

Standard Access Control Lists

This chapter describes how to configure a standard ACL and includes the following sections:

- Information About Standard ACLs, page 23-1
- Licensing Requirements for Standard ACLs, page 23-1
- Guidelines and Limitations, page 23-1
- Default Settings, page 23-2
- Adding Standard ACLs, page 23-3
- Feature History for Standard ACLs, page 23-4

Information About Standard ACLs

Standard ACLs identify the destination IP addresses of OSPF routes and can be used in a route map for OSPF redistribution. Standard ACLs cannot be applied to interfaces to control traffic.

Licensing Requirements for Standard ACLs

Model	License Requirement
ASAv	Standard or Premium License.
All other models	Base License.

Guidelines and Limitations

This section includes the guidelines and limitations for this feature:

- Context Mode Guidelines, page 23-2
- Firewall Mode Guidelines, page 23-2
- IPv6 Guidelines, page 23-2
- Additional Guidelines and Limitations, page 23-2

Context Mode Guidelines

Supported in single context mode only.

Firewall Mode Guidelines

Supported in routed and transparent firewall modes.

IPv6 Guidelines

Supports IPv6.

Additional Guidelines and Limitations

The following guidelines and limitations apply for standard ACLs:

- Standard ACLs identify the destination IP addresses (not source addresses) of OSPF routes and can be used in a route map for OSPF redistribution. Standard ACLs cannot be applied to interfaces to control traffic.
- When specifying a source, local, or destination address, use the following guidelines:
  - Use a 32-bit quantity in four-part, dotted-decimal format.
- If you add descriptive remarks to your ACL with non-English characters on one platform (such as Windows) then try to remove them from another platform (such as Linux), you might not be able to edit or delete them because the original characters might not be correctly recognized. This limitation is due to an underlying platform dependency that encodes different language characters in different ways.

Default Settings

Table 23-1 lists the default settings for standard ACL parameters.

Table 23-1 Default Standard ACL Parameters

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

Adding Standard ACLs

This section includes the following topics:

- Using Standard ACLs, page 23-3

Using Standard ACLs

Standard ACLs identify the destination IP addresses (not source addresses) of OSPF routes and can be used in a route map for OSPF redistribution. Standard ACLs cannot be applied to interfaces to control traffic.

This section includes the following topics:

- Adding a Standard ACL, page 23-3
- Adding an ACE to a Standard ACL, page 23-3
- Editing an ACE in a Standard ACL, page 23-4

Adding a Standard ACL

To add a standard ACL to your configuration, perform the following steps:

Step 1 Choose **Configuration > Firewall > Advanced > Standard ACL.**

Step 2 Click **Add**, and from the drop-down list, choose **Add ACL**.

Step 3 In the Add ACL dialog box, add a name or number (without spaces) to identify the ACL.

Step 4 Click **OK.**

The ACL name appears in the main pane.

You may add additional ACLs.

Step 5 Click **Apply** to save the ACLs to your configuration.

You can now add one or more ACEs to the newly created ACL.

To add an ACE, see Adding an ACE to a Standard ACL, page 23-3.

Adding an ACE to a Standard ACL

Before you can add an ACE to a configuration, you must first add an ACL. For information about adding a standard ACL, see Adding a Standard ACL, page 23-3. For information about editing ACEs, see Editing an ACE in a Standard ACL, page 23-4

To add an ACE to an ACL that exists in your configuration, perform the following steps:

Step 1 Choose **Configuration > Firewall > Advanced > Standard ACL.**

Step 2 In the main pane, select the ACL for which you want to add an ACE.

Step 3 Click **Add**, and choose **Add ACE** from the drop-down list.

The Add ACE dialog box appears.

Step 4 (Optional) To specify the placement of the new ACE, select an existing ACE, and click Insert... to add the ACE before the selected ACE, or click Insert After... to add the ACE after the selected ACE.

Step 5 Click one of the following radio buttons to choose an action:

- **Permit**—Permits access if the conditions are matched.
- **Deny**—Denies access if the conditions are matched.

Step 6 In the Address field, enter the IP address of the destination to which you want to perform or deny access.

You can also browse for the address of a network object by clicking the ellipsis at the end of the Address field.

Step 7 (Optional) In the Description field, enter a description that makes an ACE easier to understand.

The description can contain multiple lines; however, each line can be no more than 100 characters in length.

Step 8 Click **OK**.

The newly created ACE appears under the ACL.

Step 9 Click Apply to save the ACE to your configuration.

Editing an ACE in a Standard ACL

To edit an ACE in a standard ACL, perform the following steps:

Step 1 Choose **Configuration > Firewall > Advanced > Standard ACL.**

Step 2 In the main pane, select the existing ACE that you want to edit.

Step 3 Click **Edit.**

The Edit ACE dialog box appears.

Step 4 Enter the desired changes.

Step 5 Click **OK**.

Feature History for Standard ACLs

Table 23-2 lists the release history for this feature.

Table 23-2 Feature History for Standard ACLs

Feature Name	Releases	Feature Information
Standard ACLs	7.0(1)	Standard ACLs identify the destination IP addresses of OSPF routes, which can be used in a route map for OSPF redistribution. The feature was introduced.