



CHAPTER 10

Managing the ACE Appliance

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

- [Overview of the Admin Functions, page 10-1](#)
- [Controlling Access to the Cisco ACE Appliance, page 10-3](#)
- [Managing Users, page 10-7](#)
- [Managing User Roles, page 10-13](#)
- [Managing Domains, page 10-28](#)
- [Monitoring ACE Appliance Statistics, page 10-32](#)
- [Using Admin Tools, page 10-34](#)

For details on logging into ACE Appliance Device Manager, see [Logging Into ACE Appliance Device Manager, page 1-3](#).

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 10-1 describes the options that are displayed when you click **Admin**.

Table 10-1 Admin Menu Options

| Menu | Option | Description | Reference |
|---------------------------|--------------|--|---|
| Role-Based Access Control | Users | Manage users and their access to their context | See Managing Users , page 10-7 |
| | Active Users | Display or end session for active users | See Displaying Current User Sessions , page 10-11 or Ending Active User Sessions , page 10-12 |
| | Roles | Manage user's access to commands and resources | See Managing User Roles , page 10-13 |
| | Domains | Manage an association between a select group of context users and a select group of context objects. | See Managing Domains , page 10-28 |
| Device Management | | Check the status of the ACE Appliance Device Manager | See Monitoring ACE Appliance Statistics , page 10-32 |
| 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 11-1 |

Related Topics

- [Managing the ACE Appliance](#), page 10-1
- [Controlling Access to the Cisco ACE Appliance](#), page 10-3

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 *Cisco 4700 Series Application Control Engine Appliance Security Configuration Guide*.

**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 *Cisco 4700 Series Application Control Engine Appliance Security Configuration Guide* for details about authentication and accounting.

In addition, the role and domains that a user is associated with on a remote server will also be 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.

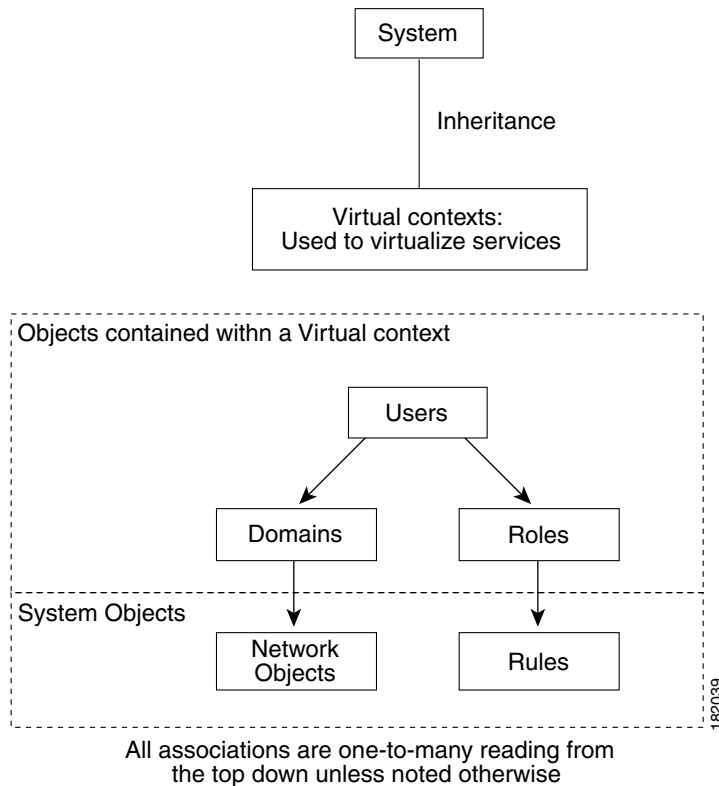
The role assigned to a user defines the tasks a user can perform and the items in the hierarchy that they can see. Roles are either predefined or set up by the system administrator. Each role, user, and domain is associated with a context. Only roles and domains associated with the Admin context can see other contexts. See [Understanding Roles, page 10-5](#) 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:

- 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 10-1 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 (except predefined roles and domains). All other users are subject to the role-based access controls illustrated in [Figure 10-1](#).

Related Topics

- [Types of Users, page 10-5](#)
- [Understanding Roles, page 10-5](#)
- [Understanding Operations Privileges, page 10-6](#)
- [Understanding Domains, page 10-7](#)
- [Managing Users, page 10-7](#)

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 10-7](#)).

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 10-7](#)
- [Guidelines for Managing Users, page 10-8](#)
- [Displaying a List of Users, page 10-8](#)
- [Creating User Accounts, page 10-8](#)

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 10-2 on page 10-9](#)). 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 10-14](#)
- [Role Mapping in ACE Appliance Device Manager, page 10-18](#)
- [Displaying User Roles, page 10-25](#)
- [Creating User Roles, page 10-25](#)
- [Modifying User Roles, page 10-26](#)
- [Deleting User Roles, page 10-27](#)

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 10-14](#)
- [Role Mapping in ACE Appliance Device Manager, page 10-18](#)
- [Managing User Roles, page 10-13](#)

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 10-28](#)
- [Guidelines for Managing Domains, page 10-28](#)

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 10-8](#)
- [Displaying a List of Users, page 10-8](#)
- [Creating User Accounts, page 10-8](#)
- [Modifying User Accounts, page 10-10](#)
- [Deleting User Accounts, page 10-10](#)
- [Displaying Current User Sessions, page 10-11](#)

**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 *Cisco 4700 Series Application Control Engine Appliance Security Configuration Guide* for details about authentication and accounting.

In addition, the role and domains that a user is associated with on a remote server will also be 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:
- User 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 10-2](#)).
-

Related Topics

- [Creating User Accounts, page 10-8](#)
- [Deleting User Accounts, page 10-10](#)
- [Managing Users, page 10-7](#)
- [Guidelines for Managing Users, page 10-8](#)

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 10-2 *User Attributes*

| Field | Description |
|--------------------------|--|
| User 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 | <p>Specifies the definition of what a user can do in this system. Choose from the following options or create your own role:</p> <ul style="list-style-type: none"> • Admin • Network-Admin • Network-Monitor • Security-Admin • Server-Appln-Maintenance • Server-Maintenance • SLB-Admin • SSL-Admin <p> Note If you need to restrict a user's access, you must assign a role-domain pair.</p> <p>See Table 10-4 on page 10-14 for details about predefined roles.</p> |
| 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

- [Creating User Accounts, page 10-8](#)
- [Deleting User Accounts, page 10-10](#)
- [Displaying a List of Users, page 10-8](#)
- [Managing Users, page 10-7](#)
- [Guidelines for Managing Users, page 10-8](#)

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 10-2](#)) and click **Deploy Now**. The Users table then appears.
-

Related Topics

- [Creating User Accounts, page 10-8](#)
- [Deleting User Accounts, page 10-10](#)
- [Displaying a List of Users, page 10-8](#)
- [Managing Users, page 10-7](#)
- [Guidelines for Managing Users, page 10-8](#)

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 10-8](#)
- [Modifying User Accounts, page 10-10](#)

- [Displaying a List of Users, page 10-8](#)
- [Managing Users, page 10-7](#)
- [Guidelines for Managing Users, page 10-8](#)

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 10-3 Active User Session Default Information

| Column | Description |
|---------------|--|
| Login Name | The name used to log into the Cisco 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 10-12](#) for details). CLI user sessions cannot be ended.

Related Topics

- [Deleting Active Users, page 10-11](#)
- [Ending Active User Sessions, page 10-12](#)
- [Displaying a List of Users, page 10-8](#)
- [Managing Users, page 10-7](#)
- [Guidelines for Managing Users, page 10-8](#)

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 10-11](#)
- [Ending Active User Sessions, page 10-12](#)
- [Managing Users, page 10-7](#)

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 10-11](#)
- [Deleting Active Users, page 10-11](#)
- [Managing Users, page 10-7](#)
- [Controlling Access to the Cisco ACE Appliance, page 10-3](#)

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 10-2](#)).
- Step 5** Click **Deploy Now** to deploy this configuration and to return to the Users table.

Related Topics

- [Managing Users, page 10-7](#)
- [Changing the Admin Password, page 10-13](#)

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 1-4](#).

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, page 10-14](#)
- [Role Mapping in ACE Appliance Device Manager, page 10-18](#)
- [Displaying User Roles, page 10-25](#)
- [Creating User Roles, page 10-25](#)
- [Modifying User Roles, page 10-26](#)
- [Deleting User Roles, page 10-27](#)

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 10-4](#). This table includes rule changes for Admin and user contexts (non-admin contexts). For detailed information on role-based access control, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*. For details on how the predefined roles are mapped to ACE Appliance Device Manager tasks/features, see [Table 10-5](#).

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 10-4 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. | <ul style="list-style-type: none"> • Debug • Create • Modify • Monitor | <ul style="list-style-type: none"> • All (context service configuration) • User Access (roles, domains, and users) • System (context administration) • changeto command (access to all contexts) |
| User Context | If created in a user context, user has complete access to and control over all objects in that context. | Create | <ul style="list-style-type: none"> • All • User Access |
| Network-Admin Role | | | |

Table 10-4 Predefined Role Rules for Admin and User Contexts

| Predefined Role/Context | Description | Operations | Features |
|-----------------------------|--|------------|---|
| Admin Context | Admin for L3 (IP and Routes) and L4 VIPs | Create | <ul style="list-style-type: none"> • Interfaces • Routing • Connection Parameters • Network Address Translation (NAT) • VIPs • Copy Configurations¹ • changeto command |
| User Context | Access to L3 (IP and Routes) and L4 VIPs | Create | <ul style="list-style-type: none"> • Interfaces • Routing • Connection Parameters • Network Address Translation (NAT) • VIPs • Copy Configurations¹ |
| Network-Monitor Role | | | |
| Admin Context | Monitoring for all features | Monitor | <ul style="list-style-type: none"> • All show commands • changeto command |
| User Context | Monitoring for all features | Monitor | <ul style="list-style-type: none"> • All show commands |
| Security-Admin Role | | | |
| Admin Context | Security features | Create | <ul style="list-style-type: none"> • Access Control Lists (ACLs) • Application Inspection • Connection parameters • Authentication, authorization and accounting (AAA) • NAT • Copy Configurations¹ • changeto command |
| | | Modify | Interface |

Table 10-4 Predefined Role Rules for Admin and User Contexts

| Predefined Role/Context | Description | Operations | Features |
|--------------------------------------|---|------------|--|
| User Context | Security features | Create | <ul style="list-style-type: none"> Access Control Lists (ACLs) Application Inspection Connection parameters Authentication, authorization and accounting (AAA) NAT Copy Configurations¹ |
| | | Modify | Interface |
| Server-Appln-Maintenance Role | | | |
| Admin Context | Server maintenance and L7 policy application | Create | <ul style="list-style-type: none"> Real Servers Server Farms Load balancing Copy Configurations¹ changeto command |
| User Context | Server maintenance and L7 policy application | Create | <ul style="list-style-type: none"> Real Servers Server Farms Load balancing Copy Configurations¹ |
| Server-Maintenance Role | | | |
| Admin Context | Server maintenance, monitoring, and debugging | Debug | <ul style="list-style-type: none"> Server Farms VIPs Probes Load Balancing |
| | | Create | changeto command |
| | | Modify | Real Servers |
| User Context | Server maintenance, monitoring, and debugging | Debug | <ul style="list-style-type: none"> Server Farms VIPs Probes Load Balancing |
| | | Modify | Real Servers |

Table 10-4 Predefined Role Rules for Admin and User Contexts

| Predefined Role/Context | Description | Operations | Features |
|-------------------------|-------------------------|------------|---|
| SLB-Admin Role | | | |
| Admin Context | Load-balancing features | Create | <ul style="list-style-type: none"> • Real Servers • Server Farms • VIP • Probes • Loadbalance • NAT • Copy Configurations¹ • changeto command |
| | | Modify | Interface |
| User Context | Load-balancing features | Create | <ul style="list-style-type: none"> • Real Servers • Server Farms • VIP • Probes • Loadbalance • NAT • Copy Configurations¹ |
| | | Modify | Interface |
| SSL-Admin Role | | | |
| Admin Context | SSL feature features | Create | <ul style="list-style-type: none"> • SSL • PKI • Copy Configurations¹ • changeto command |
| | | Modify | Interface |
| User Context | SSL feature features | Create | <ul style="list-style-type: none"> • SSL • PKI • Copy Configurations¹ |
| | | Modify | Interface |

1. For a description of the **copy** command, see the *Cisco 4700 Series Application Control Engine Appliance Command Reference*.

Related Topics

- [Role Mapping in ACE Appliance Device Manager, page 10-18](#)
- [Controlling Access to the Cisco ACE Appliance, page 10-3](#)
- [Managing Users, page 10-7](#)
- [Managing User Roles, page 10-13](#)
- [Managing Domains, page 10-28](#)

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 10-5](#) 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 10-4](#) 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. Examples of those are class maps and SNMP. To modify these features you need to select a predefined role that contains at least one feature with the Modify permission on it.

For details on predefined roles and their default privileges, see [Table 10-4](#).

Table 10-5 *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 Policy 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 Map |
| | SSL > Certificates SSL > Keys SSL > Parameter Map SSL > Chain Group Parameters SSL > CSR Parameters SSL > Proxy Service |
| | Security > ACLs |
| | Network > Port Channel Interfaces Network > GigabitEthernet Interfaces Network > VLAN Interfaces Network > BVI Interfaces Network > Static Routes |
| | High Availability (HA) > Setup |
| | HA Tracking and Failure Detection > Interfaces HA Tracking and Failure Detection > Hosts |
| | Expert > Class Map Expert > Policy Map Expert > Action List |
| Config > Operations | Real Servers Virtual Servers |

Table 10-5 Role Mapping in ACE Appliance Device Manager

| Menu Task | Features Available |
|--------------------------------------|--------------------------------|
| Monitor > Virtual Contexts | Load Balancing |
| | CPU |
| | 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 |
| Network-Admin Predefined Role | |
| Config > Virtual Contexts > | System > Primary Attributes |
| | System > SNMP |
| | System > Global Policy |
| | Load Balancing > Parameter Map |
| | Network > VLAN Interface |
| | Network > BVI Interfaces |
| | Network > Static Routes |
| | Expert > Class Map |
| Expert > Policy Map | |
| Config > Operations | Virtual Servers |
| Monitor > | Interfaces |
| | Resources |
| | Ping |
| Admin > Tools | File Browser |

Table 10-5 Role Mapping in ACE Appliance Device Manager

| Menu Task | Features Available |
|--|---|
| Network-Monitor Predefined Role¹ | |
| Config > Virtual Contexts > | System > Primary Attributes System > Syslog System > SNMP System > Global Policy |
| | Load Balancing > Virtual Servers Load Balancing > Real Servers Load Balancing > Server Farms Load Balancing > Health Monitoring Load Balancing > Stickiness Load Balancing > Parameter Map |
| | SSL > Certificates SSL > Keys SSL > Parameter Map SSL > Chain Group Parameters SSL > CSR Parameters SSL > Proxy Service |
| | Security > ACLs |
| | Network > VLAN Interfaces Network > BVI Interfaces Network > Static Routes |
| | HA Tracking and Failure Detection > Interfaces HA Tracking and Failure Detection > Hosts |
| | Expert > Class Map Expert > Policy Map Expert > Action List |
| Config > Operations | Real Servers Virtual Servers |
| Monitor > | Load Balancing Interfaces Real Servers Probes Resource Usage Ping |

Table 10-5 Role Mapping in ACE Appliance Device Manager

| Menu Task | Features Available |
|---|---|
| Security-Admin Predefined Role | |
| Config > Virtual Contexts > | System > Primary Attributes System > SNMP System > Global Policy Load Balancing > Parameter Map Security > ACLs Network > VLAN Interfaces Network > BVI Interfaces Expert > Class Map Expert > Policy Map |
| Monitor > Virtual Contexts | Resource Usage Ping |
| Admin > Tools | File Browser |
| Server-Appln Maintenance Predefined Role | |
| Config > Virtual Contexts > | System > Primary Attributes System > SNMP Load Balancing > Real Servers Load Balancing > Server Farms Load Balancing > Parameter Map Expert > Class Map Expert > Policy Map Expert > Action List |
| Config > Operations | Real Servers |
| Monitor > Virtual Contexts | Load Balancing Real Servers Resource Usage Ping |
| Admin > Tools | File Browser |

Table 10-5 Role Mapping in ACE Appliance Device Manager

| Menu Task | Features Available |
|---|--|
| Server-Maintenance Predefined Role | |
| Config > Virtual Contexts > | System > Primary Attributes System > SNMP Load Balancing > Real Servers Load Balancing > Server Farms Load Balancing > Health Monitoring Expert > Class Map Expert > Policy Map Expert > Action List |
| 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 > SNMP System > Global Policy Load Balancing > Virtual Servers Load Balancing > Real Servers Load Balancing > Server Farms Load Balancing > Health Monitoring Network > VLAN Interfaces Network > BVI Interfaces Expert > Class Map Expert > Policy Map Expert > Action List |
| Config > Operations | Real Servers Virtual Servers |
| Monitor > Virtual Contexts | Load Balancing Real Servers Probes Resource Usage Ping |

Table 10-5 Role Mapping in ACE Appliance Device Manager

| Menu Task | Features Available |
|-----------------------------|------------------------------|
| Admin > Tools | File Browser |
| SSL-Admin | |
| Config > Virtual Contexts > | System > Primary Attributes |
| | System > SNMP |
| | System > Global Policy |
| | SSL > Certificates |
| | SSL > Keys |
| | SSL > Parameter Map |
| | SSL > Chain Group Parameters |
| | SSL > CSR Parameters |
| | SSL > Proxy Service |
| | Network > VLAN Interfaces |
| Network > BVI Interfaces | |
| Expert > Class Map | |
| Expert > Policy Map | |
| Monitor > Virtual Contexts | Resource Usage |
| | Ping |
| Admin > Tools | File Browser |

1. Users assigned the Network-Monitor role will be unable to configure SNMP settings on the device because ACE Appliance Device Manager requires Modify or above permission on any feature in order to modify SNMP. If you want users to modify SNMP settings, change the predefined role to include a role that has Modify permissions.

Related Topics

- [Predefined Role Rules for Admin and User Contexts](#)
- [Controlling Access to the Cisco ACE Appliance, page 10-3](#)
- [Guidelines for Managing User Roles, page 10-14](#)
- [Managing Users, page 10-7](#)
- [Managing User Roles, page 10-13](#)
- [Managing Domains, page 10-28](#)

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 10-6](#)
- [Managing User Roles, page 10-13](#)

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, 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 10-6 *Role Attributes*

| Attribute | Description |
|-------------|----------------------------------|
| Role 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.

Table 10-7 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, Config-copy, Connection, DHCP, Fault-tolerant, Inspect, Interface, Loadbalance, NAT, PKI, Probe, Real-inservice, Routing, Rserver, Server Farm, SSL, Sticky, Syslog, and Vip. |

1. Certain features are not available for certain operations. For **modify**, the following features cannot be used: config-copy, DHCP, NAT, real-inservice, routing, and syslog.

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

Related Topics

- [Role Mapping in ACE Appliance Device Manager, page 10-18](#)
- [Understanding Operations Privileges, page 10-6](#)
- [Managing User Roles, page 10-13](#)

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 10-18](#)
- [Understanding Operations Privileges, page 10-6](#)
- [Managing User Roles, page 10-13](#)

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 10-13](#)

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 10-7 on page 10-26](#)), 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 10-13](#)
- [Role Mapping in ACE Appliance Device Manager, page 10-18](#)
- [Guidelines for Managing User Roles, page 10-14](#)

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, page 10-28](#)
- [Displaying Network Domains, page 10-28](#)
- [Creating Domains, page 10-29](#)
- [Modifying Domains, page 10-30](#)
- [Deleting Domains, page 10-31](#)

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 10-28](#)
- [Creating Domains, page 10-29](#)
- [Modifying Domains, page 10-30](#)
- [Deleting Domains, page 10-31](#)

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 10-29](#)
 - [Modifying Domains, page 10-30](#)
 - [Adding or Deleting Domain Objects from a Domain, page 10-31](#)
 - [Deleting Domains, page 10-31](#)
-

Related Topic

- [Managing Domains, page 10-28](#)
- [Guidelines for Managing Domains, page 10-28](#)

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, 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 10-8](#).

Table 10-8 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: <ul style="list-style-type: none"> • 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 10-28](#)
- [Guidelines for Managing Domains, page 10-28](#)

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 10-28](#)
- [Guidelines for Managing Domains, page 10-28](#)

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 10-28](#)
- [Guidelines for Managing Domains, page 10-28](#)

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 10-28](#)
- [Guidelines for Managing Domains, page 10-28](#)

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 10-32](#).
- **Statistics Collection**—Allows you to enable or disable ACE appliance statistic collection. See [Configuring ACE Appliance Server Statistics Collection, page 10-33](#).

If you want to see CPU-categorized statistics for a single virtual context, see [Monitoring the CPU, page 9-5](#).

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.

If you want to see interface, CPU, load balancing and other statistics per virtual context, see [Monitoring the CPU, page 9-5](#). To enable or disable ACE appliance statistic collection, see [Configuring ACE Appliance Server Statistics Collection, page 10-33](#).

Procedure

Step 1 Select **Admin > Device Management > Statistics**. The ACE appliance statistics shown in [Table 10-9](#) are displayed.

Table 10-9 ACE Appliance Server Statistics

| Name | Description |
|-------------|---|
| Owner | Process where statistics are collected. |
| Statistic | Includes the following statistics: <ul style="list-style-type: none"> • 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. |

- Step 2** Select a statistic, then click **Graph**. You can select more than one statistic by holding down Shift (to select statistics in a row) or Control (to select individual statistics) while clicking on additional statistics. ACE Appliance Device Manager queries the values and graphically displays the information.
- Step 3** To modify the information shown in the graph, you can click on any of the buttons described in [Table 1-5 on page 1-9](#).

Related Topics

- [Monitoring ACE Appliance Statistics, page 10-32](#)
- [Configuring ACE Appliance Server Statistics Collection, page 10-33](#)
- [Monitoring the CPU, page 9-5](#)

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 9-9](#).

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 10-32](#)
- [Viewing ACE Appliance Server Statistics, page 10-32](#)

Using Admin Tools

Use these Admin Tools to perform troubleshooting and diagnostics tasks:

- [Generating a Diagnostic Package, page 11-1](#)—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 11-4](#)—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 11-1](#).