CHAPTER 3

Setting Up the CiscoWorks2000 Server

The CiscoWorks2000 Server includes tools required to properly set up the server to support other CiscoWorks2000 applications. These features include:

- Setting Up User Accounts
- Using the Pluggable Authentication Modules
- Installing Client Application Manager
- Configuring the ANI Server

Setting Up User Accounts

Several CiscoWorks2000 network management and application management operations are potentially disruptive to either the network or to the applications themselves and must be protected.

To prevent such operations from being used accidentally or maliciously, CiscoWorks2000 uses a multilevel security system that only allows access to certain features to users who can authenticate themselves at the appropriate level.

CiscoWorks2000 provides two predefined login IDs, but you create additional unique login IDs for users at your company:

- guest (no password required, user role = Help Desk)
- admin (password = admin, user role = super user)

Note The login named admin is the equivalent of the superuser login for CiscoWorks2000. This login provides access to all CiscoWorks2000 tasks.

Caution When the system is installed initially, admin is the default password. To prevent all users from accessing privileged applications, change the password for admin immediately after installation. The guest login has no password. If you require passwords, add a guest password.

Understanding Security Levels

System administrators determine user security levels when they are granted access to CiscoWorks2000. When users are granted logins to the CiscoWorks2000 application, they are assigned one or more roles. The user role or combination of roles dictates which CiscoWorks2000 applications are presented to the user on the navigation tree. shows available security levels.

Table 3-1 Security Levels

Level	Description
0	Help Desk
1	Approver
2	Network Operator
4	Network Administrator
8	System Administrator

Other roles are displayed, depending on your applications. For example, two additional user roles (Developer and Export Data) are displayed in the security user account windows. These roles are available only for Management Connection and third-party developers.

To see which security levels are allowed to use the CiscoWorks2000 applications, run the **CiscoWorks2000 Server > Setup > Security > Permissions Report**.

Performing Security Tasks

Users can perform some tasks for their own accounts, but most security tasks require system administrator role privileges. When performing these security tasks (see Table 3-2), consider the following:

- CiscoWorks2000 cannot recover forgotten passwords. A system administrator-level user must either change the password or delete and then add the user again.
- The username *admin* is reserved and cannot be deleted.
- If the administrator has changed and forgotten the *admin* password, contact your Cisco technical representative.

Table 3-2 Security Tasks

Task	Purpose	Action
All Users		
View role permissions.	Displays predetermined set of applications, tools, and product features each user role can access	**CiscoWorks2000 Server > Setup > Security > Permissions Report**
Change password.	Allows users to modify their account password	**CiscoWorks2000 Server > Setup > Security > Modify My Profile**
Admin Tasks		
Add a user.	Creates a new user and provides appropriate user access level to CiscoWorks2000	**CiscoWorks2000 Server > Setup > Security > Add Users**
Delete a user.	Removes user from list	**CiscoWorks2000 Server > Setup > Security > Modify/Delete Users**
Modify a user.	Allows updates to user information, such as email address, login name, password, and access level	**CiscoWorks2000 Server > Setup > Security > Modify/Delete Users**

Table 3-2 Security Tasks (continued)

Task	Purpose	Action
View other logged-in users.	Displays information about currently logged in CiscoWorks2000 users and allows users to send a broadcast message to others	**CiscoWorks2000 Server>Setup> Security> Who Is Logged On**
Modify authentication module.	Allows the addition of new users by using another source of authentication, such as directory service	**CiscoWorks2000 Server > Security > Select Login Module**

Using the Pluggable Authentication Modules

Pluggable authentication using the CiscoWorks2000 Server security feature allows administrators to authenticate users by another source of authentication, such as a directory service. CiscoWorks2000 provides several standard pluggable authentication modules that allow the administrator of the CiscoWorks2000 Server to authenticate any CiscoWorks2000 login with NT, UNIX, TACACS+, Radius or other authentication sources.

Understanding Fall Back Options

Three login module fall back options are available on all platforms. Fall back options allow you to access the software should you accidentally lock yourself or others out. Table 3-3 describes the login module fall back options.

Table 3-3 Login Module Fall Back Options

Option	Description
Allow all CiscoWorks2000 Local users to fall back to the CiscoWorks2000 Local login.	All users can access CiscoWorks2000 using the Local login if the current login module fails.
Only allow the following user(s) to fall back to the CiscoWorks2000 Local login if preceding login fails: xxxx.	Specified users can access CiscoWorks2000 using the Local login if the current login module fails. Use commas between user names.
Allow no fall backs to the CiscoWorks2000 Local login.	No access is allowed if the current login module fails.

It is recommended that you select the option that allows specific users to fall back to the CiscoWorks2000 Local login if a preceding login fails. This way, if your server cannot authenticate the user, and the user has a local CiscoWorks2000 account, the CiscoWorks2000 Local login module authenticates the same name and password. If authentication occurs, the user can access CiscoWorks2000 even if their first-choice server is down. You may also want to test the new login module by having a user log in using the new authentication module.

Note The administrator needs to add users with more than guest privileges when choosing no local authentication source. If the system falls back to the local authentication choice a full set of user IDs and passwords is necessary.

Selecting a New Login Module

Depending on your platform, different login module features are available (see Table 3-4).

Table 3-4 Login Module Options on Supported Platforms

Module	Available on UNIX[1]	Available on Windows NT
CiscoWorks2000 Local	X	X
UNIX System Module	X	
NT Local		X
Microsoft Active Directory	X	X
Netscape LDAP	X	X
Radius	X	X
TACACS+	X	X

1. This includes the Solaris platform, but will also include other platforms as new platforms are added to the CMF support.

The following procedure describes how to select a specific login module. For information on selecting other login modules, refer to the online help.

Step 1 Select **CiscoWorks2000 Server > Setup > Security > Select Login Module**. The Select Login Module window opens.

Step 2 Select your option:

a. To view or change the current login module configuration, click **Edit Options**.

b. To select a different login module, click **Next**.

The Login Module Options window opens. Depending on your module, you might see one of the following modules:

- Local
- NT Native
- UNIX System Module
- Microsoft Active Directory
- Netscape LDAP

- Radius
- TACACS+

Step 3 Enter the data into the fields and click **Finish**. To return to the previous window and modify your entries, click **Back**.

Step 4 After you change the login module, you do not have to restart CiscoWorks2000. The next person to login after the change automatically uses the new module. Changes to the login module are logged in the NMSROOT/objects,/jrun/jsm-cw2000/logs directory.

Note If you accidentally lock yourself out of the CiscoWorks2000 software after using this option, see the "Frequently Asked Questions" in the "Troubleshooting the CiscoWorks2000 Server" chapter.

Installing Client Application Manager

You can improve the performance of some CiscoWorks2000 applications by downloading and installing server files on your local machine. Whenever a client browser connects to a CiscoWorks2000 Server, you can choose to install Client Application Manager.

You can install Client Application Manager by selecting **CiscoWorks2000 Server>Setup>Client Manager Admin** or choosing to install when the Client Application Manager dialog box appears. This dialog box appears after you access a CiscoWorks2000 application that uses Client Application Manager.

If the Client Application Manager dialog box appears after you make a selection from the navigation tree, you can choose not to install it. Click on the check box to *not* show the message again and click **No**. If you do not select the check box, the dialog box appears each time you select an application that supports client-side installed files.

Configuring the ANI Server

Some CiscoWorks2000 applications require the Asynchronous Network Interface (ANI) Server to automatically discover network devices. If your application does not use or require the ANI Server, it is not available in the navigation tree.

For applications that require the ANI Server, it is critical that you set up your network and the ANI Server to ensure that the network is properly discovered.

Setting Up Your Network

The Network Setup Overview table (see Table 3-5) provides an overview of the tasks required to ensure that ANI properly discovers your network. Detailed information and instructions are available in the online help (select **CiscoWorks2000 > Setup > ANI Server Admin**).

To perform these tasks, use the Command Line Interface (CLI) of the network devices in your network. Refer to the command reference guides for specific devices to obtain instructions about performing these tasks.

Table 3-5 Network Setup Overview

Task	Purpose
Required for Device and Physical Topology Discovery	
Upgrade software versions on devices.	To ensure that ANI Server successfully discovers and supports your network devices, upgrade your device software to the latest general deployment (GD) software release.
Verify connectivity to seed devices.	The workstation on which ANI Server is installed must have connectivity to the seed devices in your network. If devices are not reachable, they cannot be discovered.
Enable SNMP.	ANI communicates with network devices using SNMP.
Enable Cisco Discovery Protocol.	ANI Server uses Cisco Discovery Protocol (CDP) to discover your network devices and layout.
Set unique sysName variable on devices.	Using CDP, ANI identifies Cisco IOS devices by the sysName variable. If multiple devices share the same sysName variable, the devices cannot be discovered properly.

Table 3-5 Network Setup Overview (continued)

Task	Purpose
Enable ILMI on ATM devices.	ANI Server uses Integrated Local Management Interface (ILMI) to discover the ATM devices in your network.
Configure DNS.	ANI uses Domain Name Services (DNS), if available, to perform device name lookups. If DNS is not available, ANI uses IP addresses. If you use DNS, ensure that all devices have unique host names and that DNS is properly configured.
Required for Logical (VLAN and LANE) Discovery	
Note Successful logical discoveries require that you have also properly configured the network for device discoveries.	
Configure VLAN Trunk Protocol.	VLAN Trunk Protocol (VTP), and at least one VTP Server per VTP domain is required to discover, display, and configure VLANs.
Configure VLAN trunks on Fast Ethernet and Gigabit Ethernet.	If a switch is connected to Fast Ethernet links and you want to configure it to carry more than one VLAN, you must enable ISL or IEEE 802.1Q.
Create the default LANE configuration server for ATM devices.	If you are running LAN Emulation (LANE) in your network, you must set up the main configuration server.
Required for User Discovery	
Note Successful user discoveries require that you have also properly configured the network for device and logical discoveries.	
Connect users and hosts to the network.	ANI can retrieve information about end-user devices and hosts only if those devices are actively connected to the network. Also, ANI can automatically collect user names only if users are actively connected to the network.

Table 3-5 Network Setup Overview (continued)

Task	Purpose
Required for Path Determination	
Note Successful path discoveries require that you have also properly configured the network for device, logical, and user discoveries.	
Enable source routing.	ANI might not be able to trace a reliable path between two end points if source routing is disabled on any intervening routers.
Enable CDR logging on all Cisco Call Managers	The call detail record (CDR) provides information such as the IP address of the phones and gateways, telephone numbers of the involved parties, and the time that the call was made. This information is used to determine a path involving any Cisco Call Manager devices.

Setting Up the ANI Server

The ANI Server automatically discovers devices in your network at a defined interval. To do this, the ANI Server must have access to your network devices and a discovery starting point (seed device).

You provide ANI access to your network devices by ensuring that the community strings on your devices are known to the ANI Server. The ANI Server uses your specified seed device (or a set of seed devices) to initiate discovery. See Table 3-6 for a description of these and other tasks you can perform with the ANI Server.

Table 3-6 ANI Server Tasks

Task	Purpose	Action
Required for Initial Discovery		
Verify community strings.	Allows the ANI Server access to your network devices. Default community strings are *public* for the read-only string and *private* for the read-write string.	**CiscoWorks2000 Server > Setup > ANI Server Admin > SNMP Setting**

Table 3-6 ANI Server Tasks (continued)

Task	Purpose	Action
Add seed device.	Initiates network discovery.	**CiscoWorks2000 Server > Setup > ANI Server Admin > Discovery Settings**
Additional Tasks		
Schedule discovery and polling.	Sets the frequency of network discovery and polling.	**CiscoWorks2000 Server > Setup > ANI Server Admin > Discovery Schedule**
Modify SNMP settings.	Changes the number of SNMP retries and length of SNMP timeouts.	**CiscoWorks2000 Server > Setup > ANI Server Admin > SNMP Settings**
Limit discovery.	Narrows the network discovery by IP address or VTP domain.	**CiscoWorks2000 Server > Setup > ANI Server Admin > Discovery Settings**
Synchronize devices with Essentials.	Provides mechanism for sharing devices and device credentials with Resource Manager Essentials.	**CiscoWorks2000 Server > Setup > ANI Server Admin > Device Synchronization**
Schedule user and host acquisition.	Sets the frequency of user name and host acquisition.	**CiscoWorks2000 Server > Setup > ANI Server Admin > User and Host Acquisition**
Modify system resources dedicated to discovery.	Assigns more or fewer system resources to ANI discovery to affect time to complete.	**CiscoWorks2000 Server > Setup > ANI Server Admin > Performance Settings**