CHAPTER 4

Configuring Virtual Contexts

Cisco Application Control Engine Appliance Device Manager (ACE Appliance Device Manager) provides a number of options for creating, configuring, and managing ACE appliances.

Note When you use the ACE CLI to configure named objects (such as a real server, virtual server, parameter map, class map, health probe, and so on), consider that the Device Manager (DM) supports object names with an alphanumeric string of 1 to 64 characters, which can include the following special characters: underscore (_), hyphen (-), dot (.), and asterisk (*). Spaces are not allowed.

If you use the ACE CLI to configure a named object with special characters that the DM does not support, you may not be able to configure the ACE using DM.

For information about these options, see:

Using Virtual Contexts

Virtual contexts use the concept of virtualization to partition your ACE appliance into multiple virtual devices or contexts. Each context contains its own set of policies, interfaces, resources, and administrators. This feature enables you to more closely and efficiently manage resources, users, and the services you provide to your customers.

The first time you configure a virtual context, you will see only the Admin context. In addition to the configurable attributes of other virtual contexts, the Admin context can configure:

- ACE appliance licenses
- Resource classes
- Port channel, management, and gigabit Ethernet interfaces
- High Availability (HA or fault tolerance between ACE appliances)
- Application acceleration and optimization on the ACE appliance

Related Topics

- Creating Virtual Contexts, page 4-2
- Configuring Virtual Contexts, page 4-7
- Deleting Virtual Contexts, page 4-80

Creating Virtual Contexts

Use this procedure to create virtual contexts.

Note If you do not configure a management VLAN for SNMP access, the ACE Appliance Device Manager will not be able to poll the context.

Note If an ACE appliance is configured as a hot standby in a high availability pair, its configuration cannot be modified and you cannot add or modify virtual contexts. ACE appliances configured as hot standby members display *Standby Hot* in the HA State column in the All Virtual Contexts table (**Config > Virtual Contexts**). For more information, see High Availability Polling, page 11-2.

Procedure

Step 1 Choose **Config > Virtual Contexts**.

The All Virtual Contexts table appears.

Step 2 Click **Add**.

The New Virtual Context screen appears.

Step 3 Configure the virtual context using the information in Table 4-1.

Tip Fields with 2 or 3 choices use radio buttons. Fields with more than 3 choices use dropdown lists.

Table 4-1 Virtual Context Configuration Attributes

Field	Description
Basic Settings	
Name	Enter a unique name for the virtual context. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters. This field is read-only for existing contexts.
Description	Enter a brief description of the virtual context. Enter a description as an unquoted text string with a maximum of 240 alphanumeric characters.
Resource Class	Choose the resource class this virtual context is to use. Click **View** to display the information for the selected resource class.
Allocate VLANs	Enter the number of a VLAN or a range of VLANs so that the context can receive the associated traffic. You can specify VLANs in any of the following ways: • For a single VLAN, enter an integer from 2 to 4096. • For multiple, non-sequential VLANs, use comma-separated entries, such as `101, 201, 302`. • For a range of VLANs, use the format <*beginning-VLAN*>-<*ending-VLAN*>, such as `101-150`. **Note** VLANs cannot be modified in an Admin context.
Default Gateway for IPv4	Enter the IPv4 address of the default gateway. You can enter a maximum of eight addresses. Use a comma-separated list to specify multiple IP addresses, for example, such as 192.168.65.1, 192.168.64.2. Default static routes with a netmask and IP address of 0.0.0.0 previously configured on the ACE appear in this field.
Default Gateway for IPv6	Enter the IPv6 address of the default gateway or select the forward VLAN interface or BVI, as follows: • IPv6 Address field—Enter the address of the gateway router (the next-hop address for this route). Then, use the right arrow to move it to the Selected field. You can enter a maximum of eight addresses including a selected VLAN or BVI through the Outgoing Interfaces setting. Default static routes with a prefix and IP address of ::0 previously configured on the ACE appear in the Selected field. • Outgoing Interfaces—Select either VLAN or BVI used for the link-local address only. And then select the Interface Number for the VLAN or BVI.
Management Settings	
VLAN Id	Enter the VLAN number that you want to assign to the management interface. Valid values are from 2 to 4094. By default, all devices are assigned to VLAN1, known as the default VLAN. The ACE Device Manager identifies the management class maps and policy maps associated with the selected VLAN ID assigned to the management interface. This field is read-only if configured for existing contexts.
VLAN Description	Enter a description for the management interface. Enter an unquoted text string that contains a maximum of 240 alphanumeric characters including spaces.

Table 4-1 Virtual Context Configuration Attributes (continued)

Field	Description
Interface Mode	Choose the topology that reflects the relationship of the selected ACE virtual context to the real servers in the network: • **Routed**—The ACE virtual context acts as a router between the client-side network and the server-side network. In this topology, every real server for the application must be routed through the ACE virtual context, either by setting the default gateway on each real server to the virtual context server-side VLAN interface address, or by using a separate router with appropriate routes configured between the ACE virtual context and the real servers. • **Bridged**—The virtual ACE bridges two VLANs—a client-side VLAN and a real-server VLAN—on the same subnet using a bridged virtual interface (BVI). In this case, the real server routing does not change to accommodate the ACE virtual context. Instead, the virtual ACE transparently handles traffic to and from the real servers. This field is read-only if configured for existing contexts.
Management IP	Enter the IPv4 address that is to be used for remote management of the context. This address must be a unique management IP address that is not used in another context. The DM does not support duplicate management IP addresses in different contexts. **Note** The Device Manager considers an interface as a management interface if it has a management policy map associated with the VLAN interface. See the "Configuring Virtual Context VLAN Interfaces" section on page 10-10.
Management Netmask	Choose the subnet mask to apply to this IP address.
Alias IP Address	Enter the IPv4 address of the alias associated with this interface.
Peer IP Address	Enter the IPv4 address of the remote peer.
Access Permission	Choose the source IP addresses that are allowed on the management interface as follows: • **Allow All**—Allows all configured client source IP addresses on the management interface as the network traffic matching criteria. • **Deny All**—Denies all configured client source IP addresses on the management interface as the network traffic matching criteria. • **Match**—Displays the Match Conditions table, where you specify the match criteria that the ACE is to use for traffic on the management interface.

Table 4-1 Virtual Context Configuration Attributes (continued)

Field	Description
Match Conditions	When you enter the VLAN ID for the management interface, the Match Conditions table appears. To add or modify the protocols allowed on this management VLAN, do the following: 1. Click **Add** to choose a protocol for the management interface, or choose an existing protocol entry listed in the Match Conditions table and click **Edit** to modify it. 2. In the Protocol drop-down list, choose a protocol: – **HTTP**—Specifies the Hypertext Transfer Protocol (HTTP). – **HTTPS**—Specifies the Hypertext Transfer Protocol Secure (HTTPS) for connectivity with the interface using port 443. – **ICMP**—Specifies the Internet Control Message Protocol (ICMP) for Internet Protocol version 4 (IPv4). – **ICMPv6**—Specifies the Internet Control Message Protocol version 6 (ICMPv6) for Internet Protocol version 6 (IPv6). – **KALAP-UDP**—Specifies the Keepalive Appliance Protocol over UDP. – **SNMP**—Specifies the Simple Network Management Protocol (SNMP). **Note** If SNMP is not selected, the ACE Appliance Device Manager cannot poll the context. – **SSH**—Specifies a Secure Shell (SSH) connection to the ACE. – **TELNET**—Specifies a Telnet connection to the ACE. – **XML-HTTPS**—Specifies HTTPS as the transfer protocol for sending and receiving XML documents between the ACE appliance and a Network Management System (NMS) using port 10443. This option is available for ACE appliances only. 3. In the Allowed From field, specify the matching criteria for the client source IP address: – **Any**—Specifies any client source address for the management traffic classification. – **Source Address**—Specifies a client source host IP address as the network traffic matching criteria. An ICMPv6 source address only accept an IPv6 address. – **Source Netmask**—Select a subnet mask. This field is not applicable for ICMPv6. – **Source Prefix Length**—(ICMPv6 only) Enter the prefix length, a value from 1 to 128. 4. Click **OK** to accept the protocol selection or click **Cancel** to exit without accepting your entries. **Note** To remove a protocol from the management VLAN, choose the entry in the Match Conditions table, and click **Delete**.
Enable SNMP Get	Check this check box to add an SNMP Get community string to enable SNMP polling on this context. This field is read-only if configured for existing contexts.

Table 4-1 Virtual Context Configuration Attributes (continued)

Field	Description
SNMP v2c Read-Only Community String	When you check the Enable SNMP Get check box, this field appears. Enter the SNMPv2c read-only community string to be used as the SNMP Get community string. This field is read-only if configured for existing contexts. **Note** If SNMP is not an allowed protocol, the ACE Appliance Device Manager will not be able to poll the context.
Add Admin User	When initially configuring the context, check this check box to configure this context for an Admin user. When the fields appear, enter the user name and password, and confirm the password.
More Settings	
Switch Mode	Check this check box to change the way that the ACE processes TCP connections that are not destined to a VIP or that do not have any policies associated with their traffic. For such traffic, the ACE still creates connection objects but processes the connections as stateless connections, which means that they do not undergo any TCP normalization checks. With this option enabled, the ACE also creates stateless connections for non-SYN TCP packets if they satisfy all other configured requirements. This process ensures that a long-lived persistent connection passes through the ACE successfully (even if it times out) by being reestablished by any incoming packet related to the connection. By default, these stateless connections time out after 2 hours and 15 minutes unless you configure the inactivity timeout otherwise in a parameter map. When a stateless connection times out, the ACE does not send a TCP RST packet but silently closes the connection. Even though these connections are stateless, the TCP RST and FIN-ACK flags are honored and the connections are closed when the ACE sees these flags in the received packets.
Shared VLAN Host Id	Specific bank of MAC addresses that the ACE uses. Enter a number from 1 to 16. Be sure to configure different bank numbers for multiple ACEs. This field is available only in the Admin context.
Regex Compilation Timeout (minutes)	Enter the timeout for regex compilation in minutes. When you configure a regex and its compilation is longer than the configured timeout, the ACE stops the regex compilation. A valid entry is an integer from 1 to 500. The default timeout is 60. This field is available only in the Admin context.

Step 4 Do one of the following

- Click **Deploy Now** to deploy this virtual context. To configure other virtual context attributes, see Configuring Virtual Contexts, page 4-7.
- Click **Cancel** to exit this procedure without saving your entries and to return to the All Virtual Contexts table.

Related Topics

- Using Virtual Contexts, page 4-2
- Configuring Virtual Contexts, page 4-7

Configuring Virtual Contexts

After creating a virtual context, you can configure it. Configuring a virtual context involves configuring a number of attributes, grouped into *configuration subsets*. Table 4-2 describes ACE Appliance Device Manager configuration subsets and provides links to related topics.

Note If an ACE appliance is configured as a hot standby in a high availability pair, its configuration cannot be modified and you cannot add or modify virtual contexts. ACE appliances configured as hot standby members display *Standby Hot* in the HA State column in the All Virtual Contexts table (**Config > Virtual Contexts**). For more information, see High Availability Polling, page 11-2.

Note To add objects such as real servers or server farms to a customized domain, use the CLI and then use the synchronize feature in ACE Appliance Device Manager to add this object into its customized domain on ACE Appliance Device Manager. Adding objects to customized domains directly in ACE Appliance Device Manager results in the object being added to the default domain.

Synchronization options are available in the All Virtual Contexts table (**Config > Virtual Contexts**).

Tip Fields with 2 or 3 choices use radio buttons. Fields with more than 3 choices use dropdown lists.

Table 4-2 ACE Appliance and Virtual Context Configuration Options

Configuration Subset	Description	Related Topics
System	System configuration options allow you to configure: • Primary attributes such as VLANs, SNMP access, and resource class. • Syslog attributes including the type and severity of syslog messages that are to be logged, the syslog log host, log messages, and log rate limits. • SNMP attributes. • Global policy map configuration for all VLANs on a virtual context. • ACE license use on the ACE appliance. • Resource classes for allocation of ACE appliance resources. • Application acceleration and optimization on the ACE appliance. • Checkpoint (snapshot in time) of a known stable running configuration • Back up or restore the configuration and dependencies of an entire ACE or of a particular virtual context **Note** ACE appliance licenses, resource classes, and acceleration and optimization can be configured only in an Admin context.	• Configuring Virtual Context Primary Attributes, page 4-11 • Configuring Virtual Context Syslog Logging, page 4-12 • Configuring SNMP for Virtual Contexts, page 4-19 • Configuring Virtual Context Global Traffic Policies, page 4-26 • Managing ACE Appliance Licenses, page 4-27 • Managing Resource Classes, page 4-34 • Configuring Global Application Acceleration and Optimization, page 13-9 • Using the Configuration Checkpoint and Rollback Service, page 4-41 • Performing Device Backup and Restore Functions, page 4-45

Table 4-2 ACE Appliance and Virtual Context Configuration Options (continued)

Configuration Subset	Description	Related Topics
Load Balancing	Load-balancing attributes allow you to • Configure virtual servers, real servers, and server farms for load balancing • Establish the predictor method and return code checking • Implement sticky groups for session persistence • Configure parameter maps to combine related actions for policy maps Load-balancing configuration options include: • Virtual servers • Real servers • Server farms • Health monitoring • Sticky attributes • Parameter maps • Secure KAL-AP • Dynamic Workload Scaling (admin context only)	• Load Balancing Overview, page 5-1 • Configuring Virtual Servers, page 5-2 • Configuring Server Farms, page 6-18 • Configuring Health Monitoring for Real Servers, page 6-40 • Configuring Sticky Groups, page 7-11 • Configuring Parameter Maps, page 8-1 • Configuring Secure KAL-AP, page 6-68 • Configuring Dynamic Workload Scaling, page 6-14
SSL	SSL configuration options allow you to: • Import and export SSL certificates and keys • Set up SSL parameter maps and chain group parameters • Generate certificate signing requests for submission to a certificate authority • Authenticate peer certificates • Configure certificate revocation lists for use during client authentication • Configure an Online Certificate Status Protocol (OCSP) service to define the host server for certificate revocation checks using OCSP.	• Configuring SSL, page 9-1 • Using SSL Certificates, page 9-6 • Using SSL Keys, page 9-11 • Generating CSRs, page 9-26 • Configuring SSL Parameter Maps, page 9-19 • Configuring SSL Chain Group Parameters, page 9-24 • Configuring SSL Proxy Service, page 9-27 • Configuring SSL Authentication Groups, page 9-31 • Configuring SSL OCSP Service, page 9-29 • Configuring CRLs for Client Authentication, page 9-32
Security	Security configuration options allow you to create access control lists, set ACL attributes, resequence ACLs, delete ACLs, and configure object groups.	• Configuring Virtual Context Expert Options, page 4-75 • Creating ACLs, page 4-54 • Configuring Object Groups, page 4-66

Table 4-2 ACE Appliance and Virtual Context Configuration Options (continued)

Configuration Subset	Description	Related Topics
Network	Network configuration options allow you to configure: • Port channel interfaces • Gigabit Ethernet interfaces • VLAN interfaces • BVI interfaces • Network Address Translation (NAT) pools for a VLAN interface • Static routes • DHCP relay agents **Note** You can configure port channel and gigabit Ethernet interfaces only in an Admin context.	• Configuring Virtual Context BVI Interfaces, page 10-23 • Configuring Gigabit Ethernet Interfaces, page 10-5 • Configuring Virtual Context VLAN Interfaces, page 10-10 • Configuring Virtual Context BVI Interfaces, page 10-23 • Configuring VLAN Interface NAT Pools, page 10-31 • Configuring Virtual Context Static Routes, page 10-33 • Configuring Global IP DHCP, page 10-34
High Availability	High Availability (HA) attributes allow you to configure two ACE appliances for fault-tolerant redundancy. **Note** You can set up high availability only in an Admin virtual context.	• Configuring High Availability, page 11-1 • Configuring High Availability Peers, page 11-8 • Configuring ACE High Availability Groups, page 11-11
HA Tracking And Failure Detection	HA Tracking And Failure Detection attributes allow you to configure tracking processes that can help ensure reliable fault tolerance.	• High Availability Tracking and Failure Detection Overview, page 11-17 • Tracking VLAN Interfaces for High Availability, page 11-19 • Tracking Hosts for High Availability, page 11-20
Expert	Expert options allow you to: • Configure traffic policies for filtering and handling traffic received by or passing through the ACE appliance. • Configure optimization action lists. • Configure HTTP header modify action lists.	• Configuring Traffic Policies, page 12-1 • Configuring an HTTP Optimization Action List, page 13-3 • Configuring an HTTP Header Modify Action List, page 12-89

Configuring Virtual Context System Attributes

Table 4-3 identifies the ACE Appliance Device Manager virtual context System configuration options and related topics for more information.

Table 4-3 Virtual Context System Configuration Options

System Configuration Options	Related Topics
Specify virtual context primary attributes	Configuring Virtual Context Primary Attributes, page 4-11
Configure syslog options	• Configuring Virtual Context Syslog Logging, page 4-12 • Configuring Syslog Log Hosts, page 4-16 • Configuring Syslog Log Messages, page 4-17 • Configuring Syslog Log Rate Limits, page 4-18
Configure SNMP attributes	• Configuring SNMP for Virtual Contexts, page 4-19 • Configuring SNMP Version 2c Communities, page 4-20 • Configuring SNMP Version 3 Users, page 4-21 • Configuring SNMP Trap Destination Hosts, page 4-23 • Configuring SNMP Notifications, page 4-25
Establish global policy maps for all VLANs on a virtual context	Configuring Virtual Context Global Traffic Policies, page 4-26
Manage ACE appliance licenses	Managing ACE Appliance Licenses, page 4-27
Manage ACE appliance resources across virtual contexts	Managing Resource Classes, page 4-34
Establish application acceleration and optimization for the ACE appliance	Configuring Global Application Acceleration and Optimization, page 13-9
Back up or restore the configuration and dependencies of an entire ACE or of a particular virtual context	Performing Device Backup and Restore Functions, page 4-45

Configuring Virtual Context Primary Attributes

Primary attributes specify a name and resource class for each virtual context. After providing this information, you can configure other attributes, such as interfaces, monitoring, or load-balancing. For a complete list of configuration options, see Configuring Virtual Contexts, page 4-7.

Use this procedure to configure virtual context primary attributes.

Procedure

Step 1 Choose **Config > Virtual Contexts >** *context* **> System > Primary Attributes**.

The Primary Attributes configuration screen appears.

Step 2 Enter the primary attributes for this virtual context as described in Table 4-1.

Step 3 Click **Deploy Now** to deploy this configuration on the ACE appliance.

To exit this procedure without accepting your entries, select a different configuration option.

Related Topics

- Using Virtual Contexts, page 4-2
- Configuring Virtual Context VLAN Interfaces, page 10-10
- Configuring Virtual Context BVI Interfaces, page 10-23
- Configuring Virtual Context Syslog Logging, page 4-12
- Configuring Traffic Policies, page 12-1

Configuring Virtual Context Syslog Logging

The ACE Appliance Device Manager uses syslog logging to send log messages to a process which logs messages to designated locations asynchronously to the processes that generated the messages.

Procedure

Step 1 Choose **Config > Virtual Contexts >** *context* **> System > Syslog**.

The Syslog configuration screen appears.

Step 2 Enter the syslog logging attributes in the displayed fields (see Table 4-5).

All fields that require you to select syslog severity levels use the values in Table 4-4.

Table 4-4 Syslog Logging Levels

Severity	Description
0-Emergency	Unusable system
1-Critical	Critical condition
2-Warning	Warning condition
3-Alert	Immediate action required
4-Error	Error condition
5-Notification	Normal but significant condition
6-Information	Informational message only
7-Debug	Appears only during debugging

The severity level that you specify indicates that you want syslog messages at that level and the more severe levels. For example, if you specify Error, syslog displays Error, Critical, Alert, and Emergency messages.

Note If you set all syslog levels to Debug, some commands like **switchover** are not processed successfully. These commands are issued via the CLI and ACE Appliance Device Manager cannot parse the returned prompt if Debug level is enabled. Instead, a timeout message is displayed.

If you set syslog levels to Debug and then issue a command that results in a timeout message, click **Refresh** to view the result of the operation.

Note Setting all syslog levels to Debug during normal operation can degrade overall performance.

Table 4-5 Virtual Context Syslog Configuration Attributes

Field	Description	Action
Enable Syslog	This option indicates whether syslog logging should be enabled or disabled.	Check the check box to enable syslog logging or clear the check box to disable syslog logging.
Facility	The syslog daemon uses the specified syslog facility to determine how to process the messages it receives. Syslog servers file or direct messages based on the facility number in the message. For more information on the syslog daemon and facility levels, refer to your syslog daemon documentation.	Enter the facility appropriate for your network. Valid entries are 16 (LOCAL0) through 23 (LOCAL7). The default for an ACE appliance is 20 (LOCAL4).
Buffered Level	This option enables system logging to a local buffer and limits the messages sent to the buffer based on severity.	Choose the desired level for sending system log messages to a local buffer. This option is disabled by default.
Console Level	This option specifies the maximum level for system log messages sent to the console.	Select the desired level for sending system log messages to the console. This option is disabled by default. **Note** Logging into the console can degrade system performance. Therefore, we recommend that you log messages to the console only when you are testing or debugging problems. Do not use this option when the network is busy, as it can reduce ACE appliance performance.

Table 4-5 Virtual Context Syslog Configuration Attributes (continued)

Field	Description	Action
History Level	This option specifies the maximum level for system log messages sent as traps to an SNMP network management station.	Choose the desired level for sending system log messages as traps to an SNMP network management station. This option is disabled by default. **Note** For more information about configuring SNMP, see Configuring SNMP Notifications, page 4-25.
Monitor Level	This option specifies the maximum level for system log messages sent to a remote connection using Secure Shell (SSH) or Telnet on the ACE appliance.	Select the desired level for sending system log messages to a remote connection using SSH or Telnet on the ACE appliance. This option is disabled by default. **Note** You must enable remote access on the ACE appliance and establish a remote connection using the SSH or Telnet protocol from a PC for this option to work.
Persistence Level	This option specifies the maximum level for system log messages sent to Flash memory.	Select the desired level for sending system log messages to Flash memory. This option is disabled by default. **Note** We recommend that you use a lower severity level, such as 3, since logging at a high rate to Flash memory on the ACE appliance might impact performance.
Trap Level	This option specifies the maximum level for system log messages sent to a syslog server.	Select the desired level for sending system log messages to a syslog server. This option is disabled by default.
Queue Size	This option specifies the size of the buffer for storing syslog messages received from other processes within the ACE appliance while they await processing. When the queue exceeds the specified value, the excess messages are discarded.	Enter the desired queue size. Valid entries are from 0 to 8192 messages. The default is 100 messages.
Enable Timestamp	This option indicates whether syslog messages should include the date and time that the message was generated.	Check the check box to enable timestamps on syslog messages or clear the check box to disable timestamps on syslog messages. This option is disabled by default.
Enable Standby	This option indicates whether logging is enabled on the failover standby ACE appliance. When enabled: • This feature causes twice the message traffic on the syslog server. • The standby ACE appliance syslog messages remain synchronized if failover occurs.	Check the check box to enable logging on the failover standby ACE appliance or clear the check box to disable logging on the failover standby ACE appliance.

Table 4-5 Virtual Context Syslog Configuration Attributes (continued)

Field	Description	Action
Enable Fastpath Logging	This option indicates whether connection setup and teardown messages are logged.	Check the check box to enable the logging of setup and teardown messages or clear the check box to disable the logging of setup and teardown messages. This option is disabled by default.
Device Id Type	This option specifies the type of unique device identifier to be included in syslog messages sent to the syslog server. The device identifier does not appear in EMBLEM-formatted messages, SNMP traps, or on the ACE appliance console, management session, or buffer.	Select the type of device identifier to be used: • Any String—Indicates that a test string is to be used to uniquely identify syslog messages send from the ACE appliance. • Context Name—Indicates that the name of the current virtual context is to be used to uniquely identify the syslog messages sent from the ACE appliance. • Host Name—Indicates that the hostname of the ACE appliance is to be used to uniquely identify the syslog messages sent from the ACE appliance. • Interface—Indicates that the IP address of the interface is to be used to uniquely identify the syslog messages sent from the ACE appliance. • Undefined—Indicates that no identifier is to be used.
Device Interface Name	This field appears if the Device Id Type is Interface. This option specifies the logging device interface to be used to uniquely identify syslog messages sent from the ACE appliance.	Enter a text string that uniquely identifies the logging device interface name whose ID is to be included in system messages. The maximum string length is 64 characters without spaces. Do not use the following characters: & (ampersand), ‘ (single quote), “ (double quote), < (less than), > (greater than), or ? (question mark).
Logging Device Id	This field appears if the Device ID Type is Any String. This option specifies the text string to be used to uniquely identify syslog messages sent from the ACE appliance.	Enter a text string that uniquely identifies the syslog messages sent from the ACE appliance. The maximum string length is 64 characters without spaces. Do not use the following characters: & (ampersand), ‘ (single quote), “ (double quote), < (less than), > (greater than), or ? (question mark).

Step 3 Click **Deploy Now** to deploy this configuration on the ACE appliance.

To configure other Syslog attributes for this virtual context, see:

- Configuring Syslog Log Hosts, page 4-16
- Configuring Syslog Log Messages, page 4-17
- Configuring Syslog Log Rate Limits, page 4-18

Related Topics

- Configuring Virtual Contexts, page 4-7

Configuring Syslog Log Hosts

After configuring basic syslog characteristics (see Configuring Virtual Context Syslog Logging, page 4-12), you can configure the log host, log messages, and log rate limits. The tabs for these attributes appear beneath the Syslog configuration screen.

Guidelines and Restrictions

You can configure the ACE with a maximum of four log hosts per context.

Procedure

Step 1 Choose **Config > Virtual Contexts >** *context* **> System > Syslog**.

The Syslog configuration screen appears.

Step 2 Select the Log Host tab.

The Log Host table appears.

Step 3 Click **Add** to add a new log host, or select an existing log host, then click **Edit** to modify it.

The Log Host configuration screen appears.

Step 4 In the IP Address field, enter the IPv4 address of the host to be used as the syslog server.

Step 5 In the Protocol field, select TCP or UDP as the protocol to be used.

Step 6 In the Protocol Port field, enter the number of the port that the syslog server listens to for syslog messages.

Valid entries are from 1 to 65535. The default port for TCP is 1470 and for UDP it is 514.

Step 7 If it is present, check the **Default UDP** check box to specify that the ACE appliance is to default to UDP if the TCP transport fails to communicate with the syslog server.

The Default UDP check box appears if TCP is selected in the Protocol field (Step 5). Clear this check box to prevent the ACE appliance from defaulting to UDP if the TCP transport fails.

Step 8 In the Format field, indicate whether EMBLEM-format logging is to be used as follows:

- N/A—Indicates that you do not want to enable EMBLEM-format logging.
- Emblem—Indicates that EMBLEM-format logging is to be enabled for each syslog server. If you use Cisco Resource Manager Essentials (RME) software to collect and process syslog messages on your network, enable EMBLEM-format logging so that RME can handle them. Similarly, UDP needs to be enabled because the Cisco Resource Manager Essentials (RME) syslog analyzer supports only UDP syslog messages.

Step 9 Do one of the following:

- Click **Deploy Now** to deploy this configuration on the ACE appliance.
- Click **Cancel** to exit the procedure without saving your entries and to return to the Log Host table.
- Click **Add Another** to configure another syslog host.

Related Topics

- Configuring Virtual Context Syslog Logging, page 4-12
- Configuring Syslog Log Messages, page 4-17
- Configuring Syslog Log Rate Limits, page 4-18

Configuring Syslog Log Messages

After configuring basic syslog characteristics (see Configuring Virtual Context Syslog Logging, page 4-12), you can configure the log host, log messages, and log rate limits. The tabs for these attributes appear beneath the Syslog configuration screen.

Use this procedure to configure Syslog log messages.

Procedure

Step 1 Choose **Config > Virtual Contexts >** *context* **> System > Syslog**.

The Syslog configuration screen appears.

Step 2 Click the **Log Message** tab.

The Log Message table appears.

Step 3 Click **Add** to add a new entry to this table, or select an existing entry, then click **Edit** to modify it.

The Log Message configuration screen appears.

Step 4 In the Message Id field, select the system log message ID of the syslog messages that are to be sent to the syslog server or that are not to be sent to the syslog server.

Step 5 Check the **Enable State** check box to indicate that logging is enabled for the specified message ID.

Clear the check box to indicate that logging is not enabled for the specified message ID. If you check the Enable State check box, the Log Level field appears.

Step 6 In the Log Level field, select the desired level of syslog messages to be sent to the syslog server, using the levels identified in Table 4-4.

Step 7 Do one of the following:

- Click **Deploy Now** to deploy this configuration on the ACE appliance.
- Click **Cancel** to exit the procedure without saving your entries and to return to the Log Message table.
- Click **Add Another** to save your entries and to configure additional syslog message entries for this virtual context.

Related Topics

- Configuring Virtual Context Syslog Logging, page 4-12
- Configuring Syslog Log Hosts, page 4-16
- Configuring Syslog Log Rate Limits, page 4-18

Configuring Syslog Log Rate Limits

After configuring basic syslog characteristics (see Configuring Virtual Context Syslog Logging, page 4-12), you can configure the log host, log messages, and log rate limits. The tabs for these attributes appear beneath the Syslog configuration screen.

Use this procedure to limit the rate at which the ACE appliance generates messages in the syslog.

Procedure

Step 1 Choose **Config > Virtual Contexts >** *context* **> System > Syslog**.

The Syslog configuration screen appears.

Step 2 Click the **Log Rate Limit** tab.

The Log Rate Limit table appears.

Step 3 Click **Add** to add a new entry to this table, or select an existing entry, then click **Edit** to modify it.

The Log Rate Limit configuration screen appears.

Step 4 In the Type field, indicate the method by which syslog messages are to be limited as follows:

- Choose **Level** to limit syslog messages by syslog level. In the Level field, select the level of syslog messages to be sent to the syslog server, using the levels identified in Table 4-4.
- Choose **Message** to limit syslog messages by message identification number. In the Message Id field, select the syslog message ID for those messages for which you want to suppress reporting.

Step 5 Check the **Unlimited** check box to indicate that limits are not to be applied to system message logging.

Clear the Unlimited check box to indicate that limits are to be applied to system message logging. If you clear the Unlimited check box, the Rate and Time Interval fields appear.

Step 6 If you clear the Unlimited check box, specify the limits to apply to system message logging as follows:

a. In the Rate field, enter the number at which syslog message creation is to be limited. When this limit is reached, the ACE appliance limits the creation of new syslog messages to be no greater than the specified rate. Valid entries are integers from 0 to 2147483647.

b. In the Time Interval (Seconds) field, enter the length of time (in seconds) over which the system message logs should be limited. The default time interval is one second. For example, if you enter 42 in the Rate field and 60 in the Time Interval (Seconds) field, the ACE appliance limits the creation of syslog messages that are sent to a maximum of 42 messages in that 60-second period. Valid entries are from 0 to 2147483647 seconds.

Step 7 Do one of the following:

- Click **Deploy Now** to deploy this configuration on the ACE appliance.
- Click **Cancel** to exit the procedure without saving your entries and to return to the Log Rate Limit table.
- Click **Add Another** to save your entries and to add another entry to the Log Rate Limit table.

Related Topics

- Configuring Virtual Contexts, page 4-7
- Configuring Virtual Context Syslog Logging, page 4-12
- Configuring Syslog Log Hosts, page 4-16

- Configuring Syslog Log Messages, page 4-17

Configuring SNMP for Virtual Contexts

This section describes how to configure the SNMP attributes for a virtual context and contains the following topics:

- Configuring Basic SNMP Attributes, page 4-19
- Configuring SNMP Version 2c Communities, page 4-20
- Configuring SNMP Version 3 Users, page 4-21
- Configuring SNMP Trap Destination Hosts, page 4-23
- Configuring SNMP Notifications, page 4-25

Configuring Basic SNMP Attributes

Use this procedure to configure basic SNMP attributes for use with this virtual context.

Procedure

Step 1 Choose **Config > Virtual Contexts >** *context* **> System > SNMP**.

The SNMP configuration screen appears.

Step 2 Enter SNMP attributes (see Table 4-6).

Table 4-6 SNMP Attributes

Field	Description
Contact Information	Enter contact information for the SNMP server within the virtual context as a text string with a maximum of 240 characters including spaces. In addition to a name, you might want to include a phone number or e-mail address. To include spaces, add quotation marks at the beginning and end of the entry.
Location	Enter the physical location of the system as a text string with a maximum of 240 characters including spaces. To include spaces, add quotation marks at the beginning and end of the entry.
Unmask Community	Check the check box to unmask the snmpCommunityName and snmpCommunitySecurityName OIDs of the SNMP-COMMUNITY-MIB. Clear the check box to mask these OIDs. By default, they are masked (the checkbox is unchecked).

Table 4-6 SNMP Attributes (continued)

Field	Description
Trap Source Interface	Enter a valid VLAN number that identifies the interface from which the SNMP traps originate.
IETF Trap	Check the check box to indicate that the ACE appliance is to send linkUp and linkDown traps with the IETF standard IF-MIB (RFC 2863) variable bindings, consisting of ifIndex, ifAdminStatus, and ifOperStatus. Clear the check box to indicate that the ACE appliance is not to send linkUp and linkDown traps with the IETF standard IF-MIB (RFC 2863) variable bindings. Instead, the ACE appliance sends Cisco var-binds by default.

Step 3 Click **Deploy Now** to deploy this configuration on the ACE appliance.

To configure other SNMP attributes, see:

- Configuring SNMP Version 2c Communities, page 4-20
- Configuring SNMP Version 3 Users, page 4-21
- Configuring SNMP Trap Destination Hosts, page 4-23
- Configuring SNMP Notifications, page 4-25

Related Topic

Configuring Virtual Contexts, page 4-7

Configuring SNMP Version 2c Communities

After configuring basic SNMP information for a virtual context (see Configuring SNMP for Virtual Contexts, page 4-19), you can configure other SNMP attributes such as SNMP version 2c communities, SNMP version 3 users, trap destination hosts, and SNMP notification. The tabs for these attributes appear below the SNMP configuration screen.

Note All SNMP communities in ACE Appliance Device Manager are read-only communities and all communities belong to the group *network monitors*.

Use this procedure to configure SNMP version 2c communities for a virtual context.

Assumption

You have configured at least one SNMP contact (see Configuring SNMP for Virtual Contexts, page 4-19).

Procedure

Step 1 Choose **Config > Virtual Contexts >** *context* **> System > SNMP**.

The SNMP configuration screen appears.

Step 2 Click the **SNMP v2c Configuration** tab.

The SNMP v2c Configuration table appears.

Step 3 Click **Add** to add an SNMP v2c community.

The SNMP v2c Configuration screen appears.

Note You cannot modify an existing SNMP v2c community. Instead, delete the existing SNMP v2c community, then add a new one.

Step 4 In the Read-Only Community field, enter the SNMP v2c community name for this context.

Valid entries are unquoted text strings with no spaces and a maximum of 32 characters.

Step 5 Do one of the following:

- Click **Deploy Now** to deploy this configuration on the ACE appliance.
- Click **Cancel** to exit this procedure without saving your entry and to return to the SNMP v2c Community table.
- Click **Add Another** to save your entry and to configure another SNMP community for this virtual context. The screen refreshes and you can enter another community name.

Related Topics

- Configuring Virtual Contexts, page 4-7
- Configuring SNMP Version 3 Users, page 4-21
- Configuring SNMP Trap Destination Hosts, page 4-23
- Configuring SNMP Notifications, page 4-25

Configuring SNMP Version 3 Users

After configuring basic SNMP information for a virtual context (see Configuring SNMP for Virtual Contexts, page 4-19), you can configure other SNMP attributes such as SNMP version 2c communities, SNMP version 3 users, trap destination hosts, and SNMP notification. The tabs for these attributes appear below the SNMP configuration screen.

Use this procedure to configure SNMP version 3 users for a virtual context.

Assumption

You have configured at least one SNMP contact (see Configuring SNMP for Virtual Contexts, page 4-19).

Procedure

Step 1 Choose **Config > Virtual Contexts >** *context* **> System > SNMP**.

The SNMP configuration screen appears.

Step 2 Click the **SNMP v3 Configuration** tab.

The SNMP v3 Configuration table appears.

Step 3 Click **Add** to add users, or select an existing entry, then **Edit** to modify it.

The SNMP v3 Configuration screen appears.

Step 4 Enter SNMP v3 user attributes (see Table 4-7).

Table 4-7 SNMP v3 User Configuration Attributes

Field	Description
User Name	Enter the SNMP v3 username. Valid entries are unquoted text strings with no spaces and a maximum of 24 characters.
Authentication Algorithm	Select the authentication algorithm to be used for this user. • N/A—Indicates that no authentication is to be used. • Message Digest (MD5)—Indicates that Message Digest 5 is to be used as the authentication mechanism. • Secure Hash Algorithm (SHA)—Indicates that Secure Hash Algorithm is to be used as the authentication mechanism.
Authentication Password	Appears if you select an authentication algorithm. The ACE appliance automatically updates the password for the CLI user with the SNMP authentication password. Enter the authentication password for this user as follows: • If the passphrases are specified in clear text, enter an unquoted text string with no space that is from 8 to 64 alphanumeric characters in length. The password length can be an odd or even value. • If use of a localized key is enabled, enter an unquoted text string with no space that is from 8 to 130 alphanumeric characters in length. The password length must be an even value.
Confirm	Appears if you select an authentication algorithm. Reenter the authentication password.
Localized	Appears if you select an authentication algorithm. Indicate whether the password is in localized key format for security encryption: • N/A—Indicates that this option is not configured. • False—Indicates that the password is not in localized key format for encryption. • True—Indicates that the password is in localized key format for encryption.
Privacy	Appears if you select an authentication algorithm. Indicate whether encryption attributes are to be configured for this user: • N/A—Indicates that no encryption attributes are specified. • False—Indicates that encryption parameters are not to be configured for this user. • True—Indicates that encryption parameters are to be configured for this user.

Table 4-7 SNMP v3 User Configuration Attributes (continued)

Field	Description
AES 128	Appears if you set Privacy to True. Indicate whether the 128-byte Advanced Encryption standard (AES) algorithm is to be used for privacy. AES is a symmetric cipher algorithm and is one of the privacy protocols for SNMP message encryption. • N/A—Indicates that no standard is specified. • False—Indicates that AES 128 is not be used for privacy. • True—Indicates that AES 128 is to be used for privacy.
Privacy Password	Appears if you set Privacy to True. Enter the user encryption password as follows: • If the passphrases are specified in clear text, enter an unquoted text string with no space that is from 8 to 64 alphanumeric characters in length. The password length can be an odd or even value. • If use of a localized key is enabled, enter an unquoted text string with no space that is from 8 to 130 alphanumeric characters in length. The password length must be an even value.
Confirm	Appears if you set Privacy to True. Reenter the privacy password.

Step 5 Do one of the following:

- Click **Deploy Now** to deploy this configuration on the ACE appliance.
- Click **Cancel** to exit this procedure without saving your entries and to return to the SNMP v3 Configuration table.
- Click **Add Another** to save your entries and to add another entry to the SNMP v3 Configuration table. The screen refreshes and you can enter another SNMP v3 user.

Related Topics

- Configuring Virtual Contexts, page 4-7
- Configuring SNMP Version 2c Communities, page 4-20
- Configuring SNMP Trap Destination Hosts, page 4-23
- Configuring SNMP Notifications, page 4-25

Configuring SNMP Trap Destination Hosts

To receive SNMP notifications you must configure:

- At least one SNMP trap destination host. This section describes how to do this.
- At least one type of notification. See Configuring SNMP Notifications, page 4-25.

After configuring basic SNMP information for a virtual context (see Configuring SNMP for Virtual Contexts, page 4-19), you can configure other SNMP attributes such as SNMP version 2c communities, SNMP version 3 users, trap destination hosts, and SNMP notification. The tabs for these attributes appear below the SNMP configuration screen.

Use this procedure to configure SNMP trap destination hosts for a virtual context.

Assumption

You have configured at least one SNMP contact (see Configuring SNMP for Virtual Contexts, page 4-19).

Procedure

Step 1 Choose **Config > Virtual Contexts >** *context* **> System > SNMP**.

The SNMP configuration screen appears.

Step 2 Click the **Trap Destination Host** tab.

The Trap Destination Host table appears.

Step 3 Click **Add** to add a host, or select an existing entry in the table, then **Edit** to modify it.

The Trap Destination Host configuration screen appears.

Step 4 Configure the SNMP trap destination host using the information in Table 4-8.

Table 4-8 SNMP Trap Destination Host Configuration Attributes

Field	Description
IP Address	Enter the IPv4 address of the server that is to receive SNMP notifications.
Port	Enter the port to be used for SNMP notification. The default port is 162.
Version	Select the version of SNMP used to send traps: • V1—Indicates that SNMP version 1 is to be used to send traps. This option is not available for use with SNMP inform requests. • V2c—Indicates that SNMP version 2c is to be used to send traps. • V3—Indicates that SNMP version 3 is to be used to send traps. This version is the most secure model because it allows packet encryption.
Community	Enter the SNMP community string or username to be sent with the notification operation. Valid entries are unquoted text strings with no spaces and a maximum of 32 characters.
Security Level	This field appears if V3 is the selected version. Select the level of security that is to be implemented: • Auth—Indicates that Message Digest 5 (MD5) and Secure Hash Algorithm (SHA) are to be used for packet authentication. • Noauth—Indicates that the noAuthNoPriv security level is to be used. • Priv—Indicates that Data Encryption Standard (DES) is to be used for packet encryption.

Step 5 Do one of the following:

- Click **Deploy Now** to deploy this configuration on the ACE appliance.

- Click **Cancel** to exit this procedure without saving your entries and to return to the Trap Destination Host table.
- Click **Add Another** to save your entries and to add another entry to the Trap Destination Host table. The screen refreshes and you can add another trap destination host.

Related Topics

- Configuring Virtual Contexts, page 4-7
- Configuring SNMP Version 2c Communities, page 4-20
- Configuring SNMP Version 3 Users, page 4-21
- Configuring SNMP Notifications, page 4-25

Configuring SNMP Notifications

After configuring basic SNMP information for a virtual context (see Configuring SNMP for Virtual Contexts, page 4-19), you can configure other SNMP attributes such as SNMP version 2c communities, SNMP version 3 users, trap destination hosts, and SNMP notification. The tabs for these attributes appear below the SNMP configuration screen.

To receive SNMP notifications you must configure:

- At least one SNMP trap destination host. See Configuring SNMP Trap Destination Hosts, page 4-23.
- At least one type of notification. This section describes how to do this.

Use this procedure to configure SNMP notification for a virtual context.

Assumptions

- You have configured at least one SNMP contact (see Configuring SNMP for Virtual Contexts, page 4-19).
- At least one SNMP server host has been configured (see Configuring SNMP Trap Destination Hosts, page 4-23).

Procedure

Step 1 Choose **Config > Virtual Contexts >** *context* **> System > SNMP**.

The SNMP configuration screen appears.

Step 2 Click the **SNMP Notification** tab.

The SNMP Notification table appears.

Step 3 Click **Add** to add a new entry.

The SNMP Notification configuration screen appears.

Note You cannot modify an existing entry. Instead, delete the existing notification entry, then add a new one.

Step 4 In the Options field, choose the type of notifications to be sent to the SNMP host.

Some options are available only in the Admin context. The notification types are as follows:

- **License**—SNMP license notifications are to be sent. This option is available only in the Admin context.
- **SLB**—Server load-balancing notifications are to be sent.
- **SLB Real Server**—Notifications of real server state changes are to be sent.
- **SLB Server Farm**—Notifications of server farm state changes are to be sent.
- **SLB Virtual Server**—Notifications of virtual server state changes are to be sent.
- **SNMP**—SNMP notifications are to be sent.
- **SNMP Authentication**—Notifications of incorrect community strings in SNMP requests are to be sent.
- **SNMP Cold-Start**—SNMP agent restart notifications are to be sent after a cold restart (full power cycle) of the ACE. This option is available only in the Admin context.
- **SNMP Link-Down**—Notifications are to be sent when a VLAN interface is down.
- **SNMP Link-Up**—Notifications are to be sent when a VLAN interface is up.
- **Syslog**—Error message notifications (Cisco Syslog MIB) are to be sent.
- **Virtual Context**—Virtual context notifications are to be sent. This option is available only in the Admin context.

Step 5 Do one of the following:

- Click **Deploy Now** to deploy this configuration on the ACE appliance.
- Click **Cancel** to exit this procedure without saving your selection and to return to the SNMP Notification table.
- Click **Add Another** to save your entries and to add another entry to the SNMP Notification table. The screen refreshes and you can select another SNMP notification option.

Related Topics

- Configuring Virtual Contexts, page 4-7
- Configuring SNMP Version 2c Communities, page 4-20
- Configuring SNMP Version 3 Users, page 4-21

Configuring Virtual Context Global Traffic Policies

With the ACE Appliance Device Manager, you can apply traffic policies to a specific VLAN interface or to all VLAN interfaces in the same virtual context.

Use this procedure to apply a policy to all VLAN interfaces in the selected context.

To apply a policy to a specific VLAN, see Configuring Traffic Policies, page 12-1.

Note You cannot modify an existing policy. Instead, delete the existing global policy, then create a new one.

Assumption

A Layer 3/Layer 4 or Management policy map has been configured for this virtual context. For more information, see Configuring Virtual Context Policy Maps, page 12-34.

Procedure

Step 1 Choose **Config > Virtual Contexts >** *context* **> System > Global Policies**.

The Global Policies table appears.

Step 2 Click **Add** to add a new global policy.

The Global Policies configuration screen appears.

Note You cannot modify an existing policy. Instead, delete the existing global policy, then create a new one.

Step 3 In the Policy Maps field, choose the policy map that you want to apply to all VLANs in this context.

Click the **Add** button to create or edit the policy map.

Step 4 In the Direction field, verify that the policy is being applied to incoming communications.

Step 5 Do one of the following:

- Click **Deploy Now** to deploy this configuration on the ACE appliance.
- Click **Cancel** to exit the procedure without saving your entries and to return to the Global Policies table.
- Click **Add Another** to save your entries and to configure another global policy for this context.

Related Topics

- Using Virtual Contexts, page 4-2
- Configuring Virtual Context Primary Attributes, page 4-11
- Configuring Virtual Context VLAN Interfaces, page 10-10
- Configuring Virtual Context Syslog Logging, page 4-12
- Configuring Traffic Policies, page 12-1

Managing ACE Appliance Licenses

Note This functionality is available for only Admin contexts.

Cisco Systems offers licenses for ACE appliances that let you increase performance throughput, the number of default contexts, SSL TPS (transactions per second), and HTTP compression performance. For more information on these licenses, refer to the *Administration Guide, Cisco ACE Application Control Engine* on cisco.com.

You can view, install, remove, or update ACE appliance licenses using the ACE Appliance Device Manager.

Installing or updating an ACE appliance license involves two processes:

- Copying the license from a remote network server to the disk0: file system in Flash memory on the ACE appliance.
- Installing or updating the license on the ACE appliance.

You can use the ACE appliance Device Manager to perform both processes from a single dialog box. If you previously copied the license to disk0: on the ACE by using the **copy** CLI command, you can use this dialog box to install the new license or upgrade license on your ACE.

Related Topics

- Viewing ACE Appliance Licenses, page 4-28
- Installing ACE Appliance Licenses, page 4-29
- Updating ACE Appliance Licenses, page 4-31
- Uninstalling ACE Appliance Licenses, page 4-32
- Displaying the File Contents of a License, page 4-33

Viewing ACE Appliance Licenses

Note This functionality is available for only Admin contexts.

Use this procedure to view the licenses that are currently installed on an ACE appliance.

Procedure

Step 1 Choose **Config > Virtual Contexts**.

The All Virtual Context table appears.

Step 2 Choose the Admin context whose ACE appliance licenses you want to view, then click **System > Licenses**.

The following license tables appear:

- License Status Table—Provides a summary of the license status for the ACE, including:
  - Compression performance in megabits or gigabits per second
  - Application acceleration and optimization in the number of concurrent connections
  - SSL transactions per second

    Note The SSL transactions per second license does not apply to the ACE NPE software version (see the "Information About the ACE No Payload Encryption Software Version" section on page 1-2).

  - Number of supported virtual contexts
  - ACE appliance bandwidth in gigabits per second

- Installed License Files Table—Lists all installed licenses with their filenames, vendors, and expiration (expiry) dates.

Related Topics

- Managing ACE Appliance Licenses, page 4-27
- Installing ACE Appliance Licenses, page 4-29
- Updating ACE Appliance Licenses, page 4-31
- Uninstalling ACE Appliance Licenses, page 4-32
- Displaying the File Contents of a License, page 4-33

Installing ACE Appliance Licenses

Note This functionality is available for only Admin contexts.

Use this procedure to copy and install a new or upgrade ACE appliance license from a remote server onto the ACE appliance.

Assumption

- You have received the proper software license key for the ACE appliance.
- ACE appliance licenses are available on a remote server for importing to the ACE appliance, or you have received the software license key and have copied the license file to the disk0: filesystem on the ACE appliance using the **copy disk0:** CLI command.
- This functionality on the DM requires that SSH is enabled on the appliance. Also, ensure that the **ssh key rsa 1024 force** command is applied on the appliance.

Procedure

Step 1 Choose **Config > Virtual Contexts**.

The All Virtual Contexts table appears.

Step 2 Choose the Admin context you want to import and install a license for, then click **System > Licenses**.

The License Status Table and Installed License Files Table appear listing all installed licenses.

Step 3 Click **Install**.

The Install an ACE License dialog box appears.

Step 4 (Optional) If the license currently exists on the ACE disk0: file system in Flash memory, do the following:

a. In the Select an Option to Locate a License File section of the dialog box, click the **Select a license file on the ACE** option.

b. In the Select a License File on the Device (disk0) section of the dialog box, from the drop-down list, choose the name of the license file.

c. Go to Step 10.

Step 5 (Optional) If the license must be copied to the disk0: file system in Flash memory, in the Select an Option to Locate a License File section of the dialog box, click the **Import a license file from remote system** option. Go to Step 6.

Step 6 In the Protocol To Connect To Remote System field, choose the protocol to be used to import the license file from the remote server to the ACE as follows:

- If you choose FTP, the User Name and Password fields appear. Go to Step 7.
- If you choose SFTP, the User Name and Password fields appear. Go to Step 7.
- If you choose TFTP, go to Step 8.

Step 7 (Optional) If you chose FTP or SFTP, do the following:

a. In the User Name field, enter the username of the account on the network server.

b. In the Password field, enter the password for the user account.

Step 8 In the Remote System IP Address field, enter the host IPv4 address of the remote server.

For example, your entry might be 192.168.11.2.

Step 9 In the License Path In Remote System field, enter the host path and filename of the license file on the remote server in the format */path/filename* where:

- *path* represents the directory path of the license file on the remote server.
- *filename* represents the filename of the license file on the remote server.

For example, your entry might resemble /usr/bin/ACE-VIRT-020.lic.

Step 10 Do one of the following:

- Click **Install** to accept your entries and to install the license file.
- Click **Cancel** to exit this procedure without installing the license file and to return to the Licenses table.

Step 11 (Optional) After installing an ACE license, Cisco recommends that you manually synchronize the ACE Admin context with the CLI to ensure that DM accurately displays the monitored resource usage information (Monitor > Virtual Contexts > Resource Usage).

For information about synchronizing the Admin context, see the "Synchronizing Virtual Context Configurations" section on page 4-75.

Related Topics

- Managing ACE Appliance Licenses, page 4-27
- Viewing ACE Appliance Licenses, page 4-28
- Updating ACE Appliance Licenses, page 4-31
- Uninstalling ACE Appliance Licenses, page 4-32
- Displaying the File Contents of a License, page 4-33

Updating ACE Appliance Licenses

Note This functionality is available for only Admin contexts.

ACE Appliance Device Manager allows you to convert demonstration licenses to permanent licenses and to upgrade permanent licenses to increase the number of virtual contexts.

Use this procedure to install ACE appliance update licenses.

Assumption

- You have received the proper update software license for the ACE appliance.
- ACE appliance licenses are available on a remote server for importing to the ACE appliance, or you have received the update software license and have copied the license file to the disk0: filesystem on the ACE appliance using the **copy disk0:** CLI command.
- This functionality on the DM requires that SSH is enabled on the appliance. Also, ensure that the **ssh key rsa 1024 force** command is applied on the appliance.

Procedure

Step 1 Choose **Config > Virtual Contexts**.

The All Virtual Contexts table appears.

Step 2 Choose the Admin context with the license you want to update, then click **System > Licenses**.

The License Status Table and Installed License Files Table appear listing all installed licenses.

Step 3 Select the license to be updated, then click **Update**.

The Update License On The ACE dialog box appears.

Step 4 (Optional) If the update license currently exists on the ACE disk0: file system in Flash memory, do the following:

a. In the Select an Option to Locate a License File section of the dialog box, click the **Select a license file on the ACE** option.

b. In the Select a License File on the Device (disk0) section of the dialog box, choose the name of the update license file from the drop-down list.

c. Go to Step 10.

Step 5 (Optional) If the update license must be copied to the disk0: file system in Flash memory, in the Select an Option to Locate a License File section of the dialog box, click the **Import a license file from remote system** option and go to Step 6.

Step 6 In the Protocol To Connect To Remote System field, choose the protocol to be used to import the update license file from the remote server to the ACE as follows:

- If you choose FTP, the User Name and Password fields appear. Go to Step 7.
- If you choose SFTP, the User Name and Password fields appear. Go to Step 7.
- If you choose TFTP, go to Step 8.

Step 7 (Optional) If you chose FTP or SFTP, do the following:

a. In the User Name field, enter the username of the account on the network server.

b. In the Password field, enter the password for the user account.

Step 8 In the Remote System IP Address field, enter the host IPv4 address of the remote server.

For example, your entry might be 192.168.11.2.

Step 9 In the Licence Path In Remote System field, enter the host path and filename of the license file on the remote server in the format */path/filename* where:

- *path* represents the directory path of the license file on the remote server.
- *filename* represents the filename of the license file on the remote server.

For example, your entry might be /usr/bin/ACE-VIRT-020.lic.

Step 10 Do one of the following:

- Click **Update** to update the license and to return to the License table. The License table displays the updated information.
- Click **Cancel** to exit this procedure without updating the license and to return to the License table.

Step 11 (Optional) After updating an ACE license, Cisco recommends that you manually synchronize the ACE Admin context with the CLI to ensure that DM accurately displays the monitored resource usage information (Monitor > Virtual Contexts > ACE > Resource Usage).

For information about synchronizing the Admin context, see the "Synchronizing Virtual Context Configurations" section on page 4-75.

Related Topics

- Managing ACE Appliance Licenses, page 4-27
- Viewing ACE Appliance Licenses, page 4-28
- Installing ACE Appliance Licenses, page 4-29
- Uninstalling ACE Appliance Licenses, page 4-32
- Displaying the File Contents of a License, page 4-33

Uninstalling ACE Appliance Licenses

Note This functionality is available for only Admin contexts.

Caution Removing licenses can affect an ACE appliance's bandwidth or performance. For detailed information on the effect of license removal on your ACE appliance, see the *Administration Guide, Cisco ACE Application Control Engine*.

Use this procedure to remove ACE appliance licenses.

Assumption

This functionality on the DM requires that SSH is enabled on the appliance. Also, ensure that the **ssh key rsa 1024 force** command is applied on the appliance.

Procedure

Step 1 Choose **Config > Virtual Contexts**.

The All Virtual Contexts table appears.

Step 2 Choose the Admin context with the license you want to remove, then click **System > Licenses**.

Step 3 In the Installed License Files table, choose the license to be removed.

Step 4 Click **Uninstall**.

A dialog box appears, asking you to confirm the license removal process.

Note Removing licenses can affect the number of contexts, ACE appliance bandwidth, or SSL TPS (transactions per second). Be sure you understand the effect of removing the license on your environment before continuing.

Step 5 Click **OK** to confirm the removal or **Cancel** to stop the removal process.

If you click OK, a status window appears with the status of license removal. When the license has been removed, the Licenses table refreshes without the deleted license.

Step 6 (Optional) After uninstalling an ACE license, Cisco recommends that you manually synchronize the ACE Admin context with the CLI to ensure that DM accurately displays the monitored resource usage information (Monitor > Virtual Contexts > Resource Usage).

For information about synchronizing the Admin context, see the "Synchronizing Virtual Context Configurations" section on page 4-75.

Related Topics

- Managing ACE Appliance Licenses, page 4-27
- Installing ACE Appliance Licenses, page 4-29
- Updating ACE Appliance Licenses, page 4-31
- Viewing ACE Appliance Licenses, page 4-28
- Displaying the File Contents of a License, page 4-33

Displaying the File Contents of a License

Note This functionality is available for only Admin contexts.

Use this procedure to display file content information about ACE licenses.

Procedure

Step 1 Choose **Config > Virtual Contexts**.

The All Virtual Contexts table appears.

Step 2 Choose the Admin context with the license information you want to view, then choose **System > Licenses**.

The License Status Table and Installed License Files Table appear listing all installed licenses.

Step 3 Choose the installed license file with the information that you want to display, and click **View**.

DM displays the output of the **show license file** C LI command.

For example:

```
ACE-AP-C-500-LIC.lic:
SERVER this_host ANY
VENDOR cisco
INCREMENT ACE-AP-C-500-LIC cisco 1.0 permanent 1 \
    NOTICE="<LicFileID>lic.conf</LicFileID><LicLineID>0</LicLineID> \
    <PAK>dummyPak</PAK>" SIGN=222C4BCAD092
```

Step 4 Click **Close** when you finish viewing the license file information.

Related Topics

- Installing ACE Appliance Licenses, page 4-29
- Updating ACE Appliance Licenses, page 4-31

Managing Resource Classes

Resource classes are the means by which you manage virtual context access to ACE appliance resources, such as concurrent connections or bandwidth rate. ACE appliances are preconfigured with a default resource class that is applied to the Admin context and any user context upon creation. The default resource class is configured to allow a context to operate within a range that can vary from no resource access (0%) to complete resource access (100%). When you use the default resource class with multiple contexts, you run the risk of oversubscribing ACE appliance resources. This means that the ACE appliance permits all contexts to have full access to all resources on a first-come, first-served basis. When a resource is utilized to its maximum limit, the ACE appliance denies additional requests made by any context for that resource.

To avoid oversubscribing resources and to help guarantee access to a resource by any context, you can create customized resource classes that you associate with one or more contexts. A context becomes a member of the resource class when you make the association. Creating a resource class allows you to set limits on the minimum and maximum amounts of each ACE appliance resource that a member context is entitled to use. You define the minimum and maximum values as a percentage of the whole. For example, you can create a resource class that allows its member contexts access to no less that 25% of the total number of SSL connections that the ACE appliance supports.

You can limit and manage the allocation of the following ACE appliance resources:

- ACL memory
- Application acceleration connections
- Buffers for syslog messages and TCP out-of-order (OOO) segments
- Concurrent connections (through-the-ACE traffic)
- Management connections (to-the-ACE traffic)
- HTTP compression percentage
- Proxy connections
- Set resource limit as a rate (number per second)

- Regular expression (regexp) memory
- SSL connections

Note Managing the SSL connections resource does not apply to the ACE NPE software version (see the "Information About the ACE No Payload Encryption Software Version" section on page 1-2).

- Sticky entries
- Static or dynamic network address translations (Xlates)

Table 4-9 identifies and defines the resources that you can establish for resource classes.

Resource Allocation Constraints

Note This functionality is available for only Admin contexts.

The following resources are critical for maintaining connectivity to the Admin context:

- Rate Bandwidth
- Rate Management Traffic
- Rate SSL Connections
- Rate Connections
- Management Connections
- Concurrent Connections

Caution If you allocate 100% of these resources to a resource class and then apply the resource class to virtual contexts, connectivity to the Admin context can be lost.

We recommend that you create a resource class specifically for the Admin context and apply it to the context so that you can maintain IP connectivity.

Table 4-9 Resource Class Attributes

Resource	Definition
All	Limits all resources to the specified value for all contexts assigned to this resource class, except for management traffic bandwidth. Management traffic bandwidth remains at the default values until you explicitly configure a minimum value for management traffic.
Acceleration Connections	Percentage of application acceleration connections.
ACL Memory	Percentage of memory allocated for ACLs.
Buffer Syslog	Percentage of the syslog buffer.

Table 4-9 Resource Class Attributes (continued)

Resource	Definition
Concurrent Connections	Percentage of simultaneous connections. **Note** If you consume all Concurrent Connections by allocating 100% to virtual contexts, IP connectivity to the Admin context can be lost.
HTTP Compression	Percentage of compression for HTTP data.
Management Connections	Percentage of management connections. **Note** If you consume all Management Connections by allocating 100% to virtual contexts, IP connectivity to the Admin context can be lost.
Proxy Connections	Percentage of proxy connections.
Rate Bandwidth	Percentage of context throughput. This attribute limits the total ACE throughput in bytes per second for one or more contexts. **Note** If you consume all rate bandwidth by allocating 100% to virtual contexts, IP connectivity to the Admin context can be lost. The maximum bandwidth rate per context is determined by your bandwidth license. By default, the ACE supports 1 gigabit per second (Gbps) appliance throughput. You can upgrade the ACE with an optional 2-Gbps bandwidth license. When you configure a minimum bandwidth value for a resource class in the ACE, the ACE subtracts that configured value from the total bandwidth maximum value of all contexts in the ACE, regardless of the resource class with which they are associated. The total bandwidth rate of a context consists of the following two components: • Throughput—Limits through-the-ACE traffic. This is a derived value (you cannot configure it directly) and it is equal to the bandwidth rate minus the mgmt-traffic rate for the 1-Gbps and 2-Gbps licenses. • Management Traffic—Limits management (to-the-ACE) traffic in bytes per second. To guarantee a minimum amount of management traffic bandwidth, you must explicitly allocate a minimum percentage to management traffic using the Resource Classes table (**Config > Virtual Contexts >** ***admin context*** **> System > Resource Class**). When you allocate a minimum percentage of bandwidth to management traffic, the ACE subtracts that value from the maximum available management traffic bandwidth for all contexts in the ACE.
Rate Connections	Percentage of connections of any kind. **Note** If you consume all Rate Connections by allocating 100% to virtual contexts, IP connectivity to the Admin context can be lost.
Rate Inspect Connection	Percentage of application protocol inspection connections for FTP and RTSP.
Rate MAC Miss	Percentage of messages destined for the ACE appliance that are sent to the control plane when the encapsulation is not correct in packets.
Rate Management Traffic	Percentage of management traffic connections. **Note** If you consume all Rate Management Traffic by allocating 100% to virtual contexts, IP connectivity to the Admin context can be lost.

Table 4-9 Resource Class Attributes (continued)

Resource	Definition
Rate SSL Connections	**Note** This resource option is not available with the ACE NPE software version (see the "Information About the ACE No Payload Encryption Software Version" section on page 1-2). Percentage of SSL connections. **Note** If you consume all Rate Management Traffic by allocating 100% to virtual contexts, IP connectivity to the Admin context can be lost.
Rate Syslog	Percentage of syslog messages per second.
Regular Expressions	Percentage of regular expression memory.
Sticky	Percentage of entries in the sticky table.
Xlates	Percentage of network and port address translations entries.

Related Topics

- Adding Resource Classes, page 4-37
- Modifying Resource Classes, page 4-39
- Deleting Resource Classes, page 4-40
- Viewing Resource Class Use on Virtual Contexts, page 4-40

Adding Resource Classes

Note This functionality is available for only Admin contexts.

Resource classes are used when provisioning services, establishing virtual contexts, managing devices, and monitoring virtual context resource consumption.

Defining a resource class does not automatically apply it to a context. New resource classes are applied only when a resource class is assigned to a virtual context.

Caution If you allocate 100% of the resources to a resource class and then apply the resource class to virtual contexts, connectivity to the Admin context can be lost. For more information, refer to Resource Allocation Constraints, page 4-35.

Use this procedure to create a new resource class.

Procedure

Step 1 Choose **Config > Virtual Contexts >** *admin context* **> System > Resource Class**.

The Resource Classes table appears.

Step 2 Click **Add** to create a new resource class.

The New Resource Class configuration screen appears.

Step 3 In the Name field, enter a unique name for this resource class.

Valid entries are unquoted text strings with no spaces and a maximum of 64 characters.

Step 4 To use the same values for each resource, enter the following information in the All row: (See Table 4-9 for a description of the resources.)

a. In the Min. field, enter the minimum percentage of each resource you want to allocate to this resource class. Valid entries are numbers from 0 to 100 including those with decimals in increments of .01.

b. In the Max. field, choose the maximum percentage of each resource you want to allocate to this resource class:

- Equal To Min.—Indicates that the maximum percentage allocated for each resource is equal to the minimum specified in the Min. field.
- Unlimited—Indicates that there is no upper limit on the percentage of each resource that can be allocated for this resource class.

Step 5 To use different values for the resources, for each resource, choose the method for allocating resources:

- Select **Default** to use the values specified in Step 4.
- Choose **Min.** to enter a specific minimum value for the resource. In the Min. field, enter the minimum percentage of this resource you want to allocate to this resource class. For example, for ACL memory, you would enter 10 in the Min. field to indicate that you want to allocate a minimum of 10 percent of the available ACL memory to this resource class.

Step 6 If you chose **Min.**, in the Max. field, choose the maximum percentage of the resource you want to allocate to this resource class:

- **Equal To Min.**—Indicates that the maximum percentage allocated for this resource is equal to the minimum specified in the Min. field.
- **Unlimited**—Indicates that there is no upper limit on the percentage of the resource that can be allocated for this resource class.

Step 7 When you finish allocating the resources for this resource class, do one of the following:

- Click **Deploy Now** to deploy this configuration on the ACE appliance. The ACE Appliance Device Manager displays the number of virtual contexts that can be supported using this resource class in the Maximum VC column. To support more or fewer virtual contexts, choose the resource class, click **Edit**, and modify it as described in this procedure.
- Click **Cancel** to exit this procedure without saving your entries and to return to the Resource Classes table.

Related Topics

- Managing Resource Classes, page 4-34
- Modifying Resource Classes, page 4-39
- Deleting Resource Classes, page 4-40
- Viewing Resource Class Use on Virtual Contexts, page 4-40

Modifying Resource Classes

Note This functionality is available for only Admin contexts.

When you modify a resource class, the ACE Appliance Device Manager applies the changes to virtual contexts that are associated with the resource class going forward. The changes are applied to existing virtual contexts already associated with the resource class.

Caution If you allocate 100% of the resources to a resource class and then apply the resource class to virtual contexts, connectivity to the Admin context can be lost. For more information, refer to Resource Allocation Constraints, page 4-35.

Use this procedure to modify an existing resource class.

Note You cannot modify the default resource class.

Procedure

Step 1 Choose **Config > Virtual Contexts >** *admin context* **> System > Resource Class**.

The Resource Classes table appears.

Step 2 Choose the resource class you want to modify, then click **Edit**.

The Edit Resource Class configuration screen appears.

Step 3 Modify the fields as desired.

For details on setting values, see Adding Resource Classes, page 4-37. For descriptions of the resources, see Table 4-9.

Step 4 When you finish allocating the resources for this resource class, do one of the following:

- Click **Deploy Now** to deploy this configuration on the ACE appliance. The configuration screen refreshes and the Max. Provisionable field beneath the Name field indicates the number of virtual contexts that can be supported using this resource allocation. When you are satisfied with the resource allocation and have saved your entries, click **Cancel** to return to the Resource Classes table.
- Click **Cancel** to exit this procedure without saving your entries and to return to the Resource Classes table.

The ACE Appliance Device Manager applies all changes to the virtual contexts that use this resource class.

Related Topics

- Managing Resource Classes, page 4-34
- Adding Resource Classes, page 4-37
- Modifying Resource Classes, page 4-39
- Deleting Resource Classes, page 4-40
- Viewing Resource Class Use on Virtual Contexts, page 4-40

Deleting Resource Classes

Note This functionality is available for only Admin contexts.

Use this procedure to remove resource classes from the ACE Appliance Device Manager database.

Note When you remove a resource class from the ACE Appliance Device Manager, any virtual contexts that were associated with this resource class automatically become members of the default resource class. The default resource class allocates a minimum of 0.00% to a maximum of 100.00% of all ACE appliance resources to each context. You cannot modify the default resource class.

Because of the impact of resource class deletion on virtual contexts, we recommend that you view a resource class's current deployment before deleting it. See Viewing Resource Class Use on Virtual Contexts, page 4-40.

Procedure

Step 1 Choose **Config > Virtual Contexts >** *admin context* **> System > Resource Class**.

The Resource Classes table appears.

Step 2 Choose the resource class you want to remove, then click **Delete**.

A window appears, asking you to confirm the deletion.

Step 3 Click **OK** to continue deleting the resource class or click **Cancel** to keep the resource class.

The Resource Classes table refreshes with the updated information.

Related Topics

- Managing Resource Classes, page 4-34
- Adding Resource Classes, page 4-37
- Modifying Resource Classes, page 4-39
- Viewing Resource Class Use on Virtual Contexts, page 4-40

Viewing Resource Class Use on Virtual Contexts

Note This functionality is available for only Admin contexts.

Use this procedure to view a list of all virtual contexts using a selected resource class.

Procedure

Step 1 Choose **Config > Virtual Contexts >** *admin context* **> System > Resource Class**.

The Resource Classes table lists the number of virtual contexts using each resource class in the second column.

Step 2 Choose the resource class whose usage you want to view, then click **Virtual Contexts**.

The Virtual Contexts Using Resource Class table appears, listing the associated contexts.

Step 3 Click **Cancel** to return to the Resource Classes table.

Related Topics

- Managing Resource Classes, page 4-34
- Adding Resource Classes, page 4-37
- Modifying Resource Classes, page 4-39
- Deleting Resource Classes, page 4-40
- Viewing Resource Class Use on Virtual Contexts, page 4-40

Using the Configuration Checkpoint and Rollback Service

At some point, you may want to modify your ACE running configuration. If you run into a problem with the modified configuration, you may need to reboot your ACE. To prevent having to reboot your ACE after unsuccessfully modifying a running configuration, you can create a checkpoint (a snapshot in time) of a known stable running configuration before you begin to modify it. If you encounter a problem with the modifications to the running configuration, you can roll back the configuration to the previous stable configuration checkpoint.

Note Before you upgrade your ACE software, we strongly recommend that you create a checkpoint in your running configuration. For software release A4(1.0), use the backup function to create a backup of the running configuration (see the "Performing Device Backup and Restore Functions" section on page 4-45).

The ACE allows you to make a checkpoint configuration at the context level. The ACE stores the checkpoint for each context in a hidden directory in Flash memory. If, after you make configuration changes that modify the current running configuration, when you roll back the checkpoint, the ACE causes the running configuration to revert to the checkpointed configuration.

This section includes the following topics:

- Creating a Configuration Checkpoint, page 4-41
- Deleting a Configuration Checkpoint, page 4-43
- Rolling Back a Running Configuration, page 4-43
- Comparing the Checkpoint with the Running Configuration, page 4-44
- Displaying Checkpoint Information, page 4-44

Creating a Configuration Checkpoint

You can create a configuration checkpoint for a specific context. The ACE supports a maximum of 10 checkpoints for each context.

Assumption

This topic assumes the following:

- Make sure that the current running configuration is stable and is the configuration that you want to make as a checkpoint. If you change your mind after creating the checkpoint, you can delete it (see the "Deleting a Configuration Checkpoint" section on page 4-43).
- The ACE-Admin, DM-Admin, and Org-Admin predefined roles have access to the configuration checkpoint function.
- A custom role with the Device Manager Inventory and Virtual Context role tasks set to create or modify has the required privileges to create a configuration checkpoint.
- A checkpoint will not include the SSL keys/certificates, probe scripts, and licenses.
- This functionality on the DM requires that SSH is enabled on the appliance. Also, ensure that the **ssh key rsa 1024 force** command is applied on the appliance.
- Adding a checkpoint from an ACE context directly will not trigger an autosynchronization on the ACE Appliance Device Manager for that context.

Procedure

Step 1 Choose **Config > Virtual Contexts >** *admin context* **> System > Checkpoints**.

The Checkpoints table appears.

For descriptions of the checkpoints, see Table 4-10.

Table 4-10 Checkpoints Table

Field	Description
Name	Unique identifier of the checkpoint.
Size (In Bytes)	Size of the configuration checkpoint, shown in bytes.
Date (Created On)	Date that the configuration checkpoint was created.

Step 2 In the Checkpoints table, click **Create Checkpoint**.

The Create Checkpoint dialog box appears.

Step 3 In the Checkpoint Name field of the Create Checkpoint dialog box, specify a unique identifier for the checkpoint.

Enter a text string with no spaces and a maximum of 25 alphanumeric characters.

If the checkpoint already exists, you are prompted to use a different name.

Step 4 Do one of the following:

- Click **OK** to save your configuration checkpoint. You return to the Checkpoints table and the new checkpoint appears in the table.
- Click **Cancel** to exit the procedure without saving the configuration checkpoint and to return to the Checkpoints table.

Deleting a Configuration Checkpoint

You can delete a checkpoint. Deleting a checkpoint from an ACE context directly will not trigger an autosynchronization to occur on the ACE Appliance Device Manager for that context.

Prerequisite

Before you perform this procedure, make sure that you want to delete the checkpoint. Once you click the Trash icon, the ACE removes the checkpoint from Flash memory.

This functionality on the DM requires that SSH is enabled on the appliance. Also, ensure that the **ssh key rsa 1024 force** command is applied on the appliance.

Procedure

Step 1 To choose a virtual context that you want to create a configuration checkpoint, choose **Config > Virtual Contexts >** *admin context* **> System >Checkpoints**.

The Checkpoints table appears.

Step 2 In the Checkpoints table, choose the radio button to the left of any table entry, and click the **Trash** icon to delete the checkpoint.

Rolling Back a Running Configuration

You can roll back the current running configuration of a context to the previously checkpointed running configuration.

Note This functionality on the DM requires that SSH is enabled on the appliance. Also, ensure that the **ssh key rsa 1024 force** command is applied on the appliance.

Procedure

Step 1 Choose **Config > Virtual Contexts >** *admin context* **> System > Checkpoints**.

The Checkpoints table appears.

Step 2 Choose the radio button to the left of the checkpoint that you wish to roll back, and click **Rollback**.

The ACE Appliance Device Manager displays a confirmation popup window to warn you about this change and to instruct you that the rollback operation may take longer depending on the differences detected between the two configurations.

Note The ACE Appliance Device Manager synchronizes the device after performing a rollback. This synchronization may take some time.

Comparing the Checkpoint with the Running Configuration

You can compare an existing checkpoint with the running configuration.

Procedure

Step 1 Choose **Config > Virtual Contexts >** *admin context* **> System > Checkpoints**.

The Checkpoints table appears.

Step 2 In the Checkpoints table, choose the radio button to the left of the checkpoint that you want to compare, and click **Compare**.

The ACE Appliance Device Manager uses the ACE **compare** *checkpoint_name* CLI command to compare the running configuration of the specified checkpoint.

If the checkpoint configuration is the same as the running-config, the output of this command is:

```
Checkpoint config is same as running config
```

If the checkpoint configuration is different from the running-config, the output will be the difference between the two configurations. The items in red are in the current running configuration and will be removed. The items in green are not in the current running configuration and will be added.

Step 3 Click **Close** to exit the dialog box and return to the Checkpoints table.

Displaying Checkpoint Information

You can display checkpoint information.

Procedure

Step 1 Choose **Config > Virtual Contexts >** *admin context* **> System > Checkpoints**.

The Checkpoints table appears.

Step 2 In the Checkpoints table, choose the radio button to the left of the checkpoint that you want to display, and click **Details**.

The ACE Appliance Device Manager uses the ACE **show checkpoint detail** {*name*} CLI command to display the running configuration of the specified checkpoint.

Step 3 Click **Close** to exit the dialog box and return to the Checkpoints table.

Performing Device Backup and Restore Functions

The backup and restore functions allow you to back up or restore the configuration and dependencies of an entire ACE or of a particular virtual context. Configuration dependencies are those files that are required to exist on the ACE so that a configuration can be applied to it. Such files include health-monitoring scripts, SSL certificates, SSL keys, and so on.

Note This section includes information about backing up and restoring SSL files, which is not applicable with the ACE NPE software version (see the "Information About the ACE No Payload Encryption Software Version" section on page 1-2).

This feature allows you to back up and restore the following configuration files and dependencies:

- Running-configuration files
- Startup-configuration files
- Checkpoints
- SSL files (SSL certificates and keys)
- Health-monitoring scripts
- Licenses

Note The backup feature does not back up the sample SSL certificate and key pair files.

Typical uses for this feature are as follows:

- Back up a configuration for later use
- Recover a configuration that was lost because of a software failure or user error
- Restore configuration files to a new ACE when a hardware failure resulted in a Return Merchandise Authorization (RMA) of the old ACE
- Transfer the configuration files to a different ACE

The backup and restore functions are supported in both the Admin and virtual contexts. If you perform these functions in the Admin context, you can back up or restore the configuration files for either the Admin context only or for all contexts in the ACE. If you perform these functions in a virtual context, you can back up or restore the configuration files only for that context. Both the backup and the restore functions run asynchronously (in the background).

Archive Naming Conventions

Context archive files have the following naming convention format:

Hostname_ctxname_timestamp.tgz

The filename fields are as follows:

- *Hostname*—Name of the ACE. If the hostname contains special characters, the ACE uses the default hostname "switch" in the filename. For example, if the hostname is Active@~!#$%^, then the ACE assigns the following filename: switch_Admin_2009_08_30_15_45_17.tgz
- *ctxname*—Name of the context. If the context name contains special characters, the ACE uses the default context name "context" in the filename. For example, if the context name is Test!123*, then the ACE assigns the following filename: switch_context_2009_08_30_15_45_17.tgz

– *timestamp*—Date and time that the ACE created the file. The time stamp has the following 24 hour format: *YYYY_MM_DD_hh_mm_ss*

An example is as follows:

```
ACE-1_ctx1_2009_05_06_15_24_57.tgz
```

If you back up the entire ACE, the archive filename does not include the *ctxname* field. So, the format is as follows:

Hostname_timestamp.tgz

An example is as follows:

```
ACE-1_2009_05_06_15_24_57.tgz
```

Archive Directory Structure and Filenames

The ACE uses a flat directory structure for the backup archive. The ACE provides file extensions for the individual files that it backs up so that you can identify the types of files easily when restoring an archive. All files are stored in a single directory that is tarred and GZIPed as follows:

```
ACE-1_Ctx1_2009_05_06_07_24_57.tgz
 ACE-1_Ctx1_2009_05_06_07_24_57\
  context_name-running
  context_name-startup
  context_name-chkpt_name.chkpt
  context_name-cert_name.cert
  context_name-key_name.key
  context_name-script_name.tcl
  context_name-license_name.lic
```

Guidelines and Limitations

The backup and restore functions have the following configuration guidelines and limitations:

- This functionality on the DM requires that SSH is enabled on the appliance. Also, ensure that the **ssh key rsa 1024 force** command is applied on the appliance.
- Store the backup archive on disk0: in the context of the ACE where you intend to restore the files. Use the Admin context for a full backup and the corresponding context for user contexts.
- When you back up the running-configuration file, the ACE uses the output of the **show running-configuration** CLI command as the basis for the archive file.
- The ACE backs up only exportable certificates and keys.
- License files are backed up only when you back up the Admin context.
- Use a pass phrase to back up SSL keys in encrypted form. Remember the pass phrase or write it down and store it in a safe location. When you restore the encrypted keys, the ACE prompts you for the pass phrase to decrypt the keys. If you do not use a pass phrase when you back up the SSL keys, the ACE restores the keys with AES-256 encryption using OpenSSL software.
- Only probe scripts that reside in disk0: need to be backed up. The prepackaged probe scripts in the probe: directory are always available. When you perform a backup, the ACE automatically identifies and backs up the scripts in disk0: that are required by the configuration.
- The ACE does not resolve any other dependencies required by the configuration during a backup except for scripts that reside in disk0:. For example, if you configured SSL certificates in an SSL proxy in the running-configuration file, but you later deleted the certificates, the backup proceeds anyway as if the certificates still existed.

- To perform a restore operation, you must have the admin RBAC feature in your user role. DM-admin and ORG-admin have access to this feature by default. Custom roles with the Device Manager Inventory and Virtual Context role tasks set to create or modify can also access this feature.
- When you instruct the ACE to restore the archive for the entire ACE, it restores the Admin context completely first, and then it restores the other contexts. The ACE restores all dependencies before it restores the running configuration. The order in which the ACE restores dependencies is as follows:
  - License files
  - SSL certificates and key files
  - Health-monitoring scripts
  - Checkpoints
  - Startup-configuration file
  - Running-configuration file
- When you restore the ACE, previously installed license files are uninstalled and the license files in the backup file are installed in their place.
- In a redundant configuration, if the archive that you want to restore is different from the peer configurations in the FT group, redundancy may not operate properly after the restore.
- You can restore a single context from a full backup archive provided that:
  - You execute the restore operation in the context that you want to restore
  - All files dependencies for the context exist in the full backup archive
- To enable the ACE Device Manager to synchronize the CLI after a successful restore, do not navigate from the Backup / Restore page until the Latest Restore status changes from In Progress to Success. If you navigate to another page before the restore process is complete, the CLI will not synchronize until you return to the Backup / Restore page or until the automatic or manual CLI CLI synchronization occurs.

Defaults

Table 4-11 lists the default settings for the backup and restore function parameters.

Table 4-11 Default Backup and Restore Parameters

Parameter	Default
Backed up files	By default the ACE backs up the following files in the current context: • Running-configuration file • Startup-configuration file • Checkpoints • SSL certificates • SSL keys • Health-monitoring scripts • Licenses
SSL key restore encryption	None

This section includes the following topics:

Backing Up Device Configuration and Dependencies

You can create a backup of an ACE configuration and its dependencies.

Note When you perform the backup process from the Admin context, you can either back up the Admin context files only or you can back up the Admin context and all user contexts. When you back up from a user context, you back up the current context files only and cannot back up the ACE licenses.

Note If your web browser supports the Remember Passwords option and you enable this option, the web browser may fill in the Username and Password fields for user authentication. By default, these fields should be empty. You can change the username and password fields from whatever the web browser inserts into the two fields.

Procedure

Step 1 Choose **Config > Virtual Contexts > System > Backup / Restore**.

The Backup / Restore table appears and displays the latest backup and restore statistics.

Note To refresh the table content at any time, click **Poll Now**.

Note When you choose the Backup / Restore operation, the Appliance Device Manager must poll a context if that context has not been accessed previously for this operation. The polling operation, which is necessary to obtain the latest backup and restore information, can cause a delay in the display time of the Backup / Restore table.

The Backup / Restore fields are described in Table 4-12.

Table 4-12 Backup / Restore Fields

Field	Description
Latest Backup	
Backup Archive	Name of the last *.tgz file created that contains the backup files.
Type	Type of backup: Context or Full (all contexts).
Start-time	Date and time that the last backup began.
Finished-time	Date and time that the last backup ended.
Status	Status of the last context to be backed up: Success, In Progress, or Failed. Click the status link to view status details.
Current vc	Name of the last context in the backup process.

Table 4-12 Backup / Restore Fields (continued)

Field	Description
Completed	Number of context backups completed compared to the total number of context backup requests. For example: • 2/2 = Two context backups completed/Two context backups requested • 0/1 = No context backup completed/One context backup requested
Latest Restore	
Backup Archive	Name of the *.tgz file used in during the restore process.
Type	Type of restore: Context or Full (all contexts).
Start-time	Date and time that the last restore began.
Finished-time	Date and time that the last restore ended.
Status	Status of the last restore: Success, In Progress, or Failed. Click the status to view status details.
Current vc	Name of the last context in the restore process.
Completed	Number of context restores completed compared to the total number of context restore requests. For example: • 2/2 = Two context restores completed/Two context restores requested • 0/1 = No context restore completed/One context restore requested

Step 2 Click **Backup**.

The Backup window appears.

Step 3 In the Backup window, click the radio button of the location where the ACE is to save the backup files:

- **Backup config on ACE (disk0:)**—This is the default. Go to Step 9.
- **Backup config on ACE (disk0:) and then copy to remote system**—The Remote System attributes step appears. Go to Step 4.

Step 4 Click the radio button of the transfer protocol to use:

- **FTP**—File Transfer Protocol
- **SFTP**—Secure File Transfer Protocol
- **TFTP**—Trivial File Transfer Protocol

Step 5 In the Username field, enter the username that the remote server requires for user authentication.

This field appears for FTP and SFTP only.

Step 6 In the Password field, enter the password that the remote server requires for user authentication.

This field appears for FTP and SFTP only.

Step 7 In the IP Address field, enter the IP address of the remote server.

Step 8 In the Backup File Path in Remote System field, enter the full path for the remote server.

Step 9 Check the **Backup All Contexts** checkbox if you want the ACE to create a backup that contains the files of the Admin context and every user context or uncheck the check box to create a backup of the Admin context files only.

This field appears for the Admin context only.

Step 10 Indicate the components to exclude from the backup process: Checkpoints or SSL Files.

Note The SSL Files option is not available for the ACE NPE software version (see the "Information About the ACE No Payload Encryption Software Version" section on page 1-2).

To exclude a component, double-click on it in the Available box to move it to the Selected box. You can also use the right and left arrows to move selected items between the two boxes.

Caution If you exclude the SSL Files component and then restore the ACE using this archived backup, these files are removed from the ACE. To save these files prior to performing a restore with this backup, use the **crypto export** CLI command to export the keys to a remote server and use the **copy** CLI command to copy the license files to disk0: as .tar files.

Step 11 In the Pass Phrase field, enter the pass phrase that you specify to encrypt the backed up SSL keys.

Note This field is not available with the ACE NPE software version (see the "Information About the ACE No Payload Encryption Software Version" section on page 1-2).

Enter the pass phrase as an unquoted text string with no spaces and a maximum of 40 alphanumeric characters. If you enter a pass phrase but exclude the SSL files from the archive, the ACE does not use the pass phrase.

Step 12 Click **OK** to begin the backup process.

The following actions occur depending on where the ACE Device Manager saves the files:

- disk0: only—The Device Manager permits continued GUI functionality during the backup process and polls the ACE for the backup status, which it displays on the Backup / Restore page.
- disk0: and a remote server—The Device Manager suspends GUI operation and displays a "Please Wait" message in the Backup dialog box until the process is complete. During this process, the ACE Device Manager instructs the ACE to create and save the backup file locally to disk0: and then place a copy of the file on the specified remote server.

Step 13 In the Backup / Restore page, click **Poll Now** to ensure that the latest backup statistics are displayed, and then click on the Status link (**Success**, **In Progress**, or **Failed**) located in the Latest Backup column to view details of the backup operation.

If the backup status is either Success or In Progress, then the Show Backup Status Detail pop-up window appears and displays a list of the files successfully backed up. When the backup status is In Progress, the ACE Device Manager polls the ACE every 2 minutes to retrieve the latest status information and then it automatically updates the status information displayed. The polling continues until the ACE Device Manager receives a status of either Success or Failed. If the backup status is Failed, then the Show Backup Errors popup window appears, displaying the reason for the failed backup attempt.

Related Topics

- Restoring Device Configuration and Dependencies, page 4-50

Restoring Device Configuration and Dependencies

You can restore an ACE configuration and its dependencies using a backup file.

Caution The restore operation clears any existing SSL certificate and key-pair files, license files, and checkpoints in a context before it restores the backup archive file. If your configuration includes SSL files or checkpoints and you excluded them when you created the backup archive, those files will no longer exist in the context after you restore the backup archive. To preserve any existing exportable SSL certificate and key files in the context, before you execute the restore operation, export the certificates and keys that you want to keep to an FTP, SFTP, or TFTP server by using the CLI and the **crypto export** command. After you restore the archive, import the SSL files into the context. For details on exporting and importing SSL certificate and key pair files using the CLI, see the *SSL Guide, Cisco ACE Application Control Engine*.

You can also use the exclude option of the restore command to instruct the ACE not to clear the SSL files in disk0: and to ignore the SSL files in the backup archive when the ACE restores the backup.

Ignore this Caution if the ACE is using the NPE software version, which does not allow encryption protocols (see the "Information About the ACE No Payload Encryption Software Version" section on page 1-2)

Note If your web browser supports the Remember Passwords option and you enable this option, the web browser may fill in the Username and Password fields for user authentication. By default, these fields should be empty. You can change the username and password fields from whatever the web browser inserts into the two fields.

Prerequisites

If you are going to restore the Admin context files plus all user context files, use a backup file that was created from the Admin context with the Backup All Contexts checkbox checked (see the "Backing Up Device Configuration and Dependencies" section on page 4-48).

Procedure

Step 1 Choose **Config > Virtual Contexts > System > Backup / Restore**.

The Backup / Restore table appears.

Note To refresh the table content at any time, click **Poll Now**.

Note When you perform the restore process from the Admin context, you can either restore the Admin context files only or you can restore the Admin context files plus all user context files. When you perform the restore process from a user context, you can restore the current context files only.

The Backup / Restore fields are described in Table 4-12.

Step 2 Click **Restore**.

The Restore window appears.

Note The display of the Restore window may be delayed because the Device Manager is retrieving the list of the disk0: archive (*.tgz) files.

Step 3 In the Restore window, click the desired radio button to specify the location where the backup files are located saved:

- **Choose a backup file on the ACE (disk0:)**—This is the default. Go to Step 9.
- **Choose a backup file from remote system**—The Remote System attributes step appears. Go to Step 4.

Step 4 Click the radio button of the transfer protocol to use:

- **FTP**—File Transfer Protocol
- **SFTP**—Secure File Transfer Protocol
- **TFTP**—Trivial File Transfer Protocol

Step 5 In the Username field, enter the username that the remote file system requires for user authentication.

This field appears for FTP and SFTP only.

Step 6 In the Password field, enter the password that the remote file system requires for user authentication.

This field appears for FTP and SFTP only.

Step 7 In the IP Address field, enter the IP address of the remote server.

Step 8 In the Backup File Path in Remote System field, enter the full path of the backup file, including the backup filename, to be copied from the remote server.

Step 9 Check the **Restore All Contexts** checkbox if you want the ACE to restore the files for every context or uncheck the checkbox to restore the Admin context files only.

This field appears for the Admin context only.

Step 10 Check the **Exclude SSL Files** checkbox if you want to preserver the SSL files currently loaded on the ACE and not use the backup file's SSL files.

Note This checkbox is not available with the ACE NPE software version (see the "Information About the ACE No Payload Encryption Software Version" section on page 1-2).

Caution The restore function deletes all SSL files currently loaded on the ACE unless you check the Exclude SSL Files option. If you do not check this option, the restore functions loads the SSL files included in the backup file. If the backup files does not include SSL files, the ACE will not have any SSL files loaded on it when the restore process is complete. You will then need to import copies of the SSL files from a remote server.

Step 11 In the Pass Phrase field, enter the pass phrase that is used to encrypt the backed up SSL keys in the archive.

Note This field is not available with the ACE NPE software version (see the "Information About the ACE No Payload Encryption Software Version" section on page 1-2).

Enter the pass phrase as an unquoted text string with no spaces and a maximum of 40 alphanumeric characters. The Pass Phrase field does not appear when you check the Exclude SSL Files checkbox.

Step 12 Click **OK** to begin the restore process.

The following actions occur depending on where the ACE Device Manager retrieves the backup files:

- disk0: only—The ACE Device Manager permits continued GUI functionality during the restore process and polls the ACE for the backup status, which it displays on the Backup / Restore page.

Note To enable the Device Manager to synchronize the CLI after a successful restore, do not navigate from the Backup / Restore window until the Latest Restore status changes from In Progress to Success. If you navigate to another window before the restore process is complete, the CLI will not synchronize until you return to the Backup / Restore window or until the automatic or manual CLI synchronization occurs.

- disk0: and a remote server—The ACE Device Manager suspends GUI operation and displays a "Please Wait" message in the Restore dialog box until the process is complete. During this process, the ACE Device Manager instructs the ACE to copy the backup file from the specified remote server to disk0: on the ACE and then apply the backup file to the context.

Step 13 In the Backup / Restore page, click **Poll Now** to ensure that the latest restore statistics are displayed, then click on the Status link (**Success**, **In Progress**, or **Failed**) located in the Latest Backup column to view details of the restore operation.

If the restore status is either Success or In Progress, then the Show Restore Status Detail popup window appears and displays a list of the files successfully restored. When the restore status is In Progress, the ACE Device Manager polls the ACE every 2 minutes to retrieve the latest status information and then it automatically updates the status information displayed. The polling continues until the ACE Device Manager receives a status of either Success or Failed. If the restored status is Failed, then the Show Restored Errors popup window appears, displaying the reason for the failed restore attempt.

Related Topics

- Performing Device Backup and Restore Functions, page 4-45

Configuring Security with ACLs

An ACL (access control list) consists of a series of statements called ACL entries that collectively define the network traffic profile. Each entry permits or denies network traffic (inbound and outbound) to the parts of your network specified in the entry. Besides an action element ("permit" or "deny"), each entry also contains a filter element based on criteria such as source address, destination address, protocol, or protocol-specific parameters. An implicit "deny all" entry exists at the end of every ACL, so you must configure an ACL on every interface where you want to permit connections. Otherwise, the ACE denies all traffic on the interface.

ACLs provide basic security for your network by allowing you to control network connection setups rather than processing each packet. Such ACLs are commonly referred to as *security ACLs*.

You can configure ACLs as parts of other features; for example, security, network address translation (NAT), or server load balancing (SLB). The ACE merges these individual ACLs into one large ACL called a *merged ACL*. The ACL compiler then parses the merged ACL and generates the ACL lookup mechanisms. A match on this merged ACL can result in multiple actions. You can add, modify, or delete entries to an ACL already in the summary table, or add a new ACL to the list.

When you use ACLs, you may want to permit all e-mail traffic on a circuit, but block FTP traffic. You can also use ACLs to allow one client to access a part of the network and prevent another client from accessing that same area.

When configuring ACLs, you must apply an ACL to an interface to control traffic on that interface. Applying an ACL on an interface assigns the ACL and its entries to that interface.

You can apply only one extended ACL to each direction (inbound or outbound) of an interface. You can also apply the same ACL on multiple interfaces.You can apply EtherType ACLs in only the inbound direction and on only Layer 2 interfaces.

Note By default, all traffic is denied by the ACE unless explicitly allowed. Only traffic that is explicitly allowed in an ACL can pass. All other traffic is denied.

For specific procedures, see:

- Creating ACLs, page 4-54
- Setting EtherType ACL Attributes, page 4-63
- Setting Extended ACL Attributes, page 4-57
- Resequencing Extended ACLs, page 4-62
- Viewing All ACLs by Context, page 4-64
- Editing or Deleting ACLs, page 4-65

Creating ACLs

Note By default, all traffic is denied by the ACE unless explicitly allowed. Only traffic that is explicitly allowed in an ACL can pass. All other traffic is denied.

Use this procedure to create, modify, or delete ACLs.

Procedure

Step 1 Choose **Config > Virtual Contexts >** *context* **> Security > ACLs**.

The ACL summary table appears, listing the existing ACLs. ACL summary fields are described in Table 4-13.

Table 4-13 ACL Summary Table

Field	Description
Name	Enter a unique identifier for the ACL. Valid entries are unquoted text strings with a maximum of 64 alphanumeric characters.
Type	Specifies the type of ACL: • Extended—This ACL allows you to specify both the source and the destination IP addresses of traffic as well as the protocol and the action to be taken. For more information see "Setting Extended ACL Attributes". • Ethertype—This ACL controls network access for non-IP traffic based on its EtherType. An EtherType is a sub-protocol identifier. For more information see "Setting EtherType ACL Attributes".
IP Address Type	Specifies the type of IP address: • IPv4—This ACL controls network access for IPv4 traffic. • IPv6—This ACL controls network access for IPv6 traffic.
# (Line Number)	ACL line number for extended type ACL entries.
Action	Action to be taken (permit/deny).
Protocol	Protocol number or service object group to apply to this ACL entry.
Source	Source IPv6 or IPv4 address or source network object group (if configured) that is being applied to this ACL entry.
Destination	Destination IPv6 or IPv4 address or destination network object group (if configured) that is applied to this ACL entry.
ICMP	Indicates whether or not this ACL uses ICMP (Internet Control Message Protocol). For more information, see "Protocol Names and Numbers".
Interface	VLAN interface(s) that is/are associated with this ACL, for example in4,5:4out where, in denotes the input direction, out denotes the output direction.
Remark	Enter any comments you want to include for this ACL. Valid entries are unquoted text strings with a maximum of 100 characters. You can enter leading spaces at the beginning of the text or special characters. Trailing spaces are ignored.

Step 2 From the summary table, do one of the following:

- To view full details of an ACL inline, click the plus sign to the left of any table entry.
- To create an ACL, click the **Add** icon. The New Access List screen appears (go to Step 3).
- To modify an ACL, select the radio button to the left of any table entry, then click the **Edit** icon. The Edit ACL or Edit ACL entry screen appears based on the selected radio button to the left of any table entry (go to Step 3).
- To delete an ACL, select the radio button to the left of any table entry, then click the **Delete** icon.

Step 3 Add or edit required fields as described in Table 4-14.

Table 4-14 ACL Configuration Attributes

Field	Description
ACL Properties	Includes name, type (Extended, Ethertype), IP address type (IPv6 andIPv4), and remarks. For more information see "ACL Summary Table".
ACL Entries	
Entry Attributes	Includes line number, action (Permit, Deny), protocol or service object group, and associated drop down descriptor menu. For more information for these attributes, see the "Setting Extended ACL Attributes" or "Setting EtherType ACL Attributes" section.
Source	(Extended type ACL only) Source IPv6 address and prefix length, IPv4 address and netmask with port number (if configured), or network object group (if configured) that is being applied to this ACL entry. For more information see the "Setting Extended ACL Attributes" section.
Destination	(Extended type ACL only) Destination IPv6 address and prefix length, IPv4 address and netmask with port number (if configured), or network object group (if configured) that is being applied to this ACL entry. For more information see the "Setting Extended ACL Attributes" section.
Add To Table button	Used to add multiple ACL entries, adding one at a time using this button, before clicking **Deploy**. In the past only one entry could be added at a time in a two-step process hopping between two different locations in the UI.
Remove From Table button	Used to remove multiple ACL entries, removing one at a time using this button, before clicking **Deploy**.
Interfaces	
• Input/Output Direction • Currently Assigned (ACL:Direction)	Allows you to associate the ACL with one or more interfaces allowing only one input and one output ACL for each interface. The top left checkbox under the Interfaces section allows you to select and apply to all interfaces "access-group input.".

Note To add, modify, or delete Object Groups go to the "Configuring Object Groups" section on page 4-66.

Step 4 Do one of the following:

- Click **Deploy** to deploy this configuration on the ACE appliance.
- Click **Cancel** to exit this procedure without saving your entries and to return to the ACLs table.

Related Topics

- Configuring Security with ACLs, page 4-53
- Setting EtherType ACL Attributes, page 4-63
- Setting Extended ACL Attributes, page 4-57

- Resequencing Extended ACLs, page 4-62
- Editing or Deleting ACLs, page 4-65

Setting Extended ACL Attributes

Note By default, all traffic is denied by the ACE unless explicitly allowed. Only traffic that is explicitly allowed in an ACL can pass. All other traffic is denied.

An extended ACL allows you to specify both the source and the destination IP addresses of traffic as well as the protocol and the action to be taken.

For TCP, UDP, and ICMP connections, you do not need to also apply an ACL on the destination interface to allow returning traffic, because the ACE allows all returning traffic for established connections.

Note The ACE does not explicitly support standard ACLs. To configure a standard ACL, specify the destination address as **any** and do not specify the ports in an extended ACL.

Procedure

Step 1 Choose **Config > Virtual Contexts >** *context* **> Security > ACLs**.

The ACLs table appears, listing the existing ACLs.

Step 2 Click **Add**. The New Access List configuration screen appears.

Step 3 Enter the ACL name in the ACL Properties pane and choose the type as Extended.

Choose the IP Address Type as either IPV6 or IPv4.

Step 4 Configure extended ACL entries using the information in Table 4-15.

Table 4-15 Extended ACL Configuration Options

Field	Description
Entry Attributes	
Line Number	Enter a number that specifies the position of this entry in the ACL. The position of an entry affects the lookup order of the entries in an ACL. To change the sequence of existing extended ACLs, see Resequencing Extended ACLs, page 4-62.
Action	Action to be taken (permit/deny).
Service Object Group	Select a service object group to apply to this ACL.
Protocol	Select the protocol or protocol number to apply to this ACL entry. Table 4-16 lists common protocol names and numbers.
ICMP Type	Select the ICMP type or number for this protocol. • Table 4-17 lists common ICMP types and numbers, per RFC 792. • Table 4-18 lists the common ICMPv6 types and associated numbers, per RFC 4443.

Table 4-15 Extended ACL Configuration Options (continued)

Field	Description
Message Code Operator	Choose the operand to use when comparing message codes for this service object: • Equal To—The message code must be the same as the number in the Message Code field. • Greater Than—The message code must be greater than the number in the Message Code field. • Less Than—The message code must be less than the number in the Message Code field. • Not Equal To—The message code must not equal the number in the Message Code field. • Range—The message code must be within the range of codes specified by the Min. Message Code field and the Max. Message Code field.
Message Code	This field appears if you select Equal To, Greater Than, Less Than, or Not Equal To in the Message Code Operator field. Enter the ICMP message code for this service object.
Min. Message Code	This field appears if you select Range in the Message Code Operator field. Enter the number that is the beginning value for a range of services for this service object. Valid entries are integers from 0 to 255. The number in this field must be less than the number entered in the Max. Message Code field.
Max. Message Code	This field appears if you select Range in the Message Code Operator field. Enter the number that is the ending value for a range of services for this service object. Valid entries are integers from 0 to 255. The number in this field must be greater than the number entered in the Min. Message Code field.
Source	
Source Network	Defines the network traffic being received from the source network to the ACE: • Any—Select the Any radio button to indicate that network traffic from any source is allowed. • IP/Netmask—(IPv4 address type) Use this field to limit access to a specific source IP address. Enter the source IPv4 address that is allowed for this ACL and select its subnet mask. • IP/Prefix-length—(IPv6 address type) Use this field to limit access to a specific source IP address. Enter the source IPv6 address that is allowed for this ACL and its prefix length. • Network Object Group—Select a source network object group to apply to this ACL.

Table 4-15 Extended ACL Configuration Options (continued)

Field	Description
Source Port Operator	This field appears if you select TCP or UPD in the Protocol field. Choose the operand to use to compare source port numbers: • Equal To—The source port must be the same as the number in the Source Port Number field. • Greater Than—The source port must be greater than the number in the Source Port Number field. • Less Than—The source port must be less than the number in the Source Port Number field. • Not Equal To—The source port must not equal the number in the Source Port Number field. • Range—The source port must be within the range of ports specified by the Lower Source Port Number field and the Upper Source Port Number field.
Source Port Number	This field appears if you select Equal To, Greater Than, Less Than, or Not Equal To in the Source Port Operator field. Enter the port name or number from which you want to permit or deny access.
Lower Source Port Number	This field appears if you select Range in the Source Port Operator field. Enter the number of the lowest port from which you want to permit or deny access. Valid entries are integers from 0 to 65535. The number in this field must be less than the number entered in the Upper Source Port Number field.
Upper Source Port Number	This field appears if you select Range in the Source Port Operator field. Enter the port number of the upper port from which you want to permit or deny access. Valid entries are integers from 0 to 65535. The number in this field must be greater than the number entered in the Lower Source Port Number field.
Destination	
Destination Network	Defines the network traffic being transmitted to the destination network from the ACE: • Any—Select the Any radio button to indicate that network traffic to any destination is allowed. • IP/Netmask—(IPv4 address type) Use this field to limit access to a specific destination IP address. Enter the destination IPv4 address that is allowed for this ACL and select its subnet mask. • IP/Prefix-length—(IPv6 address type) Use this field to limit access to a specific destination IP address. Enter the destination IPv6 address that is allowed for this ACL and its prefix length. • Network Object Group—Select a destination network object group to apply to this ACL.

Table 4-15 Extended ACL Configuration Options (continued)

Field	Description
Destination Port Operator	This field appears if you select TCP or UPD in the Protocol field. Select the operand to use to compare destination port numbers: • Equal To—The destination port must be the same as the number in the Destination Port Number field. • Greater Than—The destination port must be greater than the number in the Destination Port Number field. • Less Than—The destination port must be less than the number in the Destination Port Number field. • Not Equal To—The destination port must not equal the number in the Destination Port Number field. • Range—The destination port must be within the range of ports specified by the Lower Destination Port Number field and the Upper Destination Port Number field.
Destination Port Number	This field appears if you select Equal To, Greater Than, Less Than, or Not Equal To in the Destination Port Operator field. Enter the port name or number from which you want to permit or deny access.
Lower Destination Port Number	This field appears if you select Range in the Destination Port Operator field. Enter the number of the lowest port to which you want to permit or deny access. Valid entries are integers from 0 to 65535. The number in this field must be less than the number entered in the Upper Destination Port Number field.
Upper Destination Port Number	This field appears if you select Range in the Destination Port Operator field. Enter the port number of the upper port to which you want to permit or deny access. Valid entries are integers from 0 to 65535. The number in this field must be greater than the number entered in the Lower Destination Port Number field.

Table 4-16 Protocol Names and Numbers

Protocol Name[1]	Protocol Number	Description
AH	51	Authentication Header
EIGRP	88	Enhanced IGRP
ESP	50	Encapsulated Security Payload
GRE	47	Generic Routing Encapsulation
ICMP	1	Internet Control Message Protocol version 4
ICMPv6[2]	58	Internet Control Message Protocol version 6
IGMP	2	Internet Group Management Protocol
IP	0 (Any)	Internet Protocol
IP-In-IP	4	IP-in-IP Layer 3 Tunneling Protocol
OSPF	89	Open Shortest Path First
PIM	103	Protocol Independent Multicast

Table 4-16 Protocol Names and Numbers (continued)

Protocol Name[1]	Protocol Number	Description
TCP	6	Transmission Control Protocol
UDP	17	User Datagram Protocol

1. For a complete list of all protocols and their numbers, see the Internet Assigned Numbers Authority available at www.iana.org/numbers/.
2. ICMPv6 is not available for an IPv4 service object group.

Table 4-17 ICMP Type Names and Numbers

ICMP Type Name	Number
Alternate-Address	6
Conversion-Error	31
Echo	8
Echo-Reply	0
Information-Reply	16
Information-Request	15
Mask-Reply	18
Mask-Request	17
Mobile-Redirect	32
Parameter-Problem	12
Redirect	5
Router-Advertisement	9
Router-Solicitation	10
Source-Quench	4
Time-Exceeded	11
Timestamp-Reply	14
Timestamp-Request	13
Traceroute	30
Unreachable	3

Table 4-18 ICMPv6 Type Names and Numbers

ICMP Type Name	Number
Echo	128
Echo-Reply	129
Information-Reply	140
Information-Request	139
Parameter-Problem	4

Table 4-18 ICMPv6 Type Names and Numbers (continued)

ICMP Type Name	Number
Redirect	137
Time-Exceeded	3
Traceroute	30
Unreachable	1

Step 5 Click **Add To Table** if you want to add one or more ACL entries to the table.

See Step 4 for information on configuring the extended ACL entries.

Step 6 Associate any VLAN interface to this ACL if required and do one of the following:

- Click **Deploy** to immediately deploy this configuration.
- Click **Cancel** to exit without saving your entries and to return to the ACL Summary table.

Related Topics

- Configuring Security with ACLs, page 4-53
- Creating ACLs, page 4-54
- Setting EtherType ACL Attributes, page 4-63
- Resequencing Extended ACLs, page 4-62
- Editing or Deleting ACLs, page 4-65

Resequencing Extended ACLs

Use this procedure to change the sequence of entries in an Extended ACL. EtherType ACL entries cannot be resequenced.

Procedure

Step 1 Choose **Config > Virtual Contexts >** *context* **> Security > ACLs**.

The ACLs table appears, listing the existing ACLs.

Step 2 Choose the Extended ACL you want to renumber, then click the **Resequence** icon appearing to the left of the filter field.

The ACL Line Number Resequence window appears.

Step 3 In the Start field, enter the number that is to be assigned to the first entry in the ACL.

Valid entries are 1 to 2147483647.

Step 4 In the Increment field, enter the number that is to be added to each entry in the ACL after the first entry. You can enter any integer.

Valid entries are 1 to 2147483647.

Step 5 Do one of the following:

- Click **Resequence** to save your entries and to return to the ACLs table.

- Click **Cancel** to exit this procedure without saving your entries and to return to the ACLs table.

Related Topics

- Configuring Security with ACLs, page 4-53
- Creating ACLs, page 4-54
- Setting EtherType ACL Attributes, page 4-63
- Setting Extended ACL Attributes, page 4-57
- Editing or Deleting ACLs, page 4-65

Setting EtherType ACL Attributes

Note By default, all traffic is denied by the ACE unless explicitly allowed. Only traffic that is explicitly allowed in an ACL can pass. All other traffic is denied.

You can configure an ACL that controls traffic based on its EtherType. An EtherType is a sub-protocol identifier. EtherType ACLs support Ethernet V2 frames. EtherType ACLs do not support 802.3-formatted frames because they use a length field as opposed to a type field. The only exception is bridge protocol data units (BPDUs), which are SNAP-encapsulated, and the ACE is designed to specifically handle BPDUs.

Procedure

Step 1 Choose **Config > Virtual Contexts >** *context* **> Security > ACLs**.

The ACLs table appears, listing the existing ACLs.

Step 2 Click **Add**.

The New Access List configuration screen appears.

Step 3 Enter the ACL name in the ACL Properties pane and choose Ethertype.

Note that the only selectable IP Address Type is IPv4.

Step 4 Choose one of the following radio buttons:

- **Deny** to indicate that the ACE is to block connections.
- **Permit** to indicate that the ACE is to allow connections.

Step 5 Choose one of the following from the Protocol field drop down menu for this ACL:

- Any—Specifies any EtherType.
- BPDU—Specifies Bridge Protocol Data Units. The ACE receives trunk port (Cisco proprietary) BPDUs because ACE ports are trunk ports. Trunk BPDUs have VLAN information inside the payload, so the ACE modifies the payload with the outgoing VLAN if you allow BPDUs. If you configure redundancy, you must allow BPDUs on both interfaces with an EtherType ACL to avoid bridging loops. For for information about configuring redundancy, refer to Configuring High Availability, page 11-1.
- IPv6—Specifies Internet Protocol version 6.

- MPLS—Specifies Multi-Protocol Label Switching. The MPLS selection applies to both MPLS unicast and MPLS multicast traffic. If you allow MPLS, ensure that Label Distribution Protocol (LDP) and Tag Distribution Protocol (TDP) TCP connections are established through the ACE by configuring both MPLS routers connected to the ACE to use the IP address on the ACE interface as the router-id for LDP or TDP sessions. LDP and TDP allow MPLS routers to negotiate the labels (addresses) used to forward packets.

Step 6 Click **Add To Table** and add one or more ACL entries if required repeating Step 4 and Step 5 as needed.

Step 7 Associate any VLAN interface to this acl if required and do one of the following:

- Click **Deploy** to immediately deploy this configuration.
- Click **Cancel** to exit without saving your entries and to return to the ACL Summary table.

Related Topics

- Configuring Security with ACLs, page 4-53
- Creating ACLs, page 4-54
- Setting Extended ACL Attributes, page 4-57
- Resequencing Extended ACLs, page 4-62
- Editing or Deleting ACLs, page 4-65

Viewing All ACLs by Context

Use this procedure to view all access control lists that have been configured.

Procedure

Step 1 Choose **Config > Virtual Contexts**.

The All Virtual Contexts table appears.

Step 2 Choose the virtual context with the ACLs you want to view, then select **Security > ACLs**.

The ACLs table appears, listing the existing ACLs with their name, their type (Extended or Ethertype), and any comments.

Related Topics

- Configuring Virtual Context Expert Options, page 4-75
- Creating ACLs, page 4-54
- Setting EtherType ACL Attributes, page 4-63
- Setting Extended ACL Attributes, page 4-57
- Editing or Deleting ACLs, page 4-65

Editing or Deleting ACLs

Use this procedure to delete or edit an ACL or any of its subentries.

Considerations

- You cannot mix IPv6 and IPv4 access-list entries in the same ACL.
- Before you change the IP address type for an existing ACL, you must remove the entries that are not applicable to the new IP address type.
- If you change the ACL protocol, the ACE removes all of the existing settings for the ACL.

Procedure

Step 1 Choose **Config > Virtual Contexts >** *context* **> Security > ACLs**.

The ACLs table appears, listing the existing ACLs.

Step 2 Click the radio button to the left of the ACL that you want to edit or delete.

Expand entries if necessary by clicking the plus sign to the left of any ACL entry until you see the subentry ACL for which you are looking, or click the **Expand All** icon to view all ACLs and subentries.

To hide the subentries under an ACL, click the minus sign to the left of any ACL entry. Click the **Collapse All** icon to hide the subentries under all ACLs.

Step 3 Do one of the following:

- Click **Edit** if you are editing an ACL or one of its entries. Edit the entry using the summary information listed in Table 4-14 if needed, and click **Deploy** when done.
- Click **Delete** if you are deleting an ACL or one of its entries. A window appears asking you to confirm the deletion. If you click **OK**, the ACLs table refreshes without the deleted ACL.

Related Topics

- Creating ACLs, page 4-54
- Setting EtherType ACL Attributes, page 4-63
- Setting Extended ACL Attributes, page 4-57
- Resequencing Extended ACLs, page 4-62

Displaying ACL Information and Statistics

You can display information and statistics for a particular ACL by using the **Details** button.

Procedure

Step 1 Choose **Config > Virtual Contexts >** *context* **> Security > ACLs**.

The ACLs table appears listing the existing ACLs.

Step 2 In the ACLs table, choose an ACL, and click **Details**.

The **show access-list** *access-list* **detail** CLI command output appears. For details about the displayed output fields, see the *Security Guide, Cisco ACE Application Control Engine*, Chapter 1, Configuring Security Access Control Lists.

Step 3 Click **Update Details** to refresh the output for the **show access-list** *access-list* **detail** CLI command.

Step 4 Click **Close** to return to the ACLs table.

Related Topics

- Configuring Virtual Context Expert Options, page 4-75
- Creating ACLs, page 4-54
- Setting Extended ACL Attributes, page 4-57
- Resequencing Extended ACLs, page 4-62
- Editing or Deleting ACLs, page 4-65

Configuring Object Groups

An object group is a logical grouping of objects such as hosts (servers and clients), services, and networks. When you create an object group, you select a type, such as network or service, and then specify the objects that belong to the groups. In all, there are four types of object groups: Network, protocol, service, and ICMP-type.

After you configure an object group, you can include it in ACLs, thereby including all objects within that group and reducing overall configuration size.

Use this procedure to configure object groups that you can associate with ACLs.

Procedure

Step 1 Choose **Config > Virtual Contexts >** *context* **> Security > Object Groups**.

The Object Groups table appears, listing existing object groups.

Step 2 Click **Add** to create a new object group, or select an existing object group, then click **Edit** to modify it.

The Object Groups configuration screen appears.

Step 3 In the Name field, enter a unique name for this object group.

Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters.

Step 4 In the Description field, enter a brief description for the object group.

Step 5 In the Type field, select the type of object group you are creating:

- **Network**—The object group is based on a group of hosts or subnet IP addresses.
- **Service**—The object group is based on TCP or UDP protocols and ports, or ICMP types, such as echo or echo-reply.

Step 6 Do one of the following:

- Click **Deploy Now** to immediately deploy this configuration. This option appears for virtual contexts. The screen refreshes with tables additional configuration options.
- Click **Cancel** to exit without saving your entries and to return to the Object Groups table.
- Click **Next** to deploy your entries and to add another entry to the Object Groups table.

Step 7 Configure objects for the object group.

For network-type object groups, options include:

- Configuring IP Addresses for Object Groups, page 4-67
- Configuring Subnet Objects for Object Groups, page 4-68

For service-type object groups, options include:

- Configuring Protocols for Object Groups, page 4-68
- Configuring TCP/UDP Service Parameters for Object Groups, page 4-69
- Configuring ICMP Service Parameters for an Object Group, page 4-72

Related Topics

- Configuring Virtual Context Expert Options, page 4-75
- Creating ACLs, page 4-54
- Setting Extended ACL Attributes, page 4-57
- Resequencing Extended ACLs, page 4-62

Configuring IP Addresses for Object Groups

Use this procedure to specify host IP addresses for network-type object groups.

Procedure

Step 1 Choose **Config > Virtual Contexts >** *context* **> Security > Object Groups**.

The Object Groups table appears, listing existing object groups.

Step 2 Choose the object group you want to configure host IP addresses for, then click the **Host Setting For Object Group** tab.

The Host Setting For Object Group table appears.

Step 3 Click **Add** to add an entry to this table.

Step 4 Choose one of the following:

- **IPv4**—A host with an IPv4 IP address. In the IPv4 Address field, enter the IP address of a host to include in this group.
- **IPv6**—A host with an IPv6 IP address. In the IPv6 Address field, enter the IP address of a host to include in this group.

Step 5 Do one of the following:

- Click **Deploy Now** to immediately deploy this configuration. This option appears for virtual contexts.
- Click **Cancel** to exit this procedure without saving your entries.
- Click **Next** to deploy your entries and to add another entry to the Host Setting table.

Related Topics

- Configuring Object Groups, page 4-66
- Configuring Subnet Objects for Object Groups, page 4-68
- Configuring Protocols for Object Groups, page 4-68
- Configuring TCP/UDP Service Parameters for Object Groups, page 4-69
- Configuring ICMP Service Parameters for an Object Group, page 4-72

Configuring Subnet Objects for Object Groups

Use this procedure to specify subnet objects for a network-type object group.

Procedure

Step 1 Choose **Config > Virtual Contexts >** *context* **> Security > Object Groups**.

The Object Groups table appears, listing existing object groups.

Step 2 Choose the object group you want to configure subnet objects for, then click the **Network Setting For Object Group** tab.

The Network Setting For Object Group table appears.

Step 3 Click **Add** to add an entry to this table.

Step 4 Choose one of the following:

- **IPv4**—A subnet object with an IPv4 IP address. In the IPv4 Address field, enter the IP address. In the Netmask field, select the subnet mask for this subnet object.
- **IPv6**—A object with an IPv6 IP address. In the IPv6 Address field, enter the IP address. In the Network Prefix Length field, enter the prefix length for this object.

Step 5 Do one of the following:

- Click **Deploy Now** to immediately deploy this configuration. This option appears for virtual contexts.
- Click **Cancel** to exit this procedure without saving your entries.
- Click **Next** to deploy your entries and to add another entry to the Network Setting table.

Related Topics

- Configuring Object Groups, page 4-66
- Configuring IP Addresses for Object Groups, page 4-67
- Configuring Protocols for Object Groups, page 4-68
- Configuring TCP/UDP Service Parameters for Object Groups, page 4-69
- Configuring ICMP Service Parameters for an Object Group, page 4-72

Configuring Protocols for Object Groups

Use this procedure to specify protocols for a service-type object group.

Procedure

Step 1 Choose **Config > Virtual Contexts >** *context* **> Security > Object Groups**.

The Object Groups table appears, listing existing object groups.

Step 2 Choose an existing service-type object group, then click the **Protocol Selection** tab.

The Protocol Selection table appears.

Step 3 Click **Add** to add an entry to this table.

Step 4 In the Protocol Number field, select the protocol or protocol number to add to this object group.

See Table 4-16 for common protocols and their numbers.

Step 5 Do one of the following:

- Click **Deploy Now** to immediately deploy this configuration. This option appears for virtual contexts.
- Click **Cancel** to exit this procedure without saving your entries.
- Click **Next** to deploy your entries and to add another entry to the Protocol Selection table.

Related Topics

- Configuring Object Groups, page 4-66
- Configuring IP Addresses for Object Groups, page 4-67
- Configuring Subnet Objects for Object Groups, page 4-68
- Configuring TCP/UDP Service Parameters for Object Groups, page 4-69
- Configuring ICMP Service Parameters for an Object Group, page 4-72

Configuring TCP/UDP Service Parameters for Object Groups

Use this procedure to add TCP or UDP service objects to a service-type object group.

Procedure

Step 1 Choose **Config > Virtual Contexts >** *context* **> Security > Object Groups**.

The Object Groups table appears, listing existing object groups.

Step 2 Choose an existing service-type object group, then select the TCP/UDP Service Parameters tab.

The TCP/UDP Service Parameters table appears.

Step 3 Click **Add** to add an entry to this table.

Step 4 Configure TCP or UDP service objects using the information in Table 4-19.

Table 4-19 TCP and UDP Service Parameters

Field	Description
Protocol	Select the protocol for this service object: • TCP—TCP is the protocol for this service object. • UDP—UDP is the protocol for this service object. • TCP And UDP—Both TCP and UDP are the protocols for this service object.
Source Port Operator	Select the operand to use when comparing source port numbers for this service object: • Equal To—The source port must be the same as the number in the Source Port field. • Greater Than—The source port must be greater than the number in the Source Port field. • Less Than—The source port must be less than the number in the Source Port field. • Not Equal To—The source port must not equal the number in the Source Port field. • Range—The source port must be within the range of ports specified by the Lower Source Port field and the Upper Source Port field.
Source Port	This field appears if you select Equal To, Greater Than, Less Than, or Not Equal To in the Source Port Operator field. Enter the source port name or number for this service object.
Lower Source Port	This field appears if you select Range in the Source Port Operator field. Enter the number that is the beginning value for a range of services for this service object. Valid entries are integers from 0 to 65535. The number in this field must be less than the number entered in the Upper Source Port field.
Upper Source Port	This field appears if you select Range in the Source Port Operator field. Enter the number that is the ending value for a range of services for this service object. Valid entries are integers from 0 to 65535. The number in this field must be greater than the number entered in the Lower Source Port field.
Destination Port Operator	Choose the operand to use when comparing destination port numbers: • Equal To—The destination port must be the same as the number in the Destination Port field. • Greater Than—The destination port must be greater than the number in the Destination Port field. • Less Than—The destination port must be less than the number in the Destination Port field. • Not Equal To—The destination port must not equal the number in the Destination Port field. • Range—The destination port must be within the range of ports specified by the Lower Destination Port field and the Upper Destination Port field.
Destination Port	This field appears if you select Equal To, Greater Than, Less Than, or Not Equal To in the Destination Port Operator field. Enter the destination port name or number for this service object.

Table 4-19 TCP and UDP Service Parameters (continued)

Field	Description
Lower Destination Port	This field appears if you select *Range* in the Destination Port Operator field. Enter the number that is the beginning value for a range of services for this service object. Valid entries are integers from 0 to 65535. The number in this field must be less than the number entered in the Upper Destination Port field.
Upper Destination Port	This field appears if you select *Range* in the Destination Port Operator field. Enter the number that is the ending value for a range of services for this service object. Valid entries are integers from 0 to 65535. The number in this field must be greater than the number entered in the Lower Destination Port field.

Step 5 Do one of the following:

- Click **Deploy Now** to immediately deploy this configuration. This option appears for virtual contexts.
- Click **Cancel** to exit this procedure without saving your entries.
- Click **Next** to deploy your entries and to add another entry to the TCP/UDP Service Parameters table.

Related Topics

- Configuring Object Groups, page 4-66
- Configuring IP Addresses for Object Groups, page 4-67
- Configuring Subnet Objects for Object Groups, page 4-68
- Configuring Protocols for Object Groups, page 4-68
- Configuring ICMP Service Parameters for an Object Group, page 4-72

Configuring ICMP Service Parameters for an Object Group

Use this procedure to add ICMP service parameters to a service-type object group.

Procedure

Step 1 Choose **Config > Virtual Contexts >** *context* **> Security > Object Groups**.

The Object Groups table appears, listing existing object groups.

Step 2 Choose an existing service-type object group, then click the **ICMP Service Parameters** tab.

The ICMP Service Parameters table appears.

Step 3 Click **Add** to add an entry to this table.

Step 4 Configure ICMP type objects using the information in Table 4-20.

Table 4-20 ICMP Type Service Parameters

Field	Description
ICMP Version	Check either of the following check boxes for the ICMP version: • ICMP—Internet Control Message Protocol (ICMP) for Internet Protocol version 4 (IPv4). • ICMPv6—Internet Control Message Protocol version 6 (ICMPv6) for Internet Protocol version 6 (IPv6).
ICMP Type	Select the ICMP type or number for this service object. Table 4-21 lists common ICMP types and numbers. Table 4-22 lists the ICMPv6 types and numbers.
Message Code Operator	Select the operand to use when comparing message codes for this service object: • Equal To—The message code must be the same as the number in the Message Code field. • Greater Than—The message code must be greater than the number in the Message Code field. • Less Than—The message code must be less than the number in the Message Code field. • Not Equal To—The message code must not equal the number in the Message Code field. • Range—The message code must be within the range of codes specified by the Min. Message Code field and the Max. Message Code field.
Message Code	This field appears if you select Equal To, Greater Than, Less Than, or Not Equal To in the Message Code Operator field. Enter the ICMP message code for this service object.

Table 4-20 ICMP Type Service Parameters (continued)

Field	Description
Min. Message Code	This field appears if you select Range in the Message Code Operator field. Enter the number that is the beginning value for a range of services for this service object. Valid entries are integers from 0 to 255. The number in this field must be less than the number entered in the Max. Message Code field.
Max. Message Code	This field appears if you select Range in the Message Code Operator field. Enter the number that is the ending value for a range of services for this service object. Valid entries are integers from 0 to 255. The number in this field must be greater than the number entered in the Min. Message Code field.

Table 4-21 ICMP Type Numbers and Names

ICMP Type Name	Number
Alternate-Address	6
Conversion-Error	31
Echo	8
Echo-Reply	0
Information-Reply	16
Information-Request	15
Mask-Reply	18
Mask-Request	17
Mobile-Redirect	32
Parameter-Problem	12
Redirect	5
Router-Advertisement	9
Router-Solicitation	10
Source-Quench	4
Time-Exceeded	11
Timestamp-Reply	14
Timestamp-Request	13
Traceroute	30
Unreachable	3

Table 4-22 ICMPv6 Type Names and Numbers

ICMP Type Name	Number
Echo	128
Echo-Reply	129

Table 4-22 ICMPv6 Type Names and Numbers (continued)

ICMP Type Name	Number
Information-Reply	140
Information-Request	139
Parameter-Problem	4
Redirect	137
Time-Exceeded	3
Traceroute	30
Unreachable	1

Step 5 Do one of the following:

- Click **Deploy Now** to immediately deploy this configuration. This option appears for virtual contexts.
- Click **Cancel** to exit this procedure without saving your entries.
- Click **Next** to deploy your entries and to add another entry to the ICMP Service Parameters table.

Related Topics

- Configuring Object Groups, page 4-66
- Configuring IP Addresses for Object Groups, page 4-67
- Configuring Subnet Objects for Object Groups, page 4-68
- Configuring Protocols for Object Groups, page 4-68
- Configuring TCP/UDP Service Parameters for Object Groups, page 4-69

Configuring Virtual Context Expert Options

Table 4-23 identifies ACE Appliance Device Manager virtual context Expert configuration options and related topics for more information.

Table 4-23 Virtual Context Expert Configuration Options

Expert Configuration Options	Related Topics
Establish traffic policies by classifying types of network traffic and then applying rules and actions for handling the traffic	• Configuring Traffic Policies, page 12-1 • Configuring Virtual Context Class Maps, page 12-8 • Configuring Virtual Context Policy Maps, page 12-34
Configure HTTP header modify action lists	Configuring an HTTP Header Modify Action List, page 12-89
Configure HTTP optimization action lists	Configuring an HTTP Optimization Action List, page 13-3

Managing Virtual Contexts

You can perform the following administrative actions on virtual contexts:

- Synchronizing Virtual Context Configurations, page 4-75
- Editing Virtual Contexts, page 4-80
- Deleting Virtual Contexts, page 4-80
- Viewing All Virtual Contexts, page 4-80

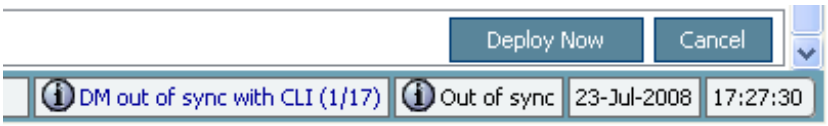
Synchronizing Virtual Context Configurations

ACE Appliance Device Manager identifies virtual contexts with different configurations on the ACE appliance and in ACE Appliance Device Manager. Discrepancies between these configurations occur when a user configures the ACE appliance directly using the CLI instead of the ACE Appliance Device Manager.

The ACE Appliance Device Manager automatically polls the CLI once every two minutes. When you use the CLI to change a virtual context's configuration on the ACE appliance, and the Device Manager detects an out-of-band configuration change in a context during this polling period, the configuration changes are applied by the Device Manager.

The status bar at the bottom right of the ACE Appliance Device Manager displays two indicators for you to monitor CLI and DM GUI synchronization status (Figure 4-1). One indicator displays ACE appliance Device Manager GUI and CLI synchronization status along with a summary count of the contexts in the various synchronization states, and the other indicator displays CLI synchronization and polling status for the active context. The status bar auto-refreshes every 10 seconds.

Figure 4-1 CLI and DM GUI Synchronization Status Bar



For example, as illustrated in Figure 4-1, the message "DM out of sync with CLI (1/17)" indicates that out of the 17 configured contexts, one context is in the "Out of sync" CLI synchronization status state.

Note If a user attempt to deploy a configuration from the ACE Appliance Device Manager (clicks the Deploy Now button) while synchronization is in process for a particular context, an error message appears indicating that synchronization is in process and the user should try to deploy the configuration at a later point in time.

ACE Appliance Device Manager provides the following options for identifying and synchronizing configuration discrepancies:

- Viewing Virtual Context Synchronization Status, page 4-76
- High Availability and Virtual Context Configuration Status, page 4-77
- Manually Synchronizing Individual Virtual Context Configurations, page 4-78
- Manually Synchronizing All Virtual Context Configurations, page 4-79

Viewing Virtual Context Synchronization Status

ACE Appliance Device Manager identifies virtual contexts with different configurations in the ACE appliance and in the ACE Appliance Device Manager. Discrepancies between these configurations occur when a user configures the ACE appliance directly using the CLI instead of ACE Appliance Device Manager.

In Config screens, CLI and DM GUI configuration status appears in the following locations in the ACE Appliance Device Manager:

- In the All Virtual Contexts table (**Config > Virtual Contexts**), in the CLI Sync Status column.
- The status bar at the bottom of the ACE Appliance Device Manager browser (see Figure 4-1).

The following reported CLI synchronization states appear in the All Virtual Context table:

- OK—The configurations for the selected virtual context are synchronized with the CLI.
- Out Of Sync—The configurations for the selected virtual context are not synchronized with the CLI.
- Sync In Progress—The CLI to DM GUI synchronization for this context is in process, either started automatically by the ACE Appliance Device Manager or manually (using either the CLI Sync or CLI Sync All buttons).

- Sync Failed—The last synchronization attempt failed and you must perform a manual synchronization using either the CLI Sync or CLI Sync All buttons. The failed state could be due to an unrecognized CLI command on the context, or due to an internal error on the ACE Appliance Device Manager. Once the problem is resolved, another manual synchronization will be required to move the context into the OK synchronization state.

The status bar at the bottom of the ACE Appliance Device Manager browser (see Figure 4-1) displays DM GUI and CLI synchronization status along with a summary count of the contexts in the various synchronization states. For example, the message "DM out of sync with CLI (1/10), DM sync with CLI failed (2/10)" indicates that out of the 10 configured contexts, one context is in the "Out Of Sync" state and two are is the "Sync Failed" state, and the remaining contexts are in the "OK" state. The status bar auto-refreshes every 10 seconds.

Note Clicking the summary count in the status bar from any context-specific page accesses the All Virtual Contexts table. You can view the CLI synchronization status for all contexts.

If a user changes the configuration for a context by using the CLI while you are viewing the All Virtual Contexts table, the information in the CLI Sync Status column does not automatically update to reflect an out-of-sync state. Click **Refresh** or set an automatic refresh rate by clicking **Auto Refresh** to view out-of-sync configurations.

For information on synchronizing out-of-sync virtual context configurations, see:

- Manually Synchronizing Individual Virtual Context Configurations, page 4-78
- Manually Synchronizing All Virtual Context Configurations, page 4-79

Related Topics

- Synchronizing Virtual Context Configurations, page 4-75
- High Availability and Virtual Context Configuration Status, page 4-77

High Availability and Virtual Context Configuration Status

In a high availability pair, the two configured virtual contexts synchronize with each other as part of their ongoing communications. However, their copies do not synchronize in ACE Appliance Device Manager and the configuration on the standby member can become out of sync with the configuration on the ACE appliance.

After the active member of a high availability pair fails and the standby member becomes active, ACE Appliance Device Manager on the newly active member detects any out-of-sync virtual context configurations and reports that status in the All Virtual Contexts table so that you can synchronize the virtual context configurations.

Note When a virtual context is in either the Standby Hot or Standby Warm state (see High Availability Polling, page 11-2), the virtual context may receive configuration changes from its ACE peer without updating the Device Manager GUI. As a result, the ACE appliance Device Manager GUI will be out of synchronization with the CLI configuration. If you need to check configuration on a standby virtual context using HA Tracking And Failure Detection (see Tracking VLAN Interfaces for High Availability, page 11-19), we recommend that you first perform a manual synchronization using either the CLI Sync or CLI Sync All buttons before checking the configuration values.

For information on synchronizing out-of-sync virtual context configurations, see:

- Manually Synchronizing Individual Virtual Context Configurations, page 4-78
- Manually Synchronizing All Virtual Context Configurations, page 4-79

Related Topics

- Viewing Virtual Context Synchronization Status, page 4-76
- Configuring ACE High Availability, page 11-8

Manually Synchronizing Individual Virtual Context Configurations

Use this procedure if you want to manually synchronize the configuration for a selected virtual context. This procedure removes the configuration information for this virtual context from ACE Appliance Device Manager and replaces it with its CLI configuration from the ACE appliance. You may want to manually synchronize a virtual context configuration if you do not want to wait for auto synchronization to occur and you want the CLI context configuration changes immediately applied to the ACE Appliance Device Manager.

Procedure

Step 1 Choose **Config > Virtual Contexts**.

The All Virtual Contexts table appears. Contexts with configurations that are not synchronized display *Out of sync* in the CLI Sync Status column.

Note If a user changes the configuration for a context by using the CLI while you are viewing the All Virtual Contexts table, the information in the CLI Sync Status column is not automatically updated to reflect an out-of-sync state. Click **Refresh** or set an automatic refresh rate by clicking **Auto Refresh** to view out-of-sync configurations.

Step 2 Choose the virtual context with the configuration that you want to synchronize, then click **CLI Sync**.

A window appears, asking you to confirm the operation.

Step 3 Click **OK** to upload the configuration from the ACE appliance or **Cancel** to exit this procedure without uploading the configuration.

If you click **OK**, the screen reports progress and then refreshes with updated configuration status in the CLI Sync Status column.

Related Topics

- Synchronizing Virtual Context Configurations, page 4-75
- Viewing Virtual Context Synchronization Status, page 4-76
- Manually Synchronizing All Virtual Context Configurations, page 4-79

Manually Synchronizing All Virtual Context Configurations

Use this procedure to manually synchronize all virtual context configurations. This procedure removes all virtual context configurations from ACE Appliance Device Manager and replaces them with their CLI configurations from the ACE appliance. You may want to manually synchronize all virtual contexts if you do not want to wait for auto-synchronization to occur and you want the CLI context configuration changes immediately applied to the ACE Appliance Device Manager.

This operation can take several minutes to finish, depending on the number of virtual contexts.

Note If you configure a virtual server using the CLI and then use the CLI Sync All option (**Config > Virtual Contexts**) to manually synchronize configurations, the configuration that appears in ACE Appliance Device Manager for the virtual server might not display all configuration options for that virtual server. The configuration that appears in ACE Appliance Device Manager depends on a number of items, such as the protocols configured in class maps or the rules defined for policy maps.

For example, if you configure a virtual server on the CLI that includes a class map that can match any protocol, you will not see the virtual server Application Acceleration and Optimization configuration subset in ACE Appliance Device Manager.

Note This procedure is available for only the admin user in an Admin context.

Procedure

Step 1 Choose **Config > Virtual Contexts**.

The All Virtual Contexts table appears.

Step 2 Click **CLI Sync All**. A window appears, asking you to confirm the operation.

Step 3 Click **OK** to continue with this option or click **Cancel** to exit this procedure.

If you click **OK**, the screen refreshes with the All Virtual Contexts table listing the contexts that have been imported so far and displays configuration update progress.

Note Depending on the number of contexts, this process can take several minutes to complete.

Step 4 Click **Refresh** to view additional contexts that have been imported.

Related Topic

- Synchronizing Virtual Context Configurations, page 4-75
- Manually Synchronizing Individual Virtual Context Configurations, page 4-78

Editing Virtual Contexts

Use this procedure to modify the configuration of an existing virtual context.

Procedure

Step 1 Choose **Config > Virtual Contexts**.

The All Virtual Contexts table appears.

Step 2 Choose the virtual context, then select the configuration attributes you want to modify.

For information on configuration options, see Configuring Virtual Contexts, page 4-7.

Step 3 Click **Deploy Now** to deploy this configuration on the ACE appliance.

To exit a procedure without saving your entries, click **Cancel**, or select another item in the menu bar or another attribute to configure. A window appears, confirming that you have not saved your entries.

Related Topic

- Using Virtual Contexts, page 4-2

Deleting Virtual Contexts

Use this procedure to remove an existing virtual context.

Procedure

Step 1 Choose **Config > Virtual Contexts**.

The All Virtual Contexts table appears.

Step 2 Chose the virtual context you want to remove, then click **Delete**.

A window appears, asking you to confirm the deletion.

Step 3 Do one of the following:

- Click **OK** to delete the selected context. The device tree refreshes and the deleted context no longer appears.
- Click **Cancel** to exit this procedure and to retain the selected context.

Related Topic

- Using Virtual Contexts, page 4-2

Viewing All Virtual Contexts

To view all virtual contexts, select **Config > Virtual Contexts**. The All Virtual Contexts table appears.

Note Clicking the summary count in the status bar from any context-specific page accesses the All Virtual Contexts table. You can then review the synchronization configuration details for all of the available contexts. If you are not the administrator, you will only see the details for your user context.

The All Virtual Contexts table displays the following information for each virtual context

- Name
- Resource class
- Management IP address
- Virtual context synchronization status; that is, whether the ACE Appliance Device Manager GUI and CLI configurations for the context are synchronized, not synchronized, being synchronized, or the synchronization attempt failed. For more information, see Viewing Virtual Context Synchronization Status, page 4-76.
- ACE high availability state; for more information on the available ACE high availability states, see High Availability Polling, page 11-2.

Note For information on the implication of ACE high availability on ACE appliance Device Manager GUI and CLI configuration synchronization, see Synchronizing High Availability Configurations with ACE Appliance Device Manager, page 11-6.

- State of the ACE high availability peer
- ACE high availability peer name
- Whether automatic synchronization for high availability pairs has been configured

Note If a user changes the configuration for a context by using the CLI while you are viewing the All Virtual Contexts table, or if the high availability state changes, the information in the table columns does not automatically update to reflect an out-of-sync state. Click **Refresh** or set an automatic refresh rate by clicking **Auto Refresh** to view out-of-sync configurations.

Note If a user creates a new virtual context in a different session while you are viewing the All Virtual Contexts table, the new virtual context does not automatically appear in this table. Click **Refresh** or set an automatic refresh rate by clicking **Auto Refresh** to view newly-created contexts.

Polling status for the selected context appears above the content area in the upper right corner (see Figure 1-2). Table 14-1 describes the various polling states.

From this screen you can:

- Add a new virtual context—See Creating Virtual Contexts, page 4-2.
- Edit an existing virtual context—See Configuring Virtual Contexts, page 4-7.
- Delete an existing virtual context—See Deleting Virtual Contexts, page 4-80.
- Manually synchronize ACE Appliance Device Manager and CLI configurations for one or all virtual contexts—See Synchronizing Virtual Context Configurations, page 4-75.

Related Topic

Managing Virtual Contexts, page 4-75