CHAPTER 2

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.

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 2-2
- Configuring Virtual Contexts, page 2-4
- Deleting Virtual Contexts, page 2-48

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 6-5.

Procedure

Step 1 Select **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 2-1.

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

Table 2-1 Virtual Context Configuration Attributes

Field	Description
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.
Resource Class	Select the resource class this virtual context is to use.
Allocate-Interface 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.
Description	Enter a brief description of the virtual context.

Table 2-1 Virtual Context Configuration Attributes (continued)

Field	Description
Policy Name	For new a new management VLAN, enter a name for the management policy. This field is read-only for existing contexts.
VLAN to use	Enter the VLAN that is to be used for remote management of the context.
Management IP	Enter the IP address that is to be used for remote management of the context. **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 VLAN Interface Policy Map Use" section on page 5-5.
Management Netmask	Select the subnet mask to apply to this IP address.
Protocols to Allow	Select the protocols to allow on this VLAN: • HTTP—Specifies the Hypertext Transfer Protocol (HTTP). • HTTPS—Specifies the secure (SSL) Hypertext Transfer Protocol (HTTP) for connectivity with the ACE Appliance Device Manager interface. • ICMP—Specifies the Internet Control Message Protocol (ICMP), commonly referred to as ping. • SNMP—Specifies the Simple Network Management Protocol (SNMP). **Note** If SNMP is not selected, the ACE Appliance Device Manager will not be able to poll the context. • SSH—Specifies a Secure Shell (SSH) connection to the ACE appliance. • TELNET—Specifies a Telnet connection to the ACE appliance. • KALAP UDP—Specifies the Keepalive Appliance Protocol over UDP. • XML-HTTPS—Specifies HTTPS as the transfer protocol for sending and receiving XML documents between the ACE appliance and a Network Management System (NMS). You can select multiple protocols by holding down the Shift key while selecting protocols.
Default Gateway IP	Enter the IP address of the default gateway. Use a comma-separated list to specify multiple IP addresses, 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 appliance appear in this field.
SNMP v2c Community	If SNMP is one of the allowed protocols, enter the SNMP version 2c community string to be used. **Note** If SNMP is not an allowed protocol, the ACE Appliance Device Manager will not be able to poll the context.

Step 4 Click

- **Deploy Now** to deploy this virtual context. To configure other virtual context attributes, see Configuring Virtual Contexts, page 2-4.
- **Cancel** to exit this procedure without saving your entries and to return to the All Virtual Contexts table.

Related Topics

- Using Virtual Contexts, page 2-1
- Configuring Virtual Contexts, page 2-4

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 2-2 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 6-5.

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 2-2 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 options. • Global policy map configuration for all VLANs on a virtual context. • ACE appliance license use on the ACE appliance. • Resource classes for allocation of ACE appliance resources. • Application acceleration and optimization on the ACE appliance. **Note** ACE appliance licenses, resource classes, and acceleration and optimization can be configured only in an Admin context.	• Configuring Virtual Context Primary Attributes, page 2-7 • Configuring Virtual Context Syslog Logging, page 2-8 • Configuring SNMP for Virtual Contexts, page 2-15 • Configuring Virtual Context Global Traffic Policies, page 2-22 • Managing ACE Appliance Licenses, page 2-23 • Managing Resource Classes, page 2-29 • Configuring Global Application Acceleration and Optimization, page 8-9
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, and implement sticky groups for session persistence. Load-balancing configuration options include: • Virtual servers • Real servers • Server farms • Health monitoring • Sticky attributes • Parameter maps	• Configuring Load Balancing, page 3-1 • Configuring Virtual Servers, page 3-4 • Configuring Server Farm Load Balancing, page 3-47 • Configuring Health Monitoring for Real Servers, page 3-57 • Configuring Load Balancing Using Sticky Groups, page 3-80 • Using Parameter Maps, page 3-85
SSL	SSL configuration options allow you to import and export SSL certificates and keys, set up SSL parameter maps and chain group parameters, and generate certificate signing requests for submission to a certificate authority.	• Configuring SSL, page 4-1 • Using SSL Certificates, page 4-2 • Using SSL Keys, page 4-5 • Generating CSRs, page 4-16 • Configuring SSL Parameter Maps, page 4-12 • Configuring SSL Chain Group Parameters, page 4-13 • Configuring SSL Proxy Service, page 4-16

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

Configuration Subset	Description	Related Topics
Security	Security configuration options allow you to create access control lists, set ACL attributes, resequence ACLs, and delete ACLs.	• Configuring Security with ACLs, page 2-36 • Configuring ACLs, page 2-37
Network	Network configuration options allow you to configure: • Port channel interfaces • Gigabit Ethernet interfaces • VLAN interfaces • BVI interfaces • Static routes **Note** You can configure port channel and gigabit Ethernet interfaces only in an Admin context.	• Configuring Port Channel Interfaces, page 5-10 • Configuring Gigabit Ethernet Interfaces, page 5-12 • Configuring Virtual Context VLAN Interfaces, page 5-1 • Configuring Virtual Context BVI Interfaces, page 5-14 • Configuring Virtual Context Static Routes, page 5-15
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 6-1 • Configuring High Availability Peers, page 6-6 • Configuring High Availability Groups, page 6-10
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 6-14 • Tracking VLAN Interfaces for High Availability, page 6-15 • Tracking Hosts for High Availability, page 6-16
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.	• Configuring Traffic Policies, page 7-1 • Configuring Action Lists, page 8-3

Configuring Virtual Context System Attributes

Table 2-3 identifies the ACE Appliance Device Manager virtual context System configuration options and related topics for more information.

Table 2-3 Virtual Context System Configuration Options

System Configuration Options	Related Topics
Specify virtual context primary attributes	Configuring Virtual Context Primary Attributes, page 2-7
Configure syslog options	• Configuring Virtual Context Syslog Logging, page 2-8 • Configuring Syslog Log Hosts, page 2-12 • Configuring Syslog Log Messages, page 2-13 • Configuring Syslog Log Rate Limits, page 2-14
Configure SNMP options	• Configuring SNMP for Virtual Contexts, page 2-15 • Configuring SNMP Version 2c Communities, page 2-16 • Configuring SNMP Version 3 Users, page 2-17 • Configuring SNMP Trap Destination Hosts, page 2-19 • Configuring SNMP Notification, page 2-20
Establish global policy maps for all VLANs on a virtual context	Configuring Virtual Context Global Traffic Policies, page 2-22
Manage ACE appliance licenses	Managing ACE Appliance Licenses, page 2-23
Manage ACE appliance resources across virtual contexts	Managing Resource Classes, page 2-29
Establish application acceleration and optimization for the ACE appliance	Configuring Global Application Acceleration and Optimization, page 8-9

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 2-4.

Use this procedure to configure virtual context primary attributes.

Procedure

Step 1 Select **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 2-1.

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 2-1
- Configuring Virtual Context VLAN Interfaces, page 5-1
- Configuring Virtual Context BVI Interfaces, page 5-14
- Configuring Virtual Context Syslog Logging, page 2-8
- Configuring Traffic Policies, page 7-1

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 Select **Config > Virtual Contexts >** ***context*** **> System > Syslog**. The Syslog configuration screen appears.

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

All fields that require you to select syslog severity levels use the values in Table 2-4.

Table 2-4 Syslog Logging Levels

Severity	Description
Emergency	Unusable system
Alert	Immediate action required
Critical	Critical condition
Error	Error condition
Warning	Warning condition
Notification	Normal but significant condition
Information	Informational message only
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 2-5 Virtual Context Syslog Configuration Attributes

Field	Description	Action
Enable Syslog	This option indicates whether syslog logging should be enabled or disabled.	Select 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.	Select 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.
History Level	This option specifies the maximum level for system log messages sent as traps to an SNMP network management station.	Select 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 Notification, page 2-20.

Table 2-5 Virtual Context Syslog Configuration Attributes (continued)

Field	Description	Action
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.	Select 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.	Select 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.
Enable Fastpath Logging	This option indicates whether connection setup and teardown messages are logged.	Select 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.

Table 2-5 Virtual Context Syslog Configuration Attributes (continued)

Field	Description	Action
Reject New Connection when TCP Queue Full	This option indicates whether the ACE appliance rejects new connections when the TCP queue is full.	Select the check box to reject new connections when the syslog daemon can no longer reach the TCP syslog server. Clear the check box to disable this feature. This option is disabled by default.
Reject New Connection when Rate Limit Reached	This option indicates whether the ACE appliance rejects new connections when the syslog message rate is reached.	Select the check box to reject new connections when the syslog message rate is reached. Clear the check box to disable this feature. This option is disabled by default.
Reject New Connection when Control Plane Buffer Full	This option indicates whether the ACE appliance rejects new connections when the syslog daemon buffer is full.	Select the check box to reject new connections when the syslog daemon buffer is full. 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: • Undefined—Indicates that no identifier is to be used. • 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. • Hostname—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. • Any String—Indicates that a test string is to be used to uniquely identify syslog messages send from the ACE appliance.
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 2-12
- Configuring Syslog Log Messages, page 2-13
- Configuring Syslog Log Rate Limits, page 2-14

Related Topics

- Configuring Virtual Contexts, page 2-4
- Configuring Syslog Log Hosts, page 2-12
- Configuring Syslog Log Messages, page 2-13
- Configuring Syslog Log Rate Limits, page 2-14

Configuring Syslog Log Hosts

After configuring basic syslog characteristics (see Configuring Virtual Context Syslog Logging, page 2-8), 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 hosts.

Procedure

Step 1 Select **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 IP 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 1024 to 65535; the default is 514.

Step 7 The Default UDP check box appears if TCP is selected in the Protocol field (Step 5). Select 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. 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:

- 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.
- N/A—Indicates that you do not want to enable EMBLEM-format logging.

Step 9 Click:

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

Related Topics

- Configuring Virtual Context Syslog Logging, page 2-8
- Configuring Syslog Log Messages, page 2-13
- Configuring Syslog Log Rate Limits, page 2-14

Configuring Syslog Log Messages

After configuring basic syslog characteristics (see Configuring Virtual Context Syslog Logging, page 2-8), 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 Select **Config > Virtual Contexts >** ***context*** **> System > Syslog**. The Syslog configuration screen appears.

Step 2 Select 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 Select 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 select 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 2-4.

Step 7 Click:

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

Related Topics

- Configuring Virtual Context Syslog Logging, page 2-8
- Configuring Syslog Log Hosts, page 2-12
- Configuring Syslog Log Rate Limits, page 2-14

Configuring Syslog Log Rate Limits

After configuring basic syslog characteristics (see Configuring Virtual Context Syslog Logging, page 2-8), 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 Select **Config > Virtual Contexts >** ***context*** **> System > Syslog**. The Syslog configuration screen appears.

Step 2 Select 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:

- Select **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.
- Select **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 2-4.

Step 5 Select 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:

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.

b. In the Time Interval 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 field, the ACE appliance limits the creation of syslog messages that are sent to a maximum of 42 messages in that 60-second period.

Step 7 Click:

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

Related Topics

- Configuring Virtual Contexts, page 2-4
- Configuring Virtual Context Syslog Logging, page 2-8
- Configuring Syslog Log Hosts, page 2-12
- Configuring Syslog Log Messages, page 2-13

Configuring SNMP for Virtual Contexts

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

Procedure

Step 1 Select **Config > Virtual Contexts >** ***context*** **> System > SNMP**. The SNMP configuration screen appears.

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

Table 2-6 SNMP Attributes

Field	Description
Contact Info	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.
VLAN Interface	Select the associated VLAN that identifies the interface from which SNMP traps originate. N/A indicates that an interface is not specified.
IETF Trap	Select 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 2-16
- Configuring SNMP Version 3 Users, page 2-17
- Configuring SNMP Trap Destination Hosts, page 2-19
- Configuring SNMP Notification, page 2-20

Related Topic

Configuring Virtual Contexts, page 2-4

Configuring SNMP Version 2c Communities

After configuring basic SNMP information for a virtual context (see Configuring SNMP for Virtual Contexts, page 2-15), 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 2-15).

Procedure

Step 1 Select **Config > Virtual Contexts >** ***context*** **> System > SNMP**. The SNMP configuration screen appears.

Step 2 Select the SNMP v2c Community tab. The SNMP v2c Community table appears.

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

- **Deploy Now** to deploy this configuration on the ACE appliance.
- **Cancel** to exit this procedure without saving your entry and to return to the SNMP v2c Community table.
- **Next** 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 2-4
- Configuring SNMP Version 3 Users, page 2-17
- Configuring SNMP Trap Destination Hosts, page 2-19
- Configuring SNMP Notification, page 2-20

Configuring SNMP Version 3 Users

After configuring basic SNMP information for a virtual context (see Configuring SNMP for Virtual Contexts, page 2-15), 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 2-15).

Procedure

Step 1 Select **Config > Virtual Contexts >** ***context*** **> System > SNMP**. The SNMP configuration screen appears.

Step 2 Select 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 2-7).

Table 2-7 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.
Auth Algorithm	Select the authentication algorithm to be used for this user. • N/A—Indicates that no authentication is to be used. • MD5—Indicates that Message Digest 5 is to be used as the authentication mechanism. • SHA—Indicates that Secure Hash Algorithm is to be used as the authentication mechanism.
Auth Password	Appears if you select an authentication algorithm. Enter the authentication password for this user. Valid entries are unquoted text strings with no spaces and a maximum of 130 alphanumeric characters. The ACE appliance automatically updates the password for the CLI user with the SNMP authentication password.
Confirm	Appears if you select an authentication algorithm. Reenter the authentication password.

Table 2-7 SNMP v3 User Configuration Attributes (continued)

Field	Description
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.
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. This password can have a minimum of 8 characters. If the passphrases are specified in clear text, you can enter a maximum of 64 alphanumeric characters. If use of a localized key is enabled, you can enter a maximum of 130 alphanumeric characters. Spaces are not allowed.
Confirm	Appears if you set Privacy to True. Reenter the privacy password.

Step 5 Click:

- **Deploy Now** to deploy this configuration on the ACE appliance.
- **Cancel** to exit this procedure without saving your entries and to return to the SNMP v3 Configuration table.
- **Next** 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 2-4
- Configuring SNMP Version 2c Communities, page 2-16
- Configuring SNMP Trap Destination Hosts, page 2-19
- Configuring SNMP Notification, page 2-20

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 Notification, page 2-20.

After configuring basic SNMP information for a virtual context (see Configuring SNMP for Virtual Contexts, page 2-15), 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 2-15).

Procedure

Step 1 Select **Config > Virtual Contexts >** ***context*** **> System > SNMP**. The SNMP configuration screen appears.

Step 2 Select 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 2-8.

Table 2-8 SNMP Trap Destination Host Configuration Attributes

Field	Description
IP Address	Enter the IP address of the server that is to receive SNMP notifications. Enter the address in dotted-decimal format, such as 192.168.11.1.
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.

Table 2-8 SNMP Trap Destination Host Configuration Attributes (continued)

Field	Description
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 Click:

- **Deploy Now** to deploy this configuration on the ACE appliance.
- **Cancel** to exit this procedure without saving your entries and to return to the Trap Destination Host table.
- **Next** 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 2-4
- Configuring SNMP Version 2c Communities, page 2-16
- Configuring SNMP Version 3 Users, page 2-17
- Configuring SNMP Notification, page 2-20

Configuring SNMP Notification

After configuring basic SNMP information for a virtual context (see Configuring SNMP for Virtual Contexts, page 2-15), 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 2-19.
- 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 2-15).
- At least one SNMP server host has been configured (see Configuring SNMP Trap Destination Hosts, page 2-19).

Procedure

Step 1 Select **Config > Virtual Contexts >** ***context*** **> System > SNMP**. The SNMP configuration screen appears.

Step 2 Select 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, select the type of notifications to be sent to the SNMP host. Some options are available only in the Admin context.

- License—Indicates that SNMP license notifications are to be sent. This option is available only in the Admin context.
- Virtual-context—Indicates that notifications are to be sent upon changes to a virtual context. This option is available only in the Admin context.
- Slb—Indicates that server load-balancing notifications are to be sent.
- Slb real—Indicates that notifications of real server state changes are to sent.
- Slb vserver—Indicates that notifications of virtual server state changes are to be sent.
- SNMP—Indicates that SNMP notifications are to be sent.
- SNMP authentication—Indicates that notifications of incorrect community strings in SNMP requests are to be sent.
- SNMP coldstart—Indicates that SNMP agent restart notifications are to be sent after a cold restart (full power cycle) of the ACE appliance. This option is available only in the Admin context.
- SNMP linkdown—Indicates that notifications are to be sent when a VLAN interface is down.
- SNMP linkup—Indicates that notifications are to be sent when a VLAN interface is up.
- Syslog—Indicates that error message notifications (Cisco Syslog MIB) are to be sent.

Step 5 Click:

- **Deploy Now** to deploy this configuration on the ACE appliance.
- **Cancel** to exit this procedure without saving your selection and to return to the SNMP Notification table.
- **Next** 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 2-4
- Configuring SNMP Version 2c Communities, page 2-16
- Configuring SNMP Version 3 Users, page 2-17

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 7-1.

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 7-27.

Procedure

Step 1 Select **Config > Virtual Contexts >** ***context*** **> System > Global Policy**. 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 Map field, select the policy map that you want to apply to all VLANs in this context.

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

Step 5 Click:

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

Related Topics

- Using Virtual Contexts, page 2-1
- Configuring Virtual Context Primary Attributes, page 2-7
- Configuring Virtual Context VLAN Interfaces, page 5-1
- Configuring Virtual Context Syslog Logging, page 2-8
- Configuring Traffic Policies, page 7-1

Managing ACE Appliance Licenses

Note This functionality is available for only Admin contexts.

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

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

Related Topics

- Viewing ACE Appliance Licenses, page 2-23
- Installing ACE Appliance Licenses, page 2-25
- Uninstalling ACE Appliance Licenses, page 2-26
- Updating ACE Appliance Licenses, page 2-27
- Displaying License Configuration and Statistics, page 2-28

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 Select **Config > Virtual Contexts**. The All Virtual Context table appears.

Step 2 Select the Admin context whose ACE appliance licenses you want to view, then click **System > Licenses**. The License table appears listing all installed licenses.

Related Topics

- Managing ACE Appliance Licenses, page 2-23
- Installing ACE Appliance Licenses, page 2-25
- Uninstalling ACE Appliance Licenses, page 2-26
- Updating ACE Appliance Licenses, page 2-27
- Displaying License Configuration and Statistics, page 2-28

Importing ACE Appliance Licenses

Note This functionality is available for only Admin contexts.

Installing ACE appliance licenses involves two steps:

1. Importing the license from a remote server onto the ACE appliance.
2. Installing the license on the ACE appliance. See Installing ACE Appliance Licenses, page 2-25.

Use this procedure to import new or upgrade ACE appliance licenses from a remote server onto the ACE appliance.

Assumption

ACE appliance licenses are available on a remote server for importing to the ACE appliance.

Procedure

Step 1 Select **Config > Virtual Contexts**. The All Virtual Contexts table appears.

Step 2 Select the Admin context you want to import a license for, then click **System > Licenses**. The License table appears listing all installed licenses.

Step 3 Click **Import License**. The Import License File dialog box appears.

Step 4 In the Protocol field, select the protocol to be used to import the license file from the remote server to the ACE appliance:

- If you select FTP, the User and Password fields appear. Continue with Step 5.
- If you select SFTP, the User and Password fields appear. Continue with Step 5.
- If you select TFTP, continue with Step 6.

Step 5 If you select FTP or SFTP:

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

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

Step 6 In the Source File Name field, enter the host IP address, path, and filename of the license file on the remote server in the format *host-ip/path/filename* where:

- *host-ip* represents the IP address of the remote server.
- *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 `192.168.11.2/usr/bin/ACE-VIRT-020.lic`.

Step 7 In the Destination field, enter the location where you want the license file to reside on the ACE appliance in preparation for installation or updating. The default location is disk0:.

Step 8 Click:

- **OK** to accept your entries and to import the file from the remote server to the ACE appliance. When the file has been imported, the License table appears, and you can continue with installing or upgrading licenses. See Installing ACE Appliance Licenses, page 2-25.
- **Cancel** to exit this procedure without importing the file from the remote server and to return to the License table.

Related Topics

- Managing ACE Appliance Licenses, page 2-23
- Installing ACE Appliance Licenses, page 2-25
- Uninstalling ACE Appliance Licenses, page 2-26
- Updating ACE Appliance Licenses, page 2-27
- Displaying License Configuration and Statistics, page 2-28

Installing ACE Appliance Licenses

Note This functionality is available for only Admin contexts.

Installing ACE appliance licenses involves two steps:

1. Importing the license from a remote server to the ACE appliance. See Importing ACE Appliance Licenses, page 2-24.
2. Installing the license on the ACE appliance.

Use this procedure to install a license on an ACE appliance.

Assumption

You have received the software license key for an ACE appliance and have imported the license file onto ACE appliance.

Procedure

Step 1 Select **Config > Virtual Contexts**. The All Virtual Contexts table appears.

Step 2 Select the Admin context for the new license, then click **System > Licenses**. The License table appears listing all installed licenses.

Step 3 Click **Install**. The Install License dialog box appears.

Step 4 In the File field, enter the name of the license file that you have imported and are now installing, such as `ACE-VIRT-020.lic`.

Step 5 In the License File Name field, enter the name that you would like to use for this license file, such as `myACE-VIRT-020.lic`.

Step 6 Click:

- **OK** to accept your entries and to install the license. When the license is installed, the License table refreshes with the new entry.
- **Cancel** to exit this procedure without installing the license and to return to the License table.

Related Topics

- Managing ACE Appliance Licenses, page 2-23
- Viewing ACE Appliance Licenses, page 2-23
- Uninstalling ACE Appliance Licenses, page 2-26
- Updating ACE Appliance Licenses, page 2-27
- Displaying License Configuration and Statistics, page 2-28

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 *Cisco Application Control Engine Module Administration Guide*.

Use this procedure to remove ACE appliance licenses.

Procedure

Step 1 Select **Config > Virtual Contexts**. The All Virtual Contexts table appears.

Step 2 Select the Admin context with the license you want to remove, then click **System > Licenses**. The License table appears listing all installed licenses.

Step 3 Select the license to be removed.

Step 4 Click **Uninstall**. A window 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 License table refreshes without the deleted license.

Related Topics

- Managing ACE Appliance Licenses, page 2-23
- Installing ACE Appliance Licenses, page 2-25
- Viewing ACE Appliance Licenses, page 2-23
- Updating ACE Appliance Licenses, page 2-27
- Displaying License Configuration and Statistics, page 2-28

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.

Updating ACE appliance licenses involves two steps:

1. Importing the new license from a remote server onto the ACE appliance. See Importing ACE Appliance Licenses, page 2-24.
2. Installing the update license on the ACE appliance.

Use this procedure to install ACE appliance update licenses.

Procedure

Step 1 Select **Config > Virtual Contexts**. The All Virtual Contexts table appears.

Step 2 Select the Admin context with the license you want to update, then click **System > Licenses**. The License table appears listing all installed licenses.

Step 3 Select the license to be updated, then click **Update**. The Update License window appears.

Step 4 In the License File Name field, enter the name that you gave the license file on the ACE appliance when you installed it, such as `myACE-VIRT-020.lic`. (See Installing ACE Appliance Licenses, page 2-25.)

Step 5 Click:

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

Related Topics

- Managing ACE Appliance Licenses, page 2-23
- Installing ACE Appliance Licenses, page 2-25
- Viewing ACE Appliance Licenses, page 2-23
- Uninstalling ACE Appliance Licenses, page 2-26
- Displaying License Configuration and Statistics, page 2-28

Displaying License Configuration and Statistics

Note This functionality is available for only Admin contexts.

Use this procedure to view information about ACE appliance licenses.

Procedure

Step 1 Select **Config > Virtual Contexts**. The All Virtual Contexts table appears.

Step 2 Select the Admin context with the license information you want to view, then select **System > Licenses**. The License table appears listing all installed licenses.

Step 3 Select the license with the information you want to view, then click **Status**. The Show License Status window appears with the following information:

- Compression performance in megabits or gigabits per second
- Web optimization in the number of connections per second
- SSL transactions per second
- Number of supported virtual contexts
- ACE appliance bandwidth in gigabits per second

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

Related Topics

- Installing ACE Appliance Licenses, page 2-25
- Updating ACE Appliance Licenses, page 2-27

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
- Buffers for syslog messages and TCP out-of-order (OOO) segments
- Concurrent connections (through-the-ACE traffic)
- Management connections (to-the-ACE traffic)
- Proxy connections
- Set resource limit as a rate (number per second)
- Regular expression (regexp) memory
- SSL connections
- Sticky entries
- Static or dynamic network address translations (Xlates)

Table 2-9 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 mgmt-traffic
- rate ssl-connections
- rate connections
- mgmt-connections
- conc-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 2-9 Resource Class Attributes

Resource	Definition
Default	Indicates that the default percentage is to be used for any resource parameter not explicitly set.
acc-connections	Percentage of application acceleration connections.
acl-memory	Percentage of memory allocated for ACLs.
conc-connections	Percentage of simultaneous connections. **Note** If you consume all conc-connections by allocating 100% to virtual contexts, IP connectivity to the Admin context can be lost.
http-comp	Percentage of compression for HTTP data.
mgmt-connections	Percentage of management connections. **Note** If you consume all mgmt-connections by allocating 100% to virtual contexts, IP connectivity to the Admin context can be lost.
proxy-connections	Percentage of proxy connections.
regexp	Percentage of regular expression memory.
sticky	Percentage of entries in the sticky table. **Note** You must configure a minimum value for sticky to allocate resources for sticky entries; the sticky software receives no resources under the unlimited setting.
xlates	Percentage of network and port address translations entries.
buffer syslog	Percentage of the syslog buffer.
rate inspect-conn	Percentage of application protocol inspection connections for FTP and RTSP.

Table 2-9 Resource Class Attributes (continued)

Resource	Definition
rate bandwidth	Percentage of context throughput. This attribute limits the total ACE appliance 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 appliance supports 1 gigabit per second (Gbps) appliance throughput. You can upgrade the ACE appliance with an optional 2-Gbps bandwidth license. When you configure a minimum bandwidth value for a resource class in the ACE appliance, the ACE appliance subtracts that configured value from the total bandwidth maximum value of all contexts in the ACE appliance, 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 appliance 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. • mgmt-traffic—Limits management (to-the-ACE appliance) 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 > *context* > System > Resource Class**). When you allocate a minimum percentage of bandwidth to management traffic, the ACE appliance subtracts that value from the maximum available management traffic bandwidth for all contexts in the ACE appliance.
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 mgmt-traffic	Percentage of management traffic connections. **Note** If you consume all rate mgmt-traffic by allocating 100% to virtual contexts, IP connectivity to the Admin context can be lost.
rate ssl-connections	Percentage of SSL connections. **Note** If you consume all rate ssl-connections by allocating 100% to virtual contexts, IP connectivity to the Admin context can be lost.
rate syslog	Percentage of syslog messages per second.
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.

Related Topics

- Adding Resource Classes, page 2-32
- Modifying Resource Classes, page 2-33
- Deleting Resource Classes, page 2-34
- Viewing Resource Class Use on Virtual Contexts, page 2-35

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 2-29.

Use this procedure to create a new resource class.

Procedure

Step 1 Select **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 In the Description field, enter a brief description for this resource class. Valid entries are unquoted text strings with a maximum of 240 alphanumeric characters.

Step 5 To use the same values for each resource, enter the following information in the Default row: (See Table 2-9 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, select 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 6 To use different values for the resources, for each resource, select the method for allocating resources:

- Select **Default** to use the values specified in Step 5.

- Select **Min** to enter a specific minimum value for the resource.

Step 7 If you select Min:

a. 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% of the available ACL memory to this resource class.

b. In the Max field, select 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 8 When you finish allocating the resources for this resource class, click:

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

Step 9 If you click **Deploy Now**, 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, select the resource class, click **Edit**, and modify it as described in this procedure.

Related Topics

- Managing Resource Classes, page 2-29
- Modifying Resource Classes, page 2-33
- Deleting Resource Classes, page 2-34
- Viewing Resource Class Use on Virtual Contexts, page 2-35

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 2-29.

Use this procedure to modify an existing resource class.

Note You cannot modify the default resource class.

Procedure

Step 1 Select **Config > Virtual Contexts >** ***admin_context*** **> System > Resource Class**. The Resource Classes table appears.

Step 2 Select 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 2-32. For descriptions of the resources, see Table 2-9.

Step 4 When you finish allocating the resources for this resource class, 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.
- **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 2-29
- Adding Resource Classes, page 2-32
- Modifying Resource Classes, page 2-33
- Deleting Resource Classes, page 2-34
- Viewing Resource Class Use on Virtual Contexts, page 2-35

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 2-35.

Procedure

Step 1 Select **Config > Virtual Contexts >** ***admin_context*** **> System > Resource Class**. The Resource Classes table appears.

Step 2 Select 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 2-29
- Adding Resource Classes, page 2-32
- Modifying Resource Classes, page 2-33
- Viewing Resource Class Use on Virtual Contexts, page 2-35

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 Select **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 Select 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 2-29
- Adding Resource Classes, page 2-32
- Modifying Resource Classes, page 2-33
- Deleting Resource Classes, page 2-34
- Viewing Resource Class Use on Virtual Contexts, page 2-35

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 appliance 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 appliance 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 entries to an ACL already in the merged list 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 Telnet 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 ACE appliances unless explicitly allowed. Only traffic that is explicitly allowed in an ACL can pass. All other traffic is denied.

Note When configuring an ACL, you must add entries. ACLs do not take effect unless entries are included.

For specific procedures, see:

- Configuring ACLs, page 2-37
- Setting EtherType ACL Attributes, page 2-38
- Setting Extended ACL Attributes, page 2-39
- Resequencing Extended ACLs, page 2-42
- Deleting ACLs, page 2-43

Configuring ACLs

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

Note When configuring an ACL, you must add entries. The ACE appliance does not recognize ACLs that do not contain entries.

Use this procedure to configure ACLs.

Procedure

Step 1 Select **Config > Virtual Contexts >** ***context*** **> Security > ACLs**. The ACLs table appears, listing the existing ACLs.

Step 2 Click **Add** to create an ACL, or select an existing ACL, then click **Edit**. The ACL configuration screen appears.

Step 3 In the Name field, enter a unique identifier for the ACL in the form of an unquoted text string with a maximum of 64 characters.

Step 4 In the Type field, select the type of ACL:

- Extended—Indicates that this ACL is used to control network access for IP traffic and to identify addresses for policy Network Address Translation (NAT).
- EtherType—Indicates that this ACL is used to control network access for non-IP traffic.

Step 5 If you select Extended, in the Remark field, enter any comments you want to include about this ACL. Valid entries are unquoted text strings with a maximum of 100 alphanumeric characters. You can enter leading spaces at the beginning of the text. Trailing spaces are ignored.

Step 6 Click:

- **Deploy Now** to deploy this configuration on the ACE appliance. Continue with Setting EtherType ACL Attributes, page 2-38 or Setting Extended ACL Attributes, page 2-39.
- **Cancel** to exit this procedure without saving your entries and to return to the ACLs table.
- **Next** to save your entries and to add another ACL.

Related Topics

- Configuring Security with ACLs, page 2-36
- Setting EtherType ACL Attributes, page 2-38
- Setting Extended ACL Attributes, page 2-39
- Resequencing Extended ACLs, page 2-42
- Deleting ACLs, page 2-43

Setting EtherType ACL Attributes

Note By default, all traffic is denied by ACE appliances 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 appliance is designed to specifically handle BPDUs.

Procedure

Step 1 Select **Config > Virtual Contexts >** ***context*** **> Security > ACLs**. The ACLs table appears, listing the existing ACLs.

Step 2 Select the EtherType ACL whose attributes you want to configure. The EtherType table appears below the ACLs table. If the table does not appear, click **Show Tabs** above the ACLs table.

Step 3 In the EtherType table, click **Add** to configure EtherType attributes. The EtherType configuration screen appears.

Note You cannot modify an existing entry in the EtherType table. Instead, delete the existing entry, then create a new one.

Step 4 In the Protocol field, select the protocol for this ACL:

- Any—Specifies any EtherType.
- BPDU—Specifies Bridge Protocol Data Units. The ACE appliance receives trunk port (Cisco proprietary) BPDUs because ACE appliance ports are trunk ports. Trunk BPDUs have VLAN information inside the payload, so the ACE appliance 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 6-1.
- 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 appliance by configuring both MPLS routers connected to the ACE appliance to use the IP address on the ACE appliance 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 5 In the Permit field, select the check box to indicate that the ACE appliance is to allow connections. Clear the check box to indicate that the ACE appliance is to block connections.

Step 6 Click:

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

- **Cancel** to exit without saving your entries and to return to the EtherType table.
- **Next** to save your entries and to configure another EtherType ACL.

Related Topics

- Configuring Security with ACLs, page 2-36
- Configuring ACLs, page 2-37
- Setting Extended ACL Attributes, page 2-39
- Resequencing Extended ACLs, page 2-42
- Deleting ACLs, page 2-43

Setting Extended ACL Attributes

Note By default, all traffic is denied by ACE appliances 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 appliance allows all returning traffic for established connections.

Note The ACE appliance 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 Select **Config > Virtual Contexts >** ***context*** **> Security > ACLs**. The ACLs table appears, listing the existing ACLs.

Step 2 Select the extended ACL whose attributes you want to configure. The Extended table appears below the ACLs table. If the table does not appear, click **Show Tabs** above the ACLs table.

Step 3 In the Extended table, click **Add** to add a new entry, or select an existing entry, then click **Edit** to modify it. The Extended configuration screen appears.

Step 4 In the Line No. field, 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. If you do not specify a line number for an entry, the ACE appliance applies a default increment and a line number to the entry and appends it to the end of the ACL. To change the sequence of existing extended ACLs, see Resequencing Extended ACLs, page 2-42.

Step 5 In the Protocol field, select the protocol or protocol number to apply to this ACL entry. (See Table 2-10.)

Table 2-10 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
IGMP	2	Internet Group Management Protocol
IP	0	Internet Protocol
IP-in-IP	4	IP-in-IP Layer 3 Tunneling Protocol
OSPF	89	Open Shortest Path First
PIM	103	Protocol Independent Multicast
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.html.

Step 6 Select the Permit check box to indicate that the ACE appliance is to allow connections. Clear the check box to indicate that the ACE appliance is to block connections.

Step 7 Select the Any Source check box to specify network traffic from any source. Clear the Any Source check box to specify network traffic from a specific IP address.

Step 8 If you clear the Any Source check box, provide the source IP information in one of the following ways:

- For a single source IP address, enter a specific IP address in the Source IP Address field and select its subnet mask in the Source Netmask field.
- For a range of source IP addresses, select the appropriate subnet mask in the Source Netmask field.

Step 9 If you select TCP or UDP, the Source Port Operator field appears. Use this field to select the operand to use when comparing source port numbers:

- Eq—Indicates that the source port must be the same as the number in the Source Port Number field.
- Gt—Indicates that the source port must be greater than the number in the Source Port Number field.
- Lt—Indicates that the source port must be less than the number in the Source Port Number field.
- Neq—Indicates that the source port must not equal the number in the Source Port Number field.
- Range—Indicates that 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.

Step 10 For TCP and UDP only, enter the following source port information:

- If you select *Lt*, *Gt*, *Eq*, or *Neq* in the Source Port Operator field, the Source Port Number field appears. In the Source Port Number field, enter the port name or number from which you want to permit or deny access.

- If you select *Range* in the Source Port Operator field, the Lower Source Port Number field and the Upper Source Port Number field appear. Enter the following information:
  - In the Lower Source Port Number 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.
  - In the Upper Source Port Number field, enter the port number of the upper port from which you want to permit or deny access. Valid entries are integers from 1 to 65535. The number in this field must be greater than the number entered in the Lower Source Port Number field.

Step 11 Select the Any Destination check box to specify network traffic intended for any IP address. Clear the Any Destination check box to specify network traffic intended for a specific IP address.

Step 12 If you clear the Any Destination check box, provide the destination IP information in one of the following ways:

- For a single destination IP address, enter the IP address in the Destination IP Address field and select its subnet mask in the Destination Netmask field.
- For a range of destination IP addresses, select the appropriate subnet mask in the Destination Netmask field.

Step 13 If you select TCP or UDP, the Destination Port Operator field appears. Use this field to select the operand to use when comparing destination port numbers:

- Eq—Indicates that the destination port must be the same as the number in the Destination Port Number field.
- Gt—Indicates that the destination port must be greater than the number in the Destination Port Number field.
- Lt—Indicates that the destination port must be less than the number in the Destination Port Number field.
- Neq—Indicates that the destination port must not equal the number in the Destination Port Number field.
- Range—Indicates that 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.

Step 14 For TCP and UDP only, enter the following destination port information:

- If you select *Lt*, *Gt*, *Eq*, or *Neq* in the Destination Port Operator field, the Destination Port Number field appears. In the Destination Port Number field, enter the port name or number to which you want to permit or deny access.
- If you select *Range* in the Destination Port Operator field, the Lower Destination Port Number field and the Upper Destination Port Number field appear. Enter the following information:
  - In the Lower Destination Port Number 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.
  - In the Upper Destination Port Number field, enter the port number of the upper port to which you want to permit or deny access. Valid entries are integers from 1 to 65535. The number in this field must be greater than the number entered in the Lower Destination Port Number field.

Step 15 Click:

- **Deploy Now** to deploy this configuration on the ACE appliance.
- **Cancel** to exit without saving your entries and to return to the Extended table.
- **Next** to save your entries and to configure another Extended ACL.

Related Topics

- Configuring Security with ACLs, page 2-36
- Configuring ACLs, page 2-37
- Setting EtherType ACL Attributes, page 2-38
- Resequencing Extended ACLs, page 2-42
- Deleting ACLs, page 2-43

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 Select **Config > Virtual Contexts >** ***context*** **> Security > ACLs**. The ACLs table appears, listing the existing ACLs.

Step 2 Select the Extended ACL you want to renumber, then click **Resequence**. 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. You can enter any integer.

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. The default is 10.

Step 5 Click:

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

Related Topics

- Configuring Security with ACLs, page 2-36
- Configuring ACLs, page 2-37
- Setting EtherType ACL Attributes, page 2-38
- Setting Extended ACL Attributes, page 2-39
- Deleting ACLs, page 2-43

Viewing All ACLs by Context

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

Procedure

Step 1 Select **Config > Virtual Contexts**. The All Virtual Contexts table appears.

Step 2 Select 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 Security with ACLs, page 2-36
- Configuring ACLs, page 2-37
- Setting EtherType ACL Attributes, page 2-38
- Setting Extended ACL Attributes, page 2-39
- Deleting ACLs, page 2-43

Deleting ACLs

Use this procedure to delete an ACL.

Procedure

Step 1 Select **Config > Virtual Contexts > *context* > Security > ACLs**. The ACLs table appears, listing the existing ACLs.

Step 2 Select the ACL you want to delete, then click **Delete**. A window appears, asking you to confirm the deletion.

Step 3 Click **OK** to delete the ACL or **Cancel** to retain the ACL. If you click **OK**, the ACLs table refreshes without the deleted ACL.

Related Topics

- Configuring ACLs, page 2-37
- Setting EtherType ACL Attributes, page 2-38
- Setting Extended ACL Attributes, page 2-39
- Resequencing Extended ACLs, page 2-42

Configuring Virtual Context Expert Options

Table 2-11 identifies ACE Appliance Device Manager virtual context Expert configuration options and related topics for more information.

Table 2-11 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 7-1 • Configuring Virtual Context Class Maps, page 7-12 • Configuring Virtual Context Policy Maps, page 7-27
Configure optimization action lists	Configuring Action Lists, page 8-3

Managing Virtual Contexts

You can perform the following administrative actions on virtual contexts:

- Synchronizing Virtual Context Configurations, page 2-45
- Editing Virtual Contexts, page 2-48
- Deleting Virtual Contexts, page 2-48
- Viewing All Virtual Contexts, page 2-44

Viewing All Virtual Contexts

To view all virtual contexts, select **Config > Virtual Contexts**. The All Virtual Contexts table appears with the following information for each virtual context:

- Name
- Resource class
- Management IP address
- Configuration status; that is, whether the ACE Appliance Device Manager and CLI configurations for the context are synchronized or not. For more information, see Viewing Virtual Context Configuration Status, page 2-45.

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 Config 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.

- High availability state; for more information on the available high availability states, see High Availability Polling, page 6-5.
- State of the high availability peer

- High availability peer name
- Whether automatic synchronization for high availability pairs has been configured

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 9-1 describes the various polling states.

From this screen you can:

- Add a new virtual context—See Creating Virtual Contexts, page 2-2.
- Edit an existing virtual context—See Configuring Virtual Contexts, page 2-4.
- Delete an existing virtual context—See Deleting Virtual Contexts, page 2-48.
- Synchronize ACE Appliance Device Manager and CLI configurations for one or all virtual contexts—See Synchronizing Virtual Context Configurations, page 2-45.

Related Topic

Managing Virtual Contexts, page 2-44

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.

For example, if you use the CLI to change a virtual context's configuration on the ACE appliance, the changes are not immediately applied to the configuration maintained by ACE Appliance Device Manager. Instead, the configurations are different until a user next accesses that virtual context using ACE Appliance Device Manager.

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

- Viewing Virtual Context Configuration Status, page 2-45
- High Availability and Virtual Context Configuration Status, page 2-46
- Synchronizing Individual Virtual Context Configurations, page 2-46
- Synchronizing All Virtual Context Configurations, page 2-47

Viewing Virtual Context Configuration Status

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 ACE Appliance Device Manager.

In Config screens, configuration status appears in one of two places:

- In the All Virtual Contexts table (**Config > Virtual Contexts**), in the Config Status column.
- In other tables or configuration screens, in the upper right corner above the content area (see Figure 1-2).

The reported configuration states are:

- OK—The configurations for the selected virtual context are synchronized.
- Out of sync—The configurations for the selected virtual context are not synchronized.

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 Config 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.

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

- Synchronizing Individual Virtual Context Configurations, page 2-46
- Synchronizing All Virtual Context Configurations, page 2-47

Related Topics

- Synchronizing Virtual Context Configurations, page 2-45
- High Availability and Virtual Context Configuration Status, page 2-46

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.

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

- Synchronizing Individual Virtual Context Configurations, page 2-46
- Synchronizing All Virtual Context Configurations, page 2-47

Related Topics

- Viewing Virtual Context Configuration Status, page 2-45
- Configuring High Availability Overview, page 6-4

Synchronizing Individual Virtual Context Configurations

Use this procedure to 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.

Procedure

Step 1 Select **Config > Virtual Contexts**. The All Virtual Contexts table appears. Contexts with configurations that are not synchronized display *Out of sync* in the Config 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 Config 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 Select the virtual context with the configuration that you want to synchronize, then click **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 Config Status column.

Related Topics

- Synchronizing Virtual Context Configurations, page 2-45
- Viewing Virtual Context Configuration Status, page 2-45
- Synchronizing All Virtual Context Configurations, page 2-47

Synchronizing All Virtual Context Configurations

Use this procedure to 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. 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 Sync All option (**Config > Virtual Contexts**) to 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 Select **Config > Virtual Contexts**. The All Virtual Contexts table appears.

Step 2 Click **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 2-45
- Synchronizing Individual Virtual Context Configurations, page 2-46

Editing Virtual Contexts

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

Procedure

Step 1 Select **Config > Virtual Contexts**. The All Virtual Contexts table appears.

Step 2 Select the virtual context, then select the configuration attributes you want to modify. For information on configuration options, see Configuring Virtual Contexts, page 2-4.

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 2-1

Deleting Virtual Contexts

Use this procedure to remove an existing virtual context.

Procedure

Step 1 Select **Config > Virtual Contexts**. The All Virtual Contexts table appears.

Step 2 Select the virtual context you want to remove, then click **Delete**. A window appears, asking you to confirm the deletion.

Step 3 Click:

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

Related Topic

- Using Virtual Contexts, page 2-1