **isis** | **raw-ipx**}. • The **bpdu** keyword is automatically converted to **dsap bpdu**. • The **isis** keyword is automatically converted to **dsap isis**. • The **eii-ipx** keyword was added. • The **ipx** keyword is automatically converted to 3 rules for **dsap ipx**, **dsap raw-ipx**, and **eii-ipx**.

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.
- Intermediate System to Intermediate System (IS-IS).
- The IEEE 802.2 Logical Link Control packet. You can control access based on the Destination Service Access Point address.

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 the inbound and outbound 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.

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

Or

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

Examples

The following example shows how to add an EtherType ACL:

```
ciscoasa(config)# access-list ETHER ethertype permit ipx
ciscoasa(config)# access-list ETHER ethertype permit bpdu
ciscoasa(config)# access-list ETHER ethertype permit dsap 0x42
ciscoasa(config)# access-list ETHER ethertype permit mpls-unicast
ciscoasa(config)# access-group ETHER in interface inside
```

In 9.9(1) and 9.6+ maintenance releases with the requisite support, the previous example would be done as follows:

```
ciscoasa(config)# access-list ETHER ethertype permit ipx

INFO: ethertype ipx is saved to config as ethertype eii-ipx
INFO: ethertype ipx is saved to config as ethertype dsap ipx
INFO: ethertype ipx is saved to config as ethertype dsap raw-ipx
ciscoasa(config)# access-list ETHER ethertype permit bpdu

INFO: ethertype bpdu is saved to config as ethertype dsap bpdu
ciscoasa(config)# access-list ETHER ethertype permit mpls-unicast

ciscoasa(config)# show access-list ETHER

access-list ETHER; 5 elements
access-list ETHER ethertype permit eii-ipx (hitcount=0)
access-list ETHER ethertype permit dsap ipx(hitcount=0)
access-list ETHER ethertype permit dsap raw-ipx(hitcount=0)
access-list ETHER ethertype permit dsap bpdu(hitcount=0)
access-list ETHER ethertype permit mpls-unicast (hitcount=0)
ciscoasa(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) to an extended ACL, 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**]] [**time-range** *time_range_name*] [**inactive**]
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**]] [**time-range** *time_range_name*] [**inactive**]

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

For ICMP traffic, with ICMP type:
access-list [**line** *line_number*] **extended** { **deny** | **permit** } { **icmp** | **icmp6** } [*user_argument*] [*security_group_argument*] *source_address_argument* [*security_group_argument*] *dest_address_argument* [*icmp_argument*] **log** [[*level*] **interval** *secs*] | **disable** | **default**]] [**time-range** *time_range_name*] [**inactive**
no access-list [**line** *line_number*] **extended** { **deny** | **permit** } { **icmp** | **icmp6** } [*user_argument*] [*security_group_argument*] *source_address_argument* [*security_group_argument*] *dest_address_argument* [*icmp_argument*] **log** [[*level*] **interval** *secs*] | **disable** | **default**]] [**time-range** *time_range_name*] [**inactive**

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.
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. • *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 IPv4 traffic only; and **any6** specifies IPv6 traffic only. • **interface***interface_name* —Specifies the name of an ASA interface. Use the interface name rather than IP address to match traffic based on which interface is the source or destination of the traffic. 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** 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. • **object-group-network-service***name*—Specifies the name of a network-service object.
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 object group for ICMP/ICMP6 created using the **object-group service** or (deprecated) **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.
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 [[*level*] [**interval** *secs*] | **disable** | **default**]	(Optional) Sets logging options when an 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 for denied packets. Log options are: • *level* —A severity level between 0 and 7. The default is 6 (informational). If you change this level for an active ACE, the new level applies to new connections; existing connections continue to be logged at the previous level. • **interval** *secs* —The time interval in seconds between syslog messages, from 1 to 600. The default is 300. This value is also used as the timeout value for deleting an inactive flow from the cache used to collect drop statistics. • **disable**—Disables all ACE logging. • **default**—Enables logging to message 106023. This setting is the same as not including the **log** option.
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; **tcp**, **udp**, **sctp** only.) Specifies the source or destination port. If you do not specify ports, all ports are matched. Note that you can also specify ports in a service object that you specify for the *protocol_argument* instead of using this argument. If you use network-service objects that specify the protocol and ports, you should not specify ports in this argument.

Available arguments include:

- *operator port* —The port name or number, between 0 and 65535. For a list of supported names, see the CLI help. Operators include:
  - **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
```

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** {**tcp** | **udp** | **tcp-udp**} command. Note that these object types are no longer recommended.

You cannot specify the recommended generic service objects, where the protocol and port are defined within the object, as the port argument. You specify these objects as part of the protocol argument

protocol_argument

Specifies the IP protocol. If you use network-service objects that specify the protocol and ports, you should specify **ip** in this argument.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. See the CLI help for the available options.
- **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, SCTP, 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.

sctp	Sets the protocol to SCTP.
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. The available arguments are the same as those described for *dest_address_argument* .
tcp	Sets the protocol to TCP.
time-range *time_range_name*	(Optional) Specifies a time range object, which determines the times of day and days of the week in which the ACE is active. If you do not include a time range, the ACE is always active. 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 username. Specify **any** to match all users with user credentials, or **none** to match addresses that are not mapped to usernames. 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. Note the double \\ separating the domain and group name.

Command Default

- Default logging for deny ACEs generates system log message 106023 for denied packets only.
- 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:

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

Command History

Release	Modification
7.0(1)	This command was added.
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 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.
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*].
9.5(2)	The **sctp** keyword was added.
9.17(1)	The **object-group-network-service** keyword was added.

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

The following commands and features 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 **wccp redirect-list group-list** command

Features That Use Mapped IP Addresses

The following features use ACLs, but these ACLs 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 Identity Firewall, FQDN, and TrustSec ACLs

The following features use ACLs, but cannot accept an ACL with identity firewall (specifying user or group names), FQDN (fully-qualified domain names), 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:

```
ciscoasa(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.

```
ciscoasa(config)# access-list ACL_IN extended deny tcp
192.168.1.0 255.255.255.0 209.165.201.0 255.255.255.224
ciscoasa(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.

```
ciscoasa(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.

```
ciscoasa(config)# access-list ACL_IN extended deny tcp any host 209.165.201.29 eq www
ciscoasa(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.

```
ciscoasa(config)# access-list ACL_IN extended deny tcp
object-group denied object-group web eq www
ciscoasa(config)# access-list ACL_IN extended permit ip any any
ciscoasa(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):

```
ciscoasa(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":

```
ciscoasa(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:

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

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

```
ciscoasa(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.

```
ciscoasa(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.

```
ciscoasa(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.

Command	Description
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 extended, EtherType, or standard access control entry, 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 the ACL.
line *line-num*	(Optional) The line number at which to insert the remark.
remark text	Text of the remark

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.

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 the end of an ACL.

```
ciscoasa(config)#
access-list MY_ACL 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.

Command	Description
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.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
8.0(2)	This command was added.

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:

```
ciscoasa(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 Access Control Entry (ACE) to a standard ACL, use the **access-list standard** command in global configuration mode. To remove an ACE, use the **no** form of this command.

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

Syntax Description

any4	Matches any IPv4 address.
deny	Denies or exempts a packet if the conditions are matched
host *ip_address*	Specifies an IPv4 host address (that is, the subnet mask is 255.255.255.255).
id	Name or number of an ACL.
ip_address subnet_mask	Specifies an IPv4 network address and subnet mask.
permit	Permits or includes a packet if the conditions are matched.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

A standard ACL is composed of all ACEs with the same ACL ID or name. Standard ACLs are used for a limited number of features, such as route maps or VPN filters. A standard ACL uses IPv4 addresses only, and defines destination addresses only.

Examples

The following example shows how to add an rule to a standard ACL:

```
ciscoasa(config)# access-list OSPF standard permit 192.168.1.0 255.255.255.0
```

Related Commands

Command	Description
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 Access Control Entry (ACE) to a webtype ACL, which filters clientless SSL VPN connections, use the **access-list webtype** command in global configuration mode. To remove the ACE, use the **no** form of this command.

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

Syntax Description

deny	Denies access if the conditions are matched.
dest_address_argument	Specifies the IP address to which the packet is being sent. Destination address options are: • **host** *ip_address* —Specifies an IPv4 host address. • *dest_ip_address mask* —Specifies an IPv4 network address and subnet mask, such as 10.100.10.0 255.255.255.0. • *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 IPv4 traffic only; and **any6** specifies IPv6 traffic only.
id	Specifies a name or number of an ACL.
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.
log [[*level*] [**interval** *secs*] | **disable** | **default**]	(Optional) Sets logging options when an ACE matches a packet. If you enter the **log** keyword without any arguments, you enable VPN filter system log message 106102 at the default level (6) and for the default interval (300 seconds). If you do not enter the **log** keyword, then the default VPN filter system log message 106103 is generated. Log options are: • *level* —A severity level between 0 and 7. The default is 6 (informational). • **interval** *secs* —The time interval in seconds between syslog messages, from 1 to 600. The default is 300. This value is also used as the timeout value for deleting an inactive flow from the cache used to collect drop statistics. • **disable**—Disables all ACE logging. • **default**—Enables logging to message 106103. This setting is the same as not including the **log** option.

operator port	(Optional) If you specify **tcp**, the destination port. If you do not specify ports, all ports are matched. 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 port.
permit	Permits access if the conditions are matched.
time_range *name*	(Optional) Specifies a time range object, which determines the times of day and days of the week in which the ACE is active. If you do not include a time range, the ACE is always active. See the **time-range** command for information about defining a time range.
url {*url_string* | **any**}	Specifies the URL to match. Use **url any** to match all URL-based traffic. Otherwise, enter a URL string, which can include wildcards. For tips on URL strings, see the usages guidelines.

Command Default

The defaults are as follows:

- ACL logging generates syslog message 106103 for denied packets.
- When the **log** optional keyword is specified, the default level for syslog message 106102 is 6 (informational).

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The **access-list webtype** command is used to configure clientless SSL VPN filtering.

Following are some tips and limitations on specifying URLs:

Select **any** to match all URLs.

- 'Permit url any' will allow all the URLs that have the format protocol://server-ip/path and will block traffic that does not match this pattern, such as port-forwarding. There should be an ACE to allow connections to the required port (port 1494 in the case of Citrix) so that an implicit deny does not occur.
- Smart tunnel and ica plug-ins are not affected by an ACL with 'permit url any' because they match smart-tunnel:// and ica:// types only.
- You can use these protocols: cifs://, citrix://, citrixs://, ftp://, http://, https://, imap4://, nfs://, pop3://, smart-tunnel://, and smtp://. You can also use wildcards in the protocol; for example, htt* matches http and https, and an asterisk * matches all protocols. For example, *://*.example.com matches any type URL-based traffic to the example.com network.
- If you specify a smart-tunnel:// URL, you can include the server name only. The URL cannot contain a path. For example, smart-tunnel://www.example.com is acceptable, but smart-tunnel://www.example.com/index.html is not.
- An asterisk * matches none or any number of characters. To match any http URL, enter http://*/*.
- A question mark ? matches any one character exactly.
- Square brackets [] are range operators, matching any character in the range. For example, to match both http://www.cisco.com:80/ and http://www.cisco.com:81/, enter **http://www.cisco.com:8[01]/**.

Examples

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

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

The following example shows how to deny access to a specific web page:

```
ciscoasa(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 on a specific server through port 8080:

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

Related Commands

Command	Description
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 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.

Command Default

The default value is single mode.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.

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:

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

Command Default

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:

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

Command History

Release	Modification
7.0(1)	This command was added.

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.

```
ciscoasa
(config)# aaa-server svrgrp1 protocol radius
ciscoasa
(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
ciscoasa
(config-aaa-server-host)# timeout 9
ciscoasa
(config-aaa-server-host)# retry-interval 7
ciscoasa
(config-aaa-server-host)#
```

```
accountinq-port 2222
ciscoasa
(config-aaa-server-host)#
exit
ciscoasa(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.

Command Default

No accounting servers are configured by default.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Imap4s configuration (deprecated)	• Yes	—	• Yes	—	—
pop3s configuration (deprecated)	• Yes	—	• Yes	—	—
Smtps configuration (deprecated)	• Yes	—	• Yes	—	—
Tunnel-group general-attributes configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.
7.1(1)	This command is available in tunnel-group general-attributes configuration mode, instead of webvpn configuration mode.
9.5(2)	This command was deprecated for the following modes: imap4s, pop3s, and smtps.
9.8(1)	This command is no longer available for IPSec LAN-to-LAN (ipsec-l2l) tunnel groups; in fact, it was never supported for IPSec LAN-to-LAN.

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 a remote-access tunnel group “xyz”:

```
ciscoasa(config)# tunnel-group xyz type remote-access
ciscoasa(config)# tunnel-group xyz general-attributes
ciscoasa(config-tunnel-general)# accounting-server-group aaa-server123
ciscoasa(config-tunnel-general)#
```

Related Commands

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

acl-netmask-convert

To specify how the ASA treats netmasks received in a downloadable ACL from a RADIUS server that is accessed by using the **aaa-server host** command, use the acl-netmask-convert command in aaa-server host configuration mode. To remove the specified behavior for the ASA, use the **no** form of this command.

acl-netmask-convert { **auto-detect** | **standard** | **wildcard** }
no acl-netmask-convert

Syntax Description

auto-detect	Specifies that the ASA should attempt to determine the type of netmask expression used. If the ASA detects a wildcard netmask expression, it converts it to a standard netmask expression. See "Usage Guidelines" for more information about this keyword.
standard	Specifies that the ASA assumes downloadable ACLs received from the RADIUS server contain only standard netmask expressions. No translation from wildcard netmask expressions is performed.
wildcard	Specifies that the ASA assumes downloadable ACLs received from the RADIUS server contain only wildcard netmask expressions and converts them all to standard netmask expressions when the ACLs are downloaded.

Command Default

By default, no conversion from wildcard netmask expressions is performed.

Command Modes

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

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

Command History

Release	Modification
7.0(4)	This command was added.

Usage Guidelines

Use the **acl-netmask-convert** command with the wildcard or auto-detect keywords when a RADIUS server provides downloadable ACLs that contain netmasks in wildcard format. The ASA expects downloadable ACLs to contain standard netmask expressions whereas Cisco VPN 3000 series concentrators expect downloadable ACLs to contain wildcard netmask expressions, which are the reverse of a standard netmas expression. A wildcard mask has ones in bit positions to ignore, zeros in bit positions to match.The **acl-netmask-convert** command helps minimize the effects of these differences upon how you configure downloadable ACLs on your RADIUS servers.

The **auto-detect** keyword is helpful when you are uncertain how the RADIUS server is configured; however, wildcard netmask expressions with "holes" in them cannot be unambiguously detected and converted. For

example, the wildcard netmask 0.0.255.0 permits anything in the third octet and can be used validly on Cisco VPN 3000 series concentrators, but the ASA may not detect this expression as a wildcard netmask.

Examples

The following example configures a RADIUS AAA server named "srvgrp1" on host "192.168.3.4", enables conversion of downloadable ACL netmasks, sets a timeout of 9 seconds, sets a retry-interval of 7 seconds, and configures authentication port 1650:

```
ciscoasa
(config)# aaa-server svrgrp1 protocol radius
ciscoasa
(config-aaa-server-group)# aaa-server svrgrp1 host 192.168.3.4
ciscoasa
(config-aaa-server-host)# acl-netmask-convert wildcard
ciscoasa
(config-aaa-server-host)# timeout 9
ciscoasa
(config-aaa-server-host)# retry-interval 7
ciscoasa
(config-aaa-server-host)#
authentication-port 1650
ciscoasa
(config-aaa-server-host)#
exit
ciscoasa
(config)#
```

Related Commands

Command	Description
aaa authentication	Enables or disables LOCAL, TACACS+, or RADIUS user authentication, on a server designated by the aaa-server command, or ASDM user authentication.
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.

action

To either apply access policies to a session or terminate the session, use the **action** command in dynamic-access-policy-record configuration mode. To reset the session to apply an access policy to a session, use the **no** form of the command.

action { **continue** | **terminate** }
no action { **continue** | **terminate** }

Syntax Description

continue	Applies the access policies to the session.
terminate	Terminates the connection.

Command Default

The default value is continue.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Dynamic-access-policy-record configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.

Usage Guidelines

Use the **continue** keyword to apply the access policies to the session in all of the selected DAP records. Use the **terminate** keyword to terminate the connection in any of the selected DAP records.

Examples

The following example shows how to terminate a session for the DAP policy Finance:

```
ciscoasa (config)#
config-dynamic-access-policy-record Finance
ciscoasa
(config-dynamic-access-policy-record)#
 action terminate
ciscoasa
(config-dynamic-access-policy-record)#
```

Related Commands

Command	Description
dynamic-access-policy-record	Creates a DAP record.

Command	Description
show running-config dynamic-access-policy-record	Displays the running configuration for all DAP records, or for the named DAP record.

action cli command

To configure actions on an event manager applet, use the **action cli command** command in event manager applet configuration mode. To remove the configured action, enter the **no action** *n* command.

action *n* **cli command "** *command* **"**
no action *n*

Syntax Description

"*command* "	Specifies the name of the command. The value of the *command* option must be in quotes; otherwise, an error occurs if the command consists of more than one word. The command runs in global configuration mode as a user with privilege level 15 (the highest). The command may not accept any input, because it is disabled. Use the **noconfirm** option if the command has it available.
n	Specifies an action ID. Valid IDs range from 0 - 42947295.

Command Default

No default behavior or values.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Event manager applet configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
9.2(1)	This command was added.

Usage Guidelines

Use this command to configure actions on an event manager applet.

Examples

The following example shows how to configure actions on an event manager applet:

```
hostname (config-applet)#
action 1 cli command "show version"
```

Related Commands

Command	Description
description	Describes an applet.
event manager run	Runs an event manager applet.

Command	Description
show event manager	Shows statistical information for each configured event manager applet.
debug event manager	Manages debugging traces for the event manager.

action-uri

To specify a web server URI to receive a username and password for single sign-on (SSO) authentication, use the **action-uri** command in aaa-server-host configuration mode. To reset the URI parameter value, use the **no** form of the command.

action-uri *string*
no action-uri

Note To configure SSO with the HTTP protocol correctly, you must have a thorough working knowledge of authentication and HTTP protocol exchanges.

Syntax Description

string The URI for an authentication program. You can enter it on multiple lines. The maximum number of characters for each line is 255. The maximum number of characters for the complete URI is 2048 characters.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.1(1)	This command was added.

Usage Guidelines

This is an SSO with HTTP Forms command. A URI or Uniform Resource Identifier is a compact string of characters that identifies a point of content on the Internet, whether it be a page of text, a video or sound clip, a still or animated image, or a software program. The most common form of URI is the web page address, which is a particular form or subset of URI called a URL.

The WebVPN server of the ASA can use a POST request to submit an SSO authentication request to an authenticating web server. To accomplish this, configure the ASA to pass a username and a password to an action URI on an authenticating web server using an HTTP POST request. The **action-uri** command specifies the location and name of the authentication program on the web server to which the ASA sends the POST request.

You can discover the action URI on the authenticating web server by connecting to the web server login page directly with a browser. The URL of the login web page displayed in your browser is the action URI for the authenticating web server.

For ease of entry, you can enter URIs on multiple, sequential lines. The ASA then concatenates the lines into the URI as you enter them. While the maximum characters per action-uri line is 255 characters, you can enter fewer characters on each line.

Note Any question mark in the string must be preceded by a CTRL-v escape sequence.

Examples

The following example specifies the URI on www.example.com:

```
ciscoasa(config)# aaa-server testgrp1 host www.example.com
ciscoasa(config-aaa-server-host)# action-uri http://www.example.com/auth/index.htm
ciscoasa(config-aaa-server-host)# action-uri l/appdir/authc/forms/MCOlogin.fcc?TYP
ciscoasa(config-aaa-server-host)# action-uri 554433&REALMOID=06-000a1311-a828-1185
ciscoasa(config-aaa-server-host)# action-uri -ab41-8333b16a0008&GUID=&SMAUTHREASON
ciscoasa(config-aaa-server-host)# action-uri =0&METHOD=GET&SMAGENTNAME=$SM$5FZmjnk
ciscoasa(config-aaa-server-host)# action-uri 3DRNwNjk2KcqVCFbIrNT9%2bJ0H0KPshFtg6r
ciscoasa(config-aaa-server-host)# action-uri B1UV2PxkHqLw%3d%3d&TARGET=https%3A%2F
ciscoasa(config-aaa-server-host)# action-uri %2Fauth.example.com
ciscoasa(config-aaa-server-host)#
```

Note You must include the hostname and protocol in the action URI. In the preceding example, these are included in http://www.example.com at the start of the URI.

Related Commands

Command	Description
auth-cookie-name	Specifies a name for the authentication cookie.
hidden-parameter	Creates hidden parameters for exchange with the SSO server.
password-parameter	Specifies the name of the HTTP POST request parameter in which a user password must be submitted for SSO authentication.
start-url	Specifies the URL at which to retrieve a pre-login cookie.
user-parameter	Specifies the name of the HTTP POST request parameter in which a username must be submitted for SSO authentication.

activate-tunnel-group-script

This command is used internally to reload an ASDM generated script file when username-from-certificate is configured in tunnel-group sub-mode.

Note Do not use this command in the ASA CLI.

activation-key

To enter a license activation key on the ASA, use the **activation-key** command in privileged EXEC mode.

activation-key [**noconfirm** *activation_key*] **activate** | **deactivate** }

Syntax Description

activate	Activates a time-based activation key. **activate** is the default value. The last time-based key that you activate for a given feature is the active one.
activation_key	Applies an activation key to the ASA. The *activation_key* is a five-element hexadecimal string with one space between each element. The leading 0x specifier is optional; all values are assumed to be hexadecimal. You can install one permanent key, and multiple time-based keys. If you enter a new permanent key, it overwrites the already installed one.
deactivate	Deactivates a time-based activation key. The activation key is still installed on the ASA when you deactivate it, and you can activate it later using the **activate** keyword. If you enter a key for the first time, and specify **deactivate**, then the key is installed on the ASA in an inactive state.
noconfirm	(Optional) Enters an activation key without prompting you for confirmation.

Command Default

By default, your ASA ships with a license already installed. This license might be the Base License, to which you want to add more licenses, or it might already have all of your licenses installed, depending on what you ordered and what your vendor installed for you. See the **show activation-key** command to determine which licenses you have installed.

Command Modes

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

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

Command History

Release	Modification
7.0(5)	Increased the following limits: • ASA5510 Base license connections from 32000 to 5000; VLANs from 0 to 10. • ASA5510 Security Plus license connections from 64000 to 130000; VLANs from 10 to 25. • ASA5520 connections from 130000 to 280000; VLANs from 25 to 100. • ASA5540 connections from 280000 to 400000; VLANs from 100 to 200.

Release	Modification
7.1(1)	SSL VPN licenses were added.
7.2(1)	A 5000-user SSL VPN license was added for the ASA 5550 and above.
7.2(2)	• The maximum number of VLANs for the Security Plus license on the ASA 5505 ASA was increased from 5 (3 fully functional; 1 failover; one restricted to a backup interface) to 20 fully functional interfaces. In addition, the number of trunk ports was increased from 1 to 8. • VLAN limits were increased for the ASA 5510 (from 10 to 50 for the Base license, and from 25 to 100 for the Security Plus license), the ASA 5520 (from 100 to 150), and the ASA 5550 (from 200 to 250).
7.2(3)	The ASA 5510 supports GE (Gigabit Ethernet) for port 0 and 1 with the Security Plus license. If you upgrade the license from Base to Security Plus, the capacity of the external Ethernet0/0 and Ethernet0/1 ports increases from the original FE (Fast Ethernet) (100 Mbps) to GE (1000 Mbps). The interface names will remain Ethernet 0/0 and Ethernet 0/1. Use the **speed** command to change the speed on the interface and use the **show interface** command to see what speed is currently configured for each interface.
8.0(2)	• The Advanced Endpoint Assessment license was added. • VPN load balancing is supported on the ASA 5510 Security Plus license.
8.0(3)	The Secure Client for Mobile license was added.
8.0(4)/8.1(2)	Support for time-based licenses was added.
8.1(2)	The number of VLANs supported on the ASA 5580 increased from 100 to 250.
8.0(4)	The UC Proxy sessions license was added.
8.2(1)	• The Botnet Traffic Filter license was added. • The AnyConnect Essentials License was added. By default, the ASA uses the AnyConnect Essentials license, but you can disable it to use other licenses by using the **no anyconnect-essentials** command. • Shared licenses for SSL VPN were added.
8.2(2)	The Mobility Proxy no longer requires the UC Proxy license.
8.3(1)	• Failover licenses no longer need to be identical on each unit. The license used for both units is the combined license from the primary and secondary units. • Time-based licenses are stackable. • The IME license was added. • You can install multiple time-based licenses, and have one license per feature active at a time. • You can activate or deactivate time-based licenses using **activate** or **deactivate** keywords.

Release	Modification

8.4(1)	• For the ASA 5550 and ASA 5585-X with SSP-10, the maximum number of contexts was increased from 50 to 100. For the ASA 5580 and 5585-X with SSP-20 and higher, the maximum was increased from 50 to 250.
	• For the ASA 5580 and 5585-X, the maximum number of VLANs was increased from 250 to 1024.
	• We increased the firewall connection limits:
	  • ASA 5580-20—1,000 K to 2,000 K.
	  • ASA 5580-40—2,000 K to 4,000 K.
	  • ASA 5585-X with SSP-10: 750 K to 1,000 K
	  • ASA 5585-X with SSP-20: 1,000 K to 2,000 K
	  • ASA 5585-X with SSP-40: 2,000 K to 4,000 K
	  • ASA 5585-X with SSP-60: 2,000 K to 10,000 K
	• For the ASA 5580, the AnyConnect VPN session limit was increased from 5,000 to 10,000.
	• For the ASA 5580, the other VPN session limit was increased from 5,000 to 10,000.
	• IPsec remote access VPN using IKEv2 was added to the AnyConnect Essentials and AnyConnect Premium licenses.
	• Site-to-site sessions were added to the Other VPN license (formerly IPsec VPN).
	• For models available with No Payload Encryption (for example, the ASA 5585-X), the ASA software disables Unified Communications and VPN features, making the ASA available for export to certain countries.

Usage Guidelines

Obtaining an Activation Key

To obtain an activation key, you need a Product Authorization Key, which you can purchase from your Cisco account representative. You need to purchase a separate Product Activation Key for each feature license. For example, if you have the Base License, you can purchase separate keys for Advanced Endpoint Assessment and for additional SSL VPN sessions.

After obtaining the Product Authorization Keys, register them on Cisco.com at one of the following URLs.

- If you are a registered user of Cisco.com, go to the following website:

http://www.cisco.com/go/license

- If you are not a registered user of Cisco.com, go to the following website:

http://www.cisco.com/go/license/public

Context Mode Guidelines

- In multiple context mode, apply the activation key in the system execution space.
- Shared licenses are not supported in multiple context mode.

Failover Guidelines

- Shared licenses are not supported in Active/Active mode.
- Failover units do not require the same license on each unit.

Older versions of ASA software required that the licenses match on each unit. Starting with Version 8.3(1), you no longer need to install identical licenses. Typically, you buy a license only for the primary unit; for Active/Standby failover, the secondary unit inherits the primary license when it becomes active. If you have licenses on both units, they combine into a single running failover cluster license.

- For the ASA 5505 and 5510, both units require the Security Plus license; the Base license does not support failover, so you cannot enable failover on a standby unit that only has the Base license.

Upgrade and Downgrade Guidelines

Your activation key remains compatible if you upgrade to the latest version from any previous version. However, you might have issues if you want to maintain downgrade capability:

- Downgrading to Version 8.1 or earlier—After you upgrade, if you activate additional feature licenses that were added *before 8.2* , then the activation key continues to be compatible with earlier versions if you downgrade. However if you activate feature licenses that were added in *8.2 or later* , then the activation key is not backwards compatible. If you have an incompatible license key, then see the following guidelines:
  - If you previously entered an activation key in an earlier version, then the ASA uses that key (without any of the new licenses you activated in Version 8.2 or later).
  - If you have a new system and do not have an earlier activation key, then you need to request a new activation key compatible with the earlier version.
- Downgrading to Version 8.2 or earlier—Version 8.3 added more robust time-based key usage as well as failover license changes:
  - If you have more than one time-based activation key active, when you downgrade, only the most recently activated time-based key can be active. Any other keys are made inactive.
  - If you have mismatched licenses on a failover pair, then downgrading will disable failover. Even if the keys are matching, the license used will no longer be a combined license.

Additional Guidelines and Limitations

- The activation key is not stored in your configuration file; it is stored as a hidden file in flash memory.
- The activation key is tied to the serial number of the device. Feature licenses cannot be transferred between devices (except in the case of a hardware failure). If you have to replace your device due to a hardware failure, contact the Cisco Licensing Team to have your existing license transferred to the new serial number. The Cisco Licensing Team will ask for the Product Authorization Key reference number and existing serial number.
- Once purchased, you cannot return a license for a refund or for an upgraded license.
- Although you can activate all license types, some features are incompatible with each other; for example, multiple context mode and VPN. In the case of the AnyConnect Essentials license, the license is incompatible with the following licenses: full SSL VPN license, shared SSL VPN license, and Advanced Endpoint Assessment license. By default, the AnyConnect Essentials license is used instead of the above

licenses, but you can disable the AnyConnect Essentials license in the configuration to restore use of the other licenses using the **no anyconnect-essentials** command.

- Some permanent licenses require you to reload the ASA after you activate them. <xref> lists the licenses that require reloading.

Table 1: Permanent License Reloading Requirements

Model	License Action Requiring Reload
ASA 5505 and ASA 5510	Changing between the Base and Security Plus license.
All models	Changing the Encryption license.
All models	Downgrading any permanent license (for example, going from 10 contexts to 2 contexts).

Examples

The following example shows how to change the activation key on the ASA:

```
ciscoasa# activation-key 0xd11b3d48 0xa80a4c0a 0x48e0fd1c 0xb0443480 0x843fc490
```

The following is sample output from the **activation-key** command that shows output for failover when the new activation key is different than the old activation key:

```
ciscoasa# activation-key 0xyadayada 0xyadayada 0xyadayada 0xyadayada 0xyadayada
Validating activation key. This may take a few minutes...
The following features available in the running permanent activation key are NOT available
 in the new activation key:
Failover is different.
   running permanent activation key: Restricted (R)
   new activation key: Unrestricted (UR)
WARNING: The running activation key was not updated with the requested key.
Proceed with updating flash activation key? [y
]
Flash permanent activation key was updated with the requested key.
```

The following is sample output from a license file:

```
Serial Number Entered: 123456789ja
Number of Virtual Firewalls Selected: 10
Formula One device: ASA 5520
Failover                       : Enabled
VPN-DES                        : Enabled
VPN-3DES-AES                   : Enabled
Security Contexts              : 10
GTP/GPRS                       : Disabled
SSL VPN Peers                  : Default
Total VPN Peers                : 750
Advanced Endpoint Assessment   : Disabled
AnyConnect for Mobile          : Enabled
AnyConnect for Cisco VPN Phone : Disabled
Shared License                 : Disabled
UC Phone Proxy Sessions        : Default
Total UC Proxy Sessions        : Default
AnyConnect Essentials          : Disabled
Botnet Traffic Filter          : Disabled
Intercompany Media Engine      : Enabled
```

```
-----------------------------------------
THE FOLLOWING ACTIVATION KEY IS VALID FOR:
ASA SOFTWARE RELEASE 8.2+ ONLY.
Platform = asa
123456789JA: yadayda1 yadayda1 yadayda1 yadayda1 yadayda1
-----------------------------------------
THE FOLLOWING ACTIVATION KEY IS VALID FOR:
ALL ASA SOFTWARE RELEASES, BUT EXCLUDES ANY
8.2+ FEATURES FOR BACKWARDS COMPATIBILITY.
Platform = asa
123456789JA: yadayda2 yadayda2 yadayda2 yadayda2 yadayda2
```

Related Commands

Command	Description
anyconnect-essentials	Enables or disables the Anyconnect Essentials license.
show activation-key	Shows the activation key.
show version	Shows the software version and activation key.

activex-relay

To incorporate applications that need ActiveX over the clientless portal, use the **activex-relay** command in group-policy webvpn configuration mode or username webvpn configuration mode. To inherit the **activex-relay** command from the default group policy, use the **no** form of this command.

activex-relay { **enable** | **disable** }
no activex-relay

Syntax Description

enable	Enables ActiveX on WebVPN sessions.
disable	Disables ActiveX on WebVPN sessions.

Command Default

No default behavior or values.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Group-policy webvpn configuration	• Yes	—	• Yes	—	—
Username webvpn configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.

Usage Guidelines

Use the **activex-relay enable** command to let users launch ActiveX from the WebVPN browser for any HTML content that has the object tags (such as images, audio, videos, JAVA applets, ActiveX, PDF, or flash). These applications use the WebVPN session to download and upload ActiveX controls. The ActiveX relay remains in force until the WebVPN session closes. If you plan to use something like Microsoft OWA 2007, you should disable ActiveX.

Note Because they have the same functionality, the **activex-relay enable** command generates smart tunnel logs even if smart tunnel is disabled.

The following example enables ActiveX controls on WebVPN sessions associated with a given group policy:

```
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# activex-relay enable
```

The following example disables ActiveX controls on WebVPN sessions associated with a given username:

```
ciscoasa(config-username-policy)# webvpn
ciscoasa(config-username-webvpn)# activex-relay disable
```