CHAPTER 4

Installing and Upgrading Server Applications

The following topics explain how to install the Security Manager server software and other server applications, such as Common Services, AUS, Performance Monitor, and RME.

- Understanding the Required Server User Accounts, page 4-1
- Using Remote Desktop Connection or VNC To Install Server Applications, page 4-2
- Installing Security Manager Server, Common Services, and AUS, page 4-3
- Installing Performance Monitor, page 4-5
- Installing Resource Manager Essentials (RME), page 4-7
- Upgrading Server Applications, page 4-9
- Migrating Security Manager to a New Computer or Operating System, page 4-15
- Updating Security Manager, Performance Monitor, and RME Licenses, page 4-16
- Obtaining Service Packs and Point Patches, page 4-17
- Adding Applications to the Server's Home Page, page 4-18
- Uninstalling Server Applications, page 4-18
- Downgrading Server Applications, page 4-19

Understanding the Required Server User Accounts

CiscoWorks Common Services and Security Manager use a multilevel security system that allows access to certain features only to users who have the required authorization. For this reason, there are three predefined user accounts that are created on any system on which you install an application that runs on top of Common Services:

- **admin**—The admin user account is equivalent to a Windows administrator and provides access to all Common Services, Security Manager, and other application tasks. You must enter the password during installation. You can use this account to initially log in to the server and to create other user accounts for normal day-to-day use of the applications.
- **casuser**—The casuser user account is equivalent to a Windows administrator and provides access to all Common Services and Security Manager tasks. You do not normally use this account directly.

  Do not modify casuser (the default service account) or directory permissions that are established during the installation of the product. Doing so can lead to problems with your being able to do the following:

  - Logging in to the web server

  - Logging in to the client
  - Performing successful backups of all databases

- *System Identity*—The system identity user account is equivalent to a Windows administrator and provides access to all Common Services and Security Manager tasks. This account does not have a fixed name; you can create the account using whatever name fits your needs. If you create the account in Common Services, you must assign it system administrator privileges; if you use Cisco Secure Access Control Server (ACS) for user authentication, you must assign it all privileges.

  If you install Cisco Security Management suite applications on separate servers (the recommended approach), you must create the same system identity user account on all servers within the multi-server setup. Communication among your servers relies on a trust model that uses certificates and shared secrets. The system identity user is considered the trustworthy account by other servers in the multi-server setup and therefore facilitates communication between servers that are part of a domain.

You can create as many additional user accounts as needed. Each user should have a unique account. To create these additional accounts, you must have system administrator authority (for example, using the admin account). When you create a user account, you must assign it a role, and this role defines what the user can do in the applications, even to the extent of what the user can see. For more information on the various types of available permissions, and how to use ACS for controlling access to the applications, see Chapter 7, "Managing User Accounts."

Using Remote Desktop Connection or VNC To Install Server Applications

We recommend that you install server applications when you are logged directly in to the server.

However, if you must do a remote installation (logging in through another workstation), consider the following tips:

- Do not attempt to install the software from a remote disk. The software installer must either be on the product DVD running on a DVD drive in the server, or the program must reside on a directly connected disk drive. The installation might appear to succeed from a remote disk, but it does not actually succeed.
- You can use Virtual Network Computing (VNC) to install the software.
- You can use Remote Desktop Connection to install the software. However, you might find that Cisco Security Agent does not stop automatically when trying to install Security Manager while two or more Remote Desktop Connection sessions are simultaneously open. This is due to a limitation of Remote Desktop Connection—the first administrator who opens a Remote Desktop Connection session is always the one who receives the query about stopping the Cisco Security Agent service. If you install Security Manager over a Remote Desktop Connection session and are not the first administrator logged in, you do not receive the query. A workaround is to enter the command **net stop CSAgent** before installing Security Manager. Otherwise, ensure that yours is the first, or only, Remote Desktop Connection session during installation.

Installing Security Manager Server, Common Services, and AUS

The main Security Manager installation program can install the following applications:

- CiscoWorks Common Services 3.3—This is the foundation software that is required by any of the server applications. You must install Common Services 3.3 (if it is not already installed) when you install Security Manager, AUS, Performance Monitor, or RME.
- Cisco Security Manager 4.0.1—This is the main server software for Security Manager.

  If the server does not already have a full, standalone version of Cisco Security Agent installed, the installation program takes the following actions:

  - On Windows 2003 R2 Enterprise Server (Service Pack 2)—32 bit, the installation program asks you whether or not you want to install Cisco Security Agent.
  - On Windows 2008 Enterprise Server (Service Pack 2)—32 bit, the installation program does not install Cisco Security Agent.
  - On Windows 2008 Enterprise Server (Service Pack 2)—64 bit, the installation program does not install Cisco Security Agent.
- Auto Update Server 4.0
- Cisco Security Manager client 4.0.1—The client software for interacting with the Security Manager server. You can install this on the same computer as the server, but you should not use this setup as the regular way of using Security Manager. For more information on recommended client installation and setup, see Chapter 5, "Installing and Configuring the Client."

Use the following procedure to install or re-install these applications. If you are upgrading from a previous version of any of these applications, before proceeding, see Upgrading Server Applications, page 4-9.

Before You Begin

- All 3.x and earlier customers need to procure a new license (or licenses) for Security Manager 4.0.1 irrespective of whether they have a valid license for any of the (older) Security Manager 3.x releases. With the exception of incremental licenses, existing Security Manager 3.x licenses are not valid for Security Manager 4.0.1.
- If you are installing the product as an upgrade to an existing version of the application that is already installed on the server, run a backup as described in Backing Up the Database for Remote Upgrades, page 4-12. Ensure that the backup completes successfully, and that your existing applications are functioning normally before installing an upgrade.
- If you have a permanent license for Security Manager, copy it to the server. The license file must be on the server to select it during installation. Do not place the file in any folder in which you will install the product.
- Ensure that you go through the Readiness Checklist for Installation, page 3-4.
- Ensure that the server meets the requirements listed in Server Requirements, page 2-3.
- We recommend that you install Security Manager on a dedicated server in a controlled environment. Installing other software applications can interfere with the normal operation of Security Manager and is not supported.
- If you re-install Common Services after installing Security Manager server or AUS, you must also re-install Security Manager or AUS.
- Do not change the system time after installing Common Services. Such changes might affect the working of some time-dependent features.

- If you want to use Cisco Secure Access Control Server (ACS) to provide AAA services for user access to Security Manager or AUS, wait until you install the applications before you configure Common Services to use ACS. For information on configuring ACS control, see Integrating Security Manager with Cisco Secure ACS, page 7-8.

  If you install Security Manager or AUS after configuring Common Services to use ACS, you are told during installation that the application that you are installing requires new tasks to be registered with ACS. Select **Yes** if you have not already registered the application (on this or another server) with ACS. If you have already registered the application, if you select Yes, you lose any customized user roles configured in ACS for the application, so you should select **No**. All Security Manager and AUS servers that use the same ACS server share user roles.

Procedure

To install Security Manager Server, Common Services, AUS, or more than one of these applications using the main Security Manager installation program, follow these steps:

Step 1 Obtain or locate the installation program. You can do any of the following:

- Insert the Security Manager installation DVD into the server's DVD drive. If the installation application does not automatically start, run the **Setup.exe** file in the **csm**<*version*>**_win_server** folder.
- Log in to your Cisco.com account and go to the Security Manager home page at http://www.cisco.com/go/csmanager. Click **Download Software** and download the compressed installation file for Security Manager.
  - Using your choice of file compression utilities, such as WinZip or the Compressed (zipped) Folders Extraction Wizard, which is provided with Windows Server 2003, extract all the files in the compressed software installation file to a temporary directory. Use a directory that does not have an excessively long path name; for instance, C: is a better choice than C:\Documents and Settings\Administrator\Desktop. Start the installation program, **Setup.exe**, which normally unzips to the same directory as the compressed file.
  - If an error message states that the file contents cannot be unpacked, we recommend that you empty the Temp directory, scan for viruses, delete the C:\Program Files\Common Files\InstallShield directory, then reboot and retry.

Step 2 Follow the installation wizard instructions. During installation, you are asked for the following information:

- Backup location—If some version of Common Services, Security Manager, or AUS is already installed, the installation program allows you to perform a database backup during the installation. If you elect to perform the backup, select the location to use for the backup. However, it is typically better practice to perform a backup before starting the installation.
- Destination folder—The folder in which you want to install the application. Accept the default unless you have a compelling reason to install it elsewhere. If you specify a folder other than the default folder, make sure that it does not contain any files and that it has fewer than 256 characters in its pathname.
- Applications—The applications you want to install. You must select Common Services to install Security Manager or AUS unless Common Services is already installed.
- License information—Select one of the following:
  - **License File Location**—Enter the full pathname of the license file or click **Browse** to find it. You can specify the permanent license file if you have previously staged it on the server.
  - **Evaluation Only**—Enables the free 90-day evaluation period.

- Admin password—The password for the **admin** user account, at least 5 characters. For more information on this and the system identity and casuser accounts, see Understanding the Required Server User Accounts, page 4-1.
- System Identity user—The username and password for the account you want to use as the system identity user. When installing Cisco Security Management Suite applications on multiple servers, use the same system identity user account on all servers.
- Create casuser—Whether to create the casuser account on new installations. You must create this user account.

Step 3 After the installation is complete, restart the server if it does not restart automatically.

Note On an infrequent and random basis, Windows on VMware ESX stops responding (stalls) during the restart after installation. If this occurs, reboot the instance of VMware ESX using VMware GUI controls.

Installing Performance Monitor

You can install Performance Monitor 4.0.1 on the following:

- A standalone server, after you install CiscoWorks Common Services 3.3. This is the recommended configuration.
- The same server on which you installed Security Manager, AUS, RME, or all three, after you install CiscoWorks Common Services 3.3. However, if you use or enable Event Management, please read Effect of Enabling Event Management, page 1-7; you cannot enable Event Management on your Security Manager server if you want to use syslog on MCP or syslog on RME on that server.

Tip This configuration is recommended only for small networks.

The Performance Monitor license is a separate file from the Security Manager license file and includes the license for RME 4.3, too. You can install the license either before or after you install Performance Monitor. For instructions on how to obtain the license file, see Effects of Licensing on Installation and Obtaining a License, page 1-6.

Before You Begin

If you are installing on a system that already has Performance Monitor, Common Services, or other CiscoWorks applications, consider the following recommendations before installing Performance Monitor on the server:

- If you have a permanent license for Performance Monitor, copy it to the server. The license file must be on the server to select it during installation.
- Back up Common Services. The backup includes data for all installed applications that use Common Services. The Performance Monitor installation program does not perform a backup during the installation. For information on performing a backup, see Backing Up the Database for Remote Upgrades, page 4-12.
- If you install Common Services and Performance Monitor on a server, and then re-install Common Services later, you must also re-install Performance Monitor.
- If you want to use Cisco Secure Access Control Server (ACS) to provide AAA services for user access to Performance Monitor, wait until you install Performance Monitor before you configure Common Services to use ACS. For information on configuring ACS control, see Integrating Security Manager with Cisco Secure ACS, page 7-8.

  If you install Performance Monitor after configuring Common Services to use ACS, you are told during installation that the application that you are installing requires new tasks to be registered with ACS. Select **Yes** if you have not already registered Performance Monitor (on this or another server) with ACS. If you have already registered Performance Monitor and you select Yes, you lose any customized user roles configured in ACS for the application, so you should select **No**. All Performance Monitor servers that use the same ACS server share user roles.

  The following procedure contains additional steps to follow if you install Performance Monitor after configuring Common Services to use ACS.

Procedure

To install Performance Monitor, follow these steps:

Step 1 If the server does not already have CiscoWorks Common Services 3.3 installed, use the Security Manager installation DVD to install Common Services. For installation instructions, see Installing Security Manager Server, Common Services, and AUS, page 4-3. Performance Monitor cannot function without Common Services 3.3, and Common Services must be installed or upgraded to version 3.3 before you install Performance Monitor.

Step 2 Obtain or locate the installation program. You can do either of the following:

- Insert the Security Manager installation DVD into the server's DVD drive. The installation program is **mcp**<*version*>**\Setup.exe**.
- Log in to your Cisco.com account and go to the Security Manager home page at http://www.cisco.com/go/csmanager. Click **Download Software** and download the installation utility for Performance Monitor.

Step 3 To start the installation, double-click the installation program and then follow the prompts.

Step 4 When you are prompted to select the licensing information, select one of the following:

- **License File Location**—Enter the full pathname of the license file or click **Browse** to find it. You can specify the permanent license file if you have staged it on the server.
- **Evaluation Only**—Enables the free 90-day evaluation period.

Performance Monitor with ACS

If you have not already configured Common Services to use ACS, skip the remaining steps in this procedure. However, if you install Performance Monitor after configuring Common Services to use ACS, you must complete the following additional steps in this procedure:

Step 5 Log in to the ACS server.

Step 6 On the ACS Server, navigate to Shared Profile Components. Verify that Performance Monitor is shown in the list of applications.

Step 7 On the ACS Server, navigate to Group Setup. Select the group name that you used to configure Security Manager.

Step 8 Click **Edit Settings**.

Step 9 On the Group Setup page, look for Performance Monitor. Check the check box to include Performance Monitor for ACS integration.

Step 10 Also on the Group Setup page, go to the next section (Performance Monitor).

Step 11 Click the **Assign a Performance Monitor on a per Network Device Group Basis** radio button.

Step 12 In the Device Group drop-down menu, select **CSM_Servers**.

Step 13 In the Performance Monitor drop-down menu, select **System Administrator**.

Step 14 Click **Submit + Restart**.

Step 15 On the Security Manager server, restart the Daemon Manager.

Step 16 Allow several minutes for the Daemons to start, or verify that they have, and log in to the Performance Monitor server.

Installing Resource Manager Essentials (RME)

You can install RME 4.3 on the following:

- A standalone server, after you install CiscoWorks Common Services 3.3. This is the recommended configuration.
- The same server on which you installed Security Manager, AUS, MCP, or all three, after you install CiscoWorks Common Services 3.3. However, If you use or enable Event Management, please read Effect of Enabling Event Management, page 1-7; you cannot enable Event Management on your Security Manager server if you want to use syslog on RME or syslog on MCP on that server.

Tip This configuration is recommended only for small networks.

The RME license is a separate file from the Security Manager license file and includes the license for Performance Monitor too. You can install the license either before or after you install RME. For instructions on how to obtain the license file, see Effects of Licensing on Installation and Obtaining a License, page 1-6.

Before You Begin

If you are installing on a system that already has RME, Common Services, or other CiscoWorks applications, consider the following recommendations before installing RME on the server:

- If you have a permanent license for RME, copy it to the server. The license file must be on the server to select it during installation.
- Back up Common Services. The backup includes data for all installed applications that use Common Services. The RME installation program does not perform a backup during the installation. For information on performing a backup, see Backing Up the Database for Remote Upgrades, page 4-12.

- If you install Common Services and RME on a server, then re-install Common Services later, you must also re-install RME.
- If you want to use Cisco Secure Access Control Server (ACS) to provide AAA services for user access to RME, wait until you install RME before you configure Common Services to use ACS. For information on configuring ACS control, see Integrating Security Manager with Cisco Secure ACS, page 7-8.

  If you install RME after configuring Common Services to use ACS, you are told during installation that the application that you are installing requires new tasks to be registered with ACS. Select **Yes** if you have not already registered RME (on this or another server) with ACS. If you have already registered RME and you select Yes, you lose any customized user roles configured in ACS for the application, so you should select **No**. All RME servers that use the same ACS server share user roles.

Procedure

To install RME, follow these steps:

Step 1 If the server does not already have CiscoWorks Common Services 3.3 installed, use the Security Manager installation DVD to install Common Services. For installation instructions, see Installing Security Manager Server, Common Services, and AUS, page 4-3. RME cannot function without Common Services 3.3, and Common Services must be installed or upgraded to version 3.3 before you install RME.

Restart the system after installing Common Services before you install RME, or the Common Services installation might fail.

Step 2 Obtain or locate the installation program. You can do any of the following:

- Insert the Security Manager installation DVD into the server's DVD drive. The installation program is **rme**<*version*>**\Setup.exe**.
- Log in to your Cisco.com account and go to the Security Manager home page at http://www.cisco.com/go/csmanager. Click **Download Software** and download the installation utility for RME.

Step 3 If McAfee VirusScan is installed on your server, confirm that VirusScan and the VirusScan feature "On-Access Scan" are running.

If VirusScan is installed but turned off, or if its On-Access Scan feature has been turned off, problems might prevent you from installing RME. In addition, any RME installations that fail for this reason might prevent Security Manager from operating correctly if it is also installed on the server (in which case you must re-install Security Manager).

Step 4 To start the installation, double-click the installation program and then follow the prompts.

During installation, you are asked for the following information:

- License information—Select one of the following:
  - **License File Location**—Enter the full pathname of the license file or click **Browse** to find it. You can specify the permanent license file if you have previously staged it on the server.
  - **Evaluation Only**—Enables the free 90-day evaluation period.
- Setup type (Typical or Custom)—Select **Typical**. The only difference between typical and custom is that a custom installation allows you to specify the database password, which is randomly generated during a typical installation. If you specify a database password, use a minimum of five characters and a maximum of 15 characters, do not start the password with a number, and do not insert spaces between characters. This password is also used while restoring or troubleshooting the database.

- Restart CiscoWorks Daemons—You are asked whether you want to restart the CiscoWorks daemons. Answer **Yes**.

Upgrading Server Applications

Application upgrade refers to the process of installing a newer version of an application while preserving the data from the older version. There are three types of upgrade paths:

- Local—You simply install the newer version on the same server that is running the old version without first uninstalling the old version. Your existing data is maintained and available in the newly installed version. Keep the following in mind when doing local upgrades:
  - Before you use this method, ensure that all applications that you are upgrading are functioning correctly. Also, perform a backup of the database and ensure that it completes successfully before installing the upgraded applications.
  - You cannot use this method if you are also upgrading the operating system on the server, for example, going from Windows 2003 to Windows 2008. If you are doing a Security Manager upgrade while also doing an operating system upgrade, use the remote backup/restore upgrade method instead. If you are upgrading the operating system while maintaining the same Security Manager release, follow the procedure described in Migrating Security Manager to a New Computer or Operating System, page 4-15.
- Remote (backup/restore)—You install the newer version on a clean server (one that does not have the older application installed) and you then restore the database from a backup created from the older version. Use this procedure if you want to install on a new server or if you prefer to clean off your server before doing an installation (in which case you create the backup before uninstalling the application).

  Note Before creating a backup of a server that is running the Security Manager server application, you must ensure that all pending data is committed. See Ensuring Security Manager Pending Data is Submitted and Approved, page 4-11.

- Indirect—If you have an older version of the application that is not supported for local or remote upgrade, you must perform a two-step process. First, you upgrade to a version that is supported for local or remote upgrade, then you perform the local or remote upgrade. Download the interim version from Cisco.com.

  If your version is not listed for indirect upgrade in the following table, you need to do three or more interim upgrade steps if you want to preserve your older data. For example, to upgrade from Performance Monitor 3.0, you must first upgrade to 3.2, from which you can upgrade to 4.0, and then to 4.0.1. For another example, Security Manager 3.0.x, you would need to upgrade to 3.1.1, then to 4.0, before upgrading to 4.0.1.

Normally when you upgrade from an earlier version of an application, both the evaluation and permanent licenses are preserved. However, all 3.x and earlier customers need to procure a new license (or licenses) for Security Manager 4.0.1 irrespective of whether they have a valid license for any of the (older) Security Manager 3.x releases. With the exception of incremental licenses, existing Security Manager 3.x licenses are not valid for Security Manager 4.0.1.

Table 4-1 explains the software versions that are supported for each upgrade path.

Note Security Manager 3.x users cannot upgrade directly to Security Manager 4.0.1. They must first upgrade to 4.0 and then to 4.0.1.

Table 4-1 Application Upgrade Paths

Upgrade Path	Applications	Supported Older Versions	Upgrade Procedure
Local	Security Manager 4.0.1 Auto Update Server 4.0	4.0	Commit any pending data; see Ensuring Security Manager Pending Data is Submitted and Approved, page 4-11. Then, install the software; see Installing Security Manager Server, Common Services, and AUS, page 4-3. Finally, make any required post-upgrade changes; see Making Required Changes After Upgrade, page 4-14.
	Performance Monitor 4.0.1	4.0	(Recommended) Back up your database; see Backing Up the Database for Remote Upgrades, page 4-12. Then, install the software; see Installing Performance Monitor, page 4-5
	RME 4.3	4.2	(Recommended) Back up your database; see Backing Up the Database for Remote Upgrades, page 4-12. Then, install the software; see Installing Resource Manager Essentials (RME), page 4-7
Remote	Security Manager 4.0.1 Auto Update Server 4.0	4.0	1. Back up the database; see Backing Up the Database for Remote Upgrades, page 4-12. 2. Install the application, see: Installing Security Manager Server, Common Services, and AUS, page 4-3 Installing Performance Monitor, page 4-5 Installing Resource Manager Essentials (RME), page 4-7 3. If necessary, transfer the database backup to the server. 4. Recover the database; see Restoring the Server Database, page 4-13. 5. Finally, make any required post-upgrade changes; see Making Required Changes After Upgrade, page 4-14.
	Performance Monitor 4.0.1	4.0	
	RME 4.3	4.2	
Indirect	Security Manager 4.0.1	3.2.2, 3.3, and 3.3.1	First, upgrade to 4.0 and carefully follow the data migration instructions in the installation guide's chapter on upgrade for 4.0. Then, use the local or remote upgrade path.
	Performance Monitor 4.0.1	3.2.2, 3.3, and 3.3.1	First upgrade to version 4.0, then use the local or remote upgrade path. See the installation guide for 4.0
	RME 4.3	Not applicable.	Not applicable. The earliest supported RME release was 4.0.3, which is supported for local or remote upgrade.

Ensuring Security Manager Pending Data is Submitted and Approved

Before you can successfully upgrade Security Manager, you must ensure that the existing Security Manager database does not contain any pending data, which is data that has not been committed to the database. You cannot restore a database from an earlier version of Security Manager if it has pending data; you can only restore a database that has pending data on a system running the same version as the backup.

Each user must submit or discard changes. If you are using Workflow mode with an approver, these submissions must also be approved. You might want to also perform a deployment after all data is committed so that all device configurations are synchronized with the Security Manager database.

- In non-Workflow mode:
  - To commit changes, select **File > Submit**.
  - To discard uncommitted changes, select **File > Discard**.
  - If you need to commit or discard changes for another user, you can take over that user's session. To take over a session, select **Tools > Security Manager Administration > Take Over User Session**, select the session, then click **Take Over Session**.
- In Workflow mode:
  - To commit and approve changes, select **Tools > Activity Manager**. From the Activity Manager window, select an activity and click **Approve**. If you are using an activity approver, click **Submit** and have the approver approve the activity.
  - To discard uncommitted changes, select **Tools > Activity Manager**. From the Activity Manager window, select the activity, then click **Discard**. Only an activity in the Edit or Edit Open state can be discarded.

Restoring Changes that You Made to Property Files

All Security Manager installations have some property files that contain data that you usually change during use:

- *$NMSROOT*\MDC\athena\config\csm.properties
- *$NMSROOT*\MDC\athena\config\DCS.properties
- *$NMSROOT*\MDC\athena\config\taskmgr.prop

Tip *$NMSROOT* is the full pathname of the Common Services installation directory (the default is C:\Program Files\CSCOpx).

If you run an upgrade or install a service pack on your current installation, Security Manager does the following:

- Installs new files in association with the upgrade or service pack.
- Compares the new files with the files that you modified during use.
- Warns you if the new files are different from the files that you changed during use. If they are, Security Manager does the following:
  - Stores the files that you changed during use, naming them <*filename*>.*org*.
  - Stores diff files for your convenience, naming them <*filename*>.*diff*.

If you receive a warning about new files being different from the files that you modified during use, use the information in <*filename*>.*org* and <*filename*>.*diff* to restore the changes that you made to property files before upgrade or service pack installation.

Backing Up the Database for Remote Upgrades

CiscoWorks Common Services manages the database for all server applications, and it is the Common Services backup/restore utilities that are used for backing up and restoring the database. Thus, when you create a backup, you are creating a backup for all CiscoWorks applications installed on the server.

Tip The backup procedure backs up the database only. If you need to back up the event data store, use the data store copy steps described in Migrating Security Manager to a New Computer or Operating System, page 4-15.

Step 1 If you are backing up a server that is running Security Manager, you can get to the backup page using a shortcut in the Security Manager client: **Tools > Backup**. Also, ensure that pending data is committed (see Ensuring Security Manager Pending Data is Submitted and Approved, page 4-11).

For servers that are not running Security Manager, to get to the backup page:

a. Log in to the Cisco Security Management Server desktop on the server (see Logging In to Server Applications Using a Web Browser, page 5-10).

b. Click the **Server Administration** panel. CiscoWorks Common Services is opened on the **Server > Admin** tab.

(If you log in to the CiscoWorks home page, select **Common Services > Server > Admin**.)

c. From the Server tab, select **Admin > Backup**.

Step 2 Select Immediate for Frequency, complete the other fields as desired, and click **Apply** to back up your data.

Backing Up the Server Database By Using the CLI

The procedure in this section describes how to back up the server database by executing a script from the Windows command line on the server.

While backing up the database, both Common Services and Security Manager processes will be shut down and restarted. Because Security Manager can take several minutes to fully restart, users might be able to start their client before the restart is complete. If this happens, they might see the message “error loading page” in device policy windows.

A single backup script is used to back up all applications installed on a CiscoWorks server; you cannot back up individual applications.

Tip The backup command backs up the database only. If you need to back up the event data store, use the data store copy steps described in Migrating Security Manager to a New Computer or Operating System, page 4-15.

Step 1 Ensure that pending data is committed (see Ensuring Security Manager Pending Data is Submitted and Approved, page 4-11).

Step 2 Back up the database by entering the following command:

*$NMSROOT***bin\perl** *$NMSROOT***bin\backup.pl** *backup_directory* [*log_filename* [**email=***email_address* [*number_of_generations* [**compress**]]]]

where:

- *$NMSROOT*—The full pathname of the Common Services installation directory (the default is C:\Program Files\CSCOpx).
- *backup_directory*—The directory where you want to create the backup. For example, C:\Backups.
- *log_filename*—(Optional) The log file for messages generated during backup. Include the path if you want it created somewhere other than the current directory. For example, C:\BackupLogs. If you do not specify a name, the log is *$NMSROOT*\log\dbbackup.log.
- **email=***email_address*—(Optional) The email address where you want notifications sent. If you do not want to specify an email address, but you need to specify a subsequent parameter, enter **email** without the equal size or address. You must configure SMTP settings in CiscoWorks Common Services to enable notifications.
- *number_of_generations*—(Optional) The maximum number of backup generations to keep in the backup directory. When the maximum is reached, old backups are deleted. The default is 0, which does not limit the number of generations kept.
- **compress**—(Optional) Whether you want the backup file to be compressed. If you do not enter this keyword, the backup is not compressed if VMS_FILEBACKUP_COMPRESS=NO is specified in the backup.properties file. Otherwise, the backup is still compressed. We recommend compressing backups.

For example, the following command assumes you are in the directory containing the perl and backup.pl commands. It creates a compressed backup and log file in the backups directory and sends notifications to admin@domain.com. You must specify a backup generation to include the compress parameter; if you specify any parameter after the log file parameter, you must include values for all preceding parameters.

perl backup.pl C:\backups C:\backups\backup.log email=admin@domain.com 0 compress

Step 3 Examine the log file to verify that the database was backed up.

Restoring the Server Database

You can restore your database by running a script from the command line. You have to shut down and restart CiscoWorks while restoring data. This procedure describes how you can restore the backed up database on your server. A single backup and restore facility exists to back up and restore all applications installed on a CiscoWorks server; you cannot back up or restore individual applications.

If you install the applications on multiple servers, ensure that you recover the database backup that contains data appropriate for the installed applications.

Tips

- You can restore backups taken from previous releases of the application if the backup is from a version supported for direct local inline upgrade to this version of the application. For information on which versions are supported for upgrade, see Upgrading Server Applications, page 4-9.

- The restore command restores the database only. If you need to restore the event data store, use the data store copy steps described in Migrating Security Manager to a New Computer or Operating System, page 4-15.

Procedure

Step 1 Stop all processes by entering the following at the command line:

net stop crmdmgtd

Step 2 Restore the database by entering the following command:

*$NMSROOT***bin\perl** *$NMSROOT***bin\restorebackup.pl** [**-t** *temporary_directory*] [**-gen** *generationNumber*] **-d** *backup_directory* [**-h**]

where:

- *$NMSROOT*—The full pathname of the Common Services installation directory (the default is C:\Program Files\CSCOpx).
- **-t** *temporary_directory*—(Optional) This is the directory or folder used by the restore program to store its temporary files. By default this directory is *$NMSROOT*\tempBackupData.
- **-gen** *generationNumber*—(Optional) The backup generation number you want to recover. By default, it is the latest generation. If generations 1 through 5 exist, 5 will be the latest.
- **-d** *backup_directory*—The backup directory that contains the backup to restore.
- **-h**—(Optional) Provides help. When used with **-d** *BackupDirectory*, help shows the correct syntax along with available suites and generations.

For example, to restore the most recent version from the c:\var\backup directory, enter the following command:

C:\Progra~1\CSCOpx\bin\perl C:\Progra~1\CSCOpx\bin\restorebackup.pl -d C:\var\backup

Tip If you are restoring a database that contains RME data, you might be asked if you want to collect inventory data. Collecting this data can take a long time. You might want to respond No and then configure RME to schedule an inventory. In RME, select **Devices > Inventory**.

Step 3 Examine the log file, *NMSROOT***log\restorebackup.log**, to verify that the database was restored.

Step 4 Restart the system by entering:

net start crmdmgtd

Step 5 If you restore a database that was backed up prior to installing a Security Manager service pack, you must reapply the service pack after restoring the database.

Making Required Changes After Upgrade

Sometimes an application upgrade changes how particular types of information is handled in a way that requires that you make some manual changes. After upgrading to this version of the product, consider the following list of required changes and perform any that apply to your situation:

- If you upgrade from any version earlier than 3.3.1, you must rediscover the inventory on any ASA 5580 device that includes a 4-port GigabitEthernet Fiber interface card (hardware type: i82571EB 4F). Inventory rediscovery overcomes a bug from previous releases that prevented changing speed nonnegotiate settings on the device. To rediscover inventory, right-click the device in Device view in the Security Manager client and select **Discover Policies on Device**, then select **Live Device** discovery and only the **Inventory** check box in the Policies to Discover group. Rediscovery replaces the Interfaces policy on the device.
- If you upgrade from 3.3.1 or lower versions, and you managed Cisco ASR 1000 Series Aggregation Services Routers that used unsupported shared port adapters (SPA), you should rediscover policies on those devices so that Security Manager can discover the SPAs that were supported starting with version 4.0. Newly supported SPAs include all Ethernet (all speeds), Serial, ATM, and Packet over Sonet (POS) shared port adapters (SPA), but not services SPAs. Rediscovery is required if you configured ATM, PVC, or dialer related policies in the device CLI.

Migrating Security Manager to a New Computer or Operating System

You might need to move Security Manager to a new server. This move might be to a new physical computer, or you might want to perform a major upgrade to the operating system on the server (such as moving from Windows 2003 to Windows 2008).

When you are not changing the Security Manager version, but you are changing the physical hardware or the operating system, you need to go through a migration process. The migration process is essentially the same as the remote backup/restore upgrade process as described in Upgrading Server Applications, page 4-9; however, additional steps are required to migrate the data contained in the Event Manager data store. Use this procedure when you need to perform Security Manager server migration.

Note Minor service pack updates to an operating system are not considered upgrades when it comes to Security Manager server-migration requirements. Server migration is required when you are moving between different major versions of the operating system, for example, as when the official name of the operating system changes.

Before You Begin

This procedure assumes that you want the target server (the server to which you are moving Security Manager) to have the same database and event data store contents as the source computer. If you started using Security Manager on the target server, you cannot merge the database or event data store of the source and target systems: you must replace the target data with the source data. Any data that existed on the target system prior to the migration will become unusable after completing the migration. Do not attempt to copy the old target-system data into the newly-migrated folder.

Also note that the steps for copying and restoring the event data store are required only if you want to preserve this data. You can skip the steps if you want to start with a fresh empty event data store.

Step 1 Do the following on the source Security Manager server (the server from which you are migrating):

a. Determine the name of the event data store folder. Using the Security Manager client, select **Tools > Security Manager Administration**, and select **Event Management** from the table of contents. The folder is shown in the Event Data Store Location field; the default is *NMSROOT***MDC\eventing\database**, where NMSROOT is the installation directory (usually C:\Program Files\CSCOpx).

b. Stop all processes by entering the following at the command line:

net stop crmdmgtd

c. Make a copy of the *NMSROOT***MDC\eventing\config\collector.properties** file and the event data store folder. Place the copy on a disk where you can access it from the target computer.

d. Back up the Security Manager database using the command line method as described in Backing Up the Server Database By Using the CLI, page 4-12.

Step 2 Prepare the new target computer. For example:

- If you are simply upgrading the operating system, but not moving to new hardware, perform the operating system upgrade and ensure that the operating system is functioning correctly. Then, install Security Manager.
- If you are moving to a new computer, ensure that it is functioning correctly and install Security Manager.

Step 3 Do the following on the target Security Manager server:

a. Stop all processes by entering the following at the command line:

net stop crmdmgtd

b. Restore the database using the procedure described in Restoring the Server Database, page 4-13.

c. If you did not restart processes after completing the database restore, restart them now:

net start crmdmgtd

d. Use the Security Manager client to log into the new server, then select **Tools > Security Manager Administration**, and select **Event Management** from the table of contents.

e. Ensure that the event data store folder exists and that it is empty (delete files if necessary). The folder must have the same name and location as the event data store had on the source server.

f. Select the correct Event Data Store Location (if the default is not already the correct folder), and deselect the **Enable Event Management** check box to stop the Event Manager service. Click **Save** to save your changes. You are prompted to verify that you want to stop the service; click **Yes**, and wait until you are notified that the service has stopped.

g. Copy the event data store backed up from the source computer to the new location on the target server.

h. Copy the backed up *NMSROOT***MDC\eventing\config\collector.properties** file from the source computer to the target server, overwriting the file on the target server.

i. Using the Security Manager client, select **Tools > Security Manager Administration**, and select **Event Management** from the table of contents. Select the **Enable Event Management** check box and click **Save**. You are prompted to verify that you want to start the service; click **Yes**, and wait until you are notified that the service has started.

Updating Security Manager, Performance Monitor, and RME Licenses

Although you can specify permanent license files during installation, you can also add licenses after you install Security Manager, Performance Monitor, or RME. The other Cisco Security Management Suite applications do not require licenses.

The process for adding licenses is different for Security Manager compared to Performance Monitor and RME. The following procedure explains both processes. Keep in mind that the Performance Monitor/RME combined license is a separate file from the Security Manager license file.

For information about obtaining the licenses, see Effects of Licensing on Installation and Obtaining a License, page 1-6.

Before You Begin

You must copy the license file to the server before adding it to the application.

Procedure

To install licenses for Security Manager, Performance Monitor, or RME, follow these steps:

Step 1 To install Security Manager licenses:

a. Log in to the server using the Security Manager client application (see Logging In to Security Manager Using the Security Manager Client, page 5-10).

b. Select **Tools > Security Manager Administration** and select **Licensing** from the table of contents.

c. Click **CSM** if the tab is not active.

d. Click **Install a License** to open the Install a License dialog box. Use this dialog box to select the license file and click **OK**. Repeat the process to add additional licenses.

Step 2 To install Performance Monitor or RME licenses:

a. Log in to the Cisco Security Management Server desktop (see Logging In to Server Applications Using a Web Browser, page 5-10).

b. Click the **Server Administration** panel. CiscoWorks Common Services is opened on the **Server > Admin** tab.

(If you log in to the CiscoWorks home page, select **Common Services > Server > Admin**.)

c. Select **Licensing**. The License Information page displays the license name, license version, status of the license, and the expiration date of the license.

d. Click **Update** and enter the path to the new license file in the License field, or click **Browse** to locate the new file.

e. Click **OK**. The system verifies whether the license file is valid and updates the license. The updated licensing information appears in the License Information page.

Obtaining Service Packs and Point Patches

Caution Do not download or open any file that claims to be a service pack or point patch for Security Manager unless you obtain it from Cisco. Third-party service packs and point patches are not supported.

After you install Security Manager or other applications, you might install a service pack or point patch from Cisco Systems to fix bugs, support new device types, or otherwise enhance the application.

- To learn when Cisco has prepared a new service pack, and to download any service pack that matters to you, open Security Manager, then select **Help > Security Manager Online**. Alternatively, go to http://www.cisco.com/go/csmanager.
- If your organization submits a Cisco TAC service request, TAC will tell you if an unscheduled point patch exists that might solve the problem you have described. Cisco does not distribute Security Manager point patches in any other way.

Service packs and point patches provide server support for client software updates and detect version level mismatches between a client and its server.

Adding Applications to the Server's Home Page

When you install Cisco Security Management Suite applications on the same server, the home page on that server displays links to the applications. However, if you install the applications on multiple servers, you need to register the applications on other servers for them to appear on a given server's home page.

You need to do this only if you want the convenience of being able to connect to all related applications from a single home page; otherwise, you can use the applications by logging in directly to each server. For instructions on logging in to a server, which opens the home page, see Logging In to Server Applications Using a Web Browser, page 5-10.

Step 1 From the Cisco Security Manager Suite home page, click the **Server Administration** link. The Common Services Admin page appears.

Step 2 Select **Server > HomePage Admin**, and select **Application Registration** from the table of contents. The Application Registrations Status page appears.

Step 3 Click **Register**. The Choose Location for Registrations page appears.

Step 4 Select **Register From Templates**, then click **Next**.

Step 5 Select the application you want linked to the home page, for example, **Monitoring, Analysis and Response System** or **RME**, then click **Next**.

Step 6 Enter the server name, server display name, and port and protocol information for the device that is running the selected application, then click **Next**.

Step 7 Verify registration information, then click **Finish**. A launch point for the application now appears on the Cisco Security Manager Suite home page.

Uninstalling Server Applications

Use this procedure to uninstall server applications. Before uninstalling an application, consider performing a backup so that you can recover your data if you decide to re-install the application. For information on performing backups, see Backing Up the Database for Remote Upgrades, page 4-12.

Before You Begin

If any version of Windows Defender is installed, disable it before you uninstall a server application. Otherwise, the uninstallation application cannot run.

Procedure

To uninstall server applications, follow these steps:

Step 1 Select **Start > Programs > Cisco Security Manager > Uninstall Cisco Security Manager**. For servers where only Performance Monitor or RME is installed, you can also use **Start > Programs > Performance Monitor > Uninstall Performance Monitor** or **CiscoWorks > Uninstall CiscoWorks**.

Step 2 You are prompted with a list of installed applications. Select all applications that you want to uninstall. Do not select Common Services unless you intend to uninstall all Cisco Security Management Suite applications.

On Windows 2003 R2 Enterprise Server (Service Pack 2)—32 bit, the installation program asks you whether or not you want to uninstall Cisco Security Agent.

You cannot uninstall external Cisco Security Agent using this method. (External Cisco Security Agent is Cisco Security Agent that is not installed as part of the Cisco Security Manager installation.) If you want to uninstall Cisco Security Agent, select **Start > Programs > Cisco Security Agent > Uninstall Cisco Security Agent**. For more information, see Uninstalling Bundled Cisco Security Agent, page B-2.

Step 3 Click **Next** twice.

The uninstaller removes the applications that you selected.

Note If the uninstallation causes an error, see Server Problems During Uninstallation, page A-8, and the "Troubleshooting and FAQs" chapter in *Installing and Getting Started With CiscoWorks LAN Management Solution 3.1*: http://www.cisco.com/en/US/products/sw/cscowork/ps3996/prod_installation_guides_list.html.

Step 4 Although no reboot is required, we recommend that you reboot the server after an uninstallation so that Registry entries and running processes on the server are in a suitable state for a future re-installation.

Step 5 Only if you uninstall all Cisco Security Management Suite applications, including Common Services:

a. If *NMSROOT* still exists, delete it, move it, or rename it. *NMSROOT* is the path to the Security Manager installation directory. The default value of *NMSROOT* is **C:\Program Files\CSCOpx**. Other values, such as **E:\Program Files\CSCOpx**, are possible as well.

b. If the C:\CMFLOCK.TXT file exists, delete it.

c. Use a Registry editor to delete these Registry entries before you re-install the applications:

- `My Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Cisco\Resource Manager`
- `My Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Cisco\MDC`

Step 6 If you disabled Windows Defender before uninstalling the applications, re-enable it now.

Downgrading Server Applications

You cannot downgrade Security Manager applications to earlier releases and preserve any configurations that you created in this release of the product. If you decide that you do not want to use this release of Security Manager, you can uninstall it and reinstall the desired older version of the product. (This

assumes that you have the required licenses and installation media for the older version.) You can then restore the desired database backup that you saved from your previous installation of the downgraded version, as described in Restoring the Server Database, page 4-13.

If you downgrade Security Manager, you must also downgrade Auto Update Server, Performance Monitor, and RME to a version supported by the Security Manager version that you reinstall.

After you restore the old database, keep in mind that it might contain device properties and policies that are no longer synchronized with the current state of the managed devices. For example, you might have upgraded the operating system on the device to one that is not directly supported by the older version of Security Manager, or you might have configured, and deployed, policies that do not exist in the older version. To ensure that the database is synchronized with the devices, consider rediscovering device policies for all managed devices. Be aware that some major changes (such as a major operating system release upgrade) require that you remove the device from the inventory and add it again. In some cases, you might need to revert an operating system upgrade (for example, ASA Software release 8.3 requires special handling and cannot be supported in downward compatibility mode, therefore, the Security Manager version you use must support it directly). See the “Managing the Device Inventory” chapter in the User Guide for Cisco Security Manager for more information.

Tip If try to manage a device and operating system release combination that the older version of Security Manager cannot manage, you will see deployment errors.