

## Adding Global Objects

---

The Objects pane provides a single location where you can configure, view, and modify the reusable components that you need to implement your policy on the security appliance. For example, once you define the hosts and networks that are covered by your security policy, you can select the host or network to which a feature applies, instead of having to redefine it every time. This saves time and ensures consistency and accuracy of your security policy. When you need to add or delete a host or network, you can use the Objects pane to change it in a single place.

This chapter includes the following sections:

- [Using Network Objects and Groups, page 8-2](#)
- [Configuring Service Groups, page 8-4](#)
- [Configuring Class Maps, page 8-7](#)
- [Configuring Inspect Maps, page 8-7](#)
- [Configuring Regular Expressions, page 8-7](#)
- [Configuring TCP Maps, page 8-14](#)
- [Configuring Global Pools, page 8-14](#)
- [Configuring Time Ranges, page 8-14](#)
- [Encrypted Traffic Inspection, page 8-16](#)

# Using Network Objects and Groups

This section describes how to use network objects and groups, and includes the following topics:

- [Network Object Overview, page 8-2](#)
- [Configuring a Network Object, page 8-2](#)
- [Configuring a Network Object Group, page 8-3](#)
- [Viewing the Usage of a Network Object or Group, page 8-4](#)

## Network Object Overview

Network objects let you predefine host and network IP addresses so that you can streamline subsequent configuration. When you configure the security policy, such as an access rule or a AAA rule, you can choose these predefined addresses instead of typing them in manually. Moreover, if you change the definition of an object, the change is inherited automatically by any rules using the object.

You can add network objects manually, or you can let ASDM automatically create objects from existing configuration, such as access rules and AAA rules. If you edit one of these derived objects, it persists even if you later delete the rule that used it. Otherwise, derived objects only reflect the current configuration if you refresh.

Grouping together multiple hosts and networks lets you easily apply a rule to a group of addresses. Multiple network object groups can be nested into a “group of groups” and used as a single group.

When you are configuring rules, the ASDM window includes an Addresses side pane at the right that shows available network objects and network object groups; you can add, edit, or delete objects directly in the side pane. You can also drag additional network objects and groups from the side pane to the source or destination of a selected access rule.

## Configuring a Network Object

To configure a network object, perform the following steps:

- 
- Step 1** From the Configuration > Firewall > Objects > Network Objects/Group pane, click **Add > Network Object** to add a new object, or choose an object and click **Edit**.

You can also add or edit network objects from the Addresses side pane in a rules window, or when you are adding a rule.

To find an object in the list, enter a name or IP address in the Filter field and click **Filter**. The wildcard characters asterisk (\*) and question mark (?) are allowed.

The Add/Edit Network Object dialog box appears.

- Step 2** Fill in the following values:

- **Name**—(Optional) The object name. Use characters a to z, A to Z, 0 to 9, a dot, a dash, or an underscore. The name must be 64 characters or less.
- **IP Address**—The IP address, either a host or network address.
- **Netmask**—The subnet mask for the IP address.
- **Description**—(Optional) The description of the network object.

- Step 3** Click **OK**.

You can now use this network object when you create a rule. For an edited object, the change is inherited automatically by any rules using the object.

**Note**

You cannot delete a network object that is in use.

**Modes**

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

## Configuring a Network Object Group

To configure a network object group, perform the following steps:

- Step 1** From the Configuration > Firewall > Objects > Network Objects/Group pane, click **Add > Network Object Group** to add a new object group, or choose an object group and click **Edit**.
- You can also add or edit network object groups from the Addresses side pane in a rules window, or when you are adding a rule.
- To find an object in the list, enter a name or IP address in the Filter field and click **Filter**. The wildcard characters asterisk (\*) and question mark (?) are allowed.
- The Add/Edit Network Object Group dialog box appears.
- Step 2** In the Group Name field, enter a group name.
- Use characters a to z, A to Z, 0 to 9, a dot, a dash, or an underscore. The name must be 64 characters or less.
- Step 3** (Optional) In the Description field, enter a description up to 200 characters in length.
- Step 4** You can add existing objects or groups to the new group (nested groups are allowed), or you can create a new address to add to the group:
- To add an existing network object or group to the new group, double-click the object in the Existing Network Objects/Groups pane.
 

You can also select the object, and then click the **Add** button. The object or group is added to the right-hand Members in Group pane.
  - To add a new address, fill in the values under the Create New Network Object Member area, and click **Add**.
 

The object or group is added to the right-hand Members in Group pane. This address is also added to the network object list.
- To remove an object, double-click it in the Members in Group pane, or click the **Remove** button.
- Step 5** After you add all the member objects, click **OK**.

You can now use this network object group when you create a rule. For an edited object group, the change is inherited automatically by any rules using the group.

**Note**

You cannot delete a network object group that is in use.

**Modes**

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

## Viewing the Usage of a Network Object or Group

To view what rules use a network object or group, from the Configuration > Firewall > Objects > Network Objects/Group pane, click the magnifying glass Find icon.

The Usages dialog box appears listing all the rules currently using the network object or group. This dialog box also lists any network object groups that contain the object.

## Configuring Service Groups

This section describes how to configure service groups, and includes the following topics:

- [Service Groups, page 8-4](#)
- [Add/Edit Service Group, page 8-5](#)
- [Browse Service Groups, page 8-6](#)

## Service Groups

The Service Groups pane lets you associate multiple services into a named group. You can specify any type of protocol and service in one group or create service groups for each of the following types:

- TCP ports
- UDP ports
- TCP-UDP ports
- ICMP types
- IP protocols

Multiple service groups can be nested into a “group of groups” and used as a single group.

You can use a service group for most configurations that require you to identify a port, ICMP type, or protocol. When you are configuring NAT or security policy rules, the ASDM window even includes a side pane at the right that shows available service groups and other global objects; you can add, edit, or delete objects directly in the side pane.

### Fields

- **Add**—Adds a service group. Choose the type of service group to add from the drop-down list or choose Service Group for multiple types.
- **Edit**—Edits a service group.
- **Delete**—Deletes a service group. When a service group is deleted, it is removed from all service groups where it is used. If a service group is used in an access rule, do not remove it. A service group used in an access rule cannot be made empty.
- **Find**—Filters the display to show only matching names. Clicking **Find** opens the Filter field. Click **Find** again to hide the Filter field.
  - **Filter field**—Enter the name of the service group. The wildcard characters asterisk (\*) and question mark (?) are allowed.
  - **Filter**—Runs the filter.
  - **Clear**—Clears the Filter field.
- **Name**—Lists the service group names. Click the plus (+) icon next to the name to expand the service group so you can view the services. Click the minus (-) icon to collapse the service group.
- **Protocol**—Lists the service group protocols.
- **Source Ports**—Lists the protocol source ports.
- **Destination Ports**—Lists the protocol destination ports.
- **ICMP Type**—Lists the service group ICMP type.
- **Description**—Lists the service group descriptions.

### Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

## Add/Edit Service Group

The Add/Edit Service Group dialog box lets you assign services to a service group. This dialog box name matches the type of service group you are adding; for example, if you are adding a TCP service group, the Add/Edit TCP Service Group dialog box is shown.

### Fields

- **Group Name**—Enter the group name, up to 64 characters in length. The name must be unique for all object groups. A service group name cannot share a name with a network object group.

- Description—Enter a description of this service group, up to 200 characters in length.
- Existing Service/Service Group—Identifies items that can be added to the service group. Choose from already defined service groups, or choose from a list of commonly used port, type, or protocol names.
  - Service Groups—The title of this table depends on the type of service group you are adding. It includes the defined service groups.
  - Predefined—Lists the predefined ports, types, or protocols.
- Create new member—Lets you create a new service group member.
  - Service Type—Lets you select the service type for the new service group member. Service types include TCP, UDP, TCP-UDP, ICMP, and protocol.
  - Destination Port/Range—Lets you enter the destination port or range for the new TCP, UDP, or TCP-UDP service group member.
  - Source Port/Range—Lets you enter the source port or range for the new TCP, UDP, or TCP-UDP service group member.
  - ICMP Type—Lets you enter the ICMP type for the new ICMP service group member.
  - Protocol—Lets you enter the protocol for the new protocol service group member.
- Members in Group—Shows items that are already added to the service group.
- Add—Adds the selected item to the service group.
- Remove—Removes the selected item from the service group.

### Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

## Browse Service Groups

The Browse Service Groups dialog box lets you choose a service group. This dialog box is used in multiple configuration screens and is named appropriately for your current task. For example, from the Add/Edit Access Rule dialog box, this dialog box is named “Browse Source Port” or “Browse Destination Port.”

### Fields

- Add—Adds a service group.
- Edit—Edits the selected service group.
- Delete—Deletes the selected service group.
- Find—Filters the display to show only matching names. Clicking **Find** opens the Filter field. Click **Find** again to hide the Filter field.

- Filter field—Enter the name of the service group. The wildcard characters asterisk (\*) and question mark (?) are allowed.
- Filter—Runs the filter.
- Clear—Clears the Filter field.
- Type—Lets you choose the type of service group to show, including TCP, UDP, TCP-UDP, ICMP, and Protocol. To view all types, choose **All**. Typically, the type of rule you configure can only use one type of service group; you cannot select a UDP service group for a TCP access rule.
- Name—Shows the name of the service group. Click the plus (+) icon next to the name of an item to expand it. Click the minus (-) icon to collapse the item.

### Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

## Configuring Class Maps

For information about class maps, see the [“Class Map Field Descriptions”](#) section on page 24-37.

## Configuring Inspect Maps

For information about inspect maps, see the [“Inspect Map Field Descriptions”](#) section on page 24-57.

## Configuring Regular Expressions

This section describes how to configure regular expressions, and includes the following topics:

- [Regular Expressions, page 8-7](#)
- [Add/Edit Regular Expression, page 8-8](#)
- [Build Regular Expression, page 8-10](#)
- [Test Regular Expression, page 8-12](#)
- [Add/Edit Regular Expression Class Map, page 8-13](#)

## Regular Expressions

Some [Configuring Class Maps](#) and [Configuring Inspect Maps](#) can specify regular expressions to match text inside a packet. Be sure to create the regular expressions before you configure the class map or inspect map, either singly or grouped together in a regular expression class map.

A regular expression matches text strings either literally as an exact string, or by using *metacharacters* so you can match multiple variants of a text string. You can use a regular expression to match the content of certain application traffic; for example, you can match body text inside an HTTP packet.

### Fields

- Regular Expressions—Shows the regular expressions
  - Name—Shows the regular expression names.
  - Value—Shows the regular expression definitions.
  - Add—Adds a regular expression.
  - Edit—Edits a regular expression.
  - Delete—Deletes a regular expression.
- Regular Expression Classes—Shows the regular expression class maps.
  - Name—Shows the regular expression class map name.
  - Match Conditions—Shows the match type and regular expressions in the class map.

Match Type—Shows the match type, which for regular expressions is always a positive match type (shown by the icon with the equal sign (=)) the criteria. (Inspection class maps allow you to create negative matches as well (shown by the icon with the red circle)). If more than one regular expression is in the class map, then each match type icon appears with “OR” next it, to indicate that this class map is a “match any” class map; traffic matches the class map if only one regular expression is matched.

Regular Expression—Lists the regular expressions included in each class map.

- Description—Shows the description of the class map.
- Add—Adds a regular expression class map.
- Edit—Edits a regular expression class map.
- Delete—Deletes a regular expression class map.

### Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

## Add/Edit Regular Expression

The Add/Edit Regular Expression dialog box lets you define and test a regular expression.

### Fields

- Name—Enter the name of the regular expression, up to 40 characters in length.
- Value—Enter the regular expression, up to 100 characters in length. You can enter the text manually, using the metacharacters in [Table 8-1](#), or you can click **Build** to use the [Build Regular Expression](#) dialog box.

**Note**

As an optimization, the security appliance searches on the deobfuscated URL. Deobfuscation compresses multiple forward slashes (/) into a single slash. For strings that commonly use double slashes, like “http://”, be sure to search for “http:/" instead.

Table 8-1 lists the metacharacters that have special meanings.

**Table 8-1** *regex Metacharacters*

Character	Description	Notes
.	Dot	Matches any single character. For example, <b>d.g</b> matches dog, dag, dtg, and any word that contains those characters, such as doggonnit.
( <i>exp</i> )	Subexpression	A subexpression segregates characters from surrounding characters, so that you can use other metacharacters on the subexpression. For example, <b>d(ola)g</b> matches dog and dag, but <b>dolag</b> matches do and ag. A subexpression can also be used with repeat quantifiers to differentiate the characters meant for repetition. For example, <b>ab(xy){3}z</b> matches abxyxyxyz.
	Alternation	Matches either expression it separates. For example, <b>dog cat</b> matches dog or cat.
?	Question mark	A quantifier that indicates that there are 0 or 1 of the previous expression. For example, <b>lo?se</b> matches lse or lose. <b>Note</b> You must enter <b>Ctrl+V</b> and then the question mark or else the help function is invoked.
*	Asterisk	A quantifier that indicates that there are 0, 1 or any number of the previous expression. For example, <b>lo*se</b> matches lse, lose, loose, etc.
+	Plus	A quantifier that indicates that there is at least 1 of the previous expression. For example, <b>lo+se</b> matches lose and loose, but not lse.
{ <i>x</i> } or { <i>x</i> ,}	Minimum repeat quantifier	Repeat at least <i>x</i> times. For example, <b>ab(xy){2,}z</b> matches abxyxyz, abxyxyxyz, and so on.
[ <i>abc</i> ]	Character class	Matches any character in the brackets. For example, <b>[abc]</b> matches a, b, or c.
[^ <i>abc</i> ]	Negated character class	Matches a single character that is not contained within the brackets. For example, <b>[^abc]</b> matches any character other than a, b, or c. <b>[^A-Z]</b> matches any single character that is not an uppercase letter.
[ <i>a-c</i> ]	Character range class	Matches any character in the range. <b>[a-z]</b> matches any lowercase letter. You can mix characters and ranges: <b>[abcq-z]</b> matches a, b, c, q, r, s, t, u, v, w, x, y, z, and so does <b>[a-cq-z]</b> . The dash (-) character is literal only if it is the last or the first character within the brackets: <b>[abc-]</b> or <b>[-abc]</b> .

Table 8-1 regex Metacharacters (continued)

Character	Description	Notes
""	Quotation marks	Preserves trailing or leading spaces in the string. For example, " test" preserves the leading space when it looks for a match.
^	Caret	Specifies the beginning of a line.
\	Escape character	When used with a metacharacter, matches a literal character. For example, \[ matches the left square bracket.
<i>char</i>	Character	When character is not a metacharacter, matches the literal character.
\r	Carriage return	Matches a carriage return 0x0d.
\n	Newline	Matches a new line 0x0a.
\t	Tab	Matches a tab 0x09.
\f	Formfeed	Matches a form feed 0x0c.
\xNN	Escaped hexadecimal number	Matches an ASCII character using hexadecimal (exactly two digits).
\NNN	Escaped octal number	Matches an ASCII character as octal (exactly three digits). For example, the character 040 represents a space.

- Build—Helps you build a regular expression using the [Build Regular Expression](#) dialog box.
- Test—Tests a regular expression against some sample text.

### Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

## Build Regular Expression

The Build Regular Expression dialog box lets you construct a regular expression out of characters and metacharacters. Fields that insert metacharacters include the metacharacter in parentheses in the field name.



### Note

As an optimization, the security appliance searches on the deobfuscated URL. Deobfuscation compresses multiple forward slashes (/) into a single slash. For strings that commonly use double slashes, like "http://", be sure to search for "http:/" instead.

## Fields

**Build Snippet**—This area lets you build text snippets of regular text or lets you insert a metacharacter into the Regular Expression field.

- Starts at the beginning of the line (^)—Indicates that the snippet should start at the beginning of a line, using the caret (^) metacharacter. Be sure to insert any snippet with this option at the beginning of the regular expression.
- Specify Character String—Enter a text string manually.
  - Character String—Enter a text string.
  - Escape Special Characters—If you entered any metacharacters in your text string that you want to be used literally, check this box to add the backslash (\) escape character before them. For example, if you enter “example.com,” this option converts it to “example\.com”.
  - Ignore Case—If you want to match upper and lower case characters, this check box automatically adds text to match both upper and lower case. For example, entering “cats” is converted to “[cC][aA][tT][sS]”.
- Specify Character—Lets you specify a metacharacter to insert in the regular expression.
  - Negate the character—Specifies not to match the character you identify.
  - Any character (.)—Inserts the period (.) metacharacter to match any character. For example, **d.g** matches dog, dag, dtg, and any word that contains those characters, such as doggonnit.
  - Character set—Inserts a character set. Text can match any character in the set. Sets include:
    - [0-9A-Za-z]
    - [0-9]
    - [A-Z]
    - [a-z]
    - [aeiou]
    - [\n\r\t] (which matches a new line, form feed, carriage return, or a tab)
 For example, if you specify [0-9A-Za-z], then this snippet will match any character from A to Z (upper or lower case) or any digit 0 through 9.
  - Special character—Inserts a character that requires an escape, including \, ?, \*, +, |, ., [, (, or ^. The escape character is the backslash (\), which is automatically entered when you choose this option.
  - Whitespace character—Whitespace characters include \n (new line), \f (form feed), \r (carriage return), or \t (tab).
  - Three digit octal number—Matches an ASCII character as octal (up to three digits). For example, the character \040 represents a space. The backslash (\) is entered automatically.
  - Two digit hexadecimal number—Matches an ASCII character using hexadecimal (exactly two digits). The backslash (\) is entered automatically.
  - Specified character—Enter any single character.
- Snippet Preview—*Display only*. Shows the snippet as it will be entered in the regular expression.
- Append Snippet—Adds the snippet to the end of the regular expression.
- Append Snippet as Alternate—Adds the snippet to the end of the regular expression separated by a pipe (|), which matches either expression it separates. For example, **dog|cat** matches dog or cat.
- Insert Snippet at Cursor—Inserts the snippet at the cursor.

**Regular Expression**—This area includes regular expression text that you can enter manually and build with snippets. You can then select text in the Regular Expression field and apply a quantifier to the selection.

- **Selection Occurrences**—Select text in the Regular Expression field, click one of the following options, and then click **Apply to Selection**. For example, if the regular expression is “test me,” and you select “me” and apply **One or more times**, then the regular expression changes to “test (me)+”.
  - **Zero or one times (?)**—A quantifier that indicates that there are 0 or 1 of the previous expression. For example, **lo?se** matches lse or lose.
  - **One or more times (+)**—A quantifier that indicates that there is at least 1 of the previous expression. For example, **lo+se** matches lose and loose, but not lse.
  - **Any number of times (\*)**—A quantifier that indicates that there are 0, 1 or any number of the previous expression. For example, **lo\*se** matches lse, lose, loose, etc.
  - **At least**—Repeat at least  $x$  times. For example, **ab(xy){2,}z** matches abxyxyz, abxyxyxyz, etc.
  - **Exactly**—Repeat exactly  $x$  times. For example, **ab(xy){3}z** matches abxyxyxyz.
  - **Apply to Selection**—Applies the quantifier to the selection.
- **Test**—Tests a regular expression against some sample text.

#### Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

## Test Regular Expression

The Test Regular Expression dialog box lets you test input text against a regular expression to make sure it matches as you intended.

#### Fields

- **Regular Expression**—Enter the regular expression you want to test. By default, the regular expression you entered in the [Add/Edit Regular Expression](#) or [Build Regular Expression](#) dialog box is input into this field. If you change the regular expression during your testing, and click **OK**, the changes are inherited by the [Add/Edit Regular Expression](#) or [Build Regular Expression](#) dialog boxes. Click **Cancel** to dismiss your changes.
- **Test String**—Enter a text string that you expect to match the regular expression.
- **Test**—Tests the Text String against the Regular Expression.
- **Test Result**—*Display only*. Shows if the test succeeded or failed.

#### Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
			Multiple	
Routed	Transparent	Single	Context	System
•	•	•	•	—

## Add/Edit Regular Expression Class Map

The Add/Edit Regular Expression Class Map dialog box groups regular expressions together. A regular expression class map can be used by inspection class maps and inspection policy maps.

### Fields

- Name—Enter a name for the class map, up to 40 characters in length. The name “class-default” is reserved. All types of class maps use the same name space, so you cannot reuse a name already used by another type of class map.
- Description—Enter a description, up to 200 characters in length.
- Available Regular Expressions—Lists the regular expressions that are not yet assigned to the class map.
  - Edit—Edits the selected regular expression.
  - New—Creates a new regular expression.
- Add—Adds the selected regular expression to the class map.
- Remove—Removes the selected regular expression from the class map.
- Configured Match Conditions—Shows the regular expressions in this class map, along with the match type.
  - Match Type—Shows the match type, which for regular expressions is always a positive match type (shown by the icon with the equal sign (=)) the criteria. (Inspection class maps allow you to create negative matches as well (shown by the icon with the red circle)). If more than one regular expression is in the class map, then each match type icon appears with “OR” next it, to indicate that this class map is a “match any” class map; traffic matches the class map if only one regular expression is matched.
  - Regular Expression—Lists the regular expression names in this class map.

### Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
			Multiple	
Routed	Transparent	Single	Context	System
•	•	•	•	—

## Configuring TCP Maps

For information about TCP maps, see the [“Enabling Connection Settings and TCP Normalization” section on page 27-8](#).

## Configuring Global Pools

For information about global pools, see the [“Using Dynamic NAT” section on page 25-16](#).

## Configuring Time Ranges

Use the Time Ranges option to create a reusable component that defines starting and ending times that can be applied to various security features. Once you have defined a time range, you can select the time range and apply it to different options that require scheduling.

The time range feature lets you define a time range that you can attach to traffic rules, or an action. For example, you can attach an access list to a time range to restrict access to the security appliance.

A time range consists of a start time, an end time, and optional recurring entries.



### Note

Creating a time range does not restrict access to the device. This pane defines the time range only.

### Fields

- Name—Specifies the name of the time range.
- Start Time—Specifies when the time range begins.
- End Time—Specifies when the time range ends.
- Recurring Entries—Specifies further constraints of active time of the range within the start and stop time specified.

### Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

## Add/Edit Time Range

The Add/Edit Time Range pane lets you define specific times and dates that you can attach to an action. For example, you can attach an access list to a time range to restrict access to the security appliance. The time range relies on the system clock of the security appliance; however, the feature works best with NTP synchronization.

**Note**

Creating a time range does not restrict access to the device. This pane defines the time range only.

**Fields**

- Time Range Name—Specifies the name of the time range. The name cannot contain a space or quotation mark, and must begin with a letter or number.
- Start now/Started—Specifies either that the time range begin immediately or that the time range has begun already. The button label changes based on the Add/Edit state of the time range configuration. If you are adding a new time range, the button displays “Start Now.” If you are editing a time range for which a fixed start time has already been defined, the button displays “Start Now.” When editing a time range for which there is no fixed start time, the button displays “Started.”
- Start at—Specifies when the time range begins.
  - Month—Specifies the month, in the range of January through December.
  - Day—Specifies the day, in the range of 01 through 31.
  - Year—Specifies the year, in the range of 1993 through 2035.
  - Hour—Specifies the hour, in the range of 00 through 23.
  - Minute—Specifies the minute, in the range of 00 through 59.
- Never end—Specifies that there is no end to the time range.
- End at (inclusive)—Specifies when the time range ends. The end time specified is inclusive. For example, if you specified that the time range expire at 11:30, the time range is active through 11:30 and 59 seconds. In this case, the time range expires when 11:31 begins.
  - Month—Specifies the month, in the range of January through December.
  - Day—Specifies the day, in the range of 01 through 31.
  - Year—Specifies the year, in the range of 1993 through 2035.
  - Hour—Specifies the hour, in the range of 00 through 23.
  - Minute—Specifies the minute, in the range of 00 through 59.
- Recurring Time Ranges—Configures daily or weekly time ranges.
  - Add—Adds a recurring time range.
  - Edit—Edits the selected recurring time range.
  - Delete—Deletes the selected recurring time range.

**Modes**

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

## Add/Edit Recurring Time Range

The Add/Edit Recurring Time Range pane lets you fine time ranges further by letting you configure them on a daily or weekly basis.


**Note**

Creating a time range does not restrict access to the device. This pane defines the time range only.

**Fields**

- Days of the week
  - Every day—Specifies every day of the week.
  - Weekdays—Specifies Monday through Friday.
  - Weekends—Specifies Saturday and Sunday.
  - On these days of the week—Lets you choose specific days of the week.
  - Daily Start Time—Specifies the hour and the minute that the time range begins.
  - Daily End Time (inclusive) area—Specifies the hour and the minute that the time range ends. The end time specified is inclusive.
- Weekly Interval
  - From—Lists the day of the week, Monday through Sunday.
  - Through—Lists the day of the week, Monday through Sunday.
  - Hour—Lists the hour, in the range of 00 through 23.
  - Minute—Lists the minute, in the range of 00 through 59.

**Modes**

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

## Encrypted Traffic Inspection

This section describes how to configure encrypted traffic inspection, and includes the following topics:

- [TLS Proxy, page 8-16](#)
- [CTL Provider, page 8-18](#)

## TLS Proxy

Use the TLS Proxy option to enable inspection of SSL encrypted VoIP signaling, namely Skinny and SIP, interacting with Cisco CallManager.

The TLS Proxy pane lets you define and configure Transaction Layer Security Proxy to enable inspection of encrypted traffic.

### Fields

- TLS Proxy Name—Lists the TLS Proxy name.
- Server—Lists the trustpoint, which is either self-signed or enrolled with a certificate server.
- Local Dynamic Certificate Issuer—Lists the local certificate authority to issue client or server dynamic certificates.
- Local Dynamic Certificate Key Pair—Lists the RSA key pair used by client or server dynamic certificates.
- Add—Adds a TLS Proxy.
- Edit—Edits a TLS Proxy.
- Delete—Deletes a TLS Proxy.
- Maximum Sessions—Lets you specify the maximum number of TLS Proxy sessions to support.
  - Specify the maximum number of TLS Proxy sessions that the ASA needs to support. By default, ASA supports 300 sessions.—Enables maximum number of sessions option.
  - Maximum number of sessions:—The minimum is 1. The maximum is dependent on the platform. The default is 300.

### Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

## Add/Edit TLS Proxy

The Add/Edit TLS Proxy dialog box lets you define the parameters for the TLS Proxy.

### Fields

- TLS Proxy Name—Specifies the TLS Proxy name.
- Server Configuration—Specifies the proxy certificate name.
  - Server—Specifies the trustpoint to be presented during the TLS handshake. The trustpoint could be self-signed or enrolled locally with the certificate service on the proxy.
- Client Configuration—Specifies the local dynamic certificate issuer and key pair.
  - Local Dynamic Certificate Issuer—Lists the local certificate authority to issue client or server dynamic certificates.
    - Certificate Authority Server—Specifies the certificate authority server.
    - Certificate—Specifies a certificate.
    - Manage—Configures the local certificate authority. To make configuration changes after it has been configured for the first time, disable the local certificate authority.

- Local Dynamic Certificate Key Pair—Lists the RSA key pair used by client dynamic certificates.
  - Key-Pair Name—Specifies a defined key pair.
  - Show—Shows the key pair details, including generation time, usage, modulus size, and key data.
  - New—Lets you define a new key pair.
- More Options—Specifies the available and active algorithms to be announced or matched during the TLS handshake.
  - Available Algorithms—Lists the available algorithms to be announced or matched during the TLS handshake: des-sha1, 3des-sha1, aes128-sha1, aes256-sha1, and null-sha1.
    - Add—Adds the selected algorithm to the active list.
    - Remove—Removes the selected algorithm from the active list.
  - Active Algorithms—Lists the active algorithms to be announced or matched during the TLS handshake: des-sha1, 3des-sha1, aes128-sha1, aes256-sha1, and null-sha1. For client proxy (acting as a TLS client to the server), the user-defined algorithms replace the original ones from the hello message for asymmetric encryption method between the two TLS legs. For example, the leg between the proxy and CallManager may be NULL cipher to offload the CallManager.
    - Move Up—Moves an algorithm up in the list.
    - Move Down—Moves an algorithm down in the list.

### Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

## CTL Provider

Use the CTL Provider option to configure Certificate Trust List provider service.

The CTL Provider pane lets you define and configure Certificate Trust List provider service to enable inspection of encrypted traffic.

### Fields

- CTL Provider Name—Lists the CTL Provider name.
- Client Details—Lists the name and IP address of the client.
  - Interface Name—Lists the defined interface name.
  - IP Address—Lists the defined interface IP address.
- Certificate Name—Lists the certificate to be exported.
- Add—Adds a CTL Provider.
- Edit—Edits a CTL Provider.

- Delete—Deletes a CTL Provider.

### Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

## Add/Edit CTL Provider

The Add/Edit CTL Provider dialog box lets you define the parameters for the CTL Provider.

### Fields

- CTL Provider Name—Specifies the CTL Provider name.
- Certificate to be Exported—Specifies the certificate to be exported to the client.
  - Certificate Name—Specifies the name of the certificate to be exported to the client.
  - Manage—Manages identity certificates.
- Client Details—Specifies the clients allowed to connect.
  - Client to be Added—Specifies the client interface and IP address to add to the client list.
    - Interface—Specifies client interface.
    - IP Address—Specifies the client IP address.
    - Add—Adds the new client to the client list.
    - Delete—Deletes the selected client from the client list.
- More Options—Specifies the available and active algorithms to be announced or matched during the TLS handshake.
  - Parse the CTL file provided by the CTL Client and install trustpoints—Trustpoints installed by this option have names prefixed with “\_internal\_CTL\_.” If disabled, each CallManager server and CAPF certificate must be manually imported and installed.
  - Port Number—Specifies the port to which the CTL provider listens. The port must be the same as the one listened to by the CallManager servers in the cluster (as configured under Enterprise Parameters on the CallManager administration page). The default is 2444.
  - Authentication—Specifies the username and password that the client authenticates with the provider.
    - Username—Client username.
    - Password—Client password.
    - Confirm Password—Client password.

### Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
			Multiple	
Routed	Transparent	Single	Context	System
•	•	•	•	—



