



Preparing to Use Essentials Applications

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

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

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](#)
- [Logging Out](#)

Preparation Overview

Table 2-1 is an overview of preparing to use Essentials applications. It contains 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, and rcp.	“Configuring the Server” section on page 2-7
2. Set up Inventory.	a. Create network inventory by either: <ul style="list-style-type: none"> • 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 2-10
	b. (Optional) Create a device view.	“Creating a Device View” section on page 2-14
	c. (Optional) Obtain login privileges to Cisco.com.	If you do not have login privileges, go to www.cisco.com , to obtain a login.
	d. (Optional) Enter device serial numbers for devices that have Contract Connection service contracts.	“Changing Device Attributes (Credentials and Serial Numbers)” section on page 2-14
	e. (Optional) Perform the following optional Inventory setup tasks: <ul style="list-style-type: none"> • Schedule inventory polling and collection. • Set change report filters. • Display a detailed device report. 	Inventory online help

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

Task	Steps	References
3. Verify Availability.	a. Create a device view with at least one device.	“Verifying Availability” section on page 2-15 and “Creating a Device View” section on page 2-14
	b. Verify that Availability functions correctly.	“Verifying Availability” section on page 2-15
4. Set up Syslog Analysis.	a. Configure your routers and switches for syslog analysis.	“Configuring Devices for Syslog Analysis” section on page 2-17
	b. Verify settings in the syslog configuration file.	“Verifying the Settings in the Syslog Configuration File” section on page 2-19
	c. Verify that Syslog messages are being processed by the Syslog Analyzer.	“Verifying the Syslog Analyzer” section on page 2-20

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

Task	Steps	References
5. Set up Software Management.	a. Add device passwords to inventory.	“Adding Device Passwords to Inventory” section on page 2-21
	b. Set Software Management preferences.	“Setting Software Management Preferences” section on page 2-21
	c. Obtain login privileges to Cisco.com for importing software images.	If you do not have login privileges, go to the www.cisco.com , to obtain a login.
	d. Set up TFTP.	“Setting Up TFTP” section on page 2-22
	e. Set up rcp	“Setting Up rcp” section on page 2-24
	f. Allow user casuser to use at and cron.	“Allowing the User casuser to Use at and cron” section on page 2-27
	g. (Optional) Perform optional setup tasks. <ul style="list-style-type: none"> • 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 Job Approval 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.	a. Enter passwords.	“Entering Device Credentials” section on page 2-28
	b. Modify device configurations.	“Modifying Device Configurations” section on page 2-28
	c. Modify device security.	“Modifying Device Security” section on page 2-29
	d. Upgrade, set up, and troubleshoot Netsys integration if you are using the Cisco Netsys application.	“Setting Up Netsys Integration” section on page 2-30
	e. Set up NetConfig: <ul style="list-style-type: none"> • Verify device configurations in configuration archive. • Verify device credentials. • Modify device security. • Verify device prompts. 	“Setting Up NetConfig” section on page 2-36 and the NetConfig online help
	f. (Optional) Perform optional NetConfig setup tasks: <ul style="list-style-type: none"> • Install Java Plugin 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 screen appears with the Login Manager displayed. To access the server from a client system, enter the URL of the server in your web browser:

- If you installed CiscoWorks2000 CD One on the default port, enter:

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

where *server_name* is the hostname of the server on which you installed Essentials.

- If an alternative port was assigned during CiscoWorks2000 CD One installation, enter:

```
http://server_name:port_number
```

where *server_name* is the name of the server on which you installed CiscoWorks2000 CD One and Essentials, and *port_number* is the alternative port assigned during the installation. See *Getting Started with the CiscoWorks2000 Server* for information about administrator logins.

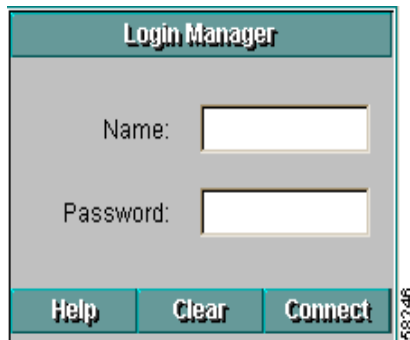
Logging In

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

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

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

Figure 2-1 Login Manager Dialog Box



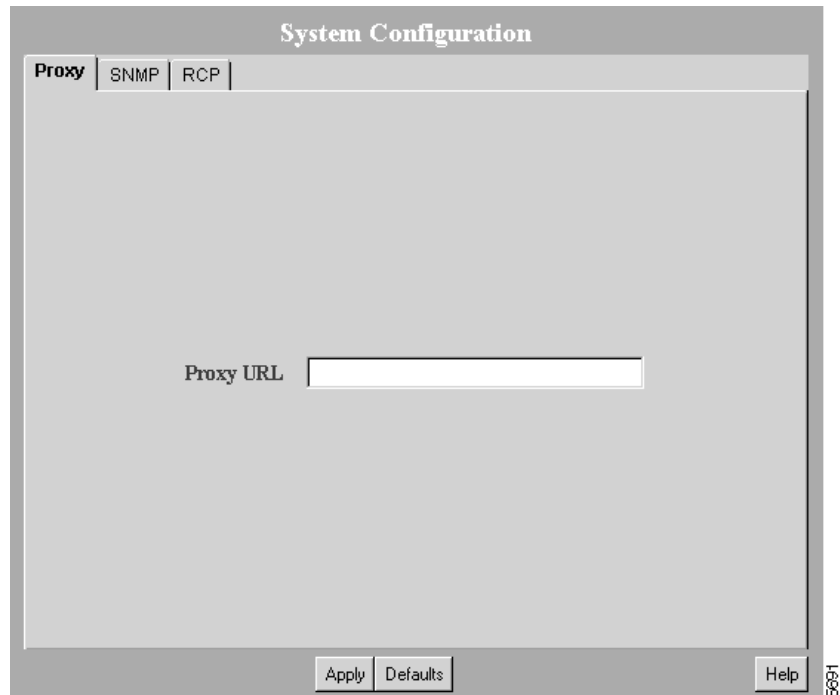
Step 2 Click **Connect**. The Login Manager dialog box is replaced by the navigation tree.

Configuring the Server

You can configure system-wide information for Essentials applications using the System Configuration option. You should verify that the defaults are correct or enter corrections.

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
- rcp

See [Table 2-2](#) for descriptions of the information in each dialog box tab.

Step 3 Click **Apply** to save changes, or click **Defaults** to apply the default.

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.

Table 2-2 System Configuration Dialog Box Information

Tab Name	Description	Fields—Values to Enter
Proxy	Used to connect to Cisco.com. 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, which includes importing and adding devices, and collecting inventory data.	<p>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.</p> <p>Fast SNMP Retry—Number of times, from 2 to 6, system tries to access devices with fast SNMP options. Default is 2.</p> <p>Slow SNMP Timeout—Amount of time, from 10 to 90 seconds, system waits for a device to respond before trying to access it again. Default is 20.</p> <p>Slow SNMP Retry—Number of times, from 2 to 6, system tries to access a device with slow SNMP options. Default is 3.</p> <p>Note The system tries the Fast SNMP Timeout and Fast SNMP Retry options first. If no response occurs after Fast Retry, the system switches to the Slow SNMP options.</p>
rcp	<p>Used to specify user during remote file transfers from devices. Authenticates rcp transfers between devices and server.</p> <p>User account must exist on UNIX systems, and should also be configured on devices as local user in the ip rcmd configuration command.</p> <p>See “Setting Up rcp” section on page 2-24.</p>	User Name—Name used by a network device when it connects to server to run rcp.

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 one managed device (a device whose inventory information is tracked by Essentials) to verify correct Essentials installation. To manage your network, you need to add device information for all your managed devices.

To populate your network inventory:

- Add devices one at a time by entering the device information manually.
- Import a group of devices from:
 - A comma-separated values (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 1-7.

Adding Device Information Manually

This section describes how to add devices one at a time and how to troubleshoot problems you might have, using this method.

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, all 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 Inventory online help.

- Step 3** Click **Next**. The Enter Login Authentication Information dialog box appears. You must fill in the Read Community String field and verify the password. For Inventory, all 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. If required, complete this dialog box. For Inventory, all fields in this dialog box are optional. 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 dialog box to check the status of the device you specified. The dialog box should contain:

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 field has 1 device, Essentials was installed and configured correctly. You might need to wait a couple of 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.

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 9** 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 10** To determine if the DIServer process is running, select **Server Configuration > 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 **Server Configuration > 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 **Server Configuration > Process Management > Start Process**. The Start Process dialog box appears.
- b. Click the **Process** radio button.
- c. In the Process Name field, select **DIServer**, then click **Finish**.

- Step 11** To return to the Add/Import Status Summary screen, select **Resource Manager Essentials > Administration > Inventory > Import Status**, then click **Update**. The device status should change to *managed* within a couple of minutes.
-

Importing Devices

You can import devices either from a file or from a local or remote NMS:

- You can extract data from your existing data source into a comma-separated value (CSV) file or device integration file (DIF), then use this file as input into the Essentials database. First create a CSV file or DIF file, then select **Resource Manager Essentials > Administration > Inventory > Import from File** to access the 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**. For more information, refer to the online help.

For a list of supported NMS software, see the [“Supported NMS Environments for Device Import”](#) section on page 1-7.

- To import devices from a remote NMS:
 - Work with the system administrator of the host on which the NMS database is running. For more information, refer to the online help.
 - 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 1-7. For additional information, refer to the online help.
 - 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:

- Increase the SNMP timeout setting. Refer to the online help for more information or see the [“Configuring the Server”](#) section on page 2-7.
- Verify that you entered correct read community strings for the devices.

For additional information, refer to the online help.

Creating a Device View

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

To create the static device view:

-
- Step 1** Select **Resource Manager Essentials > Administration > Device Views > Add Static Views**. The Add Static Views dialog box appears.
 - Step 2** Enter a view name and an optional description, and select a type of view (custom or private.) Only users with the system administrator role can create custom views.
 - Step 3** Select the view, from the Views column, that has the devices you want to add.
 - Step 4** Select the names of the devices you want, from the Device pane and move them into the Selected Devices pane.
 - Step 5** Click **Finish**. The new view is created.
 - Step 6** To add another static device view, repeat the procedure.
-

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 enter device serial numbers in the inventory 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 Device Attributes 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 the current information.
- Step 4** Edit dialog boxes as needed:
- 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** After you complete editing a dialog box:
- Click **Finish** to apply the changes and move to the next dialog box or to exit, if you are in 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 one device. You can use the view you created during Inventory setup. Use this test 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**. The Select Polled Views dialog box appears.
- 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 Availability Monitor.

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.

Specifying Country Codes

You must update the country code entry in the file, `Sa.properties` with the appropriate country code to make sure the Syslog timestamp conversion works correctly. `Sa.properties` is located in the directory, `install_dir/lib/classpath/com/cisco/nm/sysloga/sa`, where `install_dir` is the directory in which `CiscoWorks2000` is installed.

The country code is the 3-letter abbreviation specified as per the ISO_3166 document.

For a list of country codes, access the site, http://userpage.chemie.fu-berlin.de/diverse/doc/ISO_3166.html. You must restart Syslog Analyzer after you update the country code.

To terminate Syslog Analyzer, at the command prompt, enter:

```
install_dir/bin/pdterm SyslogAnalyzer.
```

To start Syslog Analyzer, at the command prompt, enter:

```
install_dir/bin/pdexec SyslogAnalyzer.
```

Configuring Devices for Syslog Analysis

Before you can use Syslog Analysis, you must configure your devices to forward messages to Essentials or to a system on which you have installed the distributed Syslog Analyzer collector. For more information about setting up devices for message logging, refer to the online help, the Cisco IOS software documentation on www.cisco.com (for Cisco IOS devices), and the appropriate reference guides.

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**.
 - Step 3 Enter the enable password. The prompt changes to `host#`.
 - Step 4 Enter **configure terminal**. You are now in configuration mode, and the prompt changes to `host(config)#`.
 - Step 5 To make sure logging is enabled, enter **logging on**.
 - Step 6 To specify the 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 7 To limit the types of messages that can be logged to the server, set the appropriate logging trap level by entering **logging trap informational**.

Severity level informational means that all messages from alert messages to informational messages (from emergencies to notifications) will be logged to the server.

- Step 8** Verify that Syslog is running:
- a. From the CiscoWorks2000 desktop, select **Server Configuration > Administration > Process Management > Process Status**. The Process Status dialog box appears.
 - b. Verify that the entry for Syslog Analyzer has the status, Running normally.
- Step 9** Verify that the Syslog configuration file settings are correct. See the [“Verifying the Settings in the Syslog Configuration File”](#) section on page 2-19 for instructions.
-

Configuring Catalyst 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** To specify the server to receive the Catalyst switch syslog messages, enter **set logging server 123.45.67.89** (where *123.45.67.89* is the IP address of the server).
- Step 5** Set the appropriate logging trap level by entering **set logging all level 6 default**. Severity level 6 means all messages from levels 0-6 (from alerts to notifications) will be logged to the server.

- Step 6** Verify that Syslog is running:
- From the CiscoWorks2000 desktop, select **Server Configuration > Admin > Process Management > Process Status**. The Process Status dialog box appears.
 - Verify that the entry for Syslog Analyzer has the status, Running normally.
- Step 7** Verify that the Syslog configuration file settings are correct. See the [“Verifying the Settings in the Syslog Configuration File” section on page 2-19](#) for instructions.
-

Verifying the Settings in the Syslog Configuration File

To check the path and permissions of the file pointed to by local7.info in the syslog configuration file /etc/syslog.conf on the server:

- Step 1** Make sure the facility.level definition is set to local7.info, and that the following line is present (note that there must be a tab between local7.info and the *path/filename*):

```
local7.info    path/filename
```

where *path/filename* is the full path to a file.

- Step 2** Make sure the syslog process (syslogd) can both read and write to the file.
- Step 3** If you modified the /etc/syslog.conf file, you must restart the syslog process (syslogd). Enter the following command to stop and restart syslogd:

```
/bin/startsrc -s syslogd start and /bin/startsrc -s syslogd stop
```

If the start and stop command does not work, enter:

```
kill -HUP `cat /etc/syslog.pid`
```

- Step 4** Make sure the Message Source in the CiscoWorks2000 Server is the same as the filename you specified in the syslog.conf file. You can check this by selecting **Resource Manager Essentials > Administration > Syslog Analysis > Change Storage Operations**.
-

Verifying the Syslog Analyzer

To verify that the Syslog Analyzer is processing 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, to change the contents of the login banner enter:

```
# enable
# configure terminal
```

The prompt changes to #>.

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

Step 3 Wait approximately 2 minutes for the server to process the Syslog message

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 that the configuration change generated.

Setting Up Software Management

Software Management performs system software upgrades, boot loader upgrades, and software configuration operations on groups of routers and switches.

Space Required for Downloaded Files

Software Management files downloaded to the server from www.cisco.com or the product CD-ROM are stored in the `/var` directory or its subdirectories. Make sure there is enough space in the `/var` directory for all files that you plan to download.

Device software image files are up to 4 MB in size. To determine how much space you need, multiply the number of device software image files you plan to store by 4 MB. For example, if you plan to store 30 software image files, you need at least 120 MB in `/var`.

In addition, you need space for some smaller downloaded files and temporary files. To accommodate these needs, add at least 20% to the space needed for software image files for your final space calculation in the `/var` directory. Using the previous example, you would need a total of at least 144 MB of available space in `/var`.

Adding Device Passwords to Inventory

Before you can use Software Management to manage device software images, you must add the required device passwords to Inventory. To add device passwords to Inventory, see the [“Changing Device Attributes \(Credentials and Serial Numbers\)”](#) section on page 2-14 or the online help.

Setting Software Management Preferences

Software Management has many preferences 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 preferences as appropriate.
For more information, refer to the online help.
- Step 3** After you complete the changes:
- Click **Finish** to save your changes.
 - Click **Default** to display the default configuration.
-

Setting Up TFTP

A file transfer server must be installed on your system. You must enable a Trivial File Transfer Protocol (TFTP) server because it is the default file transfer server type.

During Software Management installation, if the installation tool cannot find a TFTP server, it tries to add one. If the installation tool cannot find or create a TFTP server, install and enable the TFTP server and verify that a `/tftpboot` directory exists, as explained in the following sections.

Enabling the TFTP Daemon

If you are using standard AIX software, you can add and configure the TFTP server (TFTPD):

-
- Step 1** Log in as superuser.
- Step 2** Using a text editor, edit the `/etc/inetd.conf` file.
- Look in the file `/etc/inetd.conf` for the line that invokes TFTPD. If the line begins with a pound sign (`#`), remove the pound sign with your text editor. Depending on your system, the line that invokes the TFTP server might look similar to:
- ```
tftp dgram udp src root /usr/sbin/in.tftpd in.tftpd -s /tftpboot
```
- Save the changes to the edited file and exit your text editor.

**Step 3** At the UNIX prompt, enter the following command to display the process identification number for the inetd configuration:

```
/usr/bin/ps -ef | grep -v grep | grep inetd
```

The system response is similar to:

```
root 119 1 0 12:56:14 ? 0:00 /usr/bin/inetd -s
```

The first number in the output (119) is the process identification number of the inetd configuration.

**Step 4** To enable your system to read the edited /etc/inetd.conf file, enter:

```
kill -HUP 119
```

where 119 is the process identification number identified in Step 3.

**Step 5** Verify that TFTP is enabled by entering either:

```
netstat -a | grep tftp
```

which should return output similar to:

```
*.tftp Idle
```

or enter:

```
/usr/CSCOpX/bin/mping -s tftp localhost_machine_name
```

which returns the number of modules sent and received, for example:

```
sent:5 recvd:5 . . .
```

If the output shows that zero modules were received, TFTP is not enabled. Repeat these steps, beginning with Step 1, to make sure you have enabled TFTP.

---

## Creating the /tftpboot Directory

Essentials uses the /tftpboot directory when transferring files between the Essentials server and network devices. The files are removed after the transfer is complete, but multiple jobs (for example, image distribution, image import, or config file scan) could be running at the same time.

Each of these jobs requires its own space. Software image sizes, for example, can be up to 9 MB. To ensure that jobs run successfully, make sure there is sufficient space available in the /tftpboot directory.

If the /tftpboot directory does not exist on your system, you must create it:

---

**Step 1** Enter:

```
mkdir /tftpboot
```

**Step 2** Make sure all users have read, write, and execute permissions to the /tftpboot directory by entering:

```
chmod 777 /tftpboot
```

The /tftpboot directory now exists and has the correct permissions.

---

## Setting Up rcp

You can enable a remote copy (rcp) server on the server and select it as the active file transfer server. If you select rcp as the active server and then try to transfer files to a device that does not support rcp, Essentials uses TFTP to transfer the files.

## Creating the rcp Remote User Account

To use rcp, you must create a user account on the system to act as the remote user to authenticate the rcp commands issued by devices. This user account must own an empty .rhosts file in its home directory to which the user causer has write access.

You can choose the name of this user account because you can configure the Essentials server to use any user account. The default user account name is cwuser. The examples in this procedure use the default name casuser. If you choose to use a different name, substitute that name for casuser.

To create and configure the rcp remote user account, follow these steps while logged in as root:

---

**Step 1** To add a user account named cwuser to the system, enter:

```
useradd -m -c "user account to authenticate remote copy operations" \
\ cwuser
```

**Step 2** Navigate to the cwuser home directory.

**Step 3** To create the .rhosts file, enter:

```
touch .rhosts
```

**Step 4** To change the owner of the .rhosts file, enter:

```
chown cwuser:casusers .rhosts
```

**Step 5** To change the permissions of the .rhosts file, enter:

```
chmod 0664 .rhosts
```

**Step 6** If you did not use the default user name cwuser, use the user account that you created as the rcp remote user account.

- a. Log on to the server as admin.
  - b. Select **Resource Manager Essentials > Administration > System Configuration**.  
The System Configuration dialog box appears.
  - c. Select the rcp tab.
  - d. Enter the name of the user account that you just created in the User Name field, then click **Apply**.
- 

## Enabling the rcp Daemon

To add and configure standard AIX 4.3.3 rcp server software:

---

**Step 1** Log in as superuser.

**Step 2** Using a text editor, edit the /etc/inetd.conf file.

- Look in the file `/etc/inetd.conf` for the line that invokes `rshd`. If the line begins with a pound sign (`#`), remove the pound sign with a text editor. Depending on your system, the line that invokes the `rshd` server might look similar to:
 

```
shell stream tcp nowait root /usr/sbin/in.rshd in.rshd
```
- Save the changes to the edited file and exit the text editor.

**Step 3** At the UNIX prompt, enter the following to display the process identification number for the *inetd* configuration:

```
/usr/bin/ps -ef | grep -v grep | grep inetd
```

The system response is similar to:

```
root 119 1 0 12:56:14 ? 0:00 /usr/bin/inetd -s
```

The first number in the output (119) is the process identification number of the *inetd* configuration.

**Step 4** To enable your system to read the edited `/etc/inetd.conf` file, enter:

```
kill -HUP 119
```

where *119* is the process identification number identified in Step 3.

**Step 5** Verify that `rshd` is enabled by entering:

```
netstat -a | grep shell
```

which should return output similar to:

```
*.shell *.* 0 0 0 0 LISTEN
```

---

## Selecting rcp as the Active File Transfer Method

By default, Essentials uses `rcp` with devices that support `rcp`. For devices that do not support `rcp`, Essentials uses TFTP to transfer files.

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** Select **Use RCP for image transfer (when applicable)**.
- Step 3** Click **Finish**.
- 

## Allowing the User casuser to Use at and cron

Software Management uses at and cron to schedule Software Management image transfers to devices. The process that performs the download is executed as casuser, so the user casuser must be allowed to use at and cron.

To allow the user casuser to use at:

- If an at.deny file exists in the /usr/lib/cron directory, make sure casuser is not listed in it. If necessary, remove casuser from the at.deny file using a text editor.
  - If an at.allow file exists in the /usr/lib/cron directory, make sure casuser is listed in it. If necessary, add casuser to the at.allow file, using a text editor.
  - If neither an at.allow nor an at.deny file exist in the directory /usr/lib/cron, create an at.allow file and add casuser to it, using a text editor.
- 

To allow the user casuser to use cron:

- If a cron.deny file exists in the /usr/lib/cron directory, make sure casuser is not listed in it. If necessary, remove casuser from the cron.deny file, using a text editor.
  - If a cron.allow file exists in the /usr/lib/cron directory, make sure casuser is listed in it. If necessary, add casuser to the cron.allow file, using a text editor.
  - If neither a cron.allow nor a cron.deny file exists in the /usr/lib/cron directory, create a cron.allow file and add casuser to it, using a text editor.
-

# Setting Up Configuration Management

Before Configuration Management can gather device configurations, you need to update the Essentials database with passwords (credentials) and modify device configurations. If desired, you can integrate with Netsys and set up NetConfig.

## Entering Device Credentials

Before the configuration archive can use Telnet to gather device configurations, enter the following device credentials:

- Read and write community strings
- Telnet passwords for login mode and enable mode
- 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 devices or imported them into Inventory and did not specify this information, you can change the device attributes.

Refer to the [“Changing Device Attributes \(Credentials and Serial Numbers\)” section on page 2-14](#) or the Inventory online help for more information.

## Modifying Device Configurations

You need to modify your device configurations so that Configuration Management can 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

Make sure the devices are rcp-enabled by logging into each device and entering the following commands in the device configurations:

```
ip rcmd rcp-enable
ip rcmd remote-host local_username 123.45.678.90 remote_username
enable
```

where *123.45.678.90* is the IP address or hostname of the system on which Essentials is installed. The default *remote\_username* and *local\_username* are casuser.

## 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. See the [“Setting Up Syslog Analysis”](#) section on page 2-16 or refer to the online help for more information.

## Modifying Device Security

Configuration Management must be able to run certain commands on devices to archive their configurations. You must disable the security on 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                              |
|--------------------|------------|------------------------------------------|
| Catalyst commands  | set len 0  | Turns paging off for the Telnet session. |
|                    | write term | Gets the running configuration.          |
| FastSwitch command | show run   | Gets the running configuration.          |

**Table 2-3** Required Configuration Management Commands (continued)

| 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.          |

## 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 remote UNIX system.

### Supported Netsys Versions

You can integrate Configuration Management with these versions of Netsys:

- Version 4.3 for Solaris operating system
- Version 4.2 for Windows NT or earlier versions.

### 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 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 3.3, following the procedures in *Installing and Setting Up CD One on AIX* and in the “[Upgrading from a Previous Version](#)” section on [page 1-13](#) in this guide.
- Step 2** Access CiscoWorks2000 and log in as administrator.
- Step 3** Select **Resource Manager Essentials > Administration > Configuration Management > General Setup**. The Configuration Manager Admin 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 continues after the upgrade according to the previous schedule.



**Caution** You must perform this procedure before you begin the upgrade installation.

---

- 
- Step 1** Before upgrading to Essentials 3.3, 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 3.3.
- 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 3.3 is installed.
-

## Setting Up Netsys Integration 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, and 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 box appears. Go to step (j).
    - If you selected the Custom setup type, the Destination Location dialog box appears.

- i. Click **Browse** in the Destination Location dialog box, 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 servers, 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 system, enter:
 

```
crmrsh addrhost "CW2000_host SYSTEM" Administrator
crmrsh addrhost "CW2000_host casuser" Administrator
```
  - For a UNIX CiscoWorks2000 Server system, enter:
 

```
crmrsh addrhost "CW2000_host casuser" 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 Netsys-host -1 Administrator "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 integrating with Netsys running on a Windows NT system, perform these 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 CRMrsch to determine if any errors occurred.
- Select **Start > Programs > Administrative Tools (Common) > Event Viewer** to open the event viewer.
  - Select **File > Application** to view the application log.
  - Locate events with the source CRMrsch 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, as described in the following steps:
- Start the Registry Editor by entering the command **regedit** at the command prompt or in the Run dialog box.
  - Select the registry key, **My Computer > HKEY\_LOCAL\_MACHINE > SYSTEM > CurrentControlSet > Services > crmrsh > Parameters**.  
The possible values for Debug level are 0x1, 0x2, 0x4 and 0x6.
  - Set the value of Debug to 0x06 to get the most detailed debug output in the Event Viewer.

- d. To restart CRMrsch services, enter:

```
net stop crmrsh
```

```
net start crmrsh
```

- e. Repeat the Netsys setup on the CiscoWorks2000 Server and use the Event Viewer to find any errors.

**Step 4** If you see the CRMrsch 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 hostname is entered in the hosts file on the Netsys server.
- b. Determine if the CiscoWorks2000 hostname is resolved to a fully qualified name in the event log. If so, use the fully qualified hostname (for example, cw2000.cisco.com) when you enter the crmrsh addrhost command.
- c. Verify that the CiscoWorks2000 username 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 log file netsys\_debug.log, 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. Use the Archive Status report to:

- Verify that devices you want to configure have an archived configuration.
- Troubleshoot the devices that do not have an archived configuration.

- 
- 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 on archived configurations. Click **Close** to close the window and return to the Configuration Archive Status Summary dialog box.
  - Click **Failed** to display information on configurations that 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 devices whose submodules were not pulled into the archive. Click **Close** to return to the Configuration Archive Status Summary dialog box.

For more information, refer to the Configuration Management online help.

---

## Verifying Device Credentials

Verify that every device you want to configure using NetConfig has the correct device credentials entered 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 > Administrator > Inventory > Check Device Attributes**. If any devices that you want to configure have incorrect credentials, see the [“Changing Device Attributes \(Credentials and Serial Numbers\)”](#) section on page 2-14 or the online help.

## Modifying Device Security

In addition to running the configuration commands that you assign to each job, NetConfig must be able to run certain commands on devices to configure them. You must disable the security on devices that prevents NetConfig from running the commands listed in [Table 2-4](#). (Format this table. It extends beyond the page)

**Table 2-4 Required NetConfig Commands**

| Command Type         | Command            | Description                                            |
|----------------------|--------------------|--------------------------------------------------------|
| 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 commands | show run           | Gets the running configuration.                        |
|                      | reload             | Reloads or resets the device.                          |
| 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 running configuration to startup configuration. |
|                      | erase startup      | Erases the startup configuration.                      |
|                      | config t           | Enters config mode.                                    |
| exit                 | Exits config mode. |                                                        |

## Verifying Device Prompts

NetConfig requires these 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 following 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 administrator tasks, you must log out of CiscoWorks2000:

- 
- |               |                                                                                                                               |
|---------------|-------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Close all secondary browser windows. You should have only one browser window opened, displaying the CiscoWorks2000 interface. |
| <b>Step 2</b> | Click <b>Logout</b> . The Login Manager dialog box replaces the navigation tree.                                              |
-