CHAPTER 15

# Administering the Cisco Application Networking Manager

**Date: 5/8/09**

The following topics describe how to administer, maintain, and manage the ANM management system. Previous topics described how to manage your network devices on ANM, while this topic describes how to perform procedures on the system itself.


- Overview of the Admin Function, page 15-2
- Controlling Access to Cisco ANM, page 15-4
- How ANM Handles Role-Based Access Control, page 15-9
- Configuring User Authentication, page 15-33
- Managing User Accounts, page 15-40
- Displaying or Terminating Current User Sessions, page 15-44
- Managing User Roles, page 15-45
- Managing Domains, page 15-51
- Authenticating ANM Users with a AAA Server, page 15-56
- Managing ANM, page 15-63
- Lifeline Management, page 15-76

# Overview of the Admin Function

**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 | Organizations | Manage organizations, configure external authentication mechanisms | See Configuring User Authentication, page 15-33 |
| | Users | Manage users | See Managing User Accounts, page 15-40 |
| | Active Users | Display active users | See Displaying or Terminating Current User Sessions, page 15-44 |
| | Roles | Manage user roles | See Managing User Roles, page 15-45 |
| | Domains | Manage domains | See Managing Domains, page 15-51 |

*Table 15-1 Admin Menu Options*

| Menu | Option | Description | Reference |
|---|---|---|---|
| ANM Management | ANM | Checks the status of the ANM server. | See Checking the Status of the ANM Server, page 15-63 |
| | License Management | Views ANM license state, add more licenses, and tracks license information on your ACE | See Managing ANM Licenses, page 15-66 |
| | Statistics | Displays ACE statistics (for example, CPU, disk, and memory usage). | See Viewing ANM Server Statistics, page 15-72 |
| | Statistics Collection | Enables ACE server statistics polling. | See Configuring ANM Statistics Collection, page 15-72 |
| | Audit Log Settings | Allows you to specify number of audit logs saved and how many days logs are saved. | See Configuring Audit Log Settings, page 15-73 |
| | ANM Change Audit Log | Allows you to display audit logs recording any user input. | See Viewing Change Audit Logs, page 15-74 |
| | ANM Auto-Sync Settings | Allows you to specify ANM server auto sync settings | See Configuring Auto Sync Settings, page 15-74 |
| | Advanced Settings[1] | Allows you to configure the following Advanced Settins functions:<br>• Enable or disable overwrite of the ACE logging device-id while setting up syslog for autosync using Config > Devices > Setup Syslog for Autosync.<br>• Enable or disable write memory on a Config > Operations configuration. | See Configuring Advanced Settings, page 15-75 |
| Lifeline Management | | Use this tool to report a problem to the Cisco support line and generate a diagnostic package | See Lifeline Management, page 15-76 |

1. The Advanced Settings functions are available only in ANM software releases 2.1(1) and greater.

# Controlling Access to Cisco ANM

Access to ANM is based on usernames and passwords, which can be authenticated to a local database on the ANM system or to an external RADIUS, Active Directory/Lightweight Directory Access Protocol (AD/LDAPS), or TACACS+ server. For detailed procedures on remote authentication, see the "Configuring Authentication and Accounting Services" chapter of either the *Cisco ACE Module Security Configuration Guide* or *Cisco ACE 4700 Series Appliance Security Configuration Guide* on www.cisco.com.

**Note** ANM supports LDAPS is only through Active Directory (AD).

When a user logs into the system, the specific tasks they can perform and areas of the system they can use are controlled by *organizations*, *roles*, and *domains*.

An organization is a virtual group of users, their roles, and domains managed by a specific server that provides authentication to its users. Each organization has its own set of users. See Understanding Organizations, page 15-8 for information on organizations.

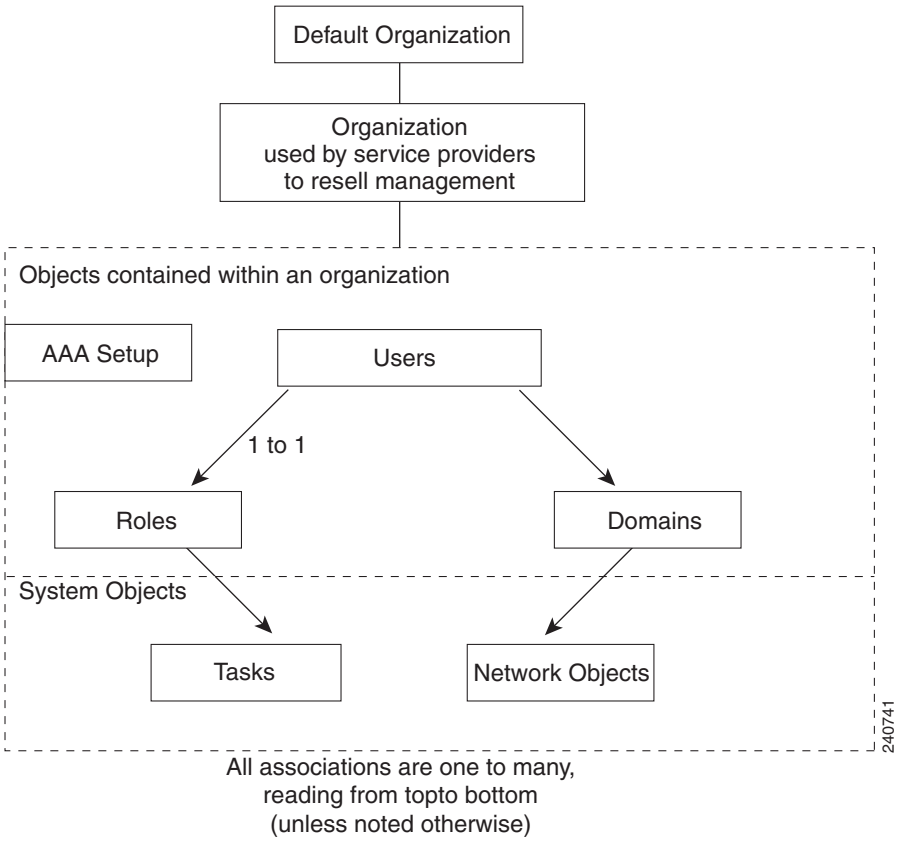
The role assigned to a user defines the tasks a user can perform and the items in the hierarchy that they can see. Roles are either pre-defined or set up by the system administrator. See Understanding Roles, page 15-6 for more information.

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

- Chassis (with VLANs)
- Virtual contexts
- Building Blocks
- Resource classes
- Real servers
- Virtual servers

Thus, role-based access control ensures that a user or organization 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 RBAC containment.

| **Organization** | | |
|---|---|---|
| Webmasters | | |
| **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. Because the organization itself is a collection, it is possible for a role to be used in many organizations. | | |

All other user interfaces, such as configuration and monitoring, 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 system administrator) can only create subdomains of the domains to which they are assigned.
- The system administrator user 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 15-6
- Understanding Roles, page 15-6
- Understanding Operations Privileges, page 15-7
- Understanding Domains, page 15-8
- Understanding Organizations, page 15-8
- Managing User Accounts, page 15-40

# Types of Users

Two types of users configure and monitor the ANM system:

- Default users—individuals associated with the data center or IT department where the ANM system is installed. The default administrative account (user ID **admin**) is a system user account that is preconfigured on the system. The default administrative password (**admin**) is also set on the system. You can change the password for the admin user account in the same manner as any user password (see Managing User Accounts, page 15-40).

  System roles are defined by the system administrator when the system is first set up. System roles are specified in terms of resource types and operations privileges. For each system role, the system administrator specifies which resource types a role can work with and what operations a role can perform on each resource type.
- Organization users—users who work for the customer of a service provider or AAA server that segments your users and to whom you want to grant access to ANM. Organization users automatically have their access limited to the organization to which they belong.

**Related Topics**

- Configuring User Authentication, page 15-33
- Managing User Accounts, page 15-40
- Authenticating ANM Users with a AAA Server, page 15-56

# Understanding Roles

Roles in the Cisco ANM system are defined by the system administrator. Roles are specified in terms of resource types and operations privileges. For each role, the system administrator specifies which resource types a role can work with and what operations a role can perform on each resource type.

When users are created, they are assigned at least one system role and inherit the operations privileges specified for each of the resource types assigned to that role.

The options a user sees in the menu are filtered according to that user's role. See Table 15-2 on page 15-11.

Roles can be applied to both default and organization users. All users are strictly limited by the combination of their operations privileges and user access. For example, a user cannot create another user who has greater privileges or access.

**Related Topics**

- Configuring User Authentication, page 15-33
- Managing User Accounts, page 15-40
- Managing User Roles, page 15-45

# Understanding Operations Privileges

Operations privileges define what users can do in the designated resource types. For example, each command and function on ANM has an assigned privilege. If a user's privileges are not sufficient, the command or function will not be available to them. The following operations privileges can be granted:

- No Access—The user has no access to this command or function.

  **Note** If a user is configured with no access to virtual contexts, it means absolutely no access to them. The most a user with this access can do is activate or suspend real servers.

- View—Allows the user to view statistics and specify parameter collection and threshold settings. Gives the user read-only or view access to system objects and information.
- Modify—Allows the user to change the persistent information associated with system objects, such as an organization record, or configuration.
- Debug—Gives the user read-only or view access to system objects and information.
- Create—Allows the user to control system objects, for example, creating them, enabling them, or powering up. Also allows the user to control system objects, for example, deleting them, disabling them, or powering down.

Privileges are hierarchical. If a user has Modify privileges, they have View privileges as well. If a user has Create or Debug privileges, they have View privileges as well.

**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**

- How ANM Handles Role-Based Access Control, page 15-9
- Managing User Roles, page 15-45
- Guidelines for Managing User Roles, page 15-46
- Understanding Predefined Roles, page 15-46
- Authenticating ANM Users with a AAA Server, page 15-56

# Understanding Domains

Domains in the Cisco ANM system are defined by the system administrator. A domain is a collection of managed objects to which a user is given access. By setting up a domain, you are filtering for a subset of objects on the network. The user is then given access to this virtual context.

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

# Understanding Organizations

An organization allows you to configure AAA server lookup for your users or set up users who work for a service provider customer. Organizations in the Cisco ANM system are defined by the system administrator.

When you use a ACE device as a AAA Server you may want to segment them for customer, business, or security reasons. If you use more than one authentication server, then you can use organizations to configure them to authenticate your users.

For example, if your company has four servers, one each for local, RADIUS, TACACS+, and LDAPS authentication, then organizations could reflect that. The Default organization in ANM is set up to act as the local server.

ANM supports different device types that have unique ways of configuring authentication access (which helps with future device support). ANM can configure which users are authenticated by which authentication servers, but does not act as a AAA server itself since this would be in conflict of its role as a RBAC administrator. This allows for the separation of authority that is needed to perform RBAC successfully.

### Related Topics

- Authenticating ANM Users with a AAA Server, page 15-56

# How ANM Handles Role-Based Access Control

This section describes how and why a system administrator might want to use the ANM role-based access control (RBAC) features.

ANM supports two distinct, but related RBAC capabilities:

1. Where ANM acts as a system and network device overseer allowing it to implement its use of RBAC, referred to as ANM RBAC.
2. That which the device enforces, referred to as device RBAC.

### Understanding ANM RBAC

ANM is a central place where you can globally set the RBAC for users, roles, and domains (as well as for virtual contexts or device types using device RBAC).

As an system administrator, you may need to delegate authority to allow another administrators to perform specific tasks on specific devices; such as activating, suspending, and monitoring traffic flow to specific real servers, but disabling any other capabilities. ANM interface enables you to accomplish this delegation with more control. For a description of how the roles map to the functions, see Table 15-2 on page 15-11.

### Understanding Device RBAC

ANM's device RBAC allows you to set up device permission levels of a more granular nature. You no longer have to provide "all-or-nothing" roles-based access of devices and device modules. Without ANM, some devices may be open to users who can perform every task on that device or module, regardless of their authorization due to permission level requirements on modules and or switches. ANM provides a central place to grant special access to users you specify. Device users, roles, and domain data are not part of, nor can they be used by ANM. Device RBAC is only for CLI access directly to the context.

For example, there may be a small number of users that need level 3 access when direct troubleshooting of ACE hardware is required. You can set up these users with or without ANM, but ANM centralizes the capability to do so. If you want to configure a network engineer with a special role, for example either ACE-Admin or Network-Admin, to provide the level 3 access. ANM accesses the ACE as a level 15 user and an admin supervisor and uses the RBAC to determine the level of access (to device types, segments, elements, subelements, and so on).

Some Cisco devices have the ability to configure RBAC directly on the device, for example the ACE. An example of a device that does not have the capability to have its own RBAC is the CSS or a CSM.

When you configure remote authentication (AAA, RADIUS, LDAPS, or TACACs+) for the ACE via ANM, users no longer have to log out to access their device via Telnet. When you manually log into a CSS, the CSS performs user authentication in a Telnet session. Telnet does not provide any domain enforcement so is less secure. For an overview on the steps that you perform to configure remote authentication with a AAA server, see the "Authenticating ANM Users with a AAA Server" section on page 15-56

If you are an admin using a CSS module outside of the ANM program, then you might have permission to do anything on this switch. If you are using ANM, you can set up better authorization for your administrators for specific devices. Better authorization controls are one of the advantages of using the ANM versus using only the CLI on the ACE hardware. You can now configure separate access for one function for this user in this domain only. ANM allows this high level of granularity and with it, more control over who does what to your devices.

You can access device RBAC using **Config > Devices** or **Config > Global >All Building Blocks**.

**Note** When configuring device RBAC via Config > Devices, an message displays reminding you that you are configuring RBAC outside of ANM for direct access. Be aware that this may contradict your ANM settings.

For more information on centralizing direct access to devices through RBAC on individual devices, see Configuring Device Role-Based Access Controls, page 2-43.

### Case Example

In this example, a CSM device must have a level 15 access which by default makes the admin a supervisor on everything in the switch (and everything in the module). Another way of looking at this is providing read-only access to everything or configuration access to everything.

ACE hardware can be configured on a virtual context to perform that task on a subset domain for every individual module, on every context, but this type of configuration must be configured individually.

A system administrator might need to configure a network admin to manage two CSM modules, one out of six virtual contexts, and all East Coast web servers. With ANM, the admin could create one configuration set that includes a user account with a Network-Admin role and a domain that includes these objects. ANM then becomes the security window through which this user passes to get to their destination for that domain and for that virtual context.

If there were six users, nine domains, and three virtual contexts, there would be 54 entries required into a AAA Server and ACE module. In ANM there is one entry completed for each of the six users.

*Table 15-2 Role Mapping in ANM*

| Role Tasks/Permissions | Resulting Menus Available |
|---|---|
| **ACE-Admin Predefined Role** | |
| Threshold/View | Monitor / Alarm Notifications / Alarms<br>Monitor / Alarm Notifications / Threshold Groups<br>Monitor / Alarm Notifications / Threshold Groups /Edit<br>Monitor / Settings / SMTP Configuration |
| Device Events/Create | Monitor / Events / Events |
| Virtual Contexts/Create | Config / Deploy<br>Config / Deploy / Deploy Now<br>Config / Deploy / Edit<br>Config / Devices / Device RBAC / Domains<br>Config / Devices / Device RBAC / Roles<br>Config / Devices / Device RBAC / Users<br>Config / Devices / Expert / Action List<br>Config / Devices / Expert / Building Block Audit<br>Config / Devices / Expert / Class Map<br>Config / Devices / Expert / Policy Map<br>Config / Devices / HA Tracking and Failure Detection / Hosts<br>Config / Devices / HA Tracking and Failure Detection / HSRP Groups<br>Config / Devices / HA Tracking and Failure Detection / Interfaces<br>Config / Devices / High Availability (HA) / Setup<br>Config / Devices / Load Balancing / Health Monitoring<br>Config / Devices / Load Balancing / Parameter Maps / Connection Parameter Map<br>Config / Devices / Load Balancing / Parameter Maps / Generic Parameter Map<br>Config / Devices / Load Balancing / Parameter Maps / HTTP Parameter Map<br>Config / Devices / Load Balancing / Parameter Maps / Optimization Parameter Map<br>Config / Devices / Load Balancing / Parameter Maps / RTSP Parameter Map |

*Table 15-2 Role Mapping in ANM*

| Role Tasks/Permissions (continued) | Resulting Menus Available (continued) |
|---|---|
| **ACE-Admin Predefined Role (continued)** | |
| Virtual Contexts/Create (continued) | Config / Devices / Load Balancing / Parameter Maps / SIP Parameter Map |
| | Config / Devices / Load Balancing / Parameter Maps / Skinny Parameter Map |
| | Config / Devices / Load Balancing / Real Servers |
| | Config / Devices / Load Balancing / Server Farms |
| | Config / Devices / Load Balancing / Stickiness |
| | Config / Devices / Load Balancing / Virtual Servers |
| | Config / Devices / Load Balancing / Virtual Servers / Add |
| | Config / Devices / Load Balancing / Virtual Servers / Edit |
| | Config / Devices / Network / BVI Interfaces |
| | Config / Devices / Network / GigabitEthernet Interfaces |
| | Config / Devices / Network / Global IP DHCP |
| | Config / Devices / Network / Port Channel Interfaces |
| | Config / Devices / Network / Static Routes |
| | Config / Devices / Network / Static VLAN |
| | Config / Devices / Network / VLAN Interfaces |
| | Config / Devices / Security / ACLs |
| | Config / Devices / Security / Object Groups |
| | Config / Devices / SSL / Auth Group Parameters |
| | Config / Devices / SSL / Certificate Revocation List |
| | Config / Devices / SSL / Certificates |
| | Config / Devices / SSL / Chain Group Parameters |
| | Config / Devices / SSL / CSR Parameters |
| | Config / Devices / SSL / Keys |
| | Config / Devices / SSL / Parameter Map |
| | Config / Devices / SSL / Proxy Service |
| | Config / Devices / System / Application Acceleration and Optimization |
| | Config / Devices / System / Global Policy |
| | Config / Devices / System / Licenses |
| | Config / Devices / System / Primary Attributes |
| | Config / Devices / System / Resource Classes |
| | Config / Devices / System / Resource Classes / Add |
| | Config / Devices / System / Resource Classes / Edit |

*Table 15-2 Role Mapping in ANM*

| Role Tasks/Permissions (continued) | Resulting Menus Available (continued) |
|---|---|
| **ACE-Admin Predefined Role (continued)** | |
| Virtual Contexts/Create (continued) | Config / Devices / System / SNMP |
| | Config / Devices / System / Syslog |
| | Config / Devices / Virtual Context Management |
| | Config / Devices / Virtual Context Management / Add |
| | Config / Devices / Virtual Context Management / Edit |
| | Config / Devices / Virtual Context Management / Extract building block |
| | Config / Devices / Virtual Context Management / Restart Polling |
| | Config / Devices / Virtual Context Management / Sync |
| | Config / Global / Building Blocks |
| | Config / Global / Building Blocks / Add |
| | Config / Global / Building Blocks / Tag |
| | Config / Global / Expert / Action List |
| | Config / Global / Expert / Class Map |
| | Config / Global / Expert / Policy Map |
| | Config / Global / Load Balancing / Health Monitoring |
| | Config / Global / Load Balancing / Parameter Maps / Connection Parameter Map |
| | Config / Global / Load Balancing / Parameter Maps / Generic Parameter Map |
| | Config / Global / Load Balancing / Parameter Maps / HTTP Parameter Map |
| | Config / Global / Load Balancing / Parameter Maps / Optimization Parameter Map |
| | Config / Global / Load Balancing / Parameter Maps / RTSP Parameter Map |
| | Config / Global / Load Balancing / Parameter Maps / SIP Parameter Map |
| | Config / Global / Load Balancing / Parameter Maps / Skinny Parameter Map |
| | Config / Global / Load Balancing / Real Servers |
| | Config / Global / Load Balancing / Server Farms |
| | Config / Global / Load Balancing / Stickiness |

*Table 15-2 Role Mapping in ANM*

| Role Tasks/Permissions (continued) | Resulting Menus Available (continued) |
|---|---|
| **ACE-Admin Predefined Role (continued)** | |
| Virtual Contexts/Create (continued) | Config / Global / Network / BVI Interfaces |
| | Config / Global / Network / Global IP DHCP |
| | Config / Global / Network / Static Routes |
| | Config / Global / Network / Static VLAN |
| | Config / Global / Network / VLAN Interfaces |
| | Config / Global / Resource Classes |
| | Config / Global / Resource Classes / Add |
| | Config / Global / Resource Classes / Audit |
| | Config / Global / Resource Classes / Edit |
| | Config / Global / Role-Based Access Control / Domains |
| | Config / Global / Role-Based Access Control / Roles |
| | Config / Global / Role-Based Access Control / Users |
| | Config / Global / Security / ACLs |
| | Config / Global / Security / Object Groups |
| | Config / Global / SSL / Auth Group Parameters |
| | Config / Global / SSL / Certificate Revocation List |
| | Config / Global / SSL / CSR Parameters |
| | Config / Global / SSL / Keys |
| | Config / Global / SSL / Parameter Map |
| | Config / Global / System / Global Policy |
| | Config / Global / System / Primary Attributes |
| | Config / Global / System / SNMP |
| | Config / Global / System / Syslog |
| | Config / Operations / Real Servers |
| | Config / Operations / Virtual Servers |
| | Config / Operations / Virtual Servers / Activate |
| | Config / Operations / Virtual Servers / Details |
| | Config / Operations / Virtual Servers / Suspend |
| | Monitor / Devices / Application Acceleration |
| | Monitor / Devices / Load Balancing |
| | Monitor / Devices / Load Balancing / Statistics |
| | Monitor / Devices / Load Balancing / Virtual Servers |

*Table 15-2 Role Mapping in ANM*

| Role Tasks/Permissions (continued) | Resulting Menus Available (continued) |
|---|---|
| **ACE-Admin Predefined Role (continued)** | |
| Virtual Contexts/Create (continued) | Monitor / Devices / Polling Settings |
| | Monitor / Devices / Resource Usage |
| | Monitor / Devices / Resource Usage |
| | Monitor / Devices / Resource Usage / Connections |
| | Monitor / Devices / Resource Usage / Features |
| | Monitor / Devices / System View |
| | Monitor / Devices / Traffic Summary |
| | Monitor / Devices / Virtual Context Management |
| | Monitor / Devices / Virtual Servers |
| | Monitor / Events /Virtual Context Management |
| | Monitor / Tools / Ping |
| | Change Password |
| | Copy License |
| | Export |
| | Generate CSR |
| | Import |
| | Install |
| | Resequence |
| | Status |
| | Uninstall |
| | Update |
| **ANM-Admin Predefined Role** | |
| All Options | All menus (ANM System, ANM User Access, and ANM Inventory) |
| **Network-Admin Predefined Role** | |
| Threshold/View | Monitor / Alarm Notifications / Alarms |
| | Monitor / Alarm Notifications / Threshold Groups |
| | Monitor / Alarm Notifications / Threshold Groups / Edit |
| | Monitor / Settings / SMTP Configuration |

*Table 15-2 Role Mapping in ANM*

| Role Tasks/Permissions (continued) | Resulting Menus Available (continued) |
|---|---|
| **Network-Admin Predefined Role (continued)** | |
| Switch/Create | Config / Devices / Device Management / Change Password |
| | Config / Devices / Device Management / Edit |
| | Config / Devices / Device Management / Sync |
| | Config / Devices / Interfaces / Access Ports |
| | Config / Devices / Interfaces / Routed Ports |
| | Config / Devices / Interfaces / Summary |
| | Config / Devices / Interfaces / Switched Virtual Interfaces |
| | Config / Devices / Interfaces / Trunk Ports |
| | Config / Devices / System / Primary Attributes |
| | Config / Devices / System / Static Routes |
| | Config / Devices / VLANs / Groups |
| | Config / Devices / VLANs / Layer 2 |
| | Config / Devices / VLANs / Layer 2 / Add |
| | Config / Devices / VLANs / Layer 2 / Edit |
| | Config / Devices / VLANs / Layer 3 |
| | Config / Devices / VLANs / Layer 3 / Add |
| | Config / Devices / VLANs / Layer 3 / Edit |
| | Config / Devices / VLANs / Summary |
| | Monitor / Events / Modules |
| Routing/Create | Config / Devices / Network / GigabitEthernet Interfaces |
| | Config / Devices / Network / Global IP DHCP |
| | Config / Devices / Network / Port Channel Interfaces |
| | Config / Devices / Network / Static Routes |
| | Config / Devices / Network / Static VLAN |
| Interface/Create | Config / Devices / Network / BVI Interfaces |
| | Config / Devices / Network / VLAN Interfaces |
| | Monitor / Devices / Traffic Summary |
| | Monitor / Tools / Ping |
| NAT/Create | No specific menus |

*Table 15-2 Role Mapping in ANM*

| Role Tasks/Permissions (continued) | Resulting Menus Available (continued) |
|---|---|
| **Network-Admin Predefined Role (continued)** | |
| Connection/Create | Config / Devices / Load Balancing / Parameter Maps / Connection Parameter Map<br>Config / Devices / Load Balancing / Parameter Maps / Generic Parameter Map<br>Config / Devices / Load Balancing / Parameter Maps / HTTP Parameter Map<br>Config / Devices / Load Balancing / Parameter Maps / Optimization Parameter Map<br>Config / Devices / Load Balancing / Parameter Maps / RTSP Parameter Map<br>Config / Devices / Load Balancing / Parameter Maps / SIP Parameter Map<br>Config / Devices / Load Balancing / Parameter Maps / Skinny Parameter Map |
| **Network-Monitor Predefined Role** | |
| Inventory (which includes Threshold, UDG, Device Events, Switch, and all Virtual Context tasks)/View | Config / Deploy<br>Config / Deploy / Edit<br>Config / Devices / Device Management<br>Config / Devices / Device Management / Edit<br>Config / Devices / Device Management / Modules<br>Config / Devices / Device RBAC / Domains<br>Config / Devices / Device RBAC / Roles<br>Config / Devices / Device RBAC / Users<br>Config / Devices / Expert / Action List<br>Config / Devices / Expert / Action List<br>Config / Devices / Expert / Building Block Audit<br>Config / Devices / Expert / Class Map<br>Config / Devices / Expert / Policy Map<br>Config / Devices / Groups<br>Config / Devices / Groups / Edit<br>Config / Devices / HA Tracking and Failure Detection / Hosts<br>Config / Devices / HA Tracking and Failure Detection / HSRP Groups |

*Table 15-2 Role Mapping in ANM*

| Role Tasks/Permissions (continued) | Resulting Menus Available (continued) |
|---|---|
| **Network-Monitor Predefined Role** | |
| Inventory/View (continued) | Config / Devices / HA Tracking and Failure Detection / Interfaces |
| | Config / Devices / High Availability (HA) / Setup |
| | Config / Devices / Interfaces / Access Ports |
| | Config / Devices / Interfaces / Routed Ports |
| | Config / Devices / Interfaces / Summary |
| | Config / Devices / Interfaces / Switched Virtual Interfaces |
| | Config / Devices / Interfaces / Trunk Ports |
| | Config / Devices / Load Balancing / Health Monitoring |
| | Config / Devices / Load Balancing / Parameter Maps / Connection Parameter Map |
| | Config / Devices / Load Balancing / Parameter Maps / Generic Parameter Map |
| | Config / Devices / Load Balancing / Parameter Maps / HTTP Parameter Map |
| | Config / Devices / Load Balancing / Parameter Maps / Optimization Parameter Map |
| | Config / Devices / Load Balancing / Parameter Maps / RTSP Parameter Map |
| | Config / Devices / Load Balancing / Parameter Maps / SIP Parameter Map |
| | Config / Devices / Load Balancing / Parameter Maps / Skinny Parameter Map |
| | Config / Devices / Load Balancing / Real Servers |
| | Config / Devices / Load Balancing / Server Farms |
| | Config / Devices / Load Balancing / Stickiness |
| | Config / Devices / Load Balancing / Virtual Servers |
| | Config / Devices / Load Balancing / Virtual Servers / Edit |
| | Config / Devices / Network / BVI Interfaces |
| | Config / Devices / Network / GigabitEthernet Interfaces |
| | Config / Devices / Network / Global IP DHCP |
| | Config / Devices / Network / Port Channel Interfaces |
| | Config / Devices / Network / Static Routes |
| | Config / Devices / Network / Static VLAN |

*Table 15-2 Role Mapping in ANM*

| Role Tasks/Permissions (continued) | Resulting Menus Available (continued) |
|---|---|
| **Network-Monitor Predefined Role (continued)** | |
| Inventory/View (continued) | Config / Devices / Network / VLAN Interfaces |
| | Config / Devices / Security / ACLs |
| | Config / Devices / Security / Object Groups |
| | Config / Devices / SSL / Auth Group Parameters |
| | Config / Devices / SSL / Certificate Revocation List |
| | Config / Devices / SSL / Certificates |
| | Config / Devices / SSL / Chain Group Parameters |
| | Config / Devices / SSL / CSR Parameters |
| | Config / Devices / SSL / Keys |
| | Config / Devices / SSL / Parameter Map |
| | Config / Devices / SSL / Proxy Service |
| | Config / Devices / System / Application Acceleration and Optimization |
| | Config / Devices / System / Global Policy |
| | Config / Devices / System / Licenses |
| | Config / Devices / System / Primary Attributes |
| | Config / Devices / System / Primary Attributes |
| | Config / Devices / System / Resource Classes |
| | Config / Devices / System / Resource Classes / Edit |
| | Config / Devices / System / SNMP |
| | Config / Devices / System / Static Routes |
| | Config / Devices / System / Syslog |
| | Config / Devices / Virtual Context Management |
| | Config / Devices / Virtual Context Management / Edit |
| | Config / Devices / VLANs / Groups |
| | Config / Devices / VLANs / Layer 2 |
| | Config / Devices / VLANs / Layer 2 / Edit |
| | Config / Devices / VLANs / Layer 3 |
| | Config / Devices / VLANs / Layer 3 / Edit |
| | Config / Devices / VLANs / Summary |
| | Config / Global / Building Blocks |
| | Config / Global / Expert / Action List |
| | Config / Global / Expert / Class Map |

*Table 15-2 Role Mapping in ANM*

| Role Tasks/Permissions (continued) | Resulting Menus Available (continued) |
|---|---|
| **Network-Monitor Predefined Role (continued)** | |
| Inventory/View (continued) | Config / Global / Expert / Policy Map |
| | Config / Global / Load Balancing / Health Monitoring |
| | Config / Global / Load Balancing / Parameter Maps / Connection Parameter Map |
| | Config / Global / Load Balancing / Parameter Maps / Generic Parameter Map |
| | Config / Global / Load Balancing / Parameter Maps / HTTP Parameter Map |
| | Config / Global / Load Balancing / Parameter Maps / Optimization Parameter Map |
| | Config / Global / Load Balancing / Parameter Maps / RTSP Parameter Map |
| | Config / Global / Load Balancing / Parameter Maps / SIP Parameter Map |
| | Config / Global / Load Balancing / Parameter Maps / Skinny Parameter Map |
| | Config / Global / Load Balancing / Real Servers |
| | Config / Global / Load Balancing / Server Farms |
| | Config / Global / Load Balancing / Stickiness |
| | Config / Global / Network / BVI Interfaces |
| | Config / Global / Network / Global IP DHCP |
| | Config / Global / Network / Static Routes |
| | Config / Global / Network / Static VLAN |
| | Config / Global / Network / VLAN Interfaces |
| | Config / Global / Resource Classes |
| | Config / Global / Resource Classes / Audit |
| | Config / Global / Resource Classes / Edit |
| | Config / Global / Role-Based Access Control / Domains |
| | Config / Global / Role-Based Access Control / Roles |
| | Config / Global / Role-Based Access Control / Users |
| | Config / Global / Security / ACLs |
| | Config / Global / Security / Object Groups |
| | Config / Global / SSL / Auth Group Parameters |
| | Config / Global / SSL / Certificate Revocation List |

*Table 15-2 Role Mapping in ANM*

| Role Tasks/Permissions (continued) | Resulting Menus Available (continued) |
|---|---|
| **Network-Monitor Predefined Role (continued)** | |
| Inventory/View (continued) | Config / Global / SSL / CSR Parameters |
| | Config / Global / SSL / Keys |
| | Config / Global / SSL / Parameter Map |
| | Config / Global / System / Global Policy |
| | Config / Global / System / Primary Attributes |
| | Config / Global / System / SNMP |
| | Config / Global / System / Syslog |
| | Config / Operations / Real Servers |
| | Config / Operations / Virtual Servers |
| | Config / Operations / Virtual Servers / Details |
| | Config / Tools / Credential Pool Management |
| | Config / Tools / IP Discovery |
| | Monitor / Alarm Notifications / Alarms |
| | Monitor / Alarm Notifications / Threshold Groups |
| | Monitor / Alarm Notifications / Threshold Groups / Edit |
| | Monitor / Devices / Application Acceleration |
| | Monitor / Devices / Device Management |
| | Monitor / Devices / Load Balancing |
| | Monitor / Devices / Load Balancing / Statistics |
| | Monitor / Devices / Load Balancing / Statistics |
| | Monitor / Devices / Load Balancing / Virtual Servers |
| | Monitor / Devices / Polling Settings |
| | Monitor / Devices / Resource Usage |
| | Monitor / Devices / Resource Usage |
| | Monitor / Devices / Resource Usage / Connections |
| | Monitor / Devices / Resource Usage / Features |
| | Monitor / Devices / System View |
| | Monitor / Devices / Traffic Summary |
| | Monitor / Devices / Virtual Context Management |
| | Monitor / Devices / Virtual Servers |
| | Monitor / Events / Events |
| | Monitor / Events / Modules |
| | Monitor / Events / Virtual Context Management |
| | Monitor / Settings / Global Polling Configuration |

*Table 15-2 Role Mapping in ANM*

| Role Tasks/Permissions (continued) | Resulting Menus Available (continued) |
|---|---|
| **Network-Monitor Predefined Role (continued)** | |
| Inventory/View (continued) | Monitor / Settings / SMTP Configuration<br>Monitor / Tools / Ping<br>Export<br>Status |
| **Org-Admin Predefined Role** | |
| ANM User Access/Create | Admin / Role-Based Access Control / Domains<br>Admin / Role-Based Access Control / Domains / Add<br>Admin / Role-Based Access Control / Domains / Edit<br>Admin / Role-Based Access Control / Roles<br>Admin / Role-Based Access Control / Roles / Add<br>Admin / Role-Based Access Control / Roles / Edit<br>Admin / Role-Based Access Control / Roles / Users<br>Admin / Role-Based Access Control / Users<br>Admin / Role-Based Access Control / Users / Add<br>Admin / Role-Based Access Control / Users / Edit |
| ANM Inventory/Create | Config / Deploy<br>Config / Deploy / Deploy Now<br>Config / Deploy / Edit<br>Config / Devices / Device Management<br>Config / Devices / Device Management / Add<br>Config / Devices / Device Management / Change Password<br>Config / Devices / Device Management / Edit<br>Config / Devices / Device Management / Modules<br>Config / Devices / Device Management / Modules / Sync<br>Config / Devices / Device Management / Restart Polling<br>Config / Devices / Device Management / Sync<br>Config / Devices / Device RBAC / Domains<br>Config / Devices / Device RBAC / Roles<br>Config / Devices / Device RBAC / Users<br>Config / Devices / Expert / Action List<br>Config / Devices / Expert / Building Block Audit<br>Config / Devices / Expert / Class Map |

*Table 15-2 Role Mapping in ANM*

| Role Tasks/Permissions (continued) | Resulting Menus Available (continued) |
|---|---|
| **Org-Admin Predefined Role (continued)** | |
| ANM Inventory/Create (continued) | Config / Devices / Expert / Policy Map |
| | Config / Devices / Groups |
| | Config / Devices / Groups / Add |
| | Config / Devices / Groups / Edit |
| | Config / Devices / HA Tracking and Failure Detection / Hosts |
| | Config / Devices / HA Tracking and Failure Detection / HSRP Groups |
| | Config / Devices / HA Tracking and Failure Detection / Interfaces |
| | Config / Devices / High Availability (HA) / Setup |
| | Config / Devices / Interfaces / Access Ports |
| | Config / Devices / Interfaces / Routed Ports |
| | Config / Devices / Interfaces / Summary |
| | Config / Devices / Interfaces / Switched Virtual Interfaces |
| | Config / Devices / Interfaces / Trunk Ports |
| | Config / Devices / Load Balancing / Health Monitoring |
| | Config / Devices / Load Balancing / Parameter Maps / Connection Parameter Map |
| | Config / Devices / Load Balancing / Parameter Maps / Generic Parameter Map |
| | Config / Devices / Load Balancing / Parameter Maps / HTTP Parameter Map |
| | Config / Devices / Load Balancing / Parameter Maps / Optimization Parameter Map |
| | Config / Devices / Load Balancing / Parameter Maps / RTSP Parameter Map |
| | Config / Devices / Load Balancing / Parameter Maps / SIP Parameter Map |
| | Config / Devices / Load Balancing / Parameter Maps / Skinny Parameter Map |
| | Config / Devices / Load Balancing / Real Servers |
| | Config / Devices / Load Balancing / Server Farms |
| | Config / Devices / Load Balancing / Stickiness |
| | Config / Devices / Load Balancing / Virtual Servers |

*Table 15-2 Role Mapping in ANM*

| Role Tasks/Permissions (continued) | Resulting Menus Available (continued) |
|---|---|
| **Org-Admin Predefined Role (continued)** | |
| ANM Inventory/Create (continued) | Config / Devices / Load Balancing / Virtual Servers / Add |
| | Config / Devices / Load Balancing / Virtual Servers / Edit |
| | Config / Devices / Network / BVI Interfaces |
| | Config / Devices / Network / GigabitEthernet Interfaces |
| | Config / Devices / Network / Global IP DHCP |
| | Config / Devices / Network / Port Channel Interfaces |
| | Config / Devices / Network / Static Routes |
| | Config / Devices / Network / Static VLAN |
| | Config / Devices / Network / VLAN Interfaces |
| | Config / Devices / Security / ACLs |
| | Config / Devices / Security / Object Groups |
| | Config / Devices / SSL / Auth Group Parameters |
| | Config / Devices / SSL / Certificate Revocation List |
| | Config / Devices / SSL / Certificates |
| | Config / Devices / SSL / Chain Group Parameters |
| | Config / Devices / SSL / CSR Parameters |
| | Config / Devices / SSL / Keys |
| | Config / Devices / SSL / Parameter Map |
| | Config / Devices / SSL / Proxy Service |
| | Config / Devices / System / Application Acceleration and Optimization |
| | Config / Devices / System / Global Policy |
| | Config / Devices / System / Licenses |
| | Config / Devices / System / Primary Attributes |
| | Config / Devices / System / Primary Attributes |
| | Config / Devices / System / Resource Classes |
| | Config / Devices / System / Resource Classes / Add |
| | Config / Devices / System / Resource Classes / Edit |
| | Config / Devices / System / SNMP |
| | Config / Devices / System / Static Routes |
| | Config / Devices / System / Syslog |
| | Config / Devices / Virtual Context Management |
| | Config / Devices / Virtual Context Management / Add |
| | Config / Devices / Virtual Context Management / Edit |

*Table 15-2 Role Mapping in ANM*

| Role Tasks/Permissions (continued) | Resulting Menus Available (continued) |
|---|---|
| **Org-Admin Predefined Role (continued)** | |
| ANM Inventory/Create (continued) | Config / Devices / Virtual Context Management / Extract building block |
| | Config / Devices / Virtual Context Management / Restart Polling |
| | Config / Devices / Virtual Context Management / Sync |
| | Config / Devices / VLANs / Groups |
| | Config / Devices / VLANs / Layer 2 |
| | Config / Devices / VLANs / Layer 2 / Add |
| | Config / Devices / VLANs / Layer 2 / Edit |
| | Config / Devices / VLANs / Layer 3 |
| | Config / Devices / VLANs / Layer 3 / Add |
| | Config / Devices / VLANs / Layer 3 / Edit |
| | Config / Devices / VLANs / Summary |
| | Config / Global / Building Blocks |
| | Config / Global / Building Blocks / Add |
| | Config / Global / Building Blocks / Tag |
| | Config / Global / Expert / Action List |
| | Config / Global / Expert / Action List |
| | Config / Global / Expert / Class Map |
| | Config / Global / Expert / Policy Map |
| | Config / Global / Load Balancing / Health Monitoring |
| | Config / Global / Load Balancing / Parameter Maps / Connection Parameter Map |
| | Config / Global / Load Balancing / Parameter Maps / Generic Parameter Map |
| | Config / Global / Load Balancing / Parameter Maps / HTTP Parameter Map |
| | Config / Global / Load Balancing / Parameter Maps / Optimization Parameter Map |
| | Config / Global / Load Balancing / Parameter Maps / RTSP Parameter Map |
| | Config / Global / Load Balancing / Parameter Maps / SIP Parameter Map |
| | Config / Global / Load Balancing / Parameter Maps / Skinny Parameter Map |

*Table 15-2 Role Mapping in ANM*

| Role Tasks/Permissions (continued) | Resulting Menus Available (continued) |
|---|---|
| **Org-Admin Predefined Role (continued)** | |
| ANM Inventory/Create (continued) | Config / Global / Load Balancing / Real Servers |
| | Config / Global / Load Balancing / Server Farms |
| | Config / Global / Load Balancing / Stickiness |
| | Config / Global / Network / BVI Interfaces |
| | Config / Global / Network / Global IP DHCP |
| | Config / Global / Network / Static Routes |
| | Config / Global / Network / Static VLAN |
| | Config / Global / Network / VLAN Interfaces |
| | Config / Global / Resource Classes |
| | Config / Global / Resource Classes / Add |
| | Config / Global / Resource Classes / Audit |
| | Config / Global / Resource Classes / Edit |
| | Config / Global / Role-Based Access Control / Domains |
| | Config / Global / Role-Based Access Control / Roles |
| | Config / Global / Role-Based Access Control / Users |
| | Config / Global / Security / ACLs |
| | Config / Global / Security / Object Groups |
| | Config / Global / SSL / Auth Group Parameters |
| | Config / Global / SSL / Certificate Revocation List |
| | Config / Global / SSL / CSR Parameters |
| | Config / Global / SSL / Keys |
| | Config / Global / SSL / Parameter Map |
| | Config / Global / System / Global Policy |
| | Config / Global / System / Primary Attributes |
| | Config / Global / System / SNMP |
| | Config / Global / System / Syslog |
| | Config / Operations / Real Servers |
| | Config / Operations / Virtual Servers |
| | Config / Operations / Virtual Servers / Activate |
| | Config / Operations / Virtual Servers / Details |
| | Config / Operations / Virtual Servers / Suspend |
| | Config / Operations / GSS VIP Answers |
| | Config / Operations / DNS Rules |

*Table 15-2 Role Mapping in ANM*

| Role Tasks/Permissions (continued) | Resulting Menus Available (continued) |
|---|---|
| **Org-Admin Predefined Role (continued)** | |
| ANM Inventory/Create (continued) | Config / Tools / Credential Pool Management |
| | Config / Tools / IP Discovery |
| | Monitor / Alarm Notifications / Alarms |
| | Monitor / Alarm Notifications / Threshold Groups |
| | Monitor / Alarm Notifications / Threshold Groups / Add |
| | Monitor / Alarm Notifications / Threshold Groups / Edit |
| | Monitor / Devices / Application Acceleration |
| | Monitor / Devices / Device Management |
| | Monitor / Devices / Load Balancing |
| | Monitor / Devices / Load Balancing / Statistics |
| | Monitor / Devices / Load Balancing / Virtual Servers |
| | Monitor / Devices / Polling Settings |
| | Monitor / Devices / Resource Usage |
| | Monitor / Devices / Resource Usage / Connections |
| | Monitor / Devices / Resource Usage / Features |
| | Monitor / Devices / System View |
| | Monitor / Devices / Traffic Summary |
| | Monitor / Devices / Virtual Context Management |
| | Monitor / Devices / Virtual Servers |
| | Monitor / Events / Events |
| | Monitor / Events / Modules |
| | Monitor / Events / Virtual Context Management |
| | Monitor / Settings / Global Polling Configuration |
| | Monitor / Settings / SMTP Configuration |
| | Monitor / Tools / Ping |
| | Change Password |
| | Copy License |
| | Export |
| | Generate CSR |
| | Import |
| | Install |
| | Resequence |
| | Status |

*Table 15-2 Role Mapping in ANM*

| Role Tasks/Permissions (continued) | Resulting Menus Available (continued) |
|---|---|
| **Org-Admin Predefined Role (continued)** | |
| ANM Inventory/Create<br>(continued) | Uninstall<br>Update |
| **Security-Admin Predefined Role** | |
| AAA/Create | No specific menu items |
| Access List/ | Config / Devices / Security / ACLs<br>Config / Devices / Security / Object Groups<br>Resequence |
| Interface/Modify | Config / Devices / Network / BVI Interfaces<br>Config / Devices / Network / VLAN Interfaces<br>Monitor / Devices / Traffic Summary<br>Monitor / Tools / Ping |
| NAT/Create | No specific menu items |
| Inspect/Create | No specific menu items |
| Connection/Create | Config / Devices / Load Balancing / Parameter Maps / Connection Parameter Map<br>Config / Devices / Load Balancing / Parameter Maps / Generic Parameter Map<br>Config / Devices / Load Balancing / Parameter Maps / HTTP Parameter Map<br>Config / Devices / Load Balancing / Parameter Maps / Optimization Parameter Map<br>Config / Devices / Load Balancing / Parameter Maps / RTSP Parameter Map<br>Config / Devices / Load Balancing / Parameter Maps / SIP Parameter Map<br>Config / Devices / Load Balancing / Parameter Maps / Skinny Parameter Map |
| **Server-Appln Maintenance Predefined Role** | |
| Threshold/View | Monitor / Alarm Notifications / Alarms<br>Monitor / Alarm Notifications / Threshold Groups<br>Monitor / Alarm Notifications / Threshold Groups/ Edit<br>Monitor / Settings / SMTP Configuration |

*Table 15-2 Role Mapping in ANM*

| Role Tasks/Permissions (continued) | Resulting Menus Available (continued) |
|---|---|
| **Security-Admin Predefined Role (continued)** | |
| VIP/View | Config / Deploy |
| | Config / Deploy / Edit |
| | Config / Devices / Load Balancing / Health Monitoring |
| | Config / Devices / Load Balancing / Real Servers |
| | Config / Devices / Load Balancing / Server Farms |
| | Config / Devices / Load Balancing / Stickiness |
| | Config / Devices / Load Balancing / Virtual Servers |
| | Config / Devices / Load Balancing / Virtual Servers / Edit |
| | Config / Operations / Real Servers |
| | Config / Operations / Virtual Servers |
| | Config / Operations / Virtual Servers / Details |
| | Monitor / Devices / Load Balancing |
| | Monitor / Devices / Load Balancing / Statistics |
| | Monitor / Devices / Load Balancing / Virtual Servers |
| | Monitor / Devices / Virtual Servers |
| **Server-Maintenance Predefined Role** | |
| Threshold/View | Monitor / Alarm Notifications / Alarms |
| | Monitor / Alarm Notifications / Threshold Groups |
| | Monitor / Alarm Notifications / Threshold Groups /Edit |
| | Monitor / Settings / SMTP Configuration |
| VIP/View | Config / Deploy |
| | Config / Deploy / Edit |
| | Config / Devices / Load Balancing / Health Monitoring |
| | Config / Devices / Load Balancing / Real Servers |
| | Config / Devices / Load Balancing / Server Farms |
| | Config / Devices / Load Balancing / Stickiness |
| | Config / Devices / Load Balancing / Virtual Servers |
| | Config / Devices / Load Balancing / Virtual Servers / Edit |
| | Config / Operations / Real Servers |
| | Config / Operations / Virtual Servers |
| | Config / Operations / Virtual Servers / Details |
| | Monitor / Devices / Load Balancing |
| | Monitor / Devices / Load Balancing / Statistics |

*Table 15-2 Role Mapping in ANM*

| Role Tasks/Permissions (continued) | Resulting Menus Available (continued) |
|---|---|
| **Security-Admin Predefined Role (continued)** | |
| VIP/View | Monitor / Devices / Load Balancing / Virtual Servers<br>Monitor / Devices / Virtual Servers |
| **SLB-Admin Predefined Role** | |
| Threshold/View | Monitor / Alarm Notifications / Alarms<br>Monitor / Alarm Notifications / Threshold Groups<br>Monitor / Alarm Notifications / Threshold Groups /Edit<br>Monitor / Settings / SMTP Configuration |
| DNS Answer Inservice/Create | Config / Operations / GSS VIP Answers |
| DNS Rule Inservice/Create | Config / Operations / DNS Rules |
| Building Block/Create | Config / Global / Building Blocks<br>Config / Global / Building Blocks / Add<br>Config / Global / Building Blocks / Tag<br>Config / Global / Expert / Action List<br>Config / Global / Expert / Action List<br>Config / Global / Expert / Class Map<br>Config / Global / Expert / Policy Map<br>Config / Global / Load Balancing / Health Monitoring<br>Config / Global / Load Balancing / Parameter Maps / Connection Parameter Map<br>Config / Global / Load Balancing / Parameter Maps / Generic Parameter Map<br>Config / Global / Load Balancing / Parameter Maps / HTTP Parameter Map<br>Config / Global / Load Balancing / Parameter 7Maps / Optimization Parameter Map<br>Config / Global / Load Balancing / Parameter Maps / RTSP Parameter Map<br>Config / Global / Load Balancing / Parameter Maps / SIP Parameter Map<br>Config / Global / Load Balancing / Parameter Maps / Skinny Parameter Map<br>Config / Global / Load Balancing / Real Servers<br>Config / Global / Load Balancing / Server Farms<br>Config / Global / Load Balancing / Stickiness |

*Table 15-2 Role Mapping in ANM*

| Role Tasks/Permissions (continued) | Resulting Menus Available (continued) |
|---|---|
| **SLB-Admin Predefined Role (continued)** | |
| Building Block/Create (continued) | Config / Global / Network / BVI Interfaces |
| | Config / Global / Network / Global IP DHCP |
| | Config / Global / Network / Static Routes |
| | Config / Global / Network / Static VLAN |
| | Config / Global / Network / VLAN Interfaces |
| | Config / Global / Role-Based Access Control / Domains |
| | Config / Global / Role-Based Access Control / Roles |
| | Config / Global / Role-Based Access Control / Users |
| | Config / Global / Security / ACLs |
| | Config / Global / Security / Object Groups |
| | Config / Global / SSL / Auth Group Parameters |
| | Config / Global / SSL / Certificate Revocation List |
| | Config / Global / SSL / CSR Parameters |
| | Config / Global / SSL / Keys |
| | Config / Global / SSL / Parameter Map |
| | Config / Global / System / Global Policy |
| | Config / Global / System / Primary Attributes |
| | Config / Global / System / SNMP |
| | Config / Global / System / Syslog |
| Interface/Modify | Config / Devices / Network / BVI Interfaces |
| | Config / Devices / Network / VLAN Interfaces |
| | Monitor / Devices / Traffic Summary |
| | Monitor / Tools / Ping |
| Expert/Create | Config / Deploy |
| | Config / Deploy / Deploy Now |
| | Config / Deploy / Edit |
| | Config / Devices / Expert / Action List |
| | Config / Devices / Expert / Action List |
| | Config / Devices / Expert / Class Map |
| | Config / Devices / Expert / Policy Map |
| | Config / Devices / Load Balancing / Health Monitoring |
| | Config / Devices / Load Balancing / Parameter Maps / Connection Parameter Map |
| | Config / Devices / Load Balancing / Parameter Maps / Generic Parameter Map |

*Table 15-2 Role Mapping in ANM*

| Role Tasks/Permissions (continued) | Resulting Menus Available (continued) |
|---|---|
| Expert/Create (continued) | Config / Devices / Load Balancing / Parameter Maps / HTTP Parameter Map |
| | Config / Devices / Load Balancing / Parameter Maps / Optimization Parameter Map |
| | Config / Devices / Load Balancing / Parameter Maps / RTSP Parameter Map |
| | Config / Devices / Load Balancing / Parameter Maps / SIP Parameter Map |
| | Config / Devices / Load Balancing / Parameter Maps / Skinny Parameter Map |
| | Config / Devices / Load Balancing / Real Servers |
| | Config / Devices / Load Balancing / Server Farms |
| | Config / Devices / Load Balancing / Stickiness |
| | Config / Devices / Load Balancing / Virtual Servers |
| | Config / Devices / Load Balancing / Virtual Servers / Add |
| | Config / Devices / Load Balancing / Virtual Servers / Edit |
| | Config / Operations / Real Servers |
| | Config / Operations / Virtual Servers |
| | Config / Operations / Virtual Servers / Activate |
| | Config / Operations / Virtual Servers / Details |
| | Config / Operations / Virtual Servers / Suspend |
| | Monitor / Devices / Load Balancing |
| | Monitor / Devices / Load Balancing / Statistics |
| | Monitor / Devices / Load Balancing / Statistics |
| | Monitor / Devices / Load Balancing / Virtual Servers |
| | Monitor / Devices / Virtual Servers |
| **SSL-Admin** | |
| SSL/Create | Config / Devices / SSL / Auth Group Parameters |
| | Config / Devices / SSL / Certificate Revocation List |
| | Config / Devices / SSL / Certificates |
| | Config / Devices / SSL / Chain Group Parameters |
| | Config / Devices / SSL / CSR Parameters |
| | Config / Devices / SSL / Keys |
| | Config / Devices / SSL / Parameter Map |

*Table 15-2 Role Mapping in ANM*

| Role Tasks/Permissions (continued) | Resulting Menus Available (continued) |
|---|---|
| SSL/Create (continued) | Config / Devices / SSL / Proxy Service<br>Export<br>Generate CSR<br>Import |

# Configuring User Authentication

In ANM, you can configure authentication for your users by specifying which AAA servers are used for specific users. You do this through *organizations*. An organization allows you to configure your AAA server lookup for your users, then associate specific users, roles, and domains with those organizations.

The following sections describe the organization authentication tasks you can complete in the ANM interface:

- Guidelines for Managing Organizations, page 15-34
- Configuring AAA Server lookup for your users—See Guidelines for Managing Organizations, page 15-34
- Changing server passwords—See Changing Authentication Server Passwords, page 15-37
- Modifying Organizations, page 15-37
- Duplicating an Organization, page 15-38
- Displaying Authentication Server Organizations, page 15-39
- Deleting Organizations, page 15-39

The Default organization (in which all users belong), authenticates users through the ANM internal mechanism, which is based on the RBAC security model. This mechanism authenticates users through the local authentication module and a local database of user IDs and passwords. If you choose to use an external authentication method, you must specify the authentication server and port.

Many organizations, however, already have an authentication service. To use your own authentication service instead of the local module, you can select one of the alternate modules:

- TACACS+
- RADIUS
- AD/LDAPS

**Note** For detailed procedures on remote authentication, see the "Configuring Authentication and Accounting Services" chapter of either the *Cisco ACE Module Security Configuration Guide* or *Cisco ACE 4700 Series Appliance Security Configuration Guide* on www.cisco.com.

After you configure an organization, all authentication transactions are performed by the authentication service associated with that organization. Users log in with the user ID and password associated with the current authentication module.

**Related Topics**

- Managing User Accounts, page 15-40
- Managing User Roles, page 15-45
- Managing Domains, page 15-51
- Authenticating ANM Users with a AAA Server, page 15-56

# Guidelines for Managing Organizations

Organizations define the mechanism for authenticating users: RADIUS, TACACS+, AD/LDAPS, or Local. When the authentication is remote, users within that organization will have their passwords validated externally.

Use this procedure to configure organizations.

**Note** All users logging into ANM must have a local account.

**Procedure**

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

**Step 2** Click **Add**.

**Step 3** Enter the name of the new organization, and notes if required. Click **Save**.

**Step 4** Enter the attributes described in Table 15-3. Certain attributes will display when specific options are selected.

*Table 15-3 Organization Attributes*

| Attribute | Description |
|---|---|
| Notes | Description of the organization or notes to administrator. |
| Organization Name | This can be different from the organization name above. Specifies the company, department, or division of the organization that administers the ANM server. Default name entered appears. |
| Account Number | Specifies an account number for the organization. |
| Contact Name | Specifies the name of the individual who is the contact in the organization. |
| Email | Specifies an address for the organization's contact person. |
| Telephone # | Specifies a telephone number for the organization's contact person. The format is free text with no embedded spaces. |
| Alternative Telephone # | Specifies an alternative telephone number for the organization's contact person. |
| Street Address | Specifies the street for the organization. |
| City | Specifies the city where the organization is located. |
| Zip Code | Specifies a zip code for the organization's address. |
| Country | Specifies the country where the organization is located. |
| Authentication | Specifies how users are to be authenticated by the system. The default authentication mechanism is ANM's internal mechanism, which is based on ANM's security model. If an external authentication method is chosen, the authentication server and port must be specified.<br>Options:<br>• Local—Specifies the use of the local database.<br>• RADIUS<br>• TACACS+<br>• AD/LDAPS (ANM requires that a Domain Controller Server certificate be installed on the Active Directory Server. For a document containing the detailed instructions, see the "Configuring an LDAP Server" section in the "Configuring Authentication and Accounting Services" chapter of either the *Cisco ACE Module Security Configuration Guide or Cisco ACE 4700 Series Appliance Security Configuration Guide* on www.cisco.com.<br>**Note** ANM itself does not perform authorization. ANM only provides authentication for users who are logging in to ANM. |

*Table 15-3 Organization Attributes (continued)*

| Attribute | Description |
|---|---|
| Authentication Port | (Optional) Specifies the UDP destination port for communicating authentication requests to the authentication server. Depending on your server, the following may be true:<br>• By default, the RADIUS authentication port is 1812 (as defined in RFC 2138 and RFC 2139). The port_number argument specifies the RADIUS port number. Valid values are from 1 to 65535.<br>• TACACS+<br>• LDAPS<br>For a document containing the detailed instructions, see the "Configuring an LDAP Server" section in the "Configuring Authentication and Accounting Services" chapter of either the *Cisco ACE Module Security Configuration Guide or Cisco ACE 4700 Series Appliance Security Configuration Guide* on www.cisco.com.<br>**Note** ANM itself does not perform authorization. ANM only provides authentication for users who are logging in to ANM. |
| Secondary Authentication Port | (Optional) Specifies another UDP destination port for communicating authentication requests to the RADIUS, TACACS+, or LDAPS server if the initial port is busy. |
| **Note** You will see the following fields if external authentication is used in the organization. | |
| Authentication Server | Specifies the IP address of a RADIUS, TACACS+, or LDAPS server for user authentication.<br>Specifies an external server when RADIUS, TACACS+, or LDAPS is to be used to authenticate users.<br>**Note** Setting the server with this command is mandatory if the authentication mechanism is anything other than default.<br>If you select an external authentication method, you might need to specify a separate user ID for the authentication server.<br>For AD/LDAPS, you must provide the FQDN of the server (which must be in the users authenticating domain).<br>**Note** ANM supports LDAPS is only through Active Directory (AD). |
| Secondary Authentication Server | (Optional) Specifies a secondary external server when Radius, TACACS+, or LDAPS is to be used to authenticate users. If you specify a secondary authentication server, ANM uses this server to authenticate users if the primary authentication server is unavailable. |
| Authentication Secret | Encrypts the traffic between the Cisco ANM and the AAA server. This string needs to be identical on both. |

**Step 5** Click **Save**.

**Related Topics**

- Managing User Accounts, page 15-40
- Changing the Admin Password, page 15-37

# Changing Authentication Server Passwords

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

**Procedure**

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

**Step 2** Select the organization you want to modify, then click **Edit**.

**Step 3** Change the password attribute in the attributes table (see Table 15-4).

**Step 4** Click **Save**.

**Step 5** The Edit User Details screen appears. Make any changes and click **Save**. When all the details are correct, click **Cancel**. The User Management table is displayed.

**Related Topics**

- Managing User Accounts, page 15-40
- Changing the Admin Password, page 15-37

# Changing the Admin Password

Each ANM 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 1-3.

**Note** For details about resetting the Admin password, see the *Installation Guide for Cisco Application Networking Manager 2.1*.

# Modifying Organizations

**Assumptions**

- ANM is installed and running.
- The organization exists in the ANM database.
- You have reviewed the guidelines for managing customer organizations (see Guidelines for Managing Organizations, page 15-34).

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

**Procedure**

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

**Step 2** Select the organization you want to modify.

**Step 3** Click **Edit**.

**Step 4** Modify any of the attributes in the attributes table (see Table 15-3).

**Step 5** Click **Save**.

**Related Topics**

Configuring User Authentication, page 15-33

# Duplicating an Organization

Use this option to create a new organization from an existing one.

**Assumptions**

- ANM is installed and running.
- The organization exists in the ANM database.
- You have reviewed the guidelines for managing customer organizations (see Guidelines for Managing Organizations, page 15-34).

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

**Procedure**

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

**Step 2** Select the organization you want to copy.

**Step 3** Click **Duplicate**.

**Step 4** At the prompt, enter a name for the new organization.

**Step 5** Click **OK.**

**Step 6** Make any changes to the organization settings (see Table 15-3).

**Step 7** Click **Save**.

**Related Topics**

Configuring User Authentication, page 15-33

# Displaying Authentication Server Organizations

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

**Procedure**

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

The list of customer organizations appears in the All Organizations table.

**Step 2** From this screen you can create a users, roles, and domains that are associated with this specific organization. You can also access organizations by selecting the organization from the object selector that displays in the top right portion of the content area.

**Related Topics**

- Understanding Organizations, page 15-8
- Configuring User Authentication, page 15-33

# Deleting Organizations

**Assumptions**

- ANM is installed and running.
- The organization exists in the ANM database.
- You have reviewed the guidelines for managing customer organizations (see Guidelines for Managing Organizations, page 15-34).

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

**Procedure**

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

The Organizations list contains a list of the existing organizations.

**Step 2** Select the organization to be deleted.

**Step 3** Click **Delete**. All users, domains, and roles within that organization are removed.

**Related Topics**

Configuring User Authentication, page 15-33

# Managing User Accounts

Use the User Management 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 User Accounts, page 15-40
- Displaying a List of Users, page 15-40
- Creating User Accounts, page 15-41
- Duplicating a User Account, page 15-42
- Modifying User Accounts, page 15-43
- Deleting User Accounts, page 15-44
- Resetting Another User's Password, page 15-43


**Note** You can create users in the organization in which you are a member. You will see users only in the organizations in which you are a member.

## Guidelines for Managing User Accounts

- User cannot log in until they have one domain and one user role associated via an organization. This can be the Default domain but a role must be specified.
- Users cannot be moved from one organization to another. Organizations are designed to be separate and distinct.
- Only users with create permissions can reset other user's password. See "Resetting Another User's Password" section on page 15-43.

## Displaying a List of Users

### Procedure

**Step 1** Select **Admin > Role-Based Access Control >** ***Organization*** **> Users**. A table of users, their role, and their domain appears.

**Step 2** From this screen you can create a new user, duplicate, modify or delete any existing user to which you have access.

### Related Topics

Managing User Accounts, page 15-40

# Creating User Accounts

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

**Procedure**

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

**Step 2** Click **Add**.

**Step 3** Complete the following required fields as illustrated in Table 15-4:

***Table 15-4 User Attributes***

| Field | Description |
|---|---|
| Login 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. |
| Name | Specifies the full name of the user. The format is free text. |
| Password | Allows you to specify a password for this user account. |
| Confirm | Renter the password for this account. |
| Email | Specifies an e-mail address for this user. |
| Telephone# | Specifies a telephone number for this user. The format is free text with no embedded spaces. |
| Role | Specifies a predefined role from the list. |
| Domains | Allows you to use the **Add** and **Remove** buttons to select domains to which this user belongs. |
| Allowed Login IP | Defines an IP address or a subnetwork from which the user is allowed to log in. You can define up to ten different addresses for a single user. Unless you specifically define IP addresses or subnetworks using this option, the user can log in from any IP address. When you enter an allowed single IP address or an allowed subnet, then the user is only allowed to log in from the specified addresses. To restrict access to a specific subnetwork, enter the IP address and the mask, for example, 10.1.200.60/255.255.255.0.<br>**Note** IP addresses 1.1.1.1 and 0.0.0.0 cannot be entered in this field. |
| Description | Enter any notes about the user. |
| First menu | Menu that displays when this user first logs in. Choose one from the pulldown menu. |
| Last Login | Last time (local time) this user logged in. |

**Step 4** Click **Save**. The Users table is displayed.

**Related Topics**

Managing User Accounts, page 15-40

# Duplicating a User Account

Use this option to create a new user account using settings from an existing user.

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

**Procedure**

**Step 1** Select **Admin > Role-Based Access Control >** ***Organization*** **> Users**. A table of users, their role and domain appears.

**Step 2** Select the user account you want to copy.

**Step 3** Click **Duplicate**.

**Step 4** At the prompt, enter a name for the new user account.

**Step 5** Click **OK**.

The Users table appears with the new user account.

**Step 6** To make changes to the user account settings as shown in Table 15-5.

***Table 15-5 Duplicate User Attributes***

| Field | Description |
|---|---|
| Login Name | Name you specified when you created the user you want to duplicate. This is 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. |
| Name | Specifies the full name of the user. The format is free text. |
| Email | Specifies an e-mail address for this user. |
| Telephone# | Specifies a telephone number for this user. The format is free text with no embedded spaces. |
| Role | Specifies a predefined role from the list. |
| Domains | Allows you to use the **Add** and **Remove** buttons to select domains to which this user belongs. |
| Allowed Login IP | Defines an IP address or a subnetwork from which the user is allowed to log in. You can define up to ten different addresses for a single user. Unless you specifically define IP addresses or subnetworks using this option, the user can log in from any IP address. When you enter an allowed single IP address or an allowed subnet, then the user is only allowed to log in from the specified addresses. To restrict access to a specific subnetwork, enter the IP address and the mask, for example, 10.1.200.60/255.255.255.0.<br>**Note** IP addresses 1.1.1.1 and 0.0.0.0 cannot be entered in this field. |
| Description | Enter any notes about the user. |

*Table 15-5 Duplicate User Attributes*

| Field | Description |
|---|---|
| First Menu | Menu that is displayed when this user first logs in. Choose one from the pulldown menu. |
| Last Login | Last time (local time) this user logged in and the IP address that was used. |

**Step 7** Click **Save**.

**Step 8** The Edit Organization User screen appears. Make any changes and click **Save**. When all the details are correct, click **Cancel**. The table of users is displayed.

**Related Topics**

Managing User Accounts, page 15-40

# Modifying User Accounts

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

**Procedure**

**Step 1** Select **Admin > Role-Based Access Control >** ***Organization*** **> Users**. A table of users, their role, and domain appears.

**Step 2** Select the user account you want to modify.

**Step 3** Click **Edit**.

**Step 4** Modify any of the attributes in the attributes table (see Table 15-4).

**Step 5** Click **Save**.

**Step 6** The Edit User Details screen appears. Make any changes and click **Save**. When all the details are correct, click **Cancel**, the User Management table is displayed.

**Related Topics**

Managing User Accounts, page 15-40

# Resetting Another User's Password

Use this procedure to reset another users's password.

**Note** You *must* have create permissions in order to reset another user's passoword.

**Step 1** Log in to ANM making sure the login username has create permissions.

**Step 2** Go to **Admin** > **Users**.

**Step 3** Select the username for which the password needs to be reset.

**Step 4** Click the **Reset Password** button. The reset password popup is displayed with the selected username in the username field.

**Step 5** Enter and confirm the new password.

**Step 6** Click **OK**.

If there are no errors, the **Password has been reset** message is displayed.

**Related Topics**

- Managing User Accounts, page 15-40
- Displaying or Terminating Current User Sessions, page 15-44

## Deleting User Accounts

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

**Procedure**

**Step 1** Select **Admin > Role-Based Access Control >** ***Organization*** **> Users**. A table of users, their role and domain appears.

**Step 2** Select the user account to be deleted, then click **Delete**.

**Step 3** Confirm deletion of the user by clicking **OK** or **Cancel** to return to the Users table.

The user account is removed from the ANM database.

**Related Topics**

Managing User Accounts, page 15-40

# Displaying or Terminating Current User Sessions

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

You can only see the users in your organization.

**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 15-6 Active User Session Information*

| Column | Description |
|---|---|
| Name | The name used to log into the Cisco ANM |
| Type Of Login | Method used to log in, for example WEB |
| Login From IP | IP address of host |
| Time Of Login | Time user logged in |

**Step 2** To terminate an active session, click **Terminate**.

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

For more details on terminating active users, see Displaying or Terminating Current User Sessions, page 15-44.

**Related Topics**

- Controlling Access to Cisco ANM, page 15-4
- Managing User Accounts, page 15-40

# Managing User Roles

Use the Roles Management feature to add, modify, and delete user-defined roles and to modify predefined roles. You cannot delete predefined roles.

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. For example, if you design a role that provides access to virtual servers, the role automatically includes access to all real servers that could be included in the virtual server.

The following sections describe how to manage user roles:

- Guidelines for Managing User Roles, page 15-46
- Displaying User Roles, page 15-48
- Creating User Roles, page 15-48
- Duplicating a User Role, page 15-49
- Modifying User Roles, page 15-50
- Deleting User Roles, page 15-50

# Guidelines for Managing User Roles

- System Administrators can view and modify all roles.
- Organization administrator users can only see and modify the users, roles, and domains in their organization.
- Other users can only view the user, roles, and domains assigned to them.
- User-defined roles can be created but follow strict rules about which tasks can be selected or deselected. See the user interface for specific dependencies or Table 15-2 on page 15-11 for role to task mapping information.
- You must have the ability to create real servers in your role and at least one virtual context in your domain before you can create real servers.
- You must have the ability to create virtual contexts in your role and an Admin context in your domain before you can create virtual contexts.
- If you upgrade to ANM 2.1, any custom roles that are migrated retain their associations but have different role definitions. We encourage you to use the ANM 2.1 predefined default roles.

# Understanding Predefined Roles

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.

The predefined roles and their default privileges are defined in Table 15-7. For detailed information on RBAC, see either the *Cisco Application Control Engine Module Virtualization Configuration Guide* or the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

***Table 15-7 ANM Predefined Role Tasks***

| Predefined Role | Description | Role Tasks/Operation Privileges[1] |
|---|---|---|
| ACE-Admin | Access to create virtual contexts and monitor threshold information. | • View Threshold<br>• Create Device Events<br>• Create Virtual Context+ |
| ANM-Admin | Access to create virtual contexts and monitor threshold information. Provides access to all features and functions. | • Create ANM System<br>• Create ANM User Access<br>• Create ANM Inventory+ |
| Network-Admin | Admin for L3 (IP and Routes) and L4 VIPs | • View Threshold<br>• Create Switch<br>• Create Routing<br>• Create Interface<br>• Create NAT<br>• Create Connection |
| Network-Monitor | Monitoring for all features | • View ANM Inventory+ |

*Table 15-7 ANM Predefined Role Tasks*

| Predefined Role | Description | Role Tasks/Operation Privileges[1] |
|---|---|---|
| Org-Admin | Access to create role-based access control and import and update device data. | • Create ANM User<br>• Create ANM Inventory+ |
| Security-Admin | Security features | • Create AAA<br>• Modify Interface<br>• Create NAT<br>• Create Inspect<br>• Create Connection |
| Server-Appln-Maintenance | Server maintenance and L7 policy application | • View Threshold<br>• View VIP<br>• View Virtual Inservice<br>• Create LoadBalancer+ |
| Server-Maintenance | Server maintenance, monitoring, and debugging | • View Threshold<br>• View VIP+<br>• Modify Real Server<br>• Debug Probe<br>• Create Real Inservice |
| SLB-Admin | Load-balancing features | • View Threshold<br>• Create Building Block<br>• Modify Interface<br>• Create Expert+ |
| SSL-Admin | SSL feature features | • Create SSL+ |

1. Where the plus sign (+) is indicated, all permissions included in this folder are included at the same privilege level, unless otherwise noted. For example, Virtual Contexts tasks are comprised of tasks such as AAA, Building Blocks, and so on. These tasks are depicted as columns in the Roles table.

# Displaying User Role Relationships

Use this procedure to display which users are associated to specific roles.

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

**Procedure**

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

**Step 2** Select a role and click **Users**. A screen displays a table containing the following. For information on how roles map to users, see Table 15-2, "Role Mapping in ANM".

From this screen you can delete or duplicate a user.

**Step 3** Click **Close** to return to the Roles table.

**Related Topics**

- Duplicating a User Account, page 15-42
- Managing User Roles, page 15-45

# 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 >** ***Organizations*** **> 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 (see Creating User Roles, page 15-48).
- View the users assigned to a role (see Displaying User Role Relationships, page 15-47).
- Modify any existing role to which you have access (see Modifying User Roles, page 15-50).
- Duplicate any existing role to which you have access (see Duplicating a User Role, page 15-49).
- Delete any existing role to which you have access (see Deleting User Roles, page 15-50).

**Related Topics**

- Understanding Operations Privileges, page 15-7
- Managing User Roles, page 15-45

# Creating User Roles

You can edit the predefined roles, or 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 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 >** ***Organization*** **> Roles**. A table of the defined roles and their settings appears.

**Step 2** Click **Add**. The New Role form appears.

**Step 3** Enter the following attributes as shown in Table 15-8:

*Table 15-8 Role Attributes*

| Attribute | Description |
|---|---|
| Name | The name of the role. |
| Description | A brief description of the role. |
| Role Tasks | A role tree that defines the operation privileges and features available to this role. |
| Resulting Menu Items | Displays a synchronized list of features in the form of menus that this role is able to access after setting the role task operation privileges. |

**Step 4** Click **Save**. The new role is added to the list of user roles.

**Step 5** To assign this new role to one or more users, go to **Admin > *Organizations* > Users**. For detailed steps, see Modifying User Accounts, page 15-43.

**Related Topics**

- Understanding Operations Privileges, page 15-7
- Managing User Roles, page 15-45

# Duplicating a User Role

Use this option to create a new user-defined role from an existing one.

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

**Procedure**

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

**Step 2** Select the role you want to copy.

**Step 3** Click **Duplicate**.

**Step 4** At the prompt, enter a name for the new role.

**Step 5** Click **OK**.

**Step 6** Make any changes to the role settings.

**Step 7** Click **Save**.

**Related Topics**

- Understanding Operations Privileges, page 15-7

- Managing User Roles, page 15-45

# 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 >** ***Organization*** **> 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 **Save**.

**Related Topics**

- Understanding Operations Privileges, page 15-7
- Managing User Roles, page 15-45

# Deleting User Roles

You can delete any user-defined roles.

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

**Procedure**

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

**Step 2** Select the role to be deleted.

**Step 3** Click **Delete**.

**Step 4** Click **OK** to confirm the deletion. Users that have the deleted role no longer have that access.

**Related Topics**

Managing User Roles, page 15-45

# 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. You can allow access to a domain by assigning it to an organization. Examples are specific virtual contexts, or specific servers within a context.

The following sections describe how to manage domains:


- Guidelines for Managing Domains, page 15-51
- Displaying Network Domains, page 15-52
- Creating a Domain, page 15-52
- Duplicating a Domain, page 15-53
- Modifying a Domain, page 15-54
- Deleting a Domain, page 15-54


## Guidelines for Managing Domains

- Domains are *logical* concepts. You do *not* delete a member of a domain when you delete the domain.
- Domains can include supported Cisco chassis, ACE modules, ACE appliances, and CSS or CSM devices, as well as their virtual contexts, building blocks, resource classes, and real and virtual servers.
- Select the Allow All setting to include current and future device objects in a domain.
- Objects must already exist in ANM. To add objects, see Adding Network Devices into ANM, page 2-8.
- You must have the ability to create real servers in your role and at least one virtual context in your domain before you can create real servers.
- You must have the ability to create virtual contexts in your role and an Admin context in your domain before you can create virtual contexts.
- Domains continue to display device information even after you remove that device from ANM. This allows the domain information to be easily reassociated if you reimport the device. The device name must remain the same for this to work properly.

**Caution** Domain objects are hierarchical. If you include a parent object in a domain, the child object is also included even though they do not display in the Object selector tree when you add or edit domains.

For example:

- Inclusion of a Catalyst device includes all cards, virtual contexts, real servers and virtual servers
- Inclusion of an ACE 4710 includes all cards, virtual contexts, real servers and virtual servers
- Inclusion of a virtual context, CSM module or CSS device includes all associated objects

### Related Topics


- Creating a Domain, page 15-52
- Modifying a Domain, page 15-54

- Displaying Network Domains, page 15-52
- Duplicating a Domain, page 15-53
- Deleting a Domain, page 15-54

# Displaying Network Domains

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

**Procedure**

**Step 1** Select **Admin > Role-Based Access Control >** ***Organization*** **> 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, then click **Edit**.

**Related Topics**

- Managing Domains, page 15-51
- Guidelines for Managing Domains, page 15-51
- Creating a Domain, page 15-52
- Duplicating a Domain, page 15-53
- Modifying a Domain, page 15-54
- Deleting a Domain, page 15-54

# Creating a Domain

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 >** ***Organization*** **> Domains**. The Domains table appears.

**Step 2** Click **Add**.

**Step 3** For the new domain, enter the following information as outlined in Table 15-9:

*Table 15-9 Domain Attributes*

| Field | Description |
|---|---|
| Name | The name of the domain. |
| Description | The description of the domain. |

*Table 15-9 Domain Attributes*

| Field | Description |
|---|---|
| Allow All | Enables all objects within this domain (current and future objects). If this check box is left empty, the Objects tree displays. |
| Objects | The collection of objects which comprise this domain. Select an object name and use the arrows to move it from the available to selected column.<br>For example, selecting a virtual context selects all real servers within that virtual context, or selecting a chassis selects the virtual contexts on that chassis. The interface does not explicitly display this in the table, but the objects are, in fact, selected.<br>See Guidelines for Managing Domains, page 15-51 for domain rules about creating virtual contexts and real servers. |

**Step 4** Click **Save**.

The Domains Edit screen updates and displays the total object number next to the object name.

**Related Topics**

- Managing Domains, page 15-51
- Guidelines for Managing Domains, page 15-51
- Displaying Network Domains, page 15-52
- Creating a Domain, page 15-52
- Duplicating a Domain, page 15-53
- Modifying a Domain, page 15-54
- Deleting a Domain, page 15-54

# Duplicating a Domain

Use this option to create a new domain from an existing one.

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

**Procedure**

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

**Step 2** Select the domain you want to copy.

**Step 3** Click **Duplicate**.

**Step 4** At the prompt, enter a name for the new domain, then click **OK.**

**Step 5** Click **Save**.

**Related Topics**

- Managing Domains, page 15-51
- Guidelines for Managing Domains, page 15-51
- Displaying Network Domains, page 15-52
- Creating a Domain, page 15-52
- Modifying a Domain, page 15-54
- Deleting a Domain, page 15-54

# Modifying a Domain

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 >** ***Organization*** **> Domains**.

**Step 2** Select the domain you want to change.

**Step 3** Click **Edit**.

**Step 4** Make the changes. For detailed domain attribute descriptions, see Table 15-9 on page 15-52.

**Step 5** Click **Save**.

**Related Topics**

- Managing Domains, page 15-51
- Guidelines for Managing Domains, page 15-51
- Displaying Network Domains, page 15-52
- Creating a Domain, page 15-52
- Duplicating a Domain, page 15-53
- Deleting a Domain, page 15-54

# Deleting a Domain

Use this option to delete a network domain from the systems. You do *not* delete objects associated with that domain when you delete the domain.

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

### Procedure

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

The Domains list contains a list of the existing domains.

**Step 2** Select the domain you want to delete.

**Step 3** Click **Delete**. A prompt asks if you to confirm this action.

**Step 4** Click **OK**. The domain is removed from the ANM database.

### Related Topics

- Managing Domains, page 15-51
- Guidelines for Managing Domains, page 15-51
- Displaying Network Domains, page 15-52
- Creating a Domain, page 15-52
- Duplicating a Domain, page 15-53
- Modifying a Domain, page 15-54

# Authenticating ANM Users with a AAA Server

RBAC is a common access control method in networking today. ANM allows the administrator to centrally control user authentication and authorization. Users may be authenticated using a local database that resides only in the ANM, or the user database may reside on an external server such as a RADIUS or TACACS+ server. In ANM, you can configure authentication for your users by specifying which AAA servers are used for specific users. You do this through organizations. An organization allows you to configure your AAA server lookup for your users, then associate specific users, roles, and domains with those organizations.

This topic describes how to configure the ANM to use a TACACS+ server for user authentication. This section is intended as a guide to help ensure proper communication with the AAA server and ANM operating as the AAA client. If a user is successfully authenticated by the TACACS+ server, then the ANM will determine the authorization for the user (what objects he or she can manipulate, and which actions he or she can take on those objects).

For details on configuring the Cisco Secure ACS, OpenLDAP Software, or another AAA server, see the documentation that is provided with the software.

Table 15-10 provides a high-level overview of the steps required to authenticate ANM users with a TACACS+ server.

**Note** For background information on configuring a AAA server, see the "Configuring Authentication and Accounting Services" chapter of either the *Cisco ACE Module Security Configuration Guide or Cisco ACE 4700 Series Appliance Security Configuration Guide* on www.cisco.com.

### Assumption

- For purposes of this example, assume usage of a Cisco Secure ACS version 4.1 server.
- Your user role determines whether you can perform the procedures outlined in this section.
- Administrative login rights are required to access the Cisco Secure ACS HTML interface.

### Related Topics

- Controlling Access to Cisco ANM, page 15-4
- How ANM Handles Role-Based Access Control, page 15-9

*Table 15-10 Authenticating ANM Users with a TACACS+ Server*

| | Task | Procedure |
|---|---|---|
| **Step 1** | Create a new organization and define the external TACACS+ server used (ANM) | External authentication servers are defined in ANM as organizations. A single server can be used in multiple organizations. To configure authentication for your users by creating a new organization and defining TACACS+ as the method of authentication, perform the following steps:<br>**Note** Your user role determines whether you can use this option.<br>1. Select **Admin > Role-Based Access Control > All Organizations**.<br>2. Click **Add**.<br>3. Enter the name of the new organization, and notes if required. Click **Save**.<br>4. Enter the attributes described in Table 15-3. Certain attributes will display when specific options are selected. Include the following organization attributes to authenticate ANM users with a TACACS+ server:<br>– Organization name<br>– TACACS+ as authentication method<br>– IP address of TACACS+ server<br>– Authentication port number<br>– Authentication secret<br>See the "Guidelines for Managing Organizations" section on page 15-34 for details on this procedure. |
| **Step 2** | Creating a new role for RBAC (ANM) | You can edit the predefined roles, or 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 privileges for each task. You can also assign this role to one or more users.<br>**Note** Your user role determines whether you can use this option.<br>To create a user role, perform the following steps:<br>1. Select **Admin > Role-Based Access Control > *Organization* > Roles**. A table of the defined roles and their settings appears.<br>2. Click **Add**. The New Role form appears.<br>3. Enter the following attributes as described in Table 15-8.<br>4. Click **Save**. The new role is added to the list of user roles. |

*Table 15-10 Authenticating ANM Users with a TACACS+ Server (continued)*

| | Task | Procedure |
|---|---|---|
| **Step 3** | Create an domain for an RBAC user<br>(ANM) | A domain defines which objects that the RBAC user will have access to. The assigned role defines which actions that user will be able to perform on those objects.<br><br>To configure a domain for an RBAC user, perform the following steps:<br><br>**Note** Your user role determines whether you can use this option.<br><br>1. Select **Admin > Role-Based Access Control > *Organization* > Domains**. The Domains table appears.<br>2. Click **Add**.<br>3. For the new domain, enter the attributes as described in Table 15-9.<br><br>**Note** If you check the Allow All checkbox, this selection enables all objects within this domain (current and future objects). If you leave this check box unchecked, the Objects tree displays. To allow a user to have access to the entire context, highlight the Virtual Contexts folder in the Objects tree, locate the specific user context, and then click the arrow to send it to the Selected box. The context name format is: `<chassis-name>:<slot-number>:<context-name>`<br><br>4. Click **Save** when all the objects that you want to allow access to are listed in the Selected box.<br><br>See the "Creating a Domain" section on page 15-52 for details on this procedure. |
| **Step 4** | Create a new organization user<br>(ANM) | Organization users are users who work for the customer of a service provider or AAA server that segments your users and to whom you want to grant access to ANM.<br><br>**Note** Your user role determines whether you can use this option.<br><br>To create an organization user, perform the following steps:<br><br>1. Select **Admin > Role-Based Access Control > *Organization* > Users**. A list of users appears.<br>2. Click **Add**.<br>3. For the new organization user, enter the attributes as described in Table 15-4. Include the following organization user attributes:<br>– Login name<br>– Predefined role<br>– Domains to which this user belongs<br>4. Click **Save**. The Users table is displayed.<br><br>See the "Creating User Accounts" section on page 15-41 for details on this procedure. |

*Table 15-10 Authenticating ANM Users with a TACACS+ Server (continued)*

| | Task | Procedure |
|---|---|---|
| **Step 5** | Access the AAA server (Cisco Secure ACS server) | To access the Cisco Secure ACS HTML interface, perform the following steps:<br>**Note** Administrative login rights are required to access the Cisco Secure ACS HTML interface.<br>1. Open a web browser for the URL of the Cisco Secure ACS HTML interface.<br>2. In the Username box, type a valid Cisco Secure ACS administrator name.<br>3. In the Password box, type the password for the administrator name you specified.<br>4. Click **Login**. The Cisco Secure ACS HTML interface appears.<br>**Note** For the ACE to properly perform user authentication using a TACACS+ server, the username and password must be identical on both ANM and the TACACS+ server.<br>For details on configuring the Cisco Secure ACS HTML server, see the documentation that is provided with the software. |
| **Step 6** | Create a new network device group (Cisco Secure ACS Server) | To create a new group of TACACS+ clients and servers on the Cisco Secure ACS HTML server, perform the following steps:<br>1. Go to the Network Configuration section of the Cisco Secure ACS HTML interface.<br>2. In the navigation bar, click the **Network Configuration** button. The Network Configuration page screen appears in the Cisco Secure ACS HTML interface.<br>3. Under the Network Device Groups table, click the **Add Entry** button to create a new group of TACACS+ clients and servers. Type the name of the new group (for example ANM).<br>4. Click **Submit**.<br>For details on configuring the Cisco Secure ACS HTML server, see the documentation that is provided with the software. |

*Table 15-10 Authenticating ANM Users with a TACACS+ Server (continued)*

| | Task | Procedure |
|---|---|---|
| **Step 7** | Specify AAA client setup for ANM<br>(Cisco Secure ACS Server) | To define the AAA client setup for ANM on the Cisco Secure ACS HTML server, perform the following steps:<br>1. Click **Add Entry** below the AAA Clients table. The Add AAA Client page appears.<br>2. Specify the following attributes:<br>– AAA Client IP Address—Client IP address of ANM that will be used for communicating with the TACACS+ server.<br>– Shared Secret—Shared secret specified on ANM.<br>– Network Device Group—ANM<br>– Authenticate Using—TACACS+ (Cisco IOS)<br>**Note** The TACACS+ (Cisco IOS) drop-down item is the title for the Cisco TACACS+ authentication function. The TACACS+ (Cisco IOS) selection activates the TACACS+ option when using Cisco Systems access servers, routers, and firewalls that support the TACACS+ authentication protocol. This includes support with ANM as well.<br>3. Click **Submit + Apply**.<br>For details on configuring the Cisco Secure ACS HTML server, see the documentation that is provided with the software. |
| **Step 8** | Specify AAA server setup<br>(Cisco Secure ACS Server) | To define the AAA server setup for ANM on the Cisco Secure ACS HTML server, perform the following steps:<br>1. Click **Add Entry** below the AAA Servers table. The Add AAA Servers page appears.<br>2. Specify the following attributes:<br>– AAA Server IP Address—IP address of the TACACS+ server.<br>– Key—Shared secret specified on ANM.<br>– Log Update/Watchdog Packets from This Remote AAA Server—Enabled<br>– Network Device Group—ANM<br>– AAA Server Type—TACACS+<br>– Traffic Type—Inbound/Outbound<br>3. Click **Submit + Apply**.<br>For details on configuring the Cisco Secure ACS HTML server, see the documentation that is provided with the software. |

*Table 15-10 Authenticating ANM Users with a TACACS+ Server (continued)*

| | Task | Procedure |
|---|---|---|
| **Step 9** | Create the ANM user on the TACACS+ server (Cisco Secure ACS Server) | To create the ANM user on the Cisco Secure ACS HTML server, perform the following steps:<br>1. Click the **User Setup** button. The User Setup screen appears.<br>2. In the User text box, enter the user name of the organization user that you created in ANM (see step 3).<br>3. Click the **Add/Edit** button.<br>4. Specify the following user attributes:<br>– Real Name—Real name of the ANM user.<br>– Description—Brief description of the user for the administrator.<br>– Password Authentication—ACS Internal Database.<br>– Password—Password for this user account. Enter this password a second time in the Confirm Password text box.<br>For details on configuring the Cisco Secure ACS HTML server, see the documentation that is provided with the software. |

*Table 15-10 Authenticating ANM Users with a TACACS+ Server (continued)*

| | Task | Procedure |
|---|---|---|
| **Step 10** | Log in to ANM using the newly created account | To test the new login credentials for user authentication, perform the following steps:<br>**1.** Login to ANM by entering the new user account in the ANM login screen. Enter the user name using the following format: *<username>@<organization>*.<br>**2.** Click **Login**. Authentication occurs between ANM and the TACACS+ server (Figure 15-2). All authentication transactions are performed by the TACACS+ authentication service associated with the associated organization.<br>**3.** ANM appears with the virtual contexts that you included as part of the domain for the RBAC user in step 3. |

*Figure 15-2 Example of Authentication Communication Between ANM and a TACACS+ Server*

| No. | Time | Source | Destination | Protocol | Info |
|---|---|---|---|---|---|
| 13 | 98.089267 | 10.86.179.214 | 10.86.178.80 | TCP | 57176 > 49 [SYN] Seq=0 Len=0 MSS=1460 TSV=258800264 |
| 14 | 0.000049 | 10.86.178.80 | 10.86.179.214 | TCP | 49 > 57176 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 M |
| 15 | 0.000113 | 10.86.179.214 | 10.86.178.80 | TCP | 57176 > 49 [ACK] Seq=1 Ack=1 Win=5840 Len=0 TSV=258 |
| 16 | 0.101786 | 10.86.179.214 | 10.86.178.80 | TACACS | Q: Authentication |
| 17 | 0.002134 | 10.86.178.80 | 10.86.179.214 | TACACS | R: Authentication |
| 18 | 0.000118 | 10.86.179.214 | 10.86.178.80 | TCP | 57176 > 49 [ACK] Seq=29 Ack=29 Win=5840 Len=0 TSV=2 |
| 19 | 0.000113 | 10.86.179.214 | 10.86.178.80 | TACACS | Q: Authentication |
| 20 | 0.069255 | 10.86.178.80 | 10.86.179.214 | TACACS | R: Authentication |
| 21 | 0.000178 | 10.86.179.214 | 10.86.178.80 | TCP | 57176 > 49 [FIN, ACK] Seq=54 Ack=47 Win=5840 Len=0 |
| 22 | 0.000046 | 10.86.178.80 | 10.86.179.214 | TCP | 49 > 57176 [ACK] Seq=47 Ack=55 Win=65482 Len=0 TSV= |
| 23 | 0.000061 | 10.86.178.80 | 10.86.179.214 | TCP | 49 > 57176 [FIN, ACK] Seq=47 Ack=55 Win=65482 Len=0 |
| 24 | 0.000107 | 10.86.179.214 | 10.86.178.80 | TCP | 57176 > 49 [ACK] Seq=55 Ack=48 Win=5840 Len=0 TSV=2 |

# Managing ANM

When you select **Admin >** ANM **Management**, you can view the following information:

- ANM—Allows you to check the status of your ACE. See Checking the Status of the ANM Server, page 15-63.
- License Management—Displays the license information stored in the ACE hardware. See Managing ANM Licenses, page 15-66.
- Statistics—Displays the ANM server statistics. See Viewing ANM Server Statistics, page 15-72.
- Statistics Collection—Allows you to enable or disable ANM server statistic collection. See Configuring ANM Statistics Collection, page 15-72.
- Audit Log Settings—Allows you to determine how long audit log records are kept. See Configuring Audit Log Settings, page 15-73.
- Change Audit Log—Displays ANM server logs. See Viewing Change Audit Logs, page 15-74.
- Auto Sync Settings—Allows you to allow ANM to automatically sync with CLI when it detects out of band changes between itself and the ACE. See Configuring Auto Sync Settings, page 15-74.
- Advanced Settings—Allows you to set the following advanced settings for ANM:
  - Enable or disable overwrite of the ACE logging device-id while setting up syslog for autosync using Config > Devices > Setup Syslog for Autosync.
  - Enable or disable write memory on a Config > Operations configuration.

  See Configuring Advanced Settings, page 15-75.

**Note** The Advanced Settings functions are available only in ANM software releases 2.1(1) and greater.

## Checking the Status of the ANM Server

The ANM server can be configured either as:

- A non-HA ANM. The non-HA ANM consists of only one host and is referred to as a standalone ANM.
- An HA (high availability or fault-tolerant) ANM, which consists of two hosts: an active ANM and a standby ANM. An HA ANM has a virtual IP address that is always assigned to the active ANM. Users log into this virtual IP address—they never log into the real IP addresses of the hosts. In addition, an HA ANM has a secondary NIC and IP address on each host over which “heartbeat” messages are used to arbitrate which host is active and which is standby.

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

Use this option to check if ANM has a backup server and to view the server status.

**Procedure**

**Step 1** Select **Admin** > ANM **Management** > ANM.

The ANM Server status screen appears. This screen contains the following information:

*Table 15-11 ANM Server Status Information*

| Field | Description |
|---|---|
| HA Replication State | Options:<br>• OK—This is an HA ANM and it is running properly.<br>• Standalone—This is a non-HA ANM, and therefore the HA attributes and operations are not meaningful.<br>• Stopped—This is an HA ANM and database replication has stopped. Under normal circumstances this is a transitory state.<br>• Failed—This is an HA ANM and database replication cannot proceed. Most likely this is because the standby ANM is not alive or is unreachable. |
| Version | The version of the ANM software. |
| Build Number and Build Timestamp | Build identification information. |
| Time Server Started | The date and time the ANM server started. |
| Virtual IP Address | Virtual IP address that associates with the active host. This IP address must be on the same subnet as the primary IP addresses of both Node 1 and Node 2. |
| Active Name | Name of Node 1, which can be displayed by issuing the **uname -n** command on the host. |
| Active IP | IP address used by Node 1 for normal (non-heartbeat related) communication. This IP address must be on the same subnet as the primary address for Node 2. |
| Active Heartbeat IP | IP address associated with the crossover network interface for Node 1. This IP address must be on the same subnet as the Heartbeat IP address for Node 2. |
| Standby Name | Name of Node 2, which can be returned by issuing the **uname -n** command on the host. |
| Standby IP | IP address used by Node 2 for normal (non-heartbeat related) communication. This IP address must be on the same subnet as the primary IP address for Node 1. |
| Standby Heartbeat IP | IP address associated with the crossover network interface for Node 2. This IP address must be on the same subnet as the Heartbeat IP address for Node 1. |

*Table 15-11 ANM Server Status Information (continued)*

| Field | Description |
|---|---|
| License Server State | Options:<br>• OK—There is a valid license on the host.<br>• Invalid—The host either contains an invalid license or there is no license present.<br>• Unknown—It is not possible to communicate with the host's license manager, therefore, the license state is unknown.<br>**Note** The Unknown and Invalid states will not display for the active (local) ANM. If the standby ANM has an Invalid license state, you should install a valid license. If the standby ANM has an Unknown license state, check that the standby ANM has been installed correctly.<br>• DEMO—Used for the demonstration purposes. It lasts for 30, 60, or 90 days from the issue day of the license. It allows you to use all features. |
| Standby License Server State | Options:<br>• OK—There is a valid license on Node 2.<br>• Invalid—Node 2 either contains an invalid license or there is no license present.<br>• Unknown—It is not possible to communicate with the license manager on Node 2, therefore, the license state is unknown.<br>**Note** The Unknown and Invalid states will not display for the active (local) ANM. If the standby ANM has an Invalid license state, you should install a valid license. If the standby ANM has an Unknown license state, check that the standby ANM has been installed correctly.<br>• DEMO—Used for the demonstration purposes. It lasts for 30, 60, or 90 days from the issue day of the license. It allows you to use all features. |

**Related Topics**


- Managing ANM Licenses, page 15-66
- Viewing ANM Server Statistics, page 15-72
- Configuring ANM Statistics Collection, page 15-72

# Managing ANM Licenses

Cisco Application Networking Manager manages software licenses for the ANM server as well as ACE devices. For information about managing ACE licenses, see Managing ACE Licenses, page 3-27. For a complete list of supported devices, see the *Supported Devices Table for the Cisco Application Networking Manager 2.1*.

Since ANM is licensed, it requires a software license key to work properly. You may be required to purchase another server license if you are using a backup server. ANM may also need additional software licenses to run large networks with many ACE devices and modules.

**Note** ANM uses TCP port 10444 for the ANM License Manager. For other port numbers, see Appendix A, "ANM Ports Reference."

Use this feature to view license state, add license files, and track license compliance information on your ANM.

This topic contains the following tasks:

- Adding Licenses into License Management, page 15-68
- Viewing Licenses in License Management, page 15-69
- Checking on License Compliance, page 15-70
- Ordering ANM Licenses, page 15-71
- Removing Licenses Files, page 15-71

For more details on ANM licenses, see Understanding ANM License Information, page 15-67 or the *Installation Guide for the Cisco Application Networking Manager 2.1*.

### Related Topics

- Understanding ANM License Information, page 15-67
- Preparing Devices for Import, page 2-4
- Managing ACE Licenses, page 3-27

## Understanding ANM License Information

When you install ANM 2.1 for the first time you need to add a license from the command line before you can access ANM. See the *Installation Guide for the Cisco Application Networking Manager 2.1* for instructions.

ANM requires licenses to manage virtual devices and to run the ANM server or servers.

Table 15-12 describes the various licenses and their purpose.

***Table 15-12 ANM License Descriptions***

| License Name | Description |
|---|---|
| ANM-AD-<count><br>ANM-AD-20 | Where A stands for ACE and D stands for devices. This product ID allows <count> number of ACE devices/modules to be managed by ANM.<br>If you have purchased two ANM-AD-10, it means that ANM is allowed to manager 20 ACE devices.<br>The maximum number of ACE devices can be managed by one ANM server is no more than 50. |
| ANM-CD-<count><br>ANM-CD-10 | Where A stands for ACE and C stands for CSS or CSM devices/modules supported. |
| ANM-AV-<supported # of virtual contexts><br>ANM-AV-100 | Where A stands for ACE and V stands for virtual contexts. This license allows ANM to manage one ACE module/device which has an ACE license supporting <number of virtual context>.<br>If you have three ACE modules with two supporting 50 virtual contexts each (ACE-VIRT-050) and one ACE supporting 250 contexts (ACE-VIRT-250), then you are required to have either two ANM-AV-50 licenses or one ANM-AV-50 licenses with count of two and one ANM-AV-250.<br>The interpretation of <supported number of virtual contexts> in ANM-AV is different from <count> in ANM-AD. |
| ANM-DEMO or DEMO | Used for the demonstration purposes. It lasts for 30, 60, or 90 days from the issue day of the license. It allows you to use all features. |
| ANM-SERVER-XX or<br>ANM-SERVER-XX-H | Used to allow access to the ANM server. Use ANM-SERVER-XX for standalone or primary servers and ANM-SERVER-XX-H for your backup server when running HA. |

### Related Topics


- Managing ACE Licenses, page 3-27
- Managing ANM Licenses, page 15-66
- Viewing Licenses in License Management, page 15-69
- Adding Licenses into License Management, page 15-68
- Ordering ANM Licenses, page 15-71
- Removing Licenses Files, page 15-71

## Adding Licenses into License Management

Use this procedure to add new ANM licenses to expand the number of network devices you can manage.

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

### Procedure

**Step 1** Select **Admin** > ANM **Management** > **License Management** > **Licenses**. The Licenses table appears.

**Step 2** Click **Install**. The New License screen appears.

**Step 3** Click **Browse** to locate the new license name. Use the browser to select the license file.

**Step 4** Click **Upload** to copy the license you entered onto the ANM Server or **Cancel** to exit.

The license file appears in the Licenses table as well as in the License Files table. From the Licenses table you can also filter, add more licenses, or alter table views. See Table 1-3 on page 1-9 for a description of the table buttons.

From the License Files table you can see the Install Status of the license file and if there are any errors. See Viewing Licenses in License Management, page 15-69 for details on what steps to do next.

### Related Topics


- Managing ACE Licenses, page 3-27
- Managing ANM Licenses, page 15-66
- Viewing Licenses in License Management, page 15-69
- Understanding ANM License Information, page 15-67
- Ordering ANM Licenses, page 15-71
- Removing Licenses Files, page 15-71

## Viewing Licenses in License Management

Use this procedure to view ANM licenses that allow you to expand the number of network devices you can manage.

**Procedure**

**Step 1** Select **Admin** > ANM **Management** > **License Management** > **Licenses**.

The License table appears. If there are license files, the License Files table also appears on the same page. This screen contains the following information (see Table 15-13 and Table 15-14):

*Table 15-13 ANM License Information*

| Field | Description |
|---|---|
| Name | Contains the license type name information about how many virtual contexts can be allocated on an ACE, as well as ANM license information.<br>• ANM_DEMO—Temporary 30, 60, or 90 day licenses; three free demos allowed.<br>• ANM_SERVER—Enables management of one ANM and two ACE devices; neither can have an ACE VIRT license (ACE_VIRT_100). Licenses contained a -H correspond to a standby ANM-SERVER node.<br>• ANM_AD—Management of devices 5, 10, 20, 50 (ANM-AD-20).<br>• ANM_CD—Enables management of CSS or CSM devices/modules.<br>• ANM_AV_xxx—Enables management of 20, 50, 100, or 250 virtual contexts.<br>For details on how to understand license name acronyms, see Understanding ANM License Information, page 15-67. |
| File Name | The name of the license file you installed on the ACE appliance. |
| Vendor | Name of vendor that supplied the license. |
| Expiry Date | Date license expires. If no expiration, permanent displays. |
| Max. Count | Number of licenses available (purchased). |

*Table 15-14 License Files*

| Field | Description |
|---|---|
| File Name | The name of the license file you installed on the ANM host. |
| Install Status | Status of the license file. Any licensing errors display here. If errors display, see Removing Licenses Files, page 15-71 for details on how to remove this file and import a working file. |

From this table you can also filter, add, or alter table views. See Table 1-3 on page 1-9 for a description of the table buttons.

### Related Topics

- Managing ACE Licenses in *Installation Guide for the Cisco Application Networking Manager 2.1*
- Understanding ANM License Information, page 15-67
- Adding Licenses into License Management, page 15-68
- Ordering ANM Licenses, page 15-71
- Managing ANM Licenses, page 15-66
- Removing Licenses Files, page 15-71
- Managing ACE Licenses, page 3-27

## Checking on License Compliance

Use this procedure to verify that the ANM licenses in your network are compliant with your ACE licenses.

### Procedure

**Step 1** Select **Admin** > ANM **Management > License Management > Compliance**.

The License Compliance table displays (see Table 15-15).

***Table 15-15 License Compliance***

| Field | Description |
|---|---|
| License Type | Lists types of licenses found. See Understanding ANM License Information, page 15-67. |
| HA | Displays Active when in HA mode or non-HA mode. Disregard this column if you are running a standalone server. |
| Total Licenses | Number of licenses present. Corresponds to maximum count on the Licenses table. |
| Used Licenses | Number of licenses in use. |
| Remaining Licenses | Number of licenses available for use. A negative number displays in red if there are not enough licenses for the network devices you are managing. A number displays highlighted in yellow if the number of licenses used is equal to the total licenses you have purchased. |
| Expiration | Expiration date (if temporary license). |

**Step 2** Click **Refresh** to update the licenses in this window.

### Related Topics

- Understanding ANM License Information, page 15-67
- Adding Licenses into License Management, page 15-68
- Ordering ANM Licenses, page 15-71
- Updating ACE Licenses, page 3-31

- Managing ACE Licenses, page 3-27

## Ordering ANM Licenses

If you need to purchase additional ANM licenses in order to be compliant with the number of ACE licenses you are managing, contact your sales team or use Cisco.com to place your order. After you receive your PAK information, you can then access the Cisco Product License Registration web site page at http://www.cisco.com/go/license. The Cisco Product License Registration web site provides you with license key/files that you can upload to ANM and ensure your compliance with software requirements.

If you already have your Product Activation Key (PAK), you can manually use the Cisco web site to obtain licenses or you can use the Cisco License Manager. Cisco License Manager performs license fulfillment for you and also deploys the licenses to network devices using a wizard-based GUI.

### Related Topics

- Managing ANM Licenses, page 15-66
- Understanding ANM License Information, page 15-67
- Adding Licenses into License Management, page 15-68
- Viewing Licenses in License Management, page 15-69
- Checking on License Compliance, page 15-70
- Managing ACE Licenses, page 3-27

## Removing Licenses Files

If your license files will not work in the ANM due to file errors, you need to remove them from the ANM host and request another license file from Cisco. There is no remove license command. You can remove the license from the operating system by deleting the file.

### Procedure

**Step 1** Log in as the root user.

**Step 2** To remove the license file, enter:

**rm /opt/CSCOanm/etc/license/<ANM_LICENSE_FILE>**

The license file is removed from the ANM host only. The license on your managed device is still valid.

**Step 3** Restart ANM to allow it to update the licenses table data. To restart ANM, see instructions in the *Installation Guide for the Cisco Application Networking Manager 2.1*.

To request another license from Cisco to replace the one that had errors, open a service request using the TAC Service Request Tool or call the Technical Assistance Center. Then add the license into ANM.

### Related Topics

- Managing ANM Licenses, page 15-66
- Understanding ANM License Information, page 15-67
- Adding Licenses into License Management, page 15-68
- Viewing Licenses in License Management, page 15-69

- Ordering ANM Licenses, page 15-71

# Viewing ANM Server Statistics

Use this procedure to display ANM statistics (for example, CPU, disk, and memory usage on the ACE).

**Procedure**

**Step 1** Select **Admin** > ANM **Management** > **Statistics**. The statistics viewer displays the fields in Table 15-16.

*Table 15-16 ACE Server Statistics*

| Name | Description |
|---|---|
| Owner | Process where statistics are collected. |
| Statistic | Includes the following statistics:<br>• CPU Usage—Overall ACE CPU busy percentage in the last 5-minute period.<br>• Disk Usage—Amount of disk space being used by the ANM server or ACE device.<br>• Memory Usage—Amount of memory being used by the ANM server or ACE hardware.<br>• 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**

- Checking the Status of the ANM Server, page 15-63
- Configuring ANM Statistics Collection, page 15-72

# Configuring ANM Statistics Collection

Use this procedure to enable ACE server statistics polling.

**Procedure**

**Step 1** Select **Admin** > ANM **Management** > **Statistics Collection**. The Primary Attributes configuration 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.

**Step 4** Click **Deploy Now** to save your entries.

**Related Topics**

- Viewing ANM Server Statistics, page 15-72
- Checking the Status of the ANM Server, page 15-63

# Configuring Audit Log Settings

Audit Log Purge Settings allow you to specify the following:

- How many days the log records in the database will be kept (default is 31).
- The maximum of log records that will be stored in the ANM database (default 100,000).

Audit Log File Purge Settings allows you to specify the following:

- The number of days worth of log record files that will be stored in the ANM database (default 31 days).
- The number of daily rolling files that will be stored in the ANM database (default 10 files each day, allowable file size is 2 Megabytes and is not configurable).

Use this procedure to determine how long audit logs are kept in the database.

**Procedure**

**Step 1** Select **Admin >** ANM **Management > Audit Log Settings**. The Audit Log Settings configuration screen appears.

Audit Log Purge Settings fields let you determine whether audit log table entries will be deleted after a certain number of days (default is 31 days) or after the table entries reach a certain size (default is 100 entries).

**Step 2** Enter the greatest number of days you would like entries to be retained in the **Number of Days** field.

**Step 3** Enter the maximum amount of log records to be stored in the ANM database in the audit log tables in the **Number of Entries (Thousand)** field (default 100,000).

Audit Log File Purge Settings fields let you determine whether to retain log files according by age (default is 31 days) or by amount saved in a given day (default is 10 entries).

**Step 4** Enter the greatest number of days you would like entries to be retained in **Number of Days** field.

**Step 5** Enter the greatest number of log files you would like retained in **Number of Daily Rolling Log Files** field.

**Step 6** Click:

- **Reset to Default** to erase changes and restore the default values.

or

- **Save Now** to save your entries.

**Related Topics**

- Configuring Audit Log Settings, page 15-73
- Viewing Change Audit Logs, page 15-74

# Viewing Change Audit Logs

Any key or change related activities to the ANM server will be logged and viewed according to your role. Use this procedure to display ANM change audit logs for example, user login attempts, create/update/delete objects such as RBAC, Global Resource Class, Credential, device group, and threshold setting.

**Procedure**

**Step 1** Select **Admin** > ANM **Management** > **ANM Change Audit Log**. The audit log displays the fields in Table 15-17.

***Table 15-17 Server Audit Log***

| Name | Description |
|---|---|
| Time | Server time stamp when user action is complete. |
| Client IP | IP address where action originated. |
| User | Email address in the following format: *username@organization name* for example, admin@cisco.com. |
| Message | Boilerplate text descriptive of action taken, usually self-explanatory (for example “User authentication succeeded.” |

**Related Topics**

- Device Audit Trail Logging, page 14-25
- Checking the Status of the ANM Server, page 15-63
- Configuring Audit Log Settings, page 15-73

# Configuring Auto Sync Settings

Use this procedure to configure ANM server auto sync settings.

**Procedure**

**Step 1** Select **Admin** > ANM **Management** > **ANM Auto Sync Settings**. The **Setup ANM auto-sync settings** screen appears.

**Step 2** In the ANM Auto sync field, select one of the following:

**Enable** to have the ANM server automatically sync with ACE CLI when it detects out of band changes.

or

**Disable** to have the ANM server warn but not take independent action when it detects out of band changes between the server and ACE CLI.

**Step 3** In the Polling Interval field, select the polling interval you would like the ANM server to employ.

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

**Related Topic**

Synchronizing Virtual Context Configurations, page 3-67

# Configuring Advanced Settings

This section includes the following topics on the use of the Advanced Settings screen:

- Configuring the Overwrite the ACE Logging device-id for the Syslog Option
- Configuring the Enable Write Mem on the Config > Operations Option

**Note** The Advanced Settings functions are available only in ANM software releases 2.1(1) and greater.

# Configuring the Overwrite the ACE Logging device-id for the Syslog Option

By default, ANM Autosync relies on the ACE logging device-id to be of type "String." A device-id setting adds explicit information that is appended to the syslog message, and is used by ANM to uniquely identify the source of a syslog message. If you configure ANM to manage syslog settings for Autosync on a virtual context (**Config > Devices > Setup Syslog for Autosync**) and the logging device-id is defined as something other than type "String" for the context, the operation fails and ANM displays "Syslog device is already configured for other purpose."

You can instruct ANM to overwrite the ACE logging device-id when you enable the synchronization of syslog messages setup of syslog for Autosync from the ACE. If any of the contexts that you are trying to set up a syslog the syslog for Autosync has a device-id setup for a type other than string, ANM will override the device-id with the ANM preferred string.

**Procedure**

Use this procedure to overwrite the ACE logging device-id.

**Step 1** Choose **Admin > ANM Management > Advanced Settings**. The Advanced Settings configuration screen appears.

**Step 2** In the Overwrite ACE Logging Device ID field, perform one of the following actions:

- Click **Enable** to overwrite the logging device-id during Setup Syslog for Autosync.
- Click **Disable** to prevent overwriting the existing logging device-id if it has been previously set up with a type other than string. If the selected context from Setup Syslog for Autosync already has a device-id that is setup with a type other than string, then the operation will report an appropriate error and ANM will not overwrite this setting. This is the default setting.

**Step 3** Click **OK** to accept your entries on the Advanced Settings configuration screen.

**Related Topic**

Enabling Setup Syslog for Autosync for Use With an ACE, page 2-18

## Configuring the Enable Write Mem on the Config > Operations Option

By default, ANM initiates a **write memory** command action after you activate or suspend changes on the ACE, CSM, or CSS through the different ANM Operations Pages (**Config > Operations**). In certain situations, such as those that involve large configurations, a **write memory** action can take an extended period of time to complete. In this case, the ANM GUI may time out. If a **write memory** action is not performed before a device reload occurs, the changes will be lost. You can instruct ANM to enable or disable write memory on a Config > Operations configuration.

**Note** The **write memory** command is the same as the **copy running-config startup-config** command; both commands save changes to the configuration.

**Note** The CSS Expert mode must be disabled if you wish to disable the Write Mem on Config > Operations feature. The Expert mode allows you to turn the CSS confirmation capability on or off; turning Expert mode on disables the CSS from prompting for confirmation when configuration changes are made. If Expert mode is enabled on the CSS, this function will cause the CSS to perform an implicit write memory action after each operational change.

**Procedure**

Use this procedure to configure the Enable Write Mem on Config > Operations feature.

**Step 1** Choose **Admin > ANM Management > Advanced Settings**. The Advanced Settings configuration screen appears.

**Step 2** In the Enable Write Mem on Config > Operations field, perform one of the following actions:

- Click **Enable** to instruct ANM to activate the write memory action on the Config > Operations screen. This is the default.
- Click **Disable** to deactivate the write memory action on the Config > Operations screen. This option will require you to periodically access the CLI for the ACE context, the CSM, or the CSS and enter the **write memory** command to commit the change to the startup-configuration.

**Step 3** Click **OK** to accept your entries on the Advanced Settings configuration screen.

# Lifeline Management

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. For more information about this feature, see Using Lifeline, page 16-4.