Preparing to Use Essentials Applications

Now that you have installed and set up Essentials, you must configure the server for Essentials and prepare Essentials applications for use.

This chapter assumes that you have performed the client setup tasks described in *Installing and Setting Up CD One on Windows NT*.

This chapter consists of:

- Preparation Overview
- Accessing the Server
- Logging In
- Configuring the Server
- Setting Up Inventory
- Verifying Availability
- Setting Up Syslog Analysis
- Setting Up Software Management
- Setting Up Configuration Management

Preparation Overview

Table 2-1 is an overview of preparing to use Essentials applications, with references to more detailed information about each task.

Table 2-1   Preparing to Use Essentials Applications Task Overview

Task	Steps	References
1 Configure the system.	Enter information about the proxy server, SNMP, SMTP, and rcp.	"Configuring the Server" section on page 2-6
2 Set up Inventory.	**Step 1** Create network inventory by either: • Adding device information by adding one device at a time. • Importing device information from a file or an NMS database.	"Adding or Importing Inventory Data" section on page 2-8
	Step 2 Create a device view.	"Creating a Device View" section on page 2-12
	Step 3 Obtain login privileges to Cisco Connection Online (CCO).	If you do not have login privileges, go to the CCO home page, www.cisco.com, to obtain a login.
	Step 4 (Optional) Enter device serial numbers for devices that have Contract Connection service contracts.	"Changing Device Attributes (Credentials and Serial Numbers)" section on page 2-12
	Step 5 (Optional) Perform the following optional Inventory setup tasks: • Schedule inventory polling and collection. • Set change report filters. • Display a detailed device report.	Inventory online help
3 Set up Availability.	**Step 1** Create a device view with at least two devices.	"Verifying Availability" section on page 2-13 and "Creating a Device View" section on page 2-12
	Step 2 Verify that Availability functions correctly.	"Verifying Availability" section on page 2-13

Table 2-1   Preparing to Use Essentials Applications Task Overview (continued)

Task	Steps		References
4 Set up Syslog Analysis.	**Step 1**	Configure your routers and switches for syslog analysis.	"Configuring Routers and Switches for Syslog Analysis" section on page 2-15
	Step 2	Verify that Syslog messages are being processed by the Syslog Analyzer.	"Verifying the Syslog Analyzer" section on page 2-16
5 Set up Software Management.	**Step 1**	Set up file transfer servers.	"Setting Up File Transfer Servers" section on page 2-17
	Step 2	Add device passwords to inventory.	"Adding Device Passwords" section on page 2-18
	Step 3	Set Software Management preferences.	"Setting Software Management Preferences" section on page 2-19
	Step 4	Obtain login privileges to CCO for importing software images.	If you do not have login privileges, go to the CCO home page, www.cisco.com, to obtain a login.
	Step 5	(Optional) Perform optional setup tasks. • Create a baseline of the devices in your network and populate the software image library. • Schedule the Browse Defects job to run periodically. • Schedule the Synchronize Library job to run periodically. • Create one or more approver lists if you want to use the Maker Checker option. • Distribute a software image to a device or group of devices.	Software Management online help

Table 2-1　　　**Preparing to Use Essentials Applications Task Overview (continued)**

Task	Steps		References
6 Set up Configuration Management.	**Step 1**	Enter passwords.	"Entering Device Credentials" section on page 2-19
	Step 2	Modify device configurations.	"Modifying Device Configurations" section on page 2-20
	Step 3	Modify device security.	"Modifying Device Security" section on page 2-21
	Step 4	Upgrade, set up, and troubleshoot Netsys integration if you are using the Cisco Netsys application.	"Setting Up Netsys Integration" section on page 2-21
	Step 5	Set up NetConfig: • Verify device configurations in configuration archive. • Verify device credentials. • Modify device security. • Verify device prompts.	"Setting Up NetConfig" section on page 2-27 and the NetConfig online help
	Step 6	(Optional) Perform optional NetConfig setup tasks: • Install Client Application Manager on client systems. • Configure default job properties. • Assign template access privileges to users. • Enable Job Approval.	NetConfig online help

Accessing the Server

When you access the CiscoWorks2000 server, the CiscoWorks2000 main screen, with the Login Manager displayed, appears. To access the server, enter the URL of the server in the web browser:

```
http://server_name:1741
```

where *server_name* is the name of the CiscoWorks2000 server and **1741** is the default TCP port.

See *Getting Started with the CiscoWorks2000 Server* for information about administrator logins.

Logging In

To perform administrator setup tasks, you must log in as system administrator.

To log in as the system administrator:

Step 1   Enter the system administrator username and password in the Login Manager dialog box (Figure 2-1). The default username and password are:

```
User Name: admin
Password: admin
```

Figure 2-1   Login Manager Dialog Box

Step 2   Click **Connect**.

The Login Manager dialog box is replaced by the navigation tree.

Configuring the Server

You can configure system-wide information for Essentials applications using the System Configuration option. You should verify that the default information is correct or enter corrected information.

To configure the system:

Step 1   Select **Resource Manager Essentials > Administration > System Configuration**. The System Configuration dialog box appears (Figure 2-2).

Figure 2-2   System Configuration Dialog Box
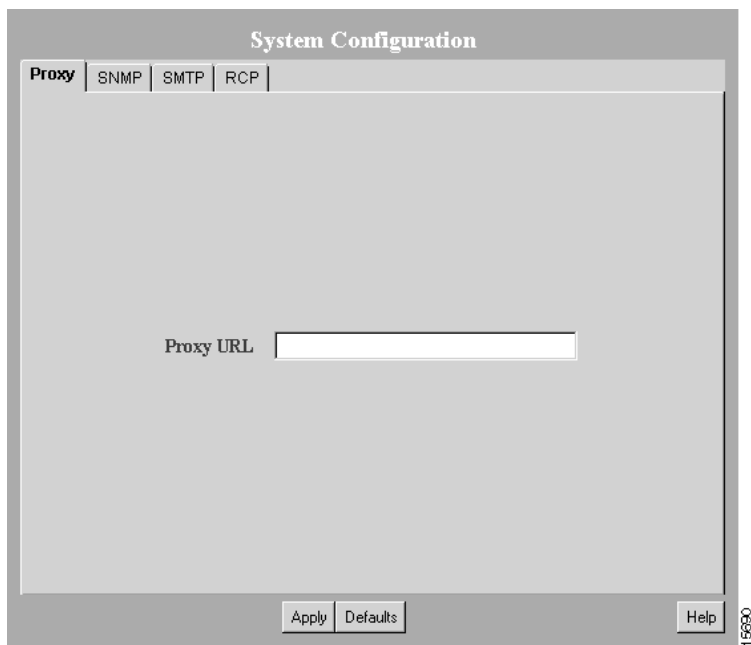
Step 2   Select one of the following tabs to enter information or to verify that the configured information is correct:

- Proxy
- SNMP

- SMTP

- rcp

See Table 2-2 for descriptions of the dialog tabs.

Table 2-2   System Configuration Dialog Box Information

Tab Name	Description	Fields—Values to Enter
Proxy	Used to connect to CCO. If server access to the outside world is controlled through a proxy server, this setting must be configured.	Proxy URL—System-wide proxy URL. There is no default.
SNMP	Used to query devices for inventory collection: includes importing and adding devices and collecting inventory data.	Fast SNMP Timeout—Amount of time, from 5 to 90 seconds, the system should wait for a device to respond before trying to access it again. Default is 5.
		Fast SNMP Retry—Number of times, from 2 to 6, system tries to access devices with fast SNMP options. Default is 2.
		Slow SNMP Timeout—Amount of time, from 10 to 90 seconds, system should wait for a device to respond before trying to access it again. Default is 20.
		Slow SNMP Retry—Enter the number of times, from 2 to 6, the system should try to access a device with slow SNMP options. Default is 3.
SMTP	Used to send email.	SMTP Server—Server name. Default is localhost.
rcp	Used to specify user during remote file transfer operations from devices. Authenticates rcp transfers between devices and the server.	User Name—Name used by a network device when it connects to the server to run rcp.
	User account should be configured on devices as local user.	
	See the "Setting Up File Transfer Servers" section on page 2-17.	

Step 3 Click **Apply** to save changed information, or click **Defaults** to apply the defaults.

Step 4 Repeat Step 2 and Step 3 until you have verified or corrected all the information displayed in the System Configuration dialog box.

The dialog box is displayed until you select another option from the navigation tree.

Setting Up Inventory

This section describes the tasks that you must perform to set up the Inventory application.

Adding or Importing Inventory Data

You must have at least two managed devices (devices whose inventory information is tracked by Essentials) to verify correct Essentials installation. To manage your network, you need to add the device information for all your managed devices.

You can populate your network inventory by:

- Adding devices one at a time by entering the device information manually.

- Importing a group of devices from:

   — A comma-separated value (CSV) file or a device integration file (DIF) that you create from another information source.

   — A supported network management system (NMS) on the same host as your server (local import).

   — A supported NMS on a different host from your server (remote import).

The supported NMS software is described in the "Supported NMS Environments for Device Import" section on page 1-5.

Adding Device Information Manually

This section describes how to add devices manually and troubleshoot problems you might have when using this method of adding devices.

Step 1   Select **Resource Manager Essentials** > **Administration > Inventory > Add Devices**. The Add a Single Device dialog box appears.

Step 2   Enter the access information and annotations for one device.

You must fill in the Device Name field with the device name or IP address. For Inventory, the other fields in this dialog box are optional. For other applications, you might need to fill in other fields. For more information, refer to the online help.

Step 3   Click **Next**. The Enter Login Authentication Information dialog box appears.

You must fill in the Read Community String and Write Community String fields and verify the passwords. For Inventory, the other fields in this dialog box are optional. For other applications, you might need to fill in other fields. For more information, refer to the online help.

Step 4   Click **Next**. The Enter Enable Authentication Information dialog box appears. For Inventory, all fields are optional. For other applications, you might need to fill in fields. For more information, refer to the online help.

Step 5   Click **Finish**. The Single Device Add dialog box appears.

Step 6   Click **View Status**. The Add/Import Status Summary dialog box appears.

Step 7   Use the Add/Import Status Summary to check the status of the device you specified. You should see the following:

Device Status	Number of Devices
Managed	0
Alias	0
Pending	1
Conflicting	0
Suspended	0
Not Responding	0
Device Attribute Errors	0

If the device responded quickly, the Managed row might already contain one device.

Step 8   Click **Update** on the Add/Import Status Summary dialog box to update device status.

If the pending count goes from 1 to 0 after you click **Update** and the Managed row has 1 device, Essentials was installed and configured correctly.

You might need to wait several minutes for the device to become managed. Click **Update** on the Add/Import Status Summary dialog box every minute or so to check current device status.

For additional information, refer to the online help.

If you added a device and the Add/Import Status Summary dialog box shows that the device status has not changed from *pending* within 15 minutes, check the status of all processes to make sure they are running normally:

Step 1   To view the latest device status information, select **Resource Manager Essentials > Administration > Inventory > Import Status**, then click **Update** in the Add/Import Status Summary dialog box.

Step 2   To determine if the DIServer process is running, select **CiscoWorks2000 Server > Administration > Process Management > Process Status**. (The DIServer is the process responsible for validating devices and changing their status from pending.)

Even if the DIServer process has the state *Running Normally*, it might be in an error state. You need to stop and restart it:

To stop the DIServer process:

(a)   Select **CiscoWorks2000 > Administration > Process Management > Stop Process**. The Stop Process dialog box appears.

(b)   Click the **Process** radio button.

(c)   In the Process Name field, select **DIServer**, then click **Finish**.

To restart the DIServer process:

(a)   Select **CiscoWorks2000 > Administration > Process Management > Start Processes**. The Start Process dialog box appears.

(b)   Click the **Process** radio button.

(c)   In the Process Name field, select **DIServer**, then click **Finish.**

Step 3   Select **Resource Manager Essentials > Administration > Inventory > Import Status** to return to the Add/Import Status Summary screen, then click **Update**. The device status should change to *managed* within a couple of minutes.

Importing Device Information

You can import devices from a file or from a local or remote network management system (NMS):

- To import devices from a file, extract data from your existing data source into a comma-separated value (CSV) file or device integration file (DIF). Select **Resource Manager Essentials > Administration > Inventory > Import from File** to access the CSV or DIF file and import the device information. For additional information, refer to the online help.

- To import devices from a local NMS database, select **Resource Manager Essentials > Administration > Inventory > Import from Local NMS**. The available databases are listed in the Local NMS Import dialog box. For information about the device import software supported for local import, see the "Supported NMS Environments for Device Import" section on page 1-5. For additional information, refer to the online help.

- To import devices from a remote NMS database:

  — You might have to work with the system administrator of the host on which the NMS database is running. For more information, refer to the online help.

  — You must perform several system and NMS configuration steps that are contingent upon the NMS you are using. For information about the device import software supported for remote import, see the "Supported NMS Environments for Device Import" section on page 1-5. For additional information, refer to the online help.

  — After you configure your system and NMS, select **Resource Manager Essentials > Administration > Inventory > Import from Remote NMS** to import devices from the databases listed in the Remote NMS Import dialog box.

If you have difficulty importing device information, try the following:

- Increase the SNMP timeout setting. Refer to the online help for more information.

- Verify that you have correct read community strings entered for the devices.

Creating a Device View

To set up and verify the Essentials applications, you must create a static device view (a grouping of devices) that includes at least two devices. For additional information, refer to the online help.

Step 1   Select **Resource Manager Essentials > Administration > Device Views > Add Static Views**. The Add Static Views dialog box appears.

Step 2   From the Views column, select the view that has the devices you want to add. If you have not previously configured any views, select **All**.

Step 3   From the Devices list, select the devices that you want to add.

Step 4   Click **Next**. The Save Static View dialog box appears.

Step 5   Enter the view name and view description.

Step 6   Click **Finish**.

Changing Device Attributes (Credentials and Serial Numbers)

To make sure your devices have the correct device access, password information, and user information, you can change the device attributes. For Contract Connection to provide accurate contract status information, you must add device serial numbers to the entries of devices that have service contracts.

To check device attributes, select **Resource Manager Essentials > Administration > Inventory > Check Device Attributes**.

To edit device attributes:

Step 1   Select **Resource Manager Essentials > Administration > Inventory > Change Device Attributes**. The Change Device Attributes dialog box appears.

Step 2   Select the device whose device information you want to edit, then click **Next**. The Change dialog box displays the options.

Step 3   Select one or more options, then click **Next**. A dialog box appears for each option you selected. The dialog box fields are blank; they do not display current information.

Step 4   Edit dialog boxes as follows:

- To retain the current value, leave the field blank.

- To change a value, enter the new information in the field. If you are changing a password, you must enter the username.

- To delete a value, click **Delete** next to the field. If you are deleting a password, you must also enter the username.

Note   Verify your entries before you click **Next** in any dialog box. If you change device attributes, you cannot undo the change, except by reediting.

Step 5   When you finish with a dialog box:

- Click **Next** to apply the changes and go to the next dialog box.

- Click **Finish** to apply the changes and exit the final dialog box.

- Click **Back** to close the dialog box without changing any information.

Verifying Availability

To verify that Availability is working correctly, you must have a test device view with at least two devices. You can use the view you created during Inventory setup, assuming that you added at least two devices to it. Use this test device view to verify that Availability displays the devices in the view in the Reachability Dashboard.

Step 1   Select **Resource Manager Essentials > Administration > Availability > Change Polling Options**.

Step 2   Select the test device view that you created from the All Views list, then click **Add** to add it to the Polled Views list.

This creates a view for Availability polling.

Note   You must add views to the Polled Views list. Only polled views are
monitored.

Step 3   Click **Next**. The Change Polling Options dialog box appears.

Step 4   Select **5 Minutes** from the Verify device reachability every drop-down list, then
click **Finish**.

Step 5   Wait for at least 10 minutes to make sure Availability polls the devices in your
test device view.

Step 6   Select **Resource Manager Essentials > Availability >
Reachability Dashboard**. The Reachability Dashboard appears.

Step 7   Click the view name. The devices in your test device view should appear in the
Reachability Dashboard.

Now that you have configured one Availability view and specified polling parameters, you
can monitor devices and run reports. For details about using Availability, refer to the
online help.

Setting Up Syslog Analysis

Syslog Analysis lets you centrally log and track messages generated by devices. You can
use the logged error message data to analyze router and network performance. You can
customize Syslog Analysis to produce the information and message reports that are
important to your operation.

Because system message logging is not part of the Windows NT operating system,
Essentials provides syslog message logging as a Windows NT service (Essentials syslog
service). The syslog service saves each system message to the default directory,
C:\Programs Files\CSCOpx. Syslog Analysis reads the syslog.log file for messages,
processes the messages, and writes them to the Essentials database. CGI scripts use the
database information to generate system message reports.

Refer to the online help for more information about Syslog Analysis.

Configuring Routers and Switches for Syslog Analysis

Before you can use Syslog Analysis, you must configure the routers (Cisco IOS devices) and switches (Catalyst 5000 family devices) to forward messages to Essentials or a system on which you have installed the distributed Syslog Analyzer collector. For more information about setting up routers for message logging, refer to the Syslog online help, the Cisco IOS Software Documentation on CCO (for Cisco IOS devices), and the appropriate Catalyst 5000 series reference guides (for Catalyst 5000 family devices).

Configuring Cisco IOS Devices

To configure Cisco IOS devices:

Step 1   Telnet to the device and log in. The prompt changes to `host>`.

Step 2   Enter **enable** and the enable password. The prompt changes to `host#`.

Step 3   Enter **configure terminal**. You are now in configuration mode, and the prompt changes to `host(config)#`.

Step 4   To make sure logging is enabled, enter **logging on**.

Step 5   To specify the Essentials server to receive the router syslog messages, enter **logging** *123.45.67.89* (where *123.45.67.89* is the IP address of the server).

Step 6   Set the logging trap level by entering **logging trap 6**.

Severity level 6 means all messages from levels 0–5 (from emergencies to notifications) will be logged to the server.

Step 7   Verify that syslog is running:

(a)   From the CiscoWorks2000 interface, select **CiscoWorks2000 Server > Administration > Process Management > Process Status**. The Process Status dialog box appears.

(b)   Verify that the entry for Syslog Analyzer has the status Running.

Configuring Catalyst 2900, 5000, and 6000 Family Devices

To configure Catalyst devices:

Step 1 Telnet to the device and log in. The prompt changes to `host>`.

Step 2 Enter **enable** and the enable password. The prompt changes to `host(enable).`

Step 3 To make sure logging is enabled, enter **set logging server enable.**

Step 4 Enter **set logging server** *123.45.67.89* (where *123.45.67.89* is the IP address of the server) to specify the server that is to receive the Catalyst switch syslog messages.

Step 5 Set the logging trap level by entering **set logging level 6**.

Severity level 6 means all messages from level 0–5 (from emergencies to notifications) will be logged to the server.

Step 6 Verify that the syslog filter file settings are correct.

Step 7 Verify that syslog is running by selecting **CiscoWorks2000 Server > Administration > Process Management > Process Status**.

Verifying the Syslog Analyzer

To verify that the Syslog Analyzer is processing syslog messages from the network:

Step 1 Log in to a managed router that is configured to send Syslog messages to the server. You must have appropriate login privileges to make configuration changes.

Step 2 Make a nondestructive change to the router configuration. For example, change the contents of the login banner by entering:

```
# enable
# configure terminal
```

The prompt changes to `#>`.

```
#> banner motd /
This is a test /
#> end
```

Step 3   Wait approximately 2 minutes for the syslog message to be processed by the server.

Step 4   Select **Resource Manager Essentials > Syslog Analysis > Standard Reports**. The Standard Reports dialog box appears.

Step 5   Select the device for which you made a change. Click **Help** if needed.

Step 6   Click **Next**. The Select Dates and Report Type dialog box appears.

Step 7   Select:

- **All Messages** in the Report Type list.

- **Today** from the Dates list.

Step 8   Click **Finish**. The Syslog-Standard report appears.

Verify that the report contains the Syslog message generated by the configuration change.

Setting Up Software Management

Software Management performs system software upgrades, boot loader upgrades, and software configuration operations on groups of routers and switches. For more information about setting up Software Management, refer to the online help.

Space Requirements for Downloaded Files

Before you can use Software Management, you must have sufficient space to store the software image files. You should have 2 to 8 MB of space for each image.

Setting Up File Transfer Servers

Essentials installs two file-transfer servers that the Software Management application uses to transfer software files:

- A Trivial File Transfer Protocol (TFTP) server

During Software Management installation, the tftpboot directory is created under the directory in which Essentials is installed (the default is C:\Program Files\CSCOpx).

This directory saves and stores files that are loaded to a device when you use Essentials applications supported by TFTP. All users have read, write, and execute privileges to the tftpboot directory.

- A remote copy (rcp) server

By default, Essentials uses rcp with devices that support rcp. For other devices, Essentials uses TFTP.

You can disable rcp if you do not want Essentials to use it with any devices:

Step 1   Select **Resource Manager Essentials > Administration > Software Management > Edit Preferences**.

Step 2   Deselect the **Use RCP for image transfer (when applicable)** check box.

Step 3   Click **Finish**.

Adding Device Passwords

Before you can use Software Management to manage device software images, you must add the required device passwords to Inventory.

Read and write community strings are required and the Telnet password is recommended. For information, see the "Changing Device Attributes (Credentials and Serial Numbers)" section on page 2-12 or refer to the online help.

Configuring the SMTP Server

Software Management uses an SMTP server on your network to deliver reports. The default location is localhost, which means that Software Management uses the SMTP server on the server.

If you want Software Management to use an SMTP server on a different system:

Step 1   Select **Resource Manager Essentials > Administration > Inventory > System Configuration**. The System Configuration dialog box appears.

Step 2   Select the SMTP tab.

Step 3   Enter the name of your SMTP server in the Server Name field.

Step 4   Click **Apply**.

Setting Software Management Preferences

Software Management has many preferences that you can set to control how the application behaves.

To set preferences:

Step 1   Select **Resource Manager Essentials > Administration > Software Management > Edit Preferences**. The Edit Preferences dialog box appears.

Step 2   Change the settings as appropriate.

For more information, refer to the online help.

Step 3   After you finish:

- Click **Finish** to save your changes.

- Click **Default** to display the default configuration.

Setting Up Configuration Management

Before Configuration Management can gather device configurations, you need to update the Essentials database with passwords, modify device configurations, and modify device security. You might also need to integrate Netsys and set up NetConfig.

Entering Device Credentials

Before the configuration archive can gather device configurations, you need to enter the following device credentials:

- Read and write community strings

- Telnet passwords for login mode and enable mode

For the configuration archive to use Telnet to gather configuration from devices, you must enter the correct credentials.

- TACACS, local, and rcp information for the devices

  — If a device is configured for TACACS authentication, add the TACACS username and password, not the Telnet passwords.

  — If a device is configured for local user authentication, add the local username and password.

If you already added or imported devices into Inventory and did not specify this information, you can change the device attributes. For information, see the "Changing Device Attributes (Credentials and Serial Numbers)" section on page 2-12, or refer to the Inventory online help.

Modifying Device Configurations

You need to modify your device configurations to enable Configuration Management to gather the configurations. After you perform the following procedures and your devices become managed, the configuration files are collected and stored in the configuration archive.

Make Sure Devices Are rcp-enabled

To make sure the devices are rcp-enabled, log in to each device and enter the following commands in the device configurations:

```
# ip rcmd rcp-enable
# ip rcmd remote-host remote_username IP_address local_username enable
```

where *IP_address* is the IP address of the system on which Essentials is installed. (Alternatively, you can enter the hostname.) The default *remote_username* and *local_username* are cwuser.

Configure Devices for Syslog Analysis

Configure your devices for Syslog Analysis if you want the device configurations to be gathered and stored automatically in the configuration archive when syslog messages are received. For information, see the "Setting Up Syslog Analysis" section on page 2-14 or refer to the online help.

Modifying Device Security

To archive device configurations, Configuration Management must be able to run certain commands on the devices. You must disable the security on the devices that prevents Configuration Management from running the commands shown in Table 2-3.

Table 2-3   Required Configuration Management Commands

Command Type	Command	Description
IOS commands	term len 0	Turns paging off for the Telnet session.
	write term	Gets the running configuration.
	show config	Gets the startup configuration.
Catalyst commands	set len 0	Turns paging off for the Telnet session.
	write term	Gets the running configuration.
Fast Switch command	show run	Gets the running configuration.

Setting Up Netsys Integration

Netsys is a Cisco network management application that you can choose to integrate with Essentials. After integration, you can pass information to Netsys from the Inventory application and receive Netsys reports that you can view from the CiscoWorks2000 interface.

When you integrate Essentials with Netsys running on a remote Windows NT system, you must perform some setup tasks that are not required when you integrate with Netsys running on the CiscoWorks2000 server or on a UNIX system.

Supported Netsys Versions

You can integrate Configuration Management with the following versions of Netsys:

- Version 4.2 for UNIX operating systems
- Version 4.0.1 for Windows NT

Upgrading Netsys Integration

When you upgrade from a previous version of Essentials, you must upgrade Netsys integration. You can choose either of the following procedures. The two procedures have different effects. The second procedure must be performed before you begin the CiscoWorks2000 upgrade.

The first procedure regenerates the baseline using the previous Netsys setup information, which is preserved during the upgrade. The previous reports are deleted and the baseline on the Netsys server is overwritten.

Step 1   Upgrade to Essentials 3.0, following the procedures in *Installing and Setting Up CD One on Windows NT* and in the "Upgrading from a Previous Version" section on page 1-8 in this guide.

Step 2   Access CiscoWorks2000 and log in as administrator.

Step 3   Select **Resource Manager Essentials > Administration > Configuration Management > General Setup**. The General Setup dialog box appears.

Step 4   Select the Netsys Setup tab.

Step 5   Select the **Create Baseline** check box, then click **Apply**.

If a message appears informing you about a timeout problem or an exception, click **Apply** to continue. The baseline regeneration proceeds.

The second procedure restores the previous Netsys setup information, baseline, and reports. Report generation will continue after the upgrade according to the previous schedule.

Note   This procedure must be performed before you begin the upgrade installation.

Step 1   Before upgrading to Essentials 3.0, copy all of the files and directories in the directory *install_dir*/htdocs/netsys to a safe place, where *install_dir* is the directory in which the previous version of Essentials is installed.

Step 2   Upgrade to Essentials 3.0.

Step 3   Restore the files and directories you backed up to the directory *install_dir*/htdocs/netsys, where *install_dir* is the directory where Essentials 3.0 is installed.

Setting Up Netsys on a Remote Windows NT System

Note   The following setup tasks are not required when Netsys is installed on the same system as CiscoWorks2000.

To integrate with Netsys running on a remote Windows NT system:

Step 1   Verify that the run_ngs.exe file exists in the Netsys installation directory on the Netsys server. Netsys is installed in the directory defined by the system variable ECSP_HOME.

Step 2   Copy the rcmf.exe file from the CiscoWorks2000 server to any directory on the Netsys server (c:\Temp is recommended).

This file is located in the *install_dir*\RemoteNetsysNT directory, where *install_dir* is the directory in which CiscoWorks2000 is installed.

Step 3   Run rcmf.exe on the Netsys server to install remote shell services:

(a)   Exit all running programs.

(b)   Open an MS-DOS window.

(c)   Navigate to the directory to which you copied rcmf.exe.

(d)   Enter **rcmf** and press the Enter key. The installation program starts. A dialog box appears asking if you want to install rcmf.

(e)   Click **Yes**. The Welcome dialog box appears.

(f)   Click **Next**. The Setup type dialog box appears.

(g)   Select the Typical or Custom setup type:

- Typical installs rcmf in the C:\Program Files\rcmf directory with no more interaction.

- Custom allows you to select the installation directory.

(h)   Click **Next**.

- If you selected the Typical setup type, the Start Copying Files dialog appears. Go to step (j).

- If you selected the Custom setup type, the Destination Location dialog appears.

(i)   In the Destination Location dialog box, click **Browse** to browse for the directory in which to install rcmf, then click **Next**. The Start Copying Files dialog box appears.

(j)   Click **Next** in the Start Copying Files dialog box to start installing files, or click **Cancel** to cancel the installation.

Rcmf is installed, and the Setup Complete dialog box appears. A CiscoWorks2000 Remote Service entry with an uninstall option is added to the Program menu.

Step 4   On the Netsys server:

(a)   Make sure that the TMPDIR system variable is defined. If it is not, define it as a full path to an existing directory.

(b)   To start the remote shell services, enter **net start crmrsh** from the directory in which you installed them.

(c)   From the directory in which you installed the remote shell services, enter the command that corresponds to your CiscoWorks server type. *CW2000_host* is the name of the CiscoWorks2000 server.

- For a Windows NT CiscoWorks2000 server, enter:

  crmrsh addrhost "*CW2000_host* **SYSTEM**" **Administrator**

  crmrsh addrhost "*CW2000_host* **bin**" **Administrator**

- For a UNIX CiscoWorks2000 server, enter:

  crmrsh addrhost "*CW2000_host* **bin**" **Administrator**

(d) Add an entry to the hosts file for the CiscoWorks2000 server. The hosts file is located in the directory c:\Winnt\system32\drivers\etc.

Step 5   Verify that the CiscoWorks2000 and Netsys servers can communicate with each other over the network by pinging each system from the other.

Step 6   Verify that remote shell services are running correctly:

(a) On the Netsys server, enter:

  crmrsh addrhost *CW2000_host username* **Administrator**

  where *CW2000_host* is the name of the CiscoWorks2000 server and *username* is an operating system login name.

(b) Log in to the CiscoWorks2000 server using the login that you entered on the Netsys server system (*username*).

(c) On the CiscoWorks2000 server, enter:

  rsh -l Administrator *Netsys_host* "**dir**"

  where *Netsys_host* is the name of the Netsys server, to list the contents of the root directory on the Netsys server.

  If a directory listing appears, the remote shell services are working.

Troubleshooting Netsys Integration Setup

If you have any problems setting up integration with Netsys running on a Windows NT system, perform the following troubleshooting steps on the Netsys server:

Step 1   Verify that the system variable TMPDIR is defined.

Step 2   Review events on the system generated by the source CRMrsh to determine if any errors occurred.

(a)   Select **Start > Programs > Administrative Tools (Common) > Event Viewer** to open the event viewer.

(b)   Select **File > Application** to view the application log.

(c)   Locate events with the source CRMrsh by using either the **View > Filter Events...** or **View > Find...** commands. Refer to the Event Viewer online help for more information.

Step 3   If the Event Viewer does not provide any useful information about Netsys integration problems, modify the debug level and repeat the setup process:

(a)   Start the Registry Editor by entering **regedit** at the command prompt or in the Run dialog box.

(b)   Select the registry key by selecting **My Computer > HKEY_LOCAL_MACHINE > SYSTEM > CurrentControlSet > Services > crmrsh > Parameters**.

The possible values for Debug level are 0x1, 0x2, 0x4 and 0x6.

(c)   Set the value of Debug to 0x06 to get the most detailed debug output in the Event Viewer.

(d)   Restart CRMrsh services by entering:

```
net stop crmrsh

net start crmrsh
```

(e)   Repeat the Netsys setup process on the CiscoWorks2000 server and use the Event Viewer to find any errors.

Step 4 If you find the CRMrsh message "The Client is not authorized to do remote commands" in the Event Viewer, follow these steps to correct the problem:

(a) Verify that the CiscoWorks2000 host name is entered in the hosts file on the Netsys server.

(b) Determine if the CiscoWorks2000 host name is resolved to a fully qualified name in the event log. If so, use the fully qualified host name (for example, cw2000.cisco.com) when you enter the crmrsh addrhost command.

(c) Verify that the CiscoWorks2000 user name is entered correctly by examining the Registry keys rhosts and rusers, which are located at the Registry path **My Computer > HKEY_LOCAL_MACHINE > SYSTEM > CurrentControlSet > Services > crmrsh > Parameters**.

Step 5 To troubleshoot other errors, examine the netsys_debug.log file, which is located in the directory specified by the value of the PX_TMPDIR environment variable.

Setting Up NetConfig

This section describes how to set up NetConfig.

Verifying Device Configurations

NetConfig can configure only devices that have archived configurations. To verify that devices you want to configure have an archived configuration and troubleshoot those that do not, use the Archive Status report.

To verify configuration archive status:

Step 1 Select **Resource Manager Essentials > Administration > Configuration Management > Archive Status**. The Configuration Archive Status Summary dialog box appears.

Step 2 Click **Update** at the bottom of the dialog box to update the archive status.

Step 3   Click on a device status to view details:

- Click **Successful** to display information about which configurations are archived. Click **Close** to close the window and return to the Configuration Archive Status Summary dialog box.

- Click **Failed** to display information about which configurations could not be obtained. To update the archive for failed devices, click on one or more device names or click **Select All**, then click **Update Archive**. The Running Configuration Status report appears. Click **Update Status** to refresh the device status in the archive. Click **Close** to return to the Configuration Archive Status Summary dialog box.

- Click **Not Supported** to display the devices not supported by the configuration archive. Click **Close** to return to the Configuration Archive Status Summary dialog box.

- Click **Partial Failure** to display the Catalyst 5000 family devices whose submodules were not pulled into the archive. Click **Close** to return to the Archive Status Summary dialog box.

For information, refer to the Configuration Management online help.

Verifying Device Credentials (Attributes)

Make sure every device you want to configure using NetConfig has correct device credentials in the Inventory application. NetConfig must have access to the correct credentials to make device configuration changes.

To verify device credentials, select **Resource Manager Essentials > Administration > Inventory > Check Device Attributes**. If any devices that you want to configure with NetConfig have incorrect credentials, see the "Changing Device Attributes (Credentials and Serial Numbers)" section on page 2-12 or refer to the online help.

Modifying Device Security

In addition to running the configuration commands that you assign to each job, NetConfig must run certain commands on devices to configure them. You must disable the security on these devices that prevents NetConfig from running the commands listed in Table 2-4.

Table 2-4   Required NetConfig Commands

Command Type	Command	Description
IOS commands	term len 0	Turns paging off for the Telnet session.
	write term	Gets the running configuration.
	show config	Gets the startup configuration.
	reload	Reloads or resets the device.
	write mem	Writes the running configuration to the startup configuration.
	erase startup	Erases the startup configuration.
	config t	Enters config mode.
	exit	Exits config mode.
Catalyst commands	set len 0	Turns paging off for the Telnet session.
	write term	Gets the running configuration.
	reload	Reloads or resets the device.
Fast Switch command	show run	Gets the running configuration.
	reload	Reloads or resets the device.

Verify Device Prompts

NetConfig requires the following CLI prompts:

- For Cisco IOS devices, the login prompt must end with a *greater-than symbol* (>), and the enable prompt must end with a *pound sign* (#).

- For Catalyst devices, the enable prompt must end with the string:

    ```
    (enable)
    ```

These are the default prompts. If you have changed the defaults, make sure the prompts meet the requirements listed above.

Logging Out

To end your system administrator tasks, you must log out of CiscoWorks2000:

Step 1   Close all secondary browser windows. You should have only one browser window opened displaying the CiscoWorks2000 desktop.

Step 2   Click **Logout**. The Login Manager dialog box replaces the navigation tree.