CHAPTER 15

Managing the ACE Appliance

The following sections describe how to manage the ACE appliance using ACE Appliance Device Manager:

For details on logging into ACE Appliance Device Manager, see Logging into ACE Appliance Device Manager, page 1-4.

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

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

Overview of the Admin Functions

Use the Admin tab to manage role-based access control, set up and view statistical data for the ACE appliance, and use troubleshooting tools for the ACE Appliance Device Manager.

Note Some of the Admin options might not be visible to some users; the roles assigned to your login determine which options are available.

Table 15-1 describes the options that are displayed when you click **Admin**.

Table 15-1 Admin Menu Options

Menu	Option	Description	Reference
Role-Based Access Control	Users	Manage users and their access to their context	See Managing Users, page 15-7
	Active Users	Display or end session for active users	See Displaying Current User Sessions, page 15-11 or Ending Active User Sessions, page 15-12
	Roles	Manage user's access to commands and resources	See Managing User Roles, page 15-14
	Domains	Manage an association between a select group of context users and a select group of context objects.	See Managing Domains, page 15-31
Device Management		Check the status of the ACE Appliance Device Manager	See Monitoring ACE Appliance Statistics, page 15-35
Tools		Report a problem to the Cisco support line and generate a diagnostic package, access files from the ACE appliance for viewing or tracking, and replace all virtual context configurations with the CLI configurations from the ACE appliance	See Using ACE Appliance Device Manager Troubleshooting Tools, page 16-1

Related Topics

- Managing the ACE Appliance, page 15-1
- Controlling Access to the Cisco ACE Appliance, page 15-3

Controlling Access to the Cisco ACE Appliance

Access to ACE Appliance Device Manager is controlled using the same username and password that access the ACE appliance. This enables authentication to a local database or to an external RADIUS, TACACS+, or LDAP server. If you choose to authenticate using AAA and not the local database, you must configure AAA using the CLI. For details on setting up remote authentication using AAA servers, see the *Security Guide, Cisco ACE Application Control Engine*.

Note The ACE supports local user authentication using a local database on the ACE or through remote authentication using one or more AAA servers. AAA remote servers are grouped into independent groups of TACACS+, RADIUS, or LDAP servers. Authentication allows you to control user access to the ACE by requiring specification of a valid username and password, or no password verification. When you configure the ACE appliance from the CLI to support the user authentication and accounting functions, the Device Manager honors the tasks that are performed by the specified remote server. See the *Security Guide, Cisco ACE Application Control Engine* for details about authentication and accounting.

In addition, the role and domains that a user is associated with on a remote server will also honored by the Device Manager.

The ACE Appliance Device Manager does not configure AAA; instead, it uses role-based access control for access to features. When a user logs into the system, the specific tasks they can perform and areas of the system they can use are controlled by *contexts*, *roles*, and *domains*. If you need to restrict a user's access, you must first assign a role-domain pair.

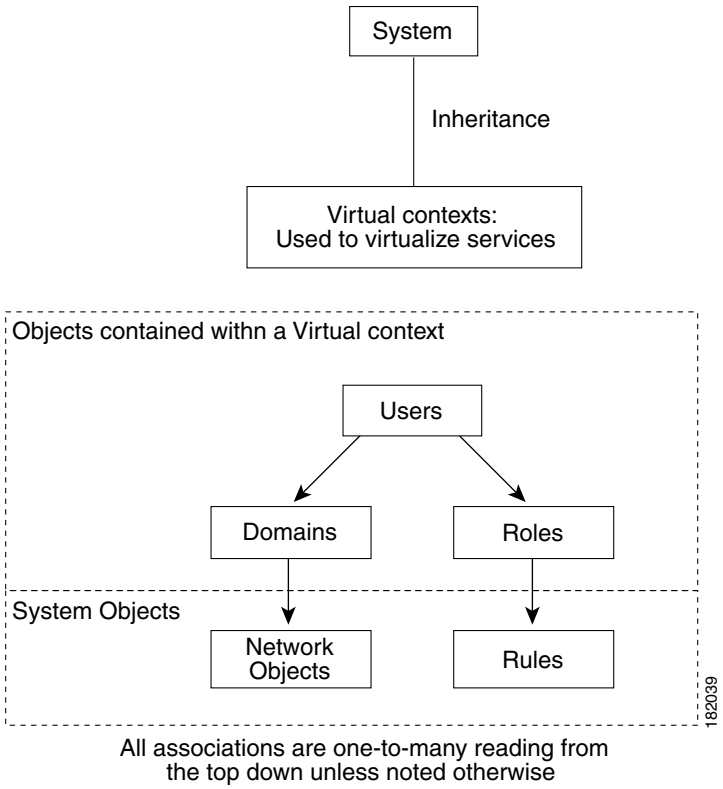
The role assigned to a user defines the tasks a user can perform and the items in the hierarchy that they can see. Roles are either predefined or set up by the system administrator. Each role, user, and domain is associated with a context. Only roles and domains associated with the Admin context can see other contexts. See Understanding Roles, page 15-5 for more information.

A domain is a collection of managed objects. When a user is given access to a domain, this acts as a filter for a subset of objects on the network which are displayed as a virtual context. The types of objects in the system that are domain controlled are as follows:

- All objects listed below
- Access list—Ethertype
- Access list—Extended
- Class-map
- Interface VLAN
- Interface BVI
- Parameter-map
- Policy-map
- Probe
- Real server
- Script
- Server farm
- Sticky

Thus, role-based access control ensures that users can view only the devices or services or perform the actions that are included in the domains to which they have been given access.

Figure 15-1 Role-Based Access Control Containment Overview



The following is an example of role-based access control containment.

Domains		
East Coast servers	Central servers	West Coast servers
Role		
Web server administrator		
Users		
User A	User B	User C
Note Each association is one-to-many.		

All other user interfaces, such as configuration, monitoring, and administration, respect this role-based access control policy:

- Roles limit the screens (or functions on those screens) that a user can see.
- Domains limit the objects that are listed on any screen that the roles allow.
- Users (other than the administrator) can create only subdomains of the domains to which they are assigned. However, no parent/child relationship is kept between domains.
- The system administrator user (Admin) can see and modify all objects. All other users are subject to the role-based access controls illustrated in Figure 15-1.

Related Topics

- Types of Users, page 15-5
- Understanding Roles, page 15-5
- Understanding Operations Privileges, page 15-6
- Understanding Domains, page 15-7
- Managing Users, page 15-7

Types of Users

Two types of users configure and monitor the ACE appliance:

- Default user—Individuals associated with the data center or IT department where the ACE appliance is installed. The default administrative account (user ID **admin**) is a system user account that is preconfigured on the system. The admin user password is previously set when the system was installed. You can change the password for the admin user account in the same manner as any user password (see Managing Users, page 15-7).

  Predefined system roles are specified in terms of roles, domains, and operations privileges. Each role can work with a specific set of operations and domains in a context.

- Assigned users—Users to whom you want to grant access to ACE appliance. You can assign users limited access by selecting roles and domains to which they belong. Users are not allowed to change to other contexts and can work with a specific set of operations and domains in the context in which they were created.

Related Topics

- Managing Users, page 15-7
- Guidelines for Managing Users, page 15-8
- Displaying a List of Users, page 15-8
- Creating User Accounts, page 15-8

Understanding Roles

User roles determine the privileges that a user has, the features they can access, and the actions they can take in a particular context.

Cisco ACE appliance provides a set of predefined roles (see Table 15-2 on page 15-9). Additional roles can also be defined by the system administrator. Roles are specified in terms of resource types and operations privileges known as rules. For each role, rules provide permissions about which resource types a role can work with and what operations a role can perform on each resource type.

Each user is assigned one role (Network-Monitor is the default) and inherit the operations privileges specified for each of the rules assigned to that role. Users are assigned one role. Each role can have different access privileges (in the form of rules) that are independent of other assigned roles.

The options a user sees in the menu are filtered according to that user's role.

Note If you need to restrict a user's access, you must assign a role-domain pair. Otherwise, no matter what roles the user may have, that user will not be able to access any specific resources, and, therefore, will have no powers on the system.

All users are strictly limited by the combination of their contexts, roles, and domains. For example, a user cannot create another user who has greater privileges or access or is outside their domain.

Roles cannot be deleted if they are currently referenced by a user. The predefined roles cannot be changed or deleted.

Related Topics

- Guidelines for Managing User Roles, page 15-14
- Role Mapping in ACE Appliance Device Manager, page 15-19
- Displaying User Roles, page 15-28
- Creating User Roles, page 15-28
- Modifying User Roles, page 15-30
- Deleting User Roles, page 15-30

Understanding Operations Privileges

Operations privileges define what users can do in the designated context. There are two levels of access. The first level is the permit or deny permission. The second level is the operations privilege the user is permitted or denied from performing. For example, each feature on the ACE appliance has an assigned privilege. If a user's privileges are not sufficient, the feature will not be available to them. The following operations privileges can be permitted or denied from least to greatest privilege levels:

- Monitor—Allows the user to view statistics and specify parameter collection.
- Modify—Allows the user to change the persistent information associated with system objects, such as a configuration.
- Debug—Allows the user to collect information on existing problems.
- Create—Allows the user to control system objects, for example, creating them, enabling them, or powering up; also has delete permission.

Privileges are hierarchical. If a user has Modify privileges, they have Monitor privileges as well. If a user has Create or Debug privileges, they have Modify privileges as well. Only Admin has Resource Class Mgmt access.

Note The ability to create automatically contains the modify function, but the reverse is not true (a user with modify privileges cannot automatically create items).

Related Topics

- Guidelines for Managing User Roles, page 15-14
- Role Mapping in ACE Appliance Device Manager, page 15-19
- Managing User Roles, page 15-14

Understanding Domains

Cisco ACE appliance provides a predefined default domain that contains all objects. You cannot modify or delete the predefined domain. Additional domains can be defined by the system administrator. A domain is a collection of managed objects to which a user is given access. By setting up a customized domain, you are filtering a subset of objects on the network. The user is then given access to this domain.

For example, a user can see only what is in the domain to which they have access (achieved through row filtering). If the default domain contains 50 objects and the customized domain, dom1, consists of the following domain objects: Rserver rs1, Rserver rs2, Serverfarm sf1, Serverfarm sf2, and Accesslist extended acl1, a user associated with domain dom1, can see only those five objects within the whole context.

The rows a user sees in any table are filtered according to the domain to which that user has access.

Note If you need to restrict a user's access, you must assign a role-domain pair. Otherwise, no matter what roles the user may have, that user will not be able to access any specific resources, and, therefore, will have no powers on the system.

Related Topics

- Managing Domains, page 15-31
- Guidelines for Managing Domains, page 15-31

Managing Users

Use the Role-Based Access Control feature to specify the people that are allowed to log onto the system. The following sections describe how to manage user accounts:

- Guidelines for Managing Users, page 15-8
- Displaying a List of Users, page 15-8
- Creating User Accounts, page 15-8
- Modifying User Accounts, page 15-10
- Deleting User Accounts, page 15-10
- Displaying Current User Sessions, page 15-11

Note The ACE supports local user authentication using a local database on the ACE or through remote authentication using one or more AAA servers. AAA remote servers are grouped into independent groups of TACACS+, RADIUS, or LDAP servers. Authentication allows you to control user access to the ACE by requiring specification of a valid username and password, or no password verification. When you configure the ACE appliance from the CLI to support the user authentication and accounting functions, the Device Manager honors the tasks that are performed by the specified remote server. See the *Security Guide, Cisco ACE Application Control Engine* for details about authentication and accounting.

In addition, the role and domains that a user is associated with on a remote server will also honored by the Device Manager.

Guidelines for Managing Users

- For users that you create in the Admin context, the default scope of access is for the entire ACE.
- If you do not assign a role to a new user, the default user role is Network-Monitor. For users that you create in other contexts, the default scope of access is the entire context.
- Users cannot log in until they are associated with a domain and a user role.
- You cannot delete roles and domains that are associated with an existing user.

Displaying a List of Users

Procedure

Step 1 Select **Admin > Role-Based Access Control > Users**. The Users table appears with the following fields:

- Name
- Expiry Date
- Role
- Domains

Step 2 You can use the options in this screen to create a new user or modify or delete any existing user to which you have access (see Table 15-2).

Related Topics

- Creating User Accounts, page 15-8
- Deleting User Accounts, page 15-10
- Managing Users, page 15-7
- Guidelines for Managing Users, page 15-8

Creating User Accounts

Note Your user role determines whether you can use this option.

Procedure

Step 1 Select **Admin > Role-Based Access Control > Users**. A list of users appears in the Users table.

Step 2 Click **Add**.

Step 3 Complete the following required fields (unless otherwise noted):

Table 15-2 User Attributes

Field	Description
Name	Specifies the name by which the user is to be identified in the system (up to 24 characters). Only letters, numbers, and underscore can be used. The field is case sensitive.
Expiry Date[1]	Date the user name is usable in the system.
Password Entered As	Specifies whether the password is entered as Clear Text or Encrypted.
Password	Allows you to specify a password for this user account. Password must be at least 8 characters long.
Confirm	Ensures password is keyed in properly.
Role	Specifies the definition of what a user can do in this system. Choose from the following options or create your own role: • Admin • Network-Admin • Network-Monitor • Security-Admin • Server-Appln-Maintenance • Server-Maintenance • SLB-Admin • SSL-Admin **Note** The SSL-Admin role is not available with the ACE NPE software version (see the "Information About the ACE No Payload Encryption Software Version" section on page 1-2). **Note** If you need to restrict a user's access, you must assign a role-domain pair. See Table 15-4 on page 15-15 for details about predefined roles.
Domains	A means for organizing the devices and their components (physical and logical) in your network.

1. Not required.

Step 4 Click **Deploy Now** to deploy this configuration. The Users table reappears.

Step 5 To add another user, click **Add Another**.

Related Topics

- Modifying User Accounts, page 15-10

- Deleting User Accounts, page 15-10
- Displaying a List of Users, page 15-8
- Managing Users, page 15-7
- Guidelines for Managing Users, page 15-8

Modifying User Accounts

Note Your user role determines whether you can use this option.

Procedure

Step 1 Select **Admin > Role-Based Access Control > Users**. The Users table appears.

Step 2 Select the user account you want to modify.

Step 3 Click **Edit**.

Step 4 The User details screen appears. Make any changes (see Table 15-2) and click **Deploy Now**.

The Users table then appears.

Related Topics

- Creating User Accounts, page 15-8
- Deleting User Accounts, page 15-10
- Displaying a List of Users, page 15-8
- Managing Users, page 15-7
- Guidelines for Managing Users, page 15-8

Deleting User Accounts

You can delete users using this procedure. You can also delete users from the Active Users window.

Note Your user role determines whether you can use this option.

Procedure

Step 1 Select **Admin > Role-Based Access Control > Users**. The Users table containing user, role, domain and other user information appears.

Step 2 Select the user account to be deleted.

Step 3 Click **Delete**.

A window appears asking you to confirm the deletion.

Step 4 Click **OK** to delete the user account or **Cancel** to exit the procedure without deleting the user. If you click OK, the window refreshes with the Users table and the deleted user account no longer appears.

Related Topics

- Creating User Accounts, page 15-8
- Modifying User Accounts, page 15-10
- Displaying a List of Users, page 15-8
- Managing Users, page 15-7
- Guidelines for Managing Users, page 15-8

Displaying Current User Sessions

You can view a list of the users currently logged into the system and end their sessions, if required.

You can see only the users in your available domains.

Note Your user role determines whether you can use this option.

Procedure

Step 1 Select **Admin > Role-Based Access Control > Active Users**.

The Active User Sessions screen displays the following information for each active user who is logged in:

Table 15-3 Active User Session Information

Column	Description
Name	The name used to log into the ACE appliance Device Manager.
Type of Login	Method used to log in, for example WEB or CLI
Login From IP	IP address of host
Time Of Login	Time user logged in

Step 2 To end an active web session, click **Terminate** (see Ending Active User Sessions, page 15-12 for details). CLI user sessions cannot be ended.

Related Topics

- Deleting Active Users, page 15-12
- Ending Active User Sessions, page 15-12
- Displaying a List of Users, page 15-8
- Managing Users, page 15-7
- Guidelines for Managing Users, page 15-8

Deleting Active Users

You can delete users using this procedure. You can also delete users using the **Admin > Role-Based Access Control > Users** menu.

Note Your user role determines whether you can use this option.

Procedure

Step 1 Select **Admin > Role-Based Access Control > Active Users**.

Step 2 Select the table rows containing the user accounts to be deleted.

Step 3 Click **Delete**.

The selected users are removed from the ACE Appliance Device Manager.

Related Topics

- Displaying Current User Sessions, page 15-11
- Ending Active User Sessions, page 15-12
- Managing Users, page 15-7

Ending Active User Sessions

When a user session is ended, the user is logged out of the interface from which the user session was initiated. If the user was making changes to a configuration, the configuration lock is released and any uncommitted configuration change is discarded.

If a user session is ended while an operation is in progress, the current operation is not stopped, but any subsequent operation is denied.

Note Your user role determines whether you can use this option.

Procedure

Step 1 Select **Admin > Role-Based Access Control > Active Users**.

Step 2 Select the table rows containing the user sessions to be ended.

Step 3 Click **Terminate**.

The selected users are forced out of the system.

Related Topics

- Displaying Current User Sessions, page 15-11
- Deleting Active Users, page 15-12
- Managing Users, page 15-7
- Controlling Access to the Cisco ACE Appliance, page 15-3

Changing User Passwords

Note Your user role determines whether you can use this option.

Procedure

Step 1 Select **Admin > Role-Based Access Control > Users**. The table of users is displayed.

Step 2 Select the user account you want to modify.

Step 3 Click **Edit**.

Step 4 Change the password attribute in the attributes table (see Table 15-2).

Step 5 Click **Deploy Now** to deploy this configuration and to return to the Users table.

Related Topics

- Managing Users, page 15-7
- Changing the Admin Password, page 15-13

Changing the Admin Password

Each ACE appliance has an admin user account built into the device. The root user ID is **admin**, and the password is set when the system is installed. For information about changing the Admin password, see Changing Your Account Password, page 1-6.

Managing User Roles

Use the Roles feature to add, modify, and delete user-defined roles. Predefined roles display with grey italic text and background and cannot be deleted or modified.

A user's role determines the tasks the user can access. Each role is associated with permissions or rules that define what feature access this role contains.

The following sections describe how to manage user roles:

Guidelines for Managing User Roles

Use these guidelines to manage roles:

- Administrators can view and modify all roles.
- Other users can only view the roles assigned to them.
- You cannot change the default roles.
- Role permissions are different based on whether they were created in an Admin context versus a non-admin or user context. If you want to allow users to switch between contexts, ensure they have a predefined role. If you want to restrict a user to only their home context, assign them a customized user role.
- Certain role features are only available to default roles, for example, an Admin role in the Admin context would have **changeto** and **system** permissions to perform tasks like license management, resource class management, HA setup, and so on. User-created roles cannot use these features.

Understanding Predefined Roles

The predefined roles and their default privileges are defined in Table 15-4. This table includes rule changes for Admin and user contexts (non-admin contexts). For detailed information on role-based access control, see the *Virtualization Guide, Cisco ACE Application Control Engine*. For details on how the predefined roles are mapped to ACE Appliance Device Manager tasks/features, see Table 15-5.

You must have one of the predefined roles in the Admin context in order to use the **changeto** command (which allows users to visit other contexts). Non-admin/user contexts do not have access to the **changeto** command; they can only visit their home context. Context administrators, who have access to multiple contexts, must explicitly log in to other contexts to which they have access.

Table 15-4 Predefined Role Rules for Admin and User Contexts

Predefined Role/Context	Description	Operations	Features
Admin Role			
Admin Context	If created in the Admin context, user has complete access to and control over all contexts, domains, roles, users, resources, and objects in the entire ACE.	• Debug • Create • Modify • Monitor	• All (context service configuration) • User Access (roles, domains, and users) • System (context administration) • **changeto** command (access to all contexts) • **exec** command (enables all default custom role commands)
User Context	If created in a user context, user has complete access to and control over all objects in that context.	Create	• All • User Access
Network-Admin Role			
Admin Context	Admin for L3 (IP and Routes) and L4 VIPs	Create	• Interfaces • Routing • Connection Parameters • Network Address Translation (NAT) • VIPs • Copy Configurations[1] • **changeto** command • **exec** command
User Context	Access to L3 (IP and Routes) and L4 VIPs	Create	• Interfaces • Routing • Connection Parameters • Network Address Translation (NAT) • VIPs • Copy Configurations[1]
Network-Monitor Role			
Admin Context	Monitoring for all features	Monitor	• All **show** commands • **changeto** command • **exec** command
User Context	Monitoring for all features	Monitor	• All **show** commands

Table 15-4 Predefined Role Rules for Admin and User Contexts

Predefined Role/Context	Description	Operations	Features
Security-Admin Role			
Admin Context	Security features	Create	• Access Control Lists (ACLs) • Application Inspection • Connection parameters • Authentication, authorization and accounting (AAA) • NAT • Copy Configurations[1] • **changeto** command • **exec** command
		Modify	Interface
User Context	Security features	Create	• Access Control Lists (ACLs) • Application Inspection • Connection parameters • Authentication, authorization and accounting (AAA) • NAT • Copy Configurations[1]
		Modify	Interface
Server-Appln-Maintenance Role			
Admin Context	Server maintenance and L7 policy application	Create	• Real Servers • Server Farms • Load balancing • Copy Configurations[1] • Real Server Inservice • **changeto** command • **exec** command
User Context	Server maintenance and L7 policy application	Create	• Real Servers • Server Farms • Load balancing • Copy Configurations[1] • Real Server Inservice

Table 15-4 Predefined Role Rules for Admin and User Contexts

Predefined Role/Context	Description	Operations	Features
Server-Maintenance Role			
Admin Context	Server maintenance, monitoring, and debugging	Debug	• Server Farms • VIPs • Probes • Load Balancing
		Create	• **changeto** command • **exec** command
		Modify	• Real Servers • Real Server Inservice
User Context	Server maintenance, monitoring, and debugging	Debug	• Server Farms • VIPs • Probes • Load Balancing
		Modify	• Real Servers • Real Server Inservice
SLB-Admin Role			
Admin Context	Load-balancing features	Create	• Real Servers • Server Farms • VIP • Probes • Loadbalance • NAT • Copy Configurations[1] • Real Server Inservice • **changeto** command • **exec** command
		Modify	Interface

Table 15-4 Predefined Role Rules for Admin and User Contexts

Predefined Role/Context	Description	Operations	Features
User Context	Load-balancing features	Create	• Real Servers • Server Farms • VIP • Probes • Loadbalance • NAT • Copy Configurations[1] • Real Server Inservice
		Modify	Interface
SSL-Admin Role			
Admin Context	SSL feature features	Create	• SSL • PKI • Copy Configurations[1] • **changeto** command • **exec** command
		Modify	Interface
User Context	SSL feature features	Create	• SSL • PKI • Copy Configurations[1]
		Modify	Interface

1. For a description of the **copy** command, see the *Command Reference, Cisco ACE Application Control Engine*.

Related Topics

- Role Mapping in ACE Appliance Device Manager, page 15-19
- Controlling Access to the Cisco ACE Appliance, page 15-3
- Managing Users, page 15-7
- Managing User Roles, page 15-14
- Managing Domains, page 15-31

Role Mapping in ACE Appliance Device Manager

When you are logged into ACE Appliance Device Manager, you see the tasks that you have been given permission to access. Table 15-5 describes the predefined roles and the menu tasks and features available to those roles. Features and menus that are not applicable for your role will not display.

Since the predefined roles encompass all the role types you may need, we encourage you to use them. If you choose to define your own roles, be aware that rules features are not a one-to-one mapping from CLI feature to ACE Appliance Device Manager menu task.

Defining the proper rules for your user-defined role will require you to create a mapping between the features in Table 15-4 and the ACE Appliance Device Manager menu tasks. For example, in order to manage virtual servers, you must select the following six menu features (Real Servers, Server Farms, VIP, Probes, Load Balancing, NAT, and Interface) in your role.

Note There are certain features in the ACE Appliance Device Manager that do not have a corresponding feature mapping on the CLI. One example of this feature is class maps. To modify these features you need to select a predefined role that a contains at least one feature with the Modify permission on it.

For details on predefined roles and their default privileges, see Table 15-4.

Table 15-5 Role Mapping in ACE Appliance Device Manager

Menu Task	Features Available
Admin Predefined Role	
Config > Virtual Contexts >	System > Primary Attributes
	System > Syslog
	System > SNMP
	System > Global Policies
	System > Licenses
	System > Resource Class
	System > Application Acceleration And Optimization
	Load Balancing > Virtual Servers
	Load Balancing > Real Servers
	Load Balancing > Server Farms
	Load Balancing > Health Monitoring
	Load Balancing > Stickiness
	Load Balancing > Parameter Maps
	Load Balancing > Secure KAL-AP
	SSL > Certificates
	SSL > Keys
	SSL > Parameter Maps
	SSL > Chain Group Parameters
	SSL > CSR Parameters
	SSL > Proxy Service
	SSL > Auth Group Parameters
	SSL > Certificate Revocation Lists (CRL)
	Security > ACLs
	Security > Object Groups

Table 15-5 Role Mapping in ACE Appliance Device Manager (continued)

Menu Task	Features Available
	Network > Port Channel Interfaces
	Network > GigabitEthernet Interfaces
	Network > VLAN Interfaces
	Network > BVI Interfaces
	Network > Static Routes
	Network > Global IP DHCP
	High Availability (HA) > Setup
	HA Tracking And Failure Detection > Interfaces
	HA Tracking And Failure Detection > Hosts
	Expert > Class Maps
	Expert > Policy Maps
	Expert > Action Lists
Config > Operations	Real Servers
	Virtual Servers
Monitor > Virtual Contexts	Load Balancing
	CPU
	Application Acceleration
	Interfaces
	Real Servers
	Statistics Collection
	Probes
	Resource Usage
	Ping
Admin > Role-Based Access Control	Users
	Active Users
	Roles
	Domains
Admin > Device Management	Statistics
	Statistics Collection
Admin > Tools	Lifeline Management
	File Browser

Table 15-5 Role Mapping in ACE Appliance Device Manager (continued)

Menu Task	Features Available
Network-Admin Predefined Role	
Config > Virtual Contexts >	System > Primary Attributes
	System > Global Policies
	Load Balancing > Parameter Maps
	Network > VLAN Interface
	Network >BVI Interfaces
	Network > Static Routes
	Network > Global IP DHCP
	Expert > Class Maps
	Expert > Policy Maps
Config > Operations	Virtual Servers
Monitor >	Application Acceleration
	Interfaces
	Real Servers
	Probes
	Resources
	Ping
Admin > Tools	File Browser

Table 15-5 Role Mapping in ACE Appliance Device Manager (continued)

Menu Task	Features Available
Network-Monitor Predefined Role	
Config > Virtual Contexts >	System > Primary Attributes
	System > Syslog
	System > Global Policies
	Load Balancing > Virtual Servers
	Load Balancing > Real Servers
	Load Balancing > Server Farms
	Load Balancing > Health Monitoring
	Load Balancing > Stickiness
	Load Balancing > Parameter Maps
	Load Balancing > Secure KAL-AP
	SSL > Certificates
	SSL > Keys
	SSL > Parameter Map
	SSL > Chain Group Parameters
	SSL > CSR Parameters
	SSL > Proxy Service
	SSL > Auth Group Parameters
	SSL > Certificate Revocation Lists (CRL)
	Security > ACLs
	Security > Object Groups
	Network > VLAN Interfaces
	Network > BVI Interfaces
	Network > Static Routes
	Network > Global IP DHCP
	HA Tracking And Failure Detection > Interfaces
	HA Tracking And Failure Detection > Hosts
	Expert > Class Maps
	Expert > Policy Maps
	Expert > Action Lists
Config > Operations	Real Servers
	Virtual Servers

Table 15-5 Role Mapping in ACE Appliance Device Manager (continued)

Menu Task	Features Available
Monitor >	Load Balancing
	Application Acceleration
	Interfaces
	Real Servers
	Probes
	Resource Usage
	Ping
Security-Admin Predefined Role	
Config > Virtual Contexts >	System > Primary Attributes
	System > Global Policies
	Load Balancing > Parameter Maps
	Security > ACLs
	Security > Object Groups
	Network > VLAN Interfaces
	Network > BVI Interfaces
	Network > Global IP DHCP
	Expert > Class Maps
	Expert > Policy Maps
Monitor > Virtual Contexts	Resource Usage
	Ping
Admin > Tools	File Browser
Server-Appln Maintenance Predefined Role	
Config > Virtual Contexts >	System > Primary Attributes
	Load Balancing > Real Servers
	Load Balancing > Server Farms
	Load Balancing > Parameter Maps
	Expert > Class Maps
	Expert > Policy Maps
	Expert > Action Lists
Config > Operations	Real Servers
Monitor > Virtual Contexts	Load Balancing
	Real Servers
	Resource Usage
	Ping
Admin > Tools	File Browser

Table 15-5 Role Mapping in ACE Appliance Device Manager (continued)

Menu Task	Features Available
Server-Maintenance Predefined Role	
Config > Virtual Contexts >	System > Primary Attributes
	Load Balancing > Real Servers
	Load Balancing > Server Farms
	Load Balancing > Health Monitoring
	Load Balancing > Parameter Maps
	Expert > Class Maps
	Expert > Policy Maps
	Expert > Action Lists
Config > Operations	Real Servers
	Virtual Servers
Monitor > Virtual Contexts	Load Balancing
	Real Servers
	Probes
	Resource Usage
	Ping
SLB-Admin Predefined Role	
Config > Virtual Contexts >	System > Primary Attributes
	System > Global Policies
	Load Balancing > Virtual Servers
	Load Balancing > Real Servers
	Load Balancing > Server Farms
	Load Balancing > Health Monitoring
	Load Balancing > Parameter Maps
	Network > VLAN Interfaces
	Network > BVI Interfaces
	Network > Global IP DHCP
	Expert > Class Maps
	Expert > Policy Maps
	Expert > Action Lists
Config > Operations	Real Servers
	Virtual Servers

Table 15-5 Role Mapping in ACE Appliance Device Manager (continued)

Menu Task	Features Available
Monitor > Virtual Contexts	Load Balancing
	Real Servers
	Probes
	Resource Usage
	Ping
Admin > Tools	File Browser
SSL-Admin	
Config > Virtual Contexts >	System > Primary Attributes
	System > Global Policies
	Load Balancing > Parameter Maps
	SSL > Certificates
	SSL > Keys
	SSL > Parameter Maps
	SSL > Chain Group Parameters
	SSL > CSR Parameters
	SSL > Proxy Service
	SSL > Auth Group Parameters
	SSL > Certificate Revocation Lists (CRL)
	Network > VLAN Interfaces
	Network > BVI Interfaces
	Network > Global IP DHCP
	Expert > Class Maps
	Expert > Policy Maps
Monitor > Virtual Contexts	Resource Usage
	Ping
Admin > Tools	File Browser

Related Topics

- Predefined Role Rules for Admin and User Contexts
- Controlling Access to the Cisco ACE Appliance, page 15-3
- Guidelines for Managing User Roles, page 15-14
- Managing Users, page 15-7
- Managing User Roles, page 15-14
- Managing Domains, page 15-31

RBAC User Role Requirements Related to Virtual Servers

If you want to create, modify, or delete a virtual server, we recommend that you use the pre-defined Admin role (see Table 15-4). Only the Admin pre-defined role supports the ability to successfully deploy a functional virtual server from the ACE appliance Device Manager.

If a user prefers to be assigned a custom role, and wants the ability to create, modify, or delete a virtual server, that user requires the proper role permissions to be defined by the administrator to allow them to perform those virtual server activities.

Note A user must be assigned with a default domain (default-domain) to be able to configure a virtual server. A domain is the namespace in which a user operates.

Note For a user with a customized role to perform configuration and operation changes from the ACE Appliance Device Manager, you must configure the role with rules that permit the create operation for the config-copy and exec-commands features.

Included below are a list of RBAC permissions which are required for a user to create, modify, or delete a virtual server:

```
-------------------------------------------
 Rule    Type    Permission      Feature
 -------------------------------------------
  1.   Permit    Create                real
  2.   Permit    Create           serverfarm
  3.   Permit    Create                 vip
  4.   Permit    Create               probe
  5.   Permit    Create         loadbalance
  6.   Permit    Create                 nat
  7.   Permit    Create           interface
  8.   Permit    Create          connection
  9.   Permit    Create                 ssl
 10.   Permit    Create                 pki
 11.   Permit    Create              sticky
 12.   Permit    Create             inspect
```

Note that certain configured virtual servers may only cover a subset of the features and may not require all the permissions outlined above. In general, the above set of permissions are required for allowing users to configure all elements of a virtual server.

Displaying User Roles

Use this option to display the existing user roles.

Note Your user role determines whether you can use this option.

Procedure

Step 1 Select **Admin > Role-Based Access Control > Roles**. A table of the defined roles and their settings appears.

Step 2 You can use the options in this screen to create a new role, filter roles based on a string, or modify or delete any existing role to which you have access.

Step 3 To view the users assigned to a role, select **Admin > Role-Based Access Control > Users.**

Related Topics

- Understanding Operations Privileges, page 15-6
- Managing User Roles, page 15-14

Creating User Roles

You can create new, user-defined roles. When you create a new role, you specify a name and description of the new role,, and then then select the operations privileges for each task. You can also assign this role to one or more users.

Note Your user role determines whether you can use this option.

Procedure

Step 1 Select **Admin > Role-Based Access Control > Roles**. A table of the defined roles and their settings appears.

Step 2 Click **Add**. The New Role configuration screen appears.

Step 3 Enter the following attributes.

Table 15-6 Role Attributes

Attribute	Description
Name	The name of the role.
Description	A brief description of the role.

Step 4 Click **Deploy Now** to deploy this configuration. The new role is added to the list of user roles and the Rules table appears below the Roles form in the content area.

Step 5 Click **Add** to create rules for this role. This role inherits the roles of the user that created it.

Step 6 To alter rules, select changes to any of the following attributes.

Note For a user with a customized role to perform configuration and operation changes from the ACE Appliance Device Manager, you must configure the role with rules that permit the create operation for the config-copy and exec-commands features.

Table 15-7 Rule Attributes

Attribute	Description
Rule Number	The number assigned to this rule.
Permission	Permit or deny the specified operation.
Operation	Create, debug, modify[1], and monitor the specified feature.
Feature	AAA, Access List, Change To Context, Config Copy, Connection, DHCP, Exec-Commands, Fault Tolerant, Inspect, Interface, Load Balance, NAT, PKI[2], Probe, Real Inservice, Routing, Real Server, Server Farm, SSL[2, 3], Sticky, Syslog, and VIP. The Changeto feature allows you to move from the Admin context to another virtual context and maintain the same role with the same privileges in the new context that you had in the Admin context. The Exec-commands feature enables all default custom role commands in the ACE. The default custom role commands are capture, debug, gunzip, mkdir, move, rmkdir, tac-pac, untar, write, and undebug.

1. Certain features are not available for certain operations. For **modify**, the following features cannot be used: Change To Context, Config-Copy, DHCP, Exec-Commands, NAT, Real Inservice, Routing, and Syslog.
2. The PKI and SSL features are not available with the ACE NPE software version (see the "Information About the ACE No Payload Encryption Software Version" section on page 1-2).
3. For all SSL-related operations, a user with a custom role should include the following two rules: A rule that includes the SSL feature, and a rule that includes the PKI feature.

Step 7 Click **Deploy Now** to update the rule for this role.

Related Topics

- Role Mapping in ACE Appliance Device Manager, page 15-19
- Understanding Operations Privileges, page 15-6
- Managing User Roles, page 15-14

Modifying User Roles

You can modify any user-defined roles.

Note Your user role determines whether you can use this option.

Procedure

Step 1 Select **Admin > Role-Based Access Control > Roles**. A table of the defined roles and their settings appears.

Step 2 Select the role you want to modify.

Step 3 Click **Edit**.

Step 4 Make the changes.

Step 5 Click **Deploy Now** to deploy this configuration and to return to the Roles table.

Related Topics

- Role Mapping in ACE Appliance Device Manager, page 15-19
- Understanding Operations Privileges, page 15-6
- Managing User Roles, page 15-14

Deleting User Roles

You can delete any user-defined roles (as long as they are not being used by a user).

Note Your user role determines whether you can use this option.

Procedure

Step 1 Select **Admin > Role-Based Access Control > Roles**. A table of the defined roles and their settings appears.

Step 2 Select the role to be deleted.

Step 3 Click **Delete**. A prompt asks you to confirm this action. Click **OK** to delete the role or Cancel to exit the procedure without deleting the role.

If you click **OK**, the window refreshes with the Roles table and the deleted user role no longer appears. Users that have the deleted role no longer have that access.

Related Topic

Managing User Roles, page 15-14

Adding, Editing, or Deleting Rules

You can change or delete rules to redefine what feature access a specific role contains.

Note Your user role determines whether you can use this option.

Procedure

Step 1 Select **Admin** > **Role-Based Access Control** > **Roles**. A table of the defined roles and their settings appears.

Step 2 Select the role to be changed. You can only change rules if only one role is selected in the pane.

Step 3 Perform any of the following tasks:

- Click **Add** to create a new rule. Enter the rule information (see Table 15-7 on page 15-29), and then click **Deploy Now**.
- Select a rule and click **Edit** to change an existing rule. Click **Deploy Now** to save this rule.
- Select the rules to remove from this role and click **Delete**. Click **OK** to confirm its deletion.

Related Topic

- Managing User Roles, page 15-14
- Role Mapping in ACE Appliance Device Manager, page 15-19
- Guidelines for Managing User Roles, page 15-14

Managing Domains

Network domains provide a means for organizing the devices and their components (physical and logical) in your network and permitting access according to the way your site is organized.

The following sections describe how to manage domains:

Guidelines for Managing Domains

- Devices and their components must already be configured in ACE Appliance Device Manager in order for them to be added to a domain.
- Domains are *logical* concepts. You do *not* delete a member of a domain when you delete the domain.

- Predefined domains cannot be modified or deleted.
- Normally, a user is associated with the default domain, which allows the user to see all configurations within the context. When a user is configured with a customized domain, then the user can see only what is in the domain.

Note To add objects 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.

Related Topics

- Displaying Network Domains, page 15-32
- Creating Domains, page 15-33
- Modifying Domains, page 15-34
- Deleting Domains, page 15-34

Displaying Network Domains

Note Your user role determines whether you can use this option.

Procedure

Step 1 Select **Admin > Role-Based Access Control > Domains**. The Domains table appears.

Step 2 Expand the table until you can see all the network domains.

Step 3 Select a domain from the Domains table to view the settings for that domain.

Step 4 You can also perform these tasks from this pane:

- Creating Domains, page 15-33
- Modifying Domains, page 15-34
- Adding or Deleting Domain Objects from a Domain, page 15-35
- Deleting Domains, page 15-34

Related Topic

- Managing Domains, page 15-31
- Guidelines for Managing Domains, page 15-31

Creating Domains

Use this option to create a new domain.

Note Your user role determines whether you can use this option.

Procedure

Step 1 Select **Admin > Role-Based Access Control > Domains**. The Domains table appears.

Step 2 Click **Add**.

Step 3 Enter the name of the new domain, and then click **Deploy Now**.

Step 4 Click **Add** in the Domain Object table that displays below the Domain form.

Step 5 Enter the attributes displayed in Table 15-8.

Table 15-8 Domain Attributes

Field	Description
Object Type	The collection of objects which comprise this domain. The following options may be available depending on your virtual context: • All • Access List Ethertype • Access List Extended • Class Map • Interface VLAN • Interface BVI • Parameter Map • Policy Map • Probe • Real Server • Script • Server Farm • Sticky
Object Name	This field appears when any specific object type is selected. Name of an existing object defined.

Step 6 Click **Deploy Now** to deploy this configuration.

Related Topic

- Managing Domains, page 15-31
- Guidelines for Managing Domains, page 15-31

Modifying Domains

Use this option to change the settings in a domain.

Note Your user role determines whether you can use this option.

Procedure

Step 1 Select **Admin > Role-Based Access Control > Domains**.

Step 2 Select the domain you want to change.

Step 3 Click **Edit**.

Step 4 Make the changes.

Step 5 Click **Deploy Now** to deploy this configuration.

Related Topics

- Managing Domains, page 15-31
- Guidelines for Managing Domains, page 15-31

Deleting Domains

Use this option to delete network domains from the system, as well as all the devices and domain objects they contain. You can only delete domains that are not associated with a user.

Note Your user role determines whether you can use this option.

Procedure

Step 1 Select **Admin > Role-Based Access Control > Domains**.

The Domains table contains a list of the existing domains.

Step 2 Select the domain you want to delete.

Step 3 Click **Delete**.

A prompt asks you to confirm this action.

Step 4 Click **OK**.

The domain is deleted from the ACE appliance.

Related Topics

- Managing Domains, page 15-31
- Guidelines for Managing Domains, page 15-31

Adding or Deleting Domain Objects from a Domain

Use this option to add or delete a network domain from the system, as well as all the devices and domain objects it contains. You can delete domains that are not associated with a user.

Note Your user role determines whether you can use this option.

Procedure

Step 1 Select **Admin > Role-Based Access Control > Domains**.

The Domains table contains a list of the existing domains.

Step 2 From the Domain table, select a domain in which you want to perform the action.

Step 3 You can then:

- Add a domain object by clicking **Add** in the Domain Object table and entering the object type and object name (if necessary). Then click **Deploy Now**.
- Select a row or rows in the Domain Object table that you want to delete and click **Delete**.

  A prompt asks you to confirm this action. Click **OK**. The domain object is deleted from the ACE appliance.

Related Topics

- Managing Domains, page 15-31
- Guidelines for Managing Domains, page 15-31

Monitoring ACE Appliance Statistics

You can view and set ACE appliance platform statistics data using the following menus:

- Statistics—Displays ACE appliance statistics and allows you to view them graphically. See Viewing ACE Appliance Server Statistics, page 15-35.
- Statistics Collection—Allows you to enable or disable ACE appliance statistic collection. See Configuring ACE Appliance Server Statistics Collection, page 15-36.

Viewing ACE Appliance Server Statistics

Use this procedure to display ACE appliance statistics (for example, CPU, disk, and memory usage) and view them graphically.

Statistics collection is enabled by default and are collected and saved to database every 5 minutes after the device SNMP credential configuration passes validation and is saved. For a newly created virtual context, the only piece of information that you need to provide in order to start statistical collection is the SNMP community information in the Config > SNMP screen.

To enable or disable ACE appliance statistic collection, see Configuring ACE Appliance Server Statistics Collection, page 15-36.

Procedure

Select **Admin > Device Management > Statistics**. The ACE appliance statistics shown in Table 15-9 are displayed.

Table 15-9 ACE Appliance Server Statistics

Name	Description
Owner	Process where statistics are collected.
Statistic	Includes the following statistics: • CPU Usage—Overall ACE appliance CPU busy percentage in the last 5-minute period. • Disk Usage—Amount of disk space being used by the ACE appliance. • Memory Usage—Amount of memory being used by the ACE appliance. • Process Uptime—Amount of time since this system was last initialized, or the amount of time since the network management portion of the system was last reinitialized.
Value	Value of the statistic.
Description	Information the statistic gathered.

Related Topics

- Monitoring ACE Appliance Statistics, page 15-35
- Configuring ACE Appliance Server Statistics Collection, page 15-36

Configuring ACE Appliance Server Statistics Collection

Use this procedure to enable ACE appliance statistics polling from the Monitor menu. The statistics collected include the following:

- CPU Usage—Overall ACE appliance CPU busy percentage in the last 5-minute period.
- Disk Usage—Amount of disk space being used by the ACE appliance.
- Memory Usage—Amount of memory being used by the ACE appliance.
- Process Uptime—Amount of time since this system was last initialized, or the amount of time since the network management portion of the system was last reinitialized.

If you want to set up collection for interface, CPU, load balancing and other statistics per virtual context, see Setting Up Virtual Contexts Statistics Collection, page 14-33.

Procedure

Step 1 Select **Admin > Device Management > Statistics Collection**. The Statistics Collection screen appears.

Step 2 In the Polling Stats field, select **Enable** to start background polling or **Disable** to stop background polling.

Step 3 In the Background Polling Interval field, select the polling interval appropriate for your networking environment. The interval range is from one minute to six hours.

Step 4 Click **OK** to save your entries.

Note These settings are not saved if you reboot your appliance. The system defaults will be restored.

Related Topics

- Monitoring ACE Appliance Statistics, page 15-35
- Viewing ACE Appliance Server Statistics, page 15-35

Using Admin Tools

Use these Admin Tools to perform troubleshooting and diagnostics tasks:

- Generating a Diagnostic Package, page 16-1—Use the troubleshooting and diagnostics tools provided by the Lifeline feature to report a critical problem to the Cisco support line and generate a diagnostic package.
- Manipulating ACE Appliance Files, page 16-6—Use the File Browser to download or upload files from the ACE appliance for viewing or tracking.

For details about these management tools, see Using ACE Appliance Device Manager Troubleshooting Tools, page 16-1.