CHAPTER 5

Installing and Upgrading Server Applications

This chapter explains how to install the Security Manager server software and other server applications, namely CiscoWorks Common Services and AUS.

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

The following five permissions are assigned and set, automatically, at the time of Security Manager installation:

- Access this computer from network - casusers
- Deny access to this computer from network - casuser
- Deny logon locally - casuser
- Log on as batch job - casuser, casusers
- Log on as a service – casuser

- *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 8, “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 perform 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 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. If you use Remote Desktop Connection, Cisco recommends using a Remote Desktop Protocol console session and not a non-console session.

Installing Security Manager Server, Common Services, and AUS

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

Note You cannot install the Cisco Security Manager bundle on a standalone Auto Update Server (AUS) installation. To install the Security Manager bundle, you must first uninstall AUS and then proceed to install the Security Manager bundle.

- CiscoWorks Common Services 4.2.2—This is the foundation software that is required by the server applications. Beginning with Security Manager 4.4, the CiscoWorks Common Services check box no longer appears on the component selection page; installation of Common Services is selected by default.
- Cisco Security Manager 4.14—This is the main server software for Security Manager.
- Auto Update Server 4.14—This is a web-based interface for upgrading device configuration files and software images on PIX firewalls and Adaptive Security Appliances (ASA) that use the auto update feature.
- Cisco Security Manager client 4.14—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 6, "Installing and Configuring the Client."

Tip Beginning with Security Manager 4.4, AUS and the Security Manager client are installed in parallel to improve installation time.

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 5-6.

Before You Begin

- Refer to the "Licensing" chapter of this installation guide
- 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 5-14. Ensure that the backup completes successfully, and that your existing applications are functioning normally before installing an upgrade.
- When installing a permanent license for Security Manager, you must stage the license file on a disk that is local to your Security Manager server. The license file must be on the server to select it during installation, because Security Manager does not see mapped drives if you use it to browse directories on your server. (Windows imposes this limitation, which serves to improve Security Manager performance and security.) Do not place the file in any folder in which you will install the product.

Note The path to the license file must not contain special characters such as the ampersand (&).

- Ensure that you go through the Readiness Checklist for Installation, page 4-3.
- Ensure that the server meets the requirements listed in Server Requirements and Recommendations, page 3-4.
- 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.
- 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 8-12.

  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.
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 operating systems supported by Security Manager 4.14, 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:\CSM" is a better choice than "C:\Cisco_Security_Manager\server\installation_directory." Start the installation program, **Setup.exe**, which normally unzips to the same directory as the compressed file.

Tip 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 (x86)\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.

Note The location that you select to use for the backup must be outside *NMSROOT*. The location *NMSROOT* is the path to the Security Manager installation directory. The default is **C:\Program Files (x86)\CSCOpx.** In particular, note that *NMSROOT*\backup must not be used for the backup.

- 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. Also, if you specify a folder other than the default folder, the path must not contain any special characters.
  The Windows Server 2012 R2 disables 8dot3 name generation on non-system drives, therefore user cannot select the Program Files (x86) folder on non-system drive paths. As a result, after setting the 8dot3 notation, the user must restart the server. Short names will not be created for existing folders after you enable 8dot3 naming on the specific drive; you must remove and recreate the folders, after a restart in order to force the short names to be created. If the existing folder was not empty, make sure that you select a new folder to proceed with installation.

Note Make sure that the installation directory path on a non-system drive, does not contain the special characters-"(" and ")". Installation will not proceed if these special characters are present.

- Applications—The applications you want to install—Security Manager, AUS, or both. CiscoWorks Common Services 4.2.2 is installed automatically when you install Security Manager or AUS.
- 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.

Note The path to the license file must not contain special characters such as the ampersand (&).

  - **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 5-1.
- 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.

Note If you have security policies on password complexity restrictions, this account creation may not succeed. In such cases, you need to manually create the casuser account (see further instructions for the casuser password in Table A-3, Causes and Workarounds for LiaisonServlet Error).

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

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, upgrading from Microsoft Windows Server 2008 R2 with SP1 Enterprise—64-bit to Microsoft Windows Server 2012 Standard—64-bit. If you are performing a Security Manager upgrade while also performing 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 5-18.
  - An error message will pop up if there is any database migration error; this will be at a point where installation can be taken forward without stopping.

Caution If you encounter a database migration error while upgrading from Cisco Security Manger 4.12 SP2, refer to the section Resolving database errors while upgrading from Cisco Security Manager 4.12 SP2, page 5-11

Note During local upgrade, the installer checks to see if Performance Monitor or Resource Manager Essentials is installed. If one or both of them are found, the installer exits with an error message stating that Performance Monitor or Resource Manager Essentials (or both) needs to be uninstalled.

- 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 Resolving database errors while upgrading from Cisco Security Manager 4.12 SP2, page 5-11.

- 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.

Note A special note applies to all indirect upgrades with event management enabled (Configuration Manager > Tools > Security Manager Administration... > Event Management > [Event Management group] > Enable Event Management. Under these conditions, a detailed view of an event (Launch > Event Viewer > Event Details > Details) will throw an error. The root cause of this error is restoring an old version of the event database followed by loading the event data. To work around this problem, identify all of your old partitions (the ones containing event data generated before your indirect upgrade) and move them to the secondary partition ("Extended Data Store Location" in the Security Manager GUI at Configuration Manager > Tools > Security Manager Administration... > Event Management).

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 Security Manager 3.0.x, you need to upgrade to 3.2.2, and then follow the indirect upgrade path to upgrade from 3.2.2 to 4.14.

Table 5-1 explains the software versions that are supported for each upgrade path.

The following upgrade paths are supported:

- 4.12 (including any service pack) > 4.14
- 4.13 (including any service pack) > 4.14

Table 5-1 Application Upgrade Paths

Upgrade Path	Applications	Supported Older Versions	Upgrade Procedure
Local	Security Manager 4.14 Auto Update Server 4.14	4.12 and 4.13	1. Commit any pending data; see: – Resolving database errors while upgrading from Cisco Security Manager 4.12 SP2, page 5-11. – Ensuring Security Manager Pending Data is Submitted and Approved, page 5-12 2. Then, install the software; see Installing Security Manager Server, Common Services, and AUS, page 5-3. 3. Finally, make any required post-upgrade changes; see Making Required Changes After Upgrade, page 5-17.

Table 5-1 Application Upgrade Paths (continued)

Upgrade Path	Applications	Supported Older Versions	Upgrade Procedure
Remote	Security Manager 4.14 Auto Update Server 4.14	4.12 and 4.13	1. Commit any pending data; see – Resolving database errors while upgrading from Cisco Security Manager 4.12 SP2, page 5-11. – Ensuring Security Manager Pending Data is Submitted and Approved, page 5-12 2. Back up the database; see Backing Up the Database for Remote Upgrades, page 5-14. 3. Install the application, see: Installing Security Manager Server, Common Services, and AUS, page 5-3 4. If necessary, transfer the database backup to the server. 5. Recover the database; see Restoring the Server Database, page 5-16. 6. Finally, make any required post-upgrade changes; see Making Required Changes After Upgrade, page 5-17.
Indirect	Security Manager 4.14	4.11, 4.10, 4.9, and 4.8	1. Commit any pending data; see Ensuring Security Manager Pending Data is Submitted and Approved, page 5-12. 2. Next, upgrade to 4.12, being careful to follow the data migration instructions in the installation guide's chapter in upgrade for 4.12. 3. Finally, upgrade to 4.14 and carefully follow the data migration instructions in this installation guide's chapter on upgrade for 4.14.
Indirect	Security Manager 4.14	4.7 and 4.6	1. Commit any pending data; see Ensuring Security Manager Pending Data is Submitted and Approved, page 5-12. 2. Next, upgrade to 4.8, being careful to follow the data migration instructions in the installation guide's chapter on upgrade for 4.8. 3. Next, upgrade to 4.10, being careful to follow the data migration instructions in the installation guide's chapter in upgrade for 4.10. 4. Next, upgrade to 4.12, being careful to follow the data migration instructions in the installation guide's chapter in upgrade for 4.12. 5. Finally, upgrade to 4.14 and carefully follow the data migration instructions in this installation guide's chapter on upgrade for 4.14.

Table 5-1 Application Upgrade Paths (continued)

Upgrade Path	Applications	Supported Older Versions	Upgrade Procedure
Indirect	Security Manager 4.14	4.5 and 4.4	1. Commit any pending data; see Ensuring Security Manager Pending Data is Submitted and Approved, page 5-12. 2. Next, upgrade to 4.6, being careful to follow the data migration instructions in the installation guide's chapter on upgrade for 4.6. 3. Next, upgrade to 4.8, being careful to follow the data migration instructions in the installation guide's chapter on upgrade for 4.8. 4. Next, upgrade to 4.10, being careful to follow the data migration instructions in the installation guide's chapter in upgrade for 4.10. 5. Next, upgrade to 4.12, being careful to follow the data migration instructions in the installation guide's chapter in upgrade for 4.12. 6. Finally, upgrade to 4.14 and carefully follow the data migration instructions in this installation guide's chapter on upgrade for 4.14.
Indirect	Security Manager 4.14	4.1, 4.1.1, 4.2 and 4.3	1. Commit any pending data; see Ensuring Security Manager Pending Data is Submitted and Approved, page 5-12. 2. Next, upgrade to 4.4, being careful to follow the data migration instructions in the installation guide's chapter on upgrade for 4.4. 3. Next, upgrade to 4.6, being careful to follow the data migration instructions in the installation guide's chapter on upgrade for 4.6. 4. Next, upgrade to 4.8, being careful to follow the data migration instructions in the installation guide's chapter on upgrade for 4.8. 5. Next, upgrade to 4.10, being careful to follow the data migration instructions in the installation guide's chapter in upgrade for 4.10. 6. Next, upgrade to 4.12, being careful to follow the data migration instructions in the installation guide's chapter in upgrade for 4.12. 7. Finally, upgrade to 4.14 and carefully follow the data migration instructions in this installation guide's chapter on upgrade for 4.14.

Table 5-1 Application Upgrade Paths (continued)

Upgrade Path	Applications	Supported Older Versions	Upgrade Procedure
Indirect	Security Manager 4.14	3.3.x	1. Commit any pending data; see Ensuring Security Manager Pending Data is Submitted and Approved, page 5-12. 2. Next, perform a remote upgrade to 4.3, being careful to follow the data migration instructions in the installation guide's chapter on upgrade for 4.3. 3. Next, upgrade to 4.5, being careful to follow the data migration instructions in the installation guide's chapter on upgrade for 4.5. 4. Next, upgrade to 4.7, being careful to follow the data migration instructions in the installation guide's chapter on upgrade for 4.7. 5. Next, upgrade to 4.9, being careful to follow the data migration instruction in the installation guide's chapter on upgrade for 4.9. 6. Next, upgrade to 4.11, being careful to follow the data migration instructions in the installation guide's chapter in upgrade for 4.11. 7. Next, upgrade to 4.12, being careful to follow the data migration instructions in the installation guide's chapter in upgrade for 4.12. 8. Finally, upgrade to 4.14 and carefully follow the data migration instructions in this installation guide's chapter on upgrade for 4.14.

Table 5-1 Application Upgrade Paths (continued)

Upgrade Path	Applications	Supported Older Versions	Upgrade Procedure
Indirect	Security Manager 4.14	3.2.x (3.2.2 only)	1. Commit any pending data; see Ensuring Security Manager Pending Data is Submitted and Approved, page 5-12. 2. Next, upgrade to 4.0, being careful to follow the data migration instructions in the installation guide's chapter on upgrade for 4.0. 3. Next, upgrade to 4.3, being careful to follow the data migration instructions in the installation guide's chapter on upgrade for 4.3. 4. Next, upgrade to 4.5, being careful to follow the data migration instructions in the installation guide's chapter on upgrade for 4.5. 5. Next, upgrade to 4.7, being careful to follow the data migration instructions in the installation guide's chapter on upgrade for 4.7. 6. Next, upgrade to 4.9, being careful to follow the data migration instructions in the installation guide's chapter on upgrade for 4.9. 7. Next, upgrade to 4.11 and carefully follow the data migration instructions in the installation guide's chapter on upgrade for 4.11. 8. Next, upgrade to 4.12, being careful to follow the data migration instructions in the installation guide's chapter in upgrade for 4.12. 9. Finally, upgrade to 4.14 and carefully follow the data migration instructions in this installation guide's chapter on upgrade for 4.14.

Resolving database errors while upgrading from Cisco Security Manager 4.12 SP2

While performing an inline (local) or remote upgrade from Cisco Security Manager 4.12 SP2, you may encounter a database migration error which impacts device deployment and configuration.

Note Inline upgrades are not supported for upgrades from Cisco Security Manager 4.12 SP2. Follow the remote upgrade procedure and refer to the steps below to resolve the database migration issues.

Perform the steps below to resolve the database migration issues:

Step 1 After installing Cisco Security Manager 4.14, navigate to ~CSCOpx\upgrade\data\412999999, open the **Admin_properties.sql** file in a text editor, such as Notepad.

Step 2 Locate the following content:

```
INSERT INTO ADMIN_PROPERTIES (PROPERTY,VALUE,DEFAULTVALUE) values
('workflow.deployjob.submittercanapprove','true','true')
```

Step 3 Replace this content with the following:

```
if not exists (select 1 from ADMIN_PROPERTIES where PROPERTY =
'workflow.deployjob.submittercanapprove') then
       INSERT INTO ADMIN_PROPERTIES (PROPERTY,VALUE,DEFAULTVALUE) values
('workflow.deployjob.submittercanapprove','true','true')
end if;
```

Step 4 Save the **Admin_properties.sql** file.

Step 5 Proceed to restore the Cisco Security Manager 4.12 SP2 database backup.

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 (x86)\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.

Editing the csm.properties File After a Remote Upgrade

After a remote upgrade, you must edit the **csm.properties** file to include newly added properties. Follow these steps:

Step 1 From *$NMSROOT*\MDC\athena\config\ subdirectory, open **csm.properties** in a text editor, such as Notepad.

(*$NMSROOT* is the full pathname of the Common Services installation directory [the default is C:\Program Files (x86)\CSCOpx])

Step 2 Add the following content to the end of the **csm.properties** file.

```
##
# Customize Activity Report Generation
##
# Report generation timeout in minutes
# Set to 10 minutes by default
#generate_activity_report_timeout=10
# Generate PDF Report
#generate_activity_pdf_report=true
# Generate HTML Report
#generate_activity_html_report=false
#
#CSCup28957::This will allow user to exclude the list of operation rows in all applicable policies from activity change report.
#excluded operations should be in comma separated and if it is empty or commented then it will include all operations.
#excluded operations::Add,Delete,Modify,Move,ReOrder,Assign,UnAssign. These names should not be modified.
#By default it is empty,if we need to exclude operation then add required excluded operation.
```

```
#ex: 1.ActChangeReport.excludedOperations=ReOrder,
2.ActChangeReport.excludedOperations=Add,ReOrder ,
3.ActChangeReport.excludedOperations=Add,Modify,Move,ReOrder
ActChangeReport.excludedOperations=
```

Note The above lines of code are commented by default. If you want to use the default values or modify the values of a particular property in the file, you must first uncomment the given line of code. For example, if you want Security Manager to generate Activity Reports in PDF format, you must change the given property as follows:

```
# Generate PDF Report
generate_activity_pdf_report=true
```

Step 3 Save, and then close, the edited file.

Step 4 Restart the **Cisco Security Manager Daemon Manager** service from **Start > Programs > Administrative Tools > Services.**

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.

Note Beginning with Security Manager 4.4, a new attribute, PURGE_DBBACKUP_LOG, has been added to the backup.properties file; it has a default value of 20, meaning that backups will be purged after 20 days. If this new attribute is set to NIL, then backups will not be purged. The dbbackup.log is created with a timestamp format of dbbackup_[YYYY-MM-DD_HH-mm-ss].log. At any point of time, a minimum of 5 dbbackup.log files will be maintained irrespective of purge configuration.

Note To back up the database, the Short Date format should be either M/d/YYYY or M/d/yy. To change the Short Date format to either M/d/YYYY or M/d/yy, select Start > Control Panel > Region and Language > Formats > Short Date, and then change the Short Date format to either M/d/YYYY or M/d/yy.

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 5-18.

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 Resolving database errors while upgrading from Cisco Security Manager 4.12 SP2, page 5-11).

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 6-12).

b. Click the **Server Administration** panel. Then select **Server > 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 5-18.

Step 1 Ensure that pending data is committed (see Resolving database errors while upgrading from Cisco Security Manager 4.12 SP2, page 5-11).

Step 2 At a command prompt, enter **net stop crmdmgtd** to stop all processes.

Step 3 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 (x86)\CSCOpx].
- *backup_directory*—The directory where you want to create the backup. For example, C:\Backups.

Note The location that you select to use for the backup must be outside *NMSROOT*. The location *NMSROOT* is the path to the Security Manager installation directory. The default is **C:\Program Files (x86)\CSCOpx.** In particular, note that *NMSROOT*\backup must not be used for the backup.

Note The backup directory should not contain any special characters.

- *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 command shown below assumes that you are in the directory containing the perl and backup.pl commands. (When you are in that directory, though, you must still specify the entire path of perl and backup.pl, fully qualified in the DOS 8.1 format with no spaces.)

The command shown below creates a compressed backup and log file in the backups directory and sends notifications to admin@domain.com.

When you use the backup.pl command, you must specify a backup generation if you want to include the compress parameter.

If you specify any parameter after the log file parameter, you must include values for all preceding parameters.

In this example, *$NMSROOT is* D:\CSM, not the default value of C:\Program Files (x86)\CSCOpx.

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

Step 4 Examine the log file to verify that the database was backed up.

Note If Security Manager restarts unexpectedly during the database backup process, the backup is interrupted and a backup lock file **backup.lock** is created in the *NMSROOT* directory. Delete the **backup.lock** file to proceed with backup.

Step 5 At a command prompt, enter **net start crmdmgtd** to restart all processes.

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 5-6.

- 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 5-18.

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** *help*] [**-m** *Email*]

where:

- *$NMSROOT*—The full pathname of the Common Services installation directory [the default is C:\Program Files (x86)\CSCOpx].
- **-t** *temporary_directory*—(Optional) This is the directory or folder used by the restore program to store its temporary files. By default this directory is *$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.
- **-m**—Use to send email on the restore status as Success or Failure.

For example, to restore the most recent version from the c:\var\backup directory, enter the following command (note that this is for a 64-bit OS):

C:\Progra~2\CSCOpx\bin\perl C:\Progra~2\CSCOpx\bin\restorebackup.pl -d C:\var\backup

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 are handled in Cisco Security Manager. You are therefore required to 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:

Note Additionally, refer to the Important Notes section of the release notes for this release for other considerations that might apply to your installation of Security Manager after an upgrade.

- 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 must 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

Note Cisco is only responsible for licensing of the pre-installed Operating System that accompanies the Cisco Unified Computing System (UCS) bundle (which has Cisco Security Manger pre-installed). Customers upgrading their Operating System while migrating to Cisco Security Manager 4.9 or later, must buy the appropriate Windows license.

Certain circumstances might require you to move Security Manager to a new server. This move might be to a new physical machine, or you might want to perform a major upgrade to the operating system on the server (such as moving from Microsoft Windows Server 2008 R2 with SP1 Enterprise—64-bit to Microsoft Windows Server 2012 Standard—64-bit, Microsoft Windows Server 2012 Datacenter—64-bit, Microsoft Windows Server 2016 Standard—64-bit, or Microsoft Windows Server 2016 Datacenter—64-bit).

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 5-6; 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.

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 (x86)\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 5-15.

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. 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.

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. 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

Although you can specify permanent license files during installation, you can also add licenses after you install Security Manager. AUS does not require a license.

Before You Begin

You must copy the license file to the server machine or to the client machine before adding it (the license) to the application. If you use the client machine, you must enable the client-side browser.

Note The path to the license file must not contain special characters such as the ampersand (&).

Tip You can also apply a license while logging into Security Manager: Security Manager will prompt with the message "Upgrade license" or "Continue Evaluation." By clicking "Upgrade License," you can apply the license.

Procedure

To install a license for Security Manager, follow these steps:

Step 1 Log in to the server using the Security Manager client application (see Logging In to Security Manager Using the Security Manager Client, page 6-10).

Step 2 Select **Tools > Security Manager Administration** and select **Licensing** from the table of contents.

Step 3 Click **CSM** if the tab is not active.

Step 4 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.

Note The path and file name are restricted to characters in the English alphabet. Japanese characters are not supported. When selecting files on a Windows Japanese OS system, the usual file separator character \ is supported, although you should be aware that it might appear as the Yen symbol (U+00A5).

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.

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 5-14.

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**.

By default, all applications will be uninstalled.

Step 2 The uninstaller removes all applications.

Note If the uninstallation causes an error, see Server Problems During Uninstallation, page 9-9, 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 3 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 4 Perform the following steps 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 (x86)\CSCOpx**. Other values, such as **E:\Program Files (x86)\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\Wow6432Node\Cisco\Resource Manager
- My Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Cisco\MDC

d. Delete any folders under *NMSROOT* that were not deleted during uninstallation.

Step 5 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 5-16.

If you downgrade Security Manager, you must also downgrade Auto Update Server 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 you try to manage a device and operating system release combination that the older version of Security Manager cannot manage, you will see deployment errors.