



CHAPTER 19

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 19-1](#)
- [Configuring Service Groups, page 19-5](#)
- [Configuring Class Maps, page 19-8](#)
- [Configuring Inspect Maps, page 19-8](#)
- [Configuring Regular Expressions, page 19-8](#)
- [Configuring TCP Maps, page 19-14](#)
- [Configuring Global Pools, page 19-14](#)
- [Configuring Time Ranges, page 19-15](#)
- [Encrypted Traffic Inspection, page 19-17](#)

Using Network Objects and Groups

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

- [Network Object Overview, page 19-2](#)
- [Configuring a Network Object, page 19-2](#)
- [Configuring a Network Object Group, page 19-3](#)
- [Using Network Objects and Groups in a Rule, page 19-4](#)
- [Viewing the Usage of a Network Object or Group, page 19-4](#)

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.

A network object group is a group containing multiple hosts and networks together. A network object group can also contain other network object groups. You can then specify the network object group as the source address or destination address in an access rule.

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 Addresses pane. You can also drag additional network objects and groups from the Addresses 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 In 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** In 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 **Add**. 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 **Remove**.
- 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
•	•	•	•	—

Using Network Objects and Groups in a Rule

When you create a rule, you can enter an IP address manually, or you can browse for a network object or group to use in the rule. To use a network object or group in a rule, perform the following steps:

-
- Step 1** From the rule dialog box, click the ... browse button next to the source or destination address field. The Browse Source Address or Browse Destination Address dialog box appears.
- Step 2** You can either add a new network object or group, or choose an existing network object or group by double-clicking it.
- 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.
- To add a new network object, see the [“Configuring a Network Object”](#) section on page 19-2.
 - To add a new network object group, see the [“Configuring a Network Object Group”](#) section on page 19-3.
- After you add a new object or double-click an existing object, it appears in the Selected Source/Destination field. For access rules, you can add multiple objects and groups in the field, separated by commas.
- Step 3** Click **OK**.
- You return to the rule dialog box.
-

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, in 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.

Modes

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

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

Configuring Service Groups

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

- [Service Groups, page 19-5](#)
- [Add/Edit Service Group, page 19-6](#)
- [Browse Service Groups, page 19-7](#)

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 Services pane at the right that shows available service groups and other global objects; you can add, edit, or delete objects directly in the Services 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 24-39.

Configuring Inspect Maps

For information about inspect maps, see the “[Inspect Map Field Descriptions](#)” section on page 24-59.

Configuring Regular Expressions

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

- [Regular Expressions](#), page 19-8
- [Add/Edit Regular Expression](#), page 19-9
- [Build Regular Expression](#), page 19-11
- [Test Regular Expression](#), page 19-13
- [Add/Edit Regular Expression Class Map](#), page 19-14

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 to 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 19-1](#), 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 19-1](#) lists the metacharacters that have special meanings.

Table 19-1 regex Metacharacters

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

Table 19-1 *regex Metacharacters (continued)*

Character	Description	Notes
<i>char</i>	Character	When character is not a metacharacter, matches the literal character.
<code>\r</code>	Carriage return	Matches a carriage return 0x0d.
<code>\n</code>	Newline	Matches a new line 0x0a.
<code>\t</code>	Tab	Matches a tab 0x09.
<code>\f</code>	Formfeed	Matches a form feed 0x0c.
<code>\xNN</code>	Escaped hexadecimal number	Matches an ASCII character using hexadecimal (exactly two digits).
<code>\WNN</code>	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		
Routed	Transparent	Single	Multiple	
			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		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Configuring TCP Maps

For information about TCP maps, see the [“Enabling Connection Limits and TCP Normalization” section on page 27-7](#).

Configuring Global Pools

For information about global pools, see the [“Using Dynamic NAT” section on page 21-16](#).

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 Wizard, page 19-17](#)
- [Phone Proxy, page 19-24](#)
- [CTL File, page 19-28](#)
- [TLS Proxy, page 19-30](#)
- [CTL Provider, page 19-32](#)

TLS Proxy Wizard



Note

This feature is not supported for ASDM version 6.1.5 or the Adaptive Security Appliance version 8.1.2.

For information on how to configure the TLS Proxy, see the following sections:

- [Configure TLS Proxy Pane, page 19-19](#)
- [Adding a TLS Proxy Instance, page 19-20](#)
- [Add TLS Proxy Instance Wizard – Server Configuration, page 19-21](#)
- [Add TLS Proxy Instance Wizard – Client Configuration, page 19-22](#)
- [Add TLS Proxy Instance Wizard – Other Steps, page 19-24](#)

Use the TLS Proxy to enable inspection of SSL encrypted VoIP signaling, namely Skinny and SIP, interacting with Cisco Call Manager. Additionally, configure the TLS Proxy on the security appliance to use the following Cisco Unified Communications features:

Table 19-2 *TLS Proxy Applications and the Security Appliance*

Application	TLS Client	TLS Server	Client Authentication	Security Appliance Server Role	Security Appliance Client Role
Mobile Advantage	CUMC	CUMA	No	Using the CUMA private key or certificate impersonation	Any static configured certificate
Presence Federation	CUP or MS LCS/OCS	CUP or MS LCS/OCS	Yes	Proxy certificate, self-signed or by internal CA	Using the CUP private key or certificate impersonation
IP Telephone (including Phone Proxy)	IP phone	CUCM	Yes	Proxy certificate, self-signed or by internal CA	Local dynamic certificate signed by the security appliance CA (might not need certificate for Phone Proxy application)

For the Mobility feature, the TLS client is a CUMA client and the TLS server is a CUMA server. The security appliance is between a CUMA client and a CUMA server. The TLS Proxy for CUMA allows the use of an imported PKCS-12 certificate for server proxy during the handshake with the client. CUMA clients are not required to present a certificate (no client authentication) during the handshake. In previous releases, the security appliance required the client to always present a valid certificate and it acted as a private certificate authority (CA) for the clients.

For the Presence Federation feature, the security appliance acts as a TLS Proxy between the Cisco Unified Presence and the foreign server. This allows the security appliance to proxy TLS messages on behalf of the server that initiates the TLS connection, and route the proxied TLS messages to the client. The security appliance stores certificate trustpoints for the server and the client, and presents these certificates on establishment of the TLS session.

The security appliance supports TLS Proxy for various voice applications. For the Phone Proxy feature, the TLS Proxy running on the security appliance has the following key features:

- The TLS Proxy is implemented on the security appliance to intercept the TLS signaling from IP phones.
- The TLS Proxy decrypts the packets, sends packets to the inspection engine for NAT rewrite and protocol conformance, optionally encrypts packets, and sends them to CUCM or sends them in clear text if the IP phone is configured to be in nonsecure mode on the CUCM.
- The TLS Proxy is a transparent proxy that works based on establishing trusted relationship between the TLS client, the proxy (the security appliance), and the TLS Server.

Configure TLS Proxy Pane

**Note**

This feature is not supported for ASDM version 6.1.5 or the Adaptive Security Appliance version 8.1.2.

You can configure the TLS Proxy from the Configuration > Firewall > Advanced > Encrypted Traffic Inspection > TLS Proxy pane. For a detailed overview of the TLS Proxy, see [TLS Proxy Wizard, page 19-17](#).

Configuring a TLS Proxy lets you use the TLS Proxy to enable inspection of SSL encrypted VoIP signaling, namely Skinny and SIP, interacting with Cisco Call Manager and enable the security appliance for the Cisco Unified Communications features:

- TLS Proxy for the Cisco Unified Presence Server (CUPS), part of Presence Federation
- TLS Proxy for the Cisco Unified Mobility Advantage (CUMA) server, part of Mobile Advantage
- Phone Proxy

Fields

- TLS Proxy Name—Lists the TLS Proxy name.
- Server Proxy Certificate—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.
- Client Proxy Certificate—Lists the proxy certificate for the TLS client. The security appliance uses the client proxy certificate to authenticate the TLS client during the handshake between the proxy and the TLS client. The certificate can be either self-signed, enrolled with a certificate authority, or issued by the third party.
- Add—Adds a TLS Proxy by launching the Add TLS Proxy Instance Wizard. See [Adding a TLS Proxy Instance, page 19-20](#) for the steps to create a TLS Proxy instance.
- Edit—Edits a TLS Proxy. The fields in the Edit panel area identical to the fields displayed when you add a TLS Proxy instance. See [Add TLS Proxy Instance Wizard – Server Configuration, page 19-21](#) and [Add TLS Proxy Instance Wizard – Client Configuration, page 19-22](#).
- 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, the ASA supports 100 sessions.
 - Maximum number of sessions—The minimum is 1. The maximum is dependent on the platform. The default is 100.

**Note**

The maximum number of sessions is global to all TLS proxy sessions.

Modes

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

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

Adding a TLS Proxy Instance



Note

This feature is not supported for ASDM version 6.1.5 or the Adaptive Security Appliance version 8.1.2.

Use the Add TLS Proxy Instance Wizard to add a TLS Proxy to enable inspection of SSL encrypted VoIP signaling, namely Skinny and SIP, interacting with Cisco Call Manager and to support the Cisco Unified Communications features on the security appliance. For a detailed overview of the TLS Proxy used by these features, see [TLS Proxy Wizard, page 19-17](#).

This wizard is available from the Configuration > Firewall > Advanced > Encrypted Traffic Inspection > TLS Proxy pane.

Step 1 Open the Configuration > Firewall > Advanced > Encrypted Traffic Inspection > TLS Proxy pane.

Step 2 To add a new TLS Proxy Instance, click **Add**.

The Add TLS Proxy Instance Wizard opens.

Step 3 In the TLS Proxy Name field, type the TLS Proxy name.

Step 4 Click **Next**.

The Add TLS Proxy Instance Wizard – Server Configuration dialog box opens. In this step of the wizard, configure the server proxy parameters for original TLS Server—the Cisco Unified Call Manager (CUCM) server, the Cisco Unified Presence Server (CUPS), or the Cisco Unified Mobility Advantage (CUMA) server. See [Add TLS Proxy Instance Wizard – Server Configuration, page 19-21](#).

After configuring the server proxy parameters, the wizard guides you through configuring client proxy parameters (see [Add TLS Proxy Instance Wizard – Client Configuration, page 19-22](#)) and provides instructions on the steps to complete outside the ASDM to make the TLS Proxy fully functional (see [Add TLS Proxy Instance Wizard – Other Steps, page 19-24](#)).

Modes

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

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

Add TLS Proxy Instance Wizard – Server Configuration

**Note**

This feature is not supported for ASDM version 6.1.5 or the Adaptive Security Appliance version 8.1.2.

Use the Add TLS Proxy Instance Wizard to add a TLS Proxy to enable inspection of SSL encrypted VoIP signaling, namely Skinny and SIP, interacting with Cisco Call Manager and to support the Cisco Unified Communications features on the security appliance. For a detailed overview of the TLS Proxy used by these features, see [TLS Proxy Wizard, page 19-17](#).

The fields in the Edit TLS Proxy dialog box are identical to the fields displayed when you add a TLS Proxy instance. Use the Edit TLS Proxy – Server Configuration tab to edit the server proxy parameters for the original TLS Server—the Cisco Unified Call Manager (CUCM) server, the Cisco Unified Presence Server (CUPS), or the Cisco Unified Mobility Advantage (CUMA) server.

The Add TLS Proxy Instance Wizard is available from the Configuration > Firewall > Advanced > Encrypted Traffic Inspection > TLS Proxy pane.

Step 1 Complete the first step of the Add TLS Proxy Instance Wizard. See [Adding a TLS Proxy Instance, page 19-20](#).

The Add TLS Proxy Instance Wizard – Server Configuration dialog box opens.

Step 2 Specify the server proxy certificate by doing one of the following:

- To add a new certificate, click **Manage**. The Manage Identify Certificates dialog box opens. See [Add TLS Proxy Instance Wizard – Client Configuration, page 19-22](#).
- To select an existing certificate, select one from the drop-down list.

The server proxy certificate is used to specify the trustpoint to present during the TLS handshake. The trustpoint can be self-signed or enrolled locally with the certificate service on the proxy. For example, for the Phone Proxy, the server proxy certificate is used by the Phone Proxy during the handshake with the IP phones.

When you are configuring the TLS Proxy for the Phone Proxy, select the certificate that has a filename beginning with **_internal_PP_**. When you create the CTL file for the Phone Proxy, the security appliance, creates an internal trustpoint used by the Phone Proxy to sign the TFTP files. The trustpoint is named **_internal_PP_ctl-instance_filename**.

When the Phone Proxy is operating in a mixed-mode CUCM cluster, you must import the CUCM certificate by clicking **Add** in the Manage Identify Certificates dialog box. See [Add/Install an Identity Certificate, page 33-12](#).

Step 3 To install the TLS server certificate in the security appliance trust store, so that the security appliance can authenticate the TLS server during TLS handshake between the proxy and the TLS server, click **Install TLS Server's Certificate**.

The Manage CA Certificates dialog box opens. See [CA Certificate Authentication, page 33-1](#). Click **Add** to open the Install Certificate dialog box. See [Add/Install a CA Certificate, page 33-3](#).

When you are configuring the TLS Proxy for the Phone Proxy, click **Install TLS Server's Certificate** and install the Cisco Unified Call Manager (CUCM) certificate so that the proxy can authenticate the IP phones on behalf of the CUCM server.

Step 4 To require the security appliance to present a certificate and authenticate the TLS client during TLS handshake, check the Enable client authentication during TLS Proxy handshake check box.

When adding a TLS Proxy Instance for Mobile Advantage (the CUMC client and CUMA server), disable the check box when the client is incapable of sending a client certificate.

See [TLS Proxy Wizard, page 19-17](#) to determine which TLS clients used by the Cisco Unified Communication features are capable of client authentication.

Step 5 Click **Next**.

The Add TLS Proxy Instance Wizard – Client Configuration dialog box opens. In this step of the wizard, configure the client proxy parameters for original TLS Client—the CUMC client for Mobile Advantage, CUP or MS LCS/OCS client for Presence Federation, or the IP phone for the Phone Proxy. See [Add TLS Proxy Instance Wizard – Client Configuration, page 19-22](#).

After configuring the client proxy parameters, the wizard provides instructions on the steps to complete outside the ASDM to make the TLS Proxy fully functional (see [Add TLS Proxy Instance Wizard – Other Steps, page 19-24](#)).

Add TLS Proxy Instance Wizard – Client Configuration



Note

This feature is not supported for ASDM version 6.1.5 or the Adaptive Security Appliance version 8.1.2.

Use the Add TLS Proxy Instance Wizard to add a TLS Proxy to enable inspection of SSL encrypted VoIP signaling, namely Skinny and SIP, interacting with Cisco Call Manager and to support the Cisco Unified Communications features on the security appliance. For a detailed overview of the TLS Proxy used by these features, see [TLS Proxy Wizard, page 19-17](#).

The fields in the Edit TLS Proxy dialog box are identical to the fields displayed when you add a TLS Proxy instance. Use the Edit TLS Proxy – Client Configuration tab to edit the client proxy parameters for the original TLS Client, such as IP phones, CUMA clients, the Cisco Unified Presence Server (CUPS), or the Microsoft OCS server.

This wizard is available from the Configuration > Firewall > Advanced > Encrypted Traffic Inspection > TLS Proxy pane.

Step 1 Complete the first two steps of the Add TLS Proxy Instance Wizard. See [Adding a TLS Proxy Instance, page 19-20](#) and [Add TLS Proxy Instance Wizard – Client Configuration, page 19-22](#).

The Add TLS Proxy Instance Wizard – Client Configuration dialog box opens.

Step 2 To specify a client proxy certificate to use for the TLS Proxy, perform the following. Select this option when the client proxy certificate is being used between two servers; for example, when configuring the TLS Proxy for Presence Federation, which uses the Cisco Unified Presence Server (CUPS), both the TLS client and TLS server are both servers.

- a. Check the Specify the proxy certificate for the TLS Client... check box.
- b. Select a certificate from the drop-down list.

Or

To create a new client proxy certificate, click **Manage**. The Manage Identify Certificates dialog box opens. See [Identity Certificates Authentication, page 33-11](#).



Note

When you are configuring the TLS Proxy for the Phone Proxy and it is using the mixed security mode for the CUCM cluster, you must configure the LDC Issuer. The LDC Issuer lists the local certificate authority to issue client or server dynamic certificates.

- Step 3** To specify an LDC Issuer to use for the TLS Proxy, perform the following. When you select and configure the LDC Issuer option, the security appliance acts as the certificate authority and issues certificates to TLS clients.
- a. Click the Specify the internal Certificate Authority to sign the local dynamic certificate for phones... check box.
 - b. Click the Certificates radio button and select a self-signed certificate from the drop-down list or click **Manage** to create a new LDC Issuer. The Manage Identify Certificates dialog box opens. See [Identity Certificates Authentication, page 33-11](#).

Or

Click the Certificate Authority radio button to specify a Certificate Authority (CA) server. When you specify a CA server, it needs to be created and enabled in the security appliance. To create and enable the CA server, click **Manage**. The Edit CA Server Settings dialog box opens. See [Local Certificate Authority, page 33-20](#).



Note To make configuration changes after the local certificate authority has been configured for the first time, disable the local certificate authority.

- c. In the Key-Pair Name field, select a key pair from the drop-list. The list contains the already defined RSA key pair used by client dynamic certificates. To see the key pair details, including generation time, usage, modulus size, and key data, click **Show**.

Or

To create a new key pair, click **New**. The Add Key Pair dialog box opens. See [Add/Install an Identity Certificate, page 33-12](#) for details about the Key Pair fields.

- Step 4** In the Security Algorithms area, specify 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 Call Manager may be NULL cipher to offload the Call Manager.

Move Up—Moves an algorithm up in the list.

Move Down—Moves an algorithm down in the list.

- Step 5** Click **Next**.

The Add TLS Proxy Instance Wizard – Other Steps dialog box opens. The Other Steps dialog box provides instructions on the steps to complete outside the ASDM to make the TLS Proxy fully functional (see [Add TLS Proxy Instance Wizard – Other Steps, page 19-24](#)).

Add TLS Proxy Instance Wizard – Other Steps



Note

This feature is not supported for ASDM version 6.1.5 or the Adaptive Security Appliance version 8.1.2.

The last dialog box of the Add TLS Proxy Instance Wizard specifies the additional steps required to make TLS Proxy fully functional. In particular, you need to perform the following tasks to complete the TLS Proxy configuration:

- Export the local CA certificate or LDC Issuer and install them on the original TLS server.
 - To export the LDC Issuer, go to Configuration > Firewall > Advanced > Certificate Management > Identity Certificates > Export. See [Export an Identity Certificate, page 33-15](#).
- For the TLS Proxy, enable Skinny and SIP inspection between the TLS server and TLS clients. See [SIP Inspection, page 24-21](#) and [Skinny \(SCCP\) Inspection, page 24-22](#). When you are configuring the TLS Proxy for Presence Federation (which uses CUP), you only enable SIP inspection because the feature supports only the SIP protocol.
- For the TLS Proxy for CUMA, enable MMP inspection. See [MMP Inspection, page 24-17](#).
- When using the internal Certificate Authority of the security appliance to sign the LDC Issuer for TLS clients, perform the following:

- Use the Cisco CTL Client to add the server proxy certificate to the CTL file and install the CTL file on the security appliance.

For information on the Cisco CTL Client, see “Configuring the Cisco CTL Client” in *Cisco Unified CallManager Security Guide*.

http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/security/5_0_4/secuauth.html

To install the CTL file on the security appliance, go to Configuration > Firewall > Advanced > Encrypted Traffic Inspection > CTL Provider > Add. The Add CTL Provider dialog box opens. For information on using this dialog box to install the CTL file, see [Add/Edit CTL Provider, page 19-33](#).

- Create a CTL provider instance for connections from the CTL clients. See [Add/Edit CTL Provider, page 19-33](#).

Phone Proxy



Note

This feature is not supported for ASDM version 6.1.5 or the Adaptive Security Appliance version 8.1.2.

For information on how to configure the Phone Proxy, see the following sections:

- [Configuring the Phone Proxy, page 19-25](#)
- [Add/Edit TFTP Server, page 19-27](#)

Use the Phone Proxy to configure a Phone Proxy between a Call Manager and IP phones. If the Phone Proxy is configured, the security appliance encrypts signaling connections from IP phones in the untrusted networks and sends them in the clear to the CUCM on a trusted network.

Configuring the Phone Proxy

**Note**

This feature is not supported for ASDM version 6.1.5 or the Adaptive Security Appliance version 8.1.2.

Configuring the Phone Proxy requires the following steps:

Step 1: Create the CTL file. See [Creating a CTL File, page 19-28](#).

Step 2: Create the TLS Proxy instance to handle the encrypted signaling. See [Adding a TLS Proxy Instance, page 19-20](#).

Step 3: Create the Phone Proxy instance. See [Creating a Phone Proxy Instance, page 19-25](#).

Step 4: Enable the Phone Proxy with SIP and Skinny inspection. See [SIP Inspection, page 24-21](#) and [Skinny \(SCCP\) Inspection, page 24-22](#).

Creating a Phone Proxy Instance

**Note**

This feature is not supported for ASDM version 6.1.5 or the Adaptive Security Appliance version 8.1.2.

Use the Configure Phone Proxy pane to add a Phone Proxy. For a detailed overview of the Phone Proxy used by the security appliance, see [Phone Proxy, page 19-24](#).

This pane is available from the Configuration > Firewall > Advanced > Encrypted Traffic Inspection > Phone Proxy pane.

Step 1 Open the Configuration > Firewall > Advanced > Encrypted Traffic Inspection > Phone Proxy pane.

Step 2 Check the Enable Phone Proxy check box to enable the feature.

Step 3 In the Media Termination Address field, type the IP address to use for media connections to the Phone Proxy.

Specify the virtual IP address that will be created for the Phone Proxy to use during media termination. Only one virtual interface can be configured per Phone Proxy instance. The Phone Proxy inserts the media termination IP address into the media address portion of the signaling messages.

The security appliance must have an IP address for media termination that meets the following criteria:

- The IP address is a publicly routable address that is an unused IP address on an attached network to the security appliance interface that will never be used by another device in your network.
- The IP address cannot be the same as the security appliance interface IP address. Specifically, it cannot be the same as the least secure interface on the security appliance.
- The IP address cannot overlap with existing static NAT rules.
- The IP address cannot be the same as the CUCM or TFTP server IP address.
- Add routes to the other interfaces so that IP phones on other interfaces can reach the media termination address.

Step 4 Specify the TLS Proxy by doing one of the following:

- To add a new TLS Proxy Instance, click **Manage**. The Configure TLS Proxy dialog box opens. See [Configure TLS Proxy Pane, page 19-19](#).
- To select an existing TLS Proxy, select one from the drop-down list.

- Step 5** In the TFTP Server Settings list, do one of the following:
- To add a new TFTP server for the Phone Proxy, click **Add**. The Add TFTP Server dialog box opens. See [Add/Edit TFTP Server, page 19-27](#).
 - To select an existing TFTP server, select one from the drop-down list.



Note The TFTP server must reside on the same interface as the Cisco Unified Call Manager. Additionally, If NAT is configured for the TFTP server, the NAT configuration must be configured prior to configuring the specifying the TFTP server while creating the Phone Proxy instance.

- Step 6** Specify the CTL File to use for the Phone Proxy by doing one of the following:
- To use an existing CTL File, check the Use the Certificate Trust List File generated by the CTL instance check box.
 - To create a new CTL file for the Phone Proxy, click the link Generate Certificate Trust List File. The Create a Certificate Trust List (CTL) File pane opens. See [Creating a CTL File, page 19-28](#).
- Step 7** To specify the security mode of the CUCM cluster, click one of the following options in the CUCM Cluster Mode field:
- Non-secure—Specifies the cluster mode to be in nonsecure mode when configuring the Phone Proxy feature.
 - Mixed—Specifies the cluster mode to be in mixed mode when configuring the Phone Proxy feature.
- Step 8** To configure the idle timeout after which the secure-phone entry is removed from the Phone Proxy database (the default is 5 minutes), enter a value in the format *hh:mm:ss*.
- Since secure phones always request a CTL file upon bootup, the Phone Proxy creates a database that marks the phone as secure. The entries in the secure phone database are removed after a specified configured timeout. The entry timestamp is updated for each registration refresh the Phone Proxy receives for SIP phones and KeepAlives for SCCP phones.
- Specify a value that is greater than the maximum timeout value for SCCP KeepAlives and SIP Register refresh. For example, if the SCCP KeepAlives are configured for 1 minute intervals and the SIP Register Refresh is configured for 3 minutes, configure this timeout value greater than 3 minutes.
- Step 9** To preserve Call Manager configuration on the IP phones, check the Preserve the Call Manager's configuration on the phone... When this option is unchecked, the following service settings are disabled on the IP phones:
- PC Port
 - Gratuitous ARP
 - Voice VLAN access
 - Web Access
 - Span to PC Port
- Step 10** To configure an HTTP proxy for the Phone Proxy feature that is written into the IP phone's configuration file under the <proxyServerURL> tag, do the following:
- Check the Configure a http-proxy which would be written into the phone's config file... check box.
 - In the IP Address field, type the IP address of the HTTP proxy and the listening port of the HTTP proxy.

The IP address you enter should be the global IP address based on where the IP phone and HTTP proxy server is located. You can enter a hostname in the IP Address field when that hostname can be resolved to an IP address by the security appliance (for example, DNS lookup is configured) because the security appliance will resolve the hostname to an IP address. If a port is not specified, the default will be 8080.

- c. In the Interface field, select the interface on which the HTTP proxy resides on the security appliance.

Setting the proxy server configuration option for the Phone Proxy allows for an HTTP proxy on the DMZ or external network in which all the IP phone URLs are directed to the proxy server for services on the phones. This setting accommodates nonsecure HTTP traffic, which is not allowed back into the corporate network.

- Step 11** To force Cisco IP Communicator (CIPC) softphones to operate in authenticated mode when CIPC softphones are deployed in a voice and data VLAN scenario, check the Enable CIPC security mode authentication check box.

Because CIPC requires an LSC to perform the TLS handshake, CIPC needs to register with the CUCM in nonsecure mode using cleartext signaling. To allow the CIPC to register, create an ACL that allows the CIPC to connect to the CUCM on the nonsecure SIP/SCCP signaling ports (5060/2000).

CIPC uses a different cipher when doing the TLS handshake and requires the null-sha1 cipher and SSL encryption be configured. To add the null-sha1 cipher, go to Configuration > Device Management > Advanced > SSL Settings > Encryption section. Select the null-sha1 SSL encryption type and add it to the Available Algorithms.

Current versions of Cisco IP Communicator (CIPC) support authenticated mode and perform TLS signaling but not voice encryption.

- Step 12** Click **Apply** to save the Phone Proxy configuration settings.

Add/Edit TFTP Server



Note

This feature is not supported for ASDM version 6.1.5 or the Adaptive Security Appliance version 8.1.2.

Use the Add/Edit TFTP Server dialog box to specify the IP address of the TFTP server and the interface on which the TFTP server resides.

The Phone Proxy must have at least one CUCM TFTP server configured. Up to five TFTP servers can be configured for the Phone Proxy.

The TFTP server is assumed to be behind the firewall on the trusted network; therefore, the Phone Proxy intercepts the requests between the IP phones and TFTP server.



Note

If NAT is configured for the TFTP server, the NAT configuration must be configured prior to specifying the TFTP server while creating the Phone Proxy instance.

Fields

TFTP Server IP Address—Specifies the address of the TFTP server. Create the TFTP server using the actual internal IP address.

Port—(Optional) Specifies the port the TFTP server is listening in on for the TFTP requests. This should be configured if it is not the default TFTP port 69.

Interface—Specifies the interface on which the TFTP server resides. The TFTP server must reside on the same interface as the Cisco Unified Call Manager (CUCM).

Modes

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

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

CTL File



Note

This feature is not supported for ASDM version 6.1.5 or the Adaptive Security Appliance version 8.1.2.

For information on how to configure CTL files, see the following sections:

- [Creating a CTL File, page 19-28](#)
- [Add/Edit Record Entry, page 19-29](#)
- [CTL Provider, page 19-32](#)

Create a Certificate Trust List (CTL) file that is required by the Phone Proxy. Specify the certificates needed by creating a new CTL file or by specifying the path of an existing CTL file to parse from Flash memory.

Create trustpoints and generate certificates for each entity in the network (CUCM, CUCM and TFTP, TFTP server, CAPF) that the IP phones must trust. The certificates are used in creating the CTL file. You need to create trustpoints for each CUCM (primary and secondary if a secondary CUCM is used) and TFTP server in the network. The trustpoints need to be in the CTL file for the phones to trust the CUCM.

Create the CTL File that will be presented to the IP phones during the TFTP. The address must be the translated or global address of the TFTP server or CUCM if NAT is configured.

When the file is created, it creates an internal trustpoint used by the Phone Proxy to sign the TFTP files. The trustpoint is named `_internal_PP_ctl-instance_filename`.

Creating a CTL File



Note

This feature is not supported for ASDM version 6.1.5 or the Adaptive Security Appliance version 8.1.2.

Use the Create a Certificate Trust List (CTL) File pane to create a CTL file for the Phone Proxy. This pane creates the CTL file that is presented to the IP phones during the TFTP handshake with the security appliance. For a detailed overview of the CTL file used by the Phone Proxy, see [CTL File, page 19-28](#).

The Create a Certificate Trust List (CTL) File pane is used to configure the attributes for generating the CTL file. The name of the CTL file instance is generated by the ASDM. When the user tries to edit the CTL file instance configuration, the ASDM automatically generates the **shutdown** CLI command first and the **no shutdown** CLI command as the last command.

This pane is available from the Configuration > Firewall > Advanced > Encrypted Traffic Inspection > CTL File pane.

-
- Step 1** Open the Configuration > Firewall > Advanced > Encrypted Traffic Inspection > CTL File pane.
- Step 2** Check the Enable Certificate Trust List File check box to enable the feature.
- Step 3** To specify the CTL file to use for the Phone Proxy, perform one of the following:
- If there is an existing CTL file available, download the CTL file to Flash memory by using the File Management Tool in the ASDM Tools menu. Select the Use certificates present in the CTL stored in flash radio button and specify the CTL file name and path in the text box.

Use an existing CTL file to install the trustpoints for each entity in the network (CUCM, CUCM and TFTP, TFTP server, CAPF) that the IP phones must trust. If you have an existing CTL file that contains the correct IP addresses of the entities (namely, the IP address that the IP phones use for the CUCM or TFTP servers), you can use it to create a new CTL file. Store a copy of the existing CTL file to Flash memory and rename it something other than `CTLFile.tlv`
 - If there is no existing CTL file available, select Create new CTL file radio button.

Add Record entries for each entity in the network such as CUCM, TFTP, and CUCM-TFTP option by clicking **Add**. The Add Record Entry dialog box opens. See [Add/Edit Record Entry, page 19-29](#).
- Step 4** Specify the number SAST certificate tokens required. The default is 2. maximum allowed is 5.
- Because the Phone Proxy generates the CTL file, it needs to create the System Administrator Security Token (SAST) key to sign the CTL file itself. This key can be generated on the security appliance. A SAST is created as a self-signed certificate. Typically, a CTL file contains more than one SAST. In case a SAST is not recoverable, the other one can be used to sign the file later.
- Step 5** Click **Apply** to save the CTL file configuration settings.
-

Add/Edit Record Entry



Note

This feature is not supported for ASDM version 6.1.5 or the Adaptive Security Appliance version 8.1.2.

Use the Add/Edit Record Entry dialog box to specify the trustpoints to be used for the creation of the CTL file.

Add additional record-entry configurations for each entity that is required in the CTL file.

Fields

Type—Specifies the type of trustpoint to create:

- `cucm`: Specifies the role of this trustpoint to be CCM. Multiple CCM trustpoints can be configured.
- `cucm-tftp`: Specifies the role of this trustpoint to be CCM+TFTP. Multiple CCM+TFTP trustpoints can be configured.
- `tftp`: Specifies the role of this trustpoint to be TFTP. Multiple TFTP trustpoints can be configured.

- **capf**: Specifies the role of this trustpoint to be CAPF. Only one CAPF trustpoint can be configured.

Address—Specifies the IP address of the trustpoint. The IP address you specify must be the global address of the TFTP server or CUCM if NAT is configured. The global IP address is the IP address as seen by the IP phones because it will be the IP address used for the CTL record for the trustpoint.

Certificate—Specifies the Identity Certificate for the record entry in the CTL file. You can create a new Identity Certificate by clicking **Manage**. The Manage Identify Certificates dialog box opens. See [Identity Certificates Authentication, page 33-11](#).

You can add an Identity Certificate by generating a self-signed certificate, obtaining the certificate through SCEP enrollment, or by importing a certificate in PKCS-12 format. Choose the best option based on the requirements for configuring the CTL file.

Domain Name—(Optional) Specifies the domain name of the trustpoint used to create the DNS field for the trustpoint. This is appended to the Common Name field of the Subject DN to create the DNS Name. The domain name should be configured when the FQDN is not configured for the trustpoint. Only one domain-name can be specified.



Note

If you are using domain names for your CUCM and TFTP server, you must configure DNS lookup on the security appliance. Add an entry for each of the outside interfaces on the security appliance into your DNS server, if such entries are not already present. Each security appliance outside IP address should have a DNS entry associated with it for lookups. These DNS entries must also be enabled for Reverse Lookup. Additionally, define your DNS server IP address on the security appliance; for example: `dns name-server 10.2.3.4` (IP address of your DNS server).

Modes

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

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

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. See [Identity Certificates Authentication, page 33-11](#)
- 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 Call Manager 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		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—