



CHAPTER 5

Upgrading and Downgrading Server Applications

This chapter describes how to upgrade and downgrade Security Manager applications. It contains these major sections:

- [Upgrading Server Applications, page 5-1](#)
- [Retrieving Certificates After Upgrading from 3.0.2 to 3.2 Using Perl Scripts, page 5-6](#)
- [Migrating AUS and Configuration Engines, page 5-8](#)
- [Migrating Catalyst 6500 and Cisco 7600 Chassis, page 5-9](#)
- [Migrating IPS Sensors, page 5-10](#)
- [Upgrading IPS Manager 3.0.2 Data, page 5-11](#)
- [Obtaining Service Packs and Point Patches, page 5-12](#)
- [Downgrading Server Applications, page 5-12](#)

Upgrading Server Applications

Security Manager supports two types of upgrades, namely, inline and backing up and restoring of data. Inline upgrade refers to running the installation for the version to which you want to upgrade without uninstalling the previous version of Security Manager from a server. Upgrade using backup and restore refers to backing up the database from the server running a previous version of Security Manager and restoring the backed up data on the server you want to upgrade after installing the later version of Security Manager. If you are performing an upgrade using the backup and restore method on the same server, you must uninstall the previous version after backing up the data and then perform restoration of the database after installing the new version.



Note

Security Manager 3.2 requires that you use Common Services 3.1. Therefore, if you upgrade from an earlier Security Manager version, the installed Common Services version is also upgraded.

You can upgrade to Security Manager 3.2 from any of the following previous versions: 3.0.2, 3.0.2 SP1, 3.1, 3.1.1, 3.1.1 SP1 and SP2

The following sections describe the procedure to upgrade to Security Manager 3.2 using inline and backup and restore methods:

- [Upgrading to Security Manager 3.2 Using Inline Method, page 5-2](#)
- [Upgrading to Security Manager 3.2 by Backing Up and Restoring the Database, page 5-4](#)

Upgrading to Security Manager 3.2 Using Inline Method

The following procedure describes how to use the inline method to upgrade to Security Manager 3.2 on a server where Security Manager 3.0.2, 3.1, or 3.1.1 is installed.

Step 1 Before you can successfully upgrade to Security Manager 3.2, you must make sure that the existing Security Manager database does not contain any pending data, meaning data that has not been committed to the database. If the existing Security Manager database contains pending data, you must commit or discard all uncommitted changes before upgrading:

- a. In non-Workflow mode:
 - To commit changes, select **File > Submit**.
 - To discard uncommitted changes, select **File > Discard**.



Note If there are multiple users with pending data, the changes for those users must also be committed or discarded. 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, and click **Take Over Session**.

- b. In Workflow mode:
 - To commit changes, select **Tools > Activity Manager**. From the Activity Manager window, select an activity, then click **Submit**.



Note If you have enabled the activity approval requirement, you must also approve all activities after submitting. To approve an activity, select **Tools > Activity Manager**. From the Activity Manager window, select an activity and click **Approve**.

- To discard uncommitted changes, select **Tools > Activity Manager**. From the Activity Manager window, select an activity, then click **Discard**. Only an activity in the Edit or Edit Open state can be discarded.

Step 2 To upgrade in place, simply run the installer for Security Manager 3.2. For step-by-step instructions, see [Installing Server Applications, page 4-1](#).

Perform one or all of the following, depending on the Security Manager version from which you upgraded and the types of devices that you are managing.

- If you have used Security Manager 3.0.2 or 3.0.2 SP1 to manage Catalyst 6500 Series switches or Cisco 7600 Series routers, see [Migrating Catalyst 6500 and Cisco 7600 Chassis, page 5-9](#), for important steps that we recommend you to complete after upgrade.
- If you have used Security Manager 3.0.2 or 3.0.2 SP1 to manage IPS sensors, see [Migrating IPS Sensors, page 5-10](#) to retrieve the inventory information for such sensors to the Security Manager database.

- If you have used an earlier version of Security Manager to manage devices that were configured to receive configuration updates from AUS and Configuration Engines, see [Migrating AUS and Configuration Engines, page 5-8](#) to import these servers into Security Manager after upgrade.

Step 3 After you upgrade Security Manager, overwrite the existing version of the Security Manager client on your client system by running the 3.2 version of the client installation software. For instructions, see [Chapter 6, “Installing or Uninstalling Security Manager Client.”](#)

If you selected the option to install the client software from the component selection screen of the server installation wizard, the 3.2 version of the client is already available on your system.

Known Problem

This section contains information about a problem known to exist in Cisco Security Manager 3.2.

Identifier: CSCso48972

Headline: Upgrade:3.0.2SP1 to 3.2 - Client Installer link on CSMS homepage fails

Symptom: HTTP “403 Forbidden” error when user tries to download Cisco Security Manager Client Installer from Cisco Security Management Suite (CSMS) Web page.

Conditions: Upon Cisco Security Manager 3.0.2 SP1 upgrade to Cisco Security Manager 3.2

Workaround:

Please use one of the following three workarounds.

Workaround No. 1—Server-side workaround (a permanent fix for all remote Cisco Security Manager clients—recommended)

-
- Step 1** Login to CiscoWorks using link “https://SERVER-IP” as “admin”
 - Step 2** Browse to CSMSHomePage > Server > Security, and then click on “Browser-Server Security Mode Setup” in the TOC
 - Step 3** Click **Apply**.
 - Step 4** Restart the Cisco Security Manager Daemon Manager or restart the server
 - Step 5** Login to CiscoWorks, which is running in http mode now, using link “http://SERVER-IP:1741” as “admin”
 - Step 6** Browse to CSMS HomePage > Server > Security, and then click on “Browser-Server Security Mode Setup” in the TOC
 - Step 7** Click **Apply**.
 - Step 8** Restart the Cisco Security Manager Daemon Manager or restart the server
 - Step 9** Log in to CiscoWorks, which is running in https mode now, using link “https://SERVER-IP” as “admin”
 - Step 10** Click on CSM Client Installer on the CSMS home page, and then proceed with Save.

Workaround No. 2—Client-Side Workaround with DVD available (a per-client fix)

-
- Step 1** Using the Cisco Security Manager 3.2 DVD, choose the Install option.

Step 2 Select the option to install the Cisco Security Manager 3.2 Client and proceed

Workaround No. 3—Client-Side Workaround without DVD available (a per-client fix)

Step 1 In the browser with the “403 Forbidden” error, change the address bar link as follows: Replace the protocol “http” with “https” and remove the “:1741” port number after which the link would look similar to “https://SERVER-IP/desktop/CSMClientSetup.exe”

Step 2 Press Enter, after which a popup appears prompting to save or run the installer

Upgrading to Security Manager 3.2 by Backing Up and Restoring the Database

The following procedure describes how to back up the database on a server where Security Manager 3.0.2, 3.1, or 3.1.1 (or any of its related applications) is installed and restore it after installing Security Manager 3.2 on the server.

Step 1 Before you can successfully upgrade to Security Manager 3.2, you must make sure that the existing Security Manager database does not contain any pending data, meaning data that has not been committed to the database. If the existing Security Manager database contains pending data, you must commit or discard all uncommitted changes before upgrading:

- a. In non-Workflow mode:
 - To commit changes, select **File > Submit**.
 - To discard uncommitted changes, select **File > Discard**.



Note If there are multiple users with pending data, the changes for those users must also be committed or discarded. 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, and click **Take Over Session**.

- b. In Workflow mode:
 - To commit changes, select **Tools > Activity Manager**. From the Activity Manager window, select an activity, then click **Submit**.



Note If you have enabled the activity approval requirement, you must also approve all activities after submitting. To approve an activity, select **Tools > Activity Manager**. From the Activity Manager window, select an activity and click **Approve**.

- To discard uncommitted changes, select **Tools > Activity Manager**. From the Activity Manager window, select an activity, then click **Discard**. Only an activity in the Edit or Edit Open state can be discarded.

Step 2 Create a backup of the database for Security Manager 3.0.2, 3.1, or 3.1.1 by selecting **Tools > Backup**.



Note If network management applications, such as Tivoli, were used to install Cygwin on the same system where a Security Manager server was installed, backup of the Security Manager database fails.

You cannot perform a backup of the database on Security Manager servers placed across sites or locations by using a mapped network drive.

Step 3 Uninstall Security Manager 3.0.2, 3.1, or 3.1.1. See [Uninstalling and Reinstalling Server Applications, page 4-6](#).

If you want to restore the backed up database on a different server than the one running Security Manager 3.0.2, 3.1, or 3.1.1, skip this step and proceed to [Step 4](#).

A version of Cisco Security Agent is installed on your Security Manager server. When you explicitly uninstall Security Manager, the Cisco Security Agent software remains on your server.

- If Cisco Security Agent is the fully configurable, commercial version, it will never be overwritten by a Security Manager installation or uninstallation.
- If Cisco Security Agent is the customized and standalone version, with predefined policies that you cannot change, it will be overwritten only when you install a new Security Manager version.
- You can uninstall Cisco Security Agent manually, but we recommend that you do not. See [Uninstalling the Standalone Agent, page B-3](#).

Step 4 Install Security Manager 3.2. See [Installing Server Applications, page 4-1](#).

Step 5 Restore the database from the backup corresponding to the version to which you want to upgrade. See [Restoring the Security Manager Database, page 5-5](#).

Perform one or all of the following, depending on the Security Manager version from which you upgraded and the types of devices that you are managing.

- If you have used Security Manager 3.0.2 or 3.0.2 SP1 to manage Catalyst 6500 Series switches or Cisco 7600 Series routers, see [Migrating Catalyst 6500 and Cisco 7600 Chassis, page 5-9](#), for important steps that we recommend you to complete after upgrade.
- If you have used Security Manager 3.0.2 or 3.0.2 SP1 to manage IPS sensors, see [Migrating IPS Sensors, page 5-10](#) to retrieve the inventory information for such sensors to the Security Manager database.
- If you have used an earlier version of Security Manager to manage devices that were configured to receive configuration updates from AUS and Configuration Engines, see [Migrating AUS and Configuration Engines, page 5-8](#) to import these servers into Security Manager after upgrade.

Restoring the Security Manager 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 Security Manager database on your server. make sure you have the correct permissions, and do the following:

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

```
net stop crmdmgt
```

Step 2 Restore the database by entering:

```
NMSROOT\bin\perl NMSROOT\bin\restorebackup.pl [-t temporary directory] [-gen generationNumber] [-d backup directory] [-h]
```

where:

- *NMSROOT*—(Required) Environment variable containing full pathname of the Common Services installation directory (by default, C:\Program Files\CSCOpX, where C: is the System Drive).
- *-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*. You can customize this by specifying your own temporary directory to avoid overloading *NMSROOT*.
- *-d BKP*—(Required) The backup directory to use.
- *-h*—(Optional) Provides help. When used with *-d BackupDirectory*, shows correct syntax along with available suites and generations.

To restore the most recent version, enter the following command:

```
NMSROOT\bin\perl NMSROOT\bin\restorebackup.pl -d backup directory
```

For example, *-d drive:\var\backup*

Step 3 Examine the log file in the following location to verify that the database was restored by entering:

```
NMSROOT\log\restorebackup.log
```

Step 4 Restart the system by entering:

```
net start crmdmgt
```

Retrieving Certificates After Upgrading from 3.0.2 to 3.2 Using Perl Scripts

When you upgrade a Security Manager 3.0.2 server to 3.2 by backing up and restoring the database, the certificate thumbprints of the devices added to the Security Manager inventory are preserved in the 3.2 certificate data store if certificate authentication was enabled in 3.0.2. However, if you did not enable certificate authentication in the 3.0.2 server, certificate validation for devices using SSL is disabled in 3.2 and device certificate thumbprints are not saved in the 3.2 certificate data store.

If you disabled certificate authentication for devices in 3.0.2 and want to enable certificate authentication for those devices after upgrading to 3.2, you can run perl scripts from the Security Manager server CLI to retrieve device certificates to the Security Manager certificate data store. You can either choose to retrieve certificate thumbprints and add them to Security Manager in a single step, or perform this operation using two separate scripts. The following two scripts enable you to add certificates to Security Manager quickly in bulk without having to manually retrieve them for each device.

- **getCerts.pl**—Exports device credentials to a .csv file from DCR and saves it at the specified location on the Security Manager server. You can use this script with the *[-a]* argument to add the exported credentials to the Security Manager certificate store, or add the certificates to Security Manager as a separate step by running the *loadCerts.pl* script.



Note Use the [-a] argument only if you trust the validity of the certificates retrieved from the devices.

- **loadCerts.pl**—Loads certificates to Security Manager from the CSV file generated using the getCerts.pl script.

After running these scripts to load certificates to the Security Manager certificate store, you can enable certificate authentication for the devices for which it is disabled from the Device Communication settings window.

To retrieve device certificates from live devices and add them to the Security Manager database after you upgrade to 3.2, follow these steps.

Before You Begin

- You must be logged in to Security Manager as an administrator, to run this script.
- To export device credentials using DCR, from the CiscoWorks home page, select **Common Services > Device and Credentials > Device Management**. You must select CSV as your output file format while exporting credential details. For more information, see the *User Guide for CiscoWorks Common Services 3.1*.
- Before you add the device certificate to Security Manager, check whether the certificate is authentic by verifying its attributes such as the validity period, end-host identity information, encryption keys that will be used for secure communications, and the signature of the issuing Certificate Authority. If you run the getCerts.pl script with the [-a] argument, you might want to verify the validity of the certificates before running the script because the certificates are automatically added to Security Manager at the end of running of the script.

-
- Step 1** Open the Windows command prompt on the Security Manager server.
- Step 2** Navigate to the directory `NMSROOT\CSCOPx\bin`, where `NMSROOT` is the Security Manager installation directory. For example, enter `cd C:\Progra~1\CSCOPx\bin` if `C:\Progra~1\CSCOPx\` is the directory where you installed Security Manager.
- Step 3** Enter `getCerts.pl [-h] [-v] [-a] <input_csv_file> <output_cert_file>`
where:
- [-h]—(Optional) Displays the help associated with this utility, along with usage guidelines.
 - [-v]—(Optional) Specifies verbose mode.
 - [-a]—(Optional) Enables Security Manager to automatically obtain device certificates from live devices and load the thumbprints into the Security Manager certificate data store.
 - <input_csv_file>—(Required) Specifies the name of the file to which a list of devices is exported from DCR in CSV format.
 - <output_cert_file>—(Required) Specifies the location and name of the file in which device certificate details are saved.

If you run the getCerts.pl script without specifying the [-a] argument, you can view and modify the output file to remove certificate details for any device.

To load device certificates to Security Manager from the file to which they were exported from DCR using the getCerts.pl script, follow these steps.

Before You Begin

- If you ran the `getCerts.pl` script with the optional `[-a]` argument, the following procedure is not required because the certificates would have been already added to the certificate data store.
- If the Security Manager server is running when you execute the following script, the script tries to refresh the certificate cache.
- You must be logged in to Security Manager as an administrator, to run this script.

-
- Step 1** Open the Windows command prompt on the Security Manager server.
- Step 2** Navigate to the directory `NMSROOT\CSCOPx\bin`, where `NMSROOT` is the Security Manager installation directory. For example, enter `cd C:\Program~1\CSCOPx\bin` if `C:\Program~1\CSCOPx\` is the directory where you installed Security Manager.
- Step 3** Enter `loadCerts.pl [-h] [-v] [-a] <input_file>`

where:

- `[-h]`—(Optional) Displays the help associated with this utility, along with usage guidelines.
- `[-v]`—(Optional) Specifies verbose mode.
- `[-a]`—(Optional) Enables Security Manager to automatically obtain device certificates from DCR and load the thumbprints into the certificate data store.
- `<input_file>`—(Required) Specifies the name of the file generated by the `getCerts.pl` script and that contains device certificates. You must specify the same filename you entered in the `<output_cert_file>` argument while running the `getCerts.pl` script.

If a device cannot be reached from Security Manager, the certificate for that device is not retrieved when you run the `getCerts.pl` script. If you ran the script in verbose mode, the action performed by the script when connectivity to a device fails is displayed.

Migrating AUS and Configuration Engines

When you upgrade from a previous version of Security Manager to 3.2, the Auto Update Servers (AUS) and Configuration Engines that are configured in the earlier versions of Security Manager are not available in the 3.2 database. Although devices managed by AUS and CNS are migrated after the upgrade to 3.2, AUS and Configuration Engines are not migrated. As a result, the association of these devices with the AUS and Configuration Engines that manage them is removed. Devices managed by AUS and CNS are displayed with a red X icon partially covering the device icon in the device selection tree. You can either manually create and assign AUS and Configuration Engines to these devices or you can also add these servers by importing them from an inventory file exported from CiscoWorks Common Services Device Credential Repository (DCR).

The following procedure describes how you can create and assign AUS and Configuration Engines to devices managed by AUS and CNS after upgrading from a previous version of Security Manager.

**Note**

If you import the servers into Security Manager from an export file, you bypass the procedure described in this section.

-
- Step 1** Install the new Security Manager Client software version on a client system (see [Installing Security Manager Client, page 6-8](#)), then use that client system to log in to your upgraded Security Manager server.
- Step 2** Click the **Device View** button on the toolbar. The Devices page appears.
- In the device selection tree, a red X partially covers each icon that represents your security appliances and routers to which assignment of AUS and Configuration Engines has been removed after the upgrade.
- Step 3** Click any red X icon in the device selection tree. A warning message is displayed stating that AUS and Configuration Engine information was not migrated after the upgrade process. You are prompted to manually reconfigure these servers or use the Add Device from File option in the New Device wizard to import these servers from DCR. Click **Yes** to add these servers manually. The Device Server Assignment dialog box is displayed.
- Alternatively, right-click any red X icon in the device selection tree, then select the **Update Server Info** option to display the Device Server Assignment dialog box.
- Step 4** From the Available Device pane, select a device, or devices from different device groups, or select an entire group, then click >>. The individual device or devices in the selected device group move to the Selected Devices pane.
- Step 5** To add a new AUS or Configuration Engine server, select **Add Server** from the Server drop-down list to open the Server Properties dialog box.
- Step 6** After you specify the properties of an Auto Update Server or Configuration Engine, click **OK** to save the settings and close the Server Properties dialog box.
- Step 7** Click **OK** to save the settings in the Device Server Assignment dialog box. The devices in the Selected Devices pane are assigned to the AUS or Configuration Engine that you added.
-

Migrating Catalyst 6500 and Cisco 7600 Chassis

Security Manager 3.1 and later differ significantly from earlier releases in its features for managing Catalyst 6500 Series switches and Cisco 7600 Series routers, as well as their associated services modules (blades) and security contexts. Earlier Security Manager versions in the 3.0.x train used features from an embedded variant of CiscoView Device Manager, which versions 3.1 and later does not include. This version offers greater integration with, and consistency with, other Security Manager features.

The installation utility for Security Manager automatically detects if an older Security Manager version is present on your server. In most cases, information from the older Security Manager database is added automatically to the new database as part of the process of upgrading to the newer Security Manager version. However, the new methods for managing 6500 Series and 7600 Series devices are different enough from the old methods that you must do more than simply install the newer Security Manager version, in order to manage these devices in your network.

Step 1 Upgrade from the older Security Manager version to the newer version. See [Upgrading Server Applications, page 5-1](#).

Catalyst 6500 Series switches, Cisco 7600 Series routers, their services modules, and their security contexts are migrated automatically, along with all associated VPN policies and firewall policies. However, old inventory information from earlier Security Manager versions is discarded—including, for example, the records of described interfaces and configured VLANs.

When the installation utility reaches its “Important Instructions” page, it specifies a location on your server from which to access a migration report file. In most cases, the location will be `NMSROOT\MDC\log\readme.txt`, where `NMSROOT` is the path to the Security Manager installation directory. The default is `C:\Program Files\CSCOpX`.

Step 2 Open and print the migration report; it contains important information that you should read.

Step 3 Install the new Security Manager Client software version on a client system (see [Installing Security Manager Client, page 6-8](#)), then use that client system to log in to your upgraded Security Manager server.

Step 4 To use Device view, click the **Device View** button on the main toolbar.

You must use Device view, *not* Policy view.

In the device selection tree, a red X partially covers each of the icons that represent your 6500 Series and 7600 Series chassis, as well as the services modules and security contexts associated with those chassis, as a visual cue to indicate that inventory information is not yet available for them.



-
- Note**
- Until you complete this procedure, do not deploy any chassis, services module, or security context that uses a red X icon. If you try, the deployment will fail.
 - Other device lists in the Security Manager GUI (such as the lists for deployment and policy assignment) do not include *any* icons for these chassis, services modules, or security contexts.
-

Step 5 Click any red X icon in the device selection tree.

Security Manager contacts the live device and automatically retrieves its inventory information. The red X is cleared from the icon. The chassis, services module, or security context is now available to you for deployments from Security Manager.

Migrating IPS Sensors

Security Manager 3.1 and later differ significantly from earlier releases in the features for managing:

- Cisco Intrusion Prevention System (IPS) sensors:
 - Appliances
 - Switch modules
 - Network modules
 - Security Service modules (SSMs)

- Cisco IOS IPS devices:
 - Cisco IOS routers with IPS-enabled images
 - Cisco Integrated Services Routers (ISRs)

Earlier Security Manager versions used features from a helper application called IPS Manager, which this version does not provide. Instead, this Security Manager version has fully integrated IPS management features.

The installation utility for Security Manager automatically detects if an older Security Manager version is present on your server. In most cases, information from the older Security Manager database is added automatically to the new database as part of the process of upgrading to the newer Security Manager version. However, the new methods for managing Cisco IPS sensors and Cisco IOS IPS devices are different enough from the old methods that migration of IPS sensors is not supported when upgrading from a version earlier than 3.1 to 3.1 or later.

Upgrading IPS Manager 3.0.2 Data

To transfer IPS Manager 3.0.2 data to Security Manager 3.2:

-
- Step 1** Before you upgrade to Security Manager 3.2, log in to your system running IPS Manager 3.0.2.
 - Step 2** Navigate to the Common Services panel from the CiscoWorks or Cisco Security Management Suite home page.
 - Step 3** Export your IPS devices from the Device Credential Repository (DCR). For detailed instructions on how to export devices from DCR, see the *User Guide for CiscoWorks Common Services 3.1* at the following URL:
http://www.cisco.com/en/US/docs/net_mgmt/cisoworks_common_services_software/3.1/user/guide/dcr.html#wp1378454.
 - Step 4** Upgrade your server running IPS Manager 3.0.2 to Security Manager 3.2. See [Upgrading Server Applications, page 5-1](#) for more information.
 - Step 5** After the upgrade is complete, add your IPS devices to Security Manager 3.2 from the file you exported from DCR by using the “Add Device From File” option in the New Device wizard.
 - a. Copy the CSV file from Security Manager 3.0.2 to the Security Manager 3.2 server file directory, e.g., C:\temp.
 - b. Open the Security Manager client and from the Security Manager client, click on File > New Device...
 - c. On step 1 in the panel, choose the last radio button: "Add Device From File"; then click Next.
 - d. On Step 2, click on the "Browse" button on the top of the panel to open a Server side file browser.
 - e. On the file chooser, select the location of the CSV file that just copied over to the server, e.g. C:\temp, and then pick the CSV file, make sure the "Files of type" is "Device Credentials Repository (*.csv)".
 - f. Click OK to dispose of the file chooser.
 - g. The device(s) should be imported and discoverable in Security Manager 3.2.
-

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

- To learn when Cisco has prepared a new, regularly scheduled service pack, and to download any service pack that matters to you, open Security Manager, then select **Help > Security Manager Online**. Alternatively, point your browser 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.

Downgrading Server Applications

Security Manager supports downgrading from release 3.2 to release 3.0.2, 3.1, or 3.1.1 (including downgrades to IPS Manager and AUS), but only when you meet all of these conditions:

- You upgraded previously from the relevant release to release 3.2.
- You kept a copy of the backup that Security Manager created when you upgraded.
- You have the installation DVDs for both the old version and the new version.

To downgrade:

-
- Step 1** Uninstall Security Manager 3.2 and AUS 3.2. See [Uninstalling and Reinstalling Server Applications, page 4-6](#).
 - Step 2** Install Security Manager 3.0.2, 3.1, or 3.1.1 and (optionally) AUS 3.0.2 or 3.1. See [Installation Guide for Cisco Security Manager 3.1 or 3.0.2](#) on Cisco.com.
 - Step 3** (Optional) If you have an installation DVD for Security Manager 3.1 but not for 3.1.1, obtain the upgrade utility from <http://www.cisco.com/go/csmanager>, then upgrade from 3.1 to 3.1.1.
 - Step 4** Restore your database from the backup corresponding to the version to which you want to downgrade. See [Restoring the Security Manager Database, page 5-5](#).

**Note**

Your downgraded copy of Security Manager 3.0.x or 3.1.x includes only the information that you saved *before* you upgraded to release 3.2.

You must ensure that applications that reside with Security Manager on the same server, such as Common Services and RME, are running a version that is compatible with the version to which Security Manager is downgraded.

If any of the devices restored from the backed-up database are running a software version that is not supported by the downgraded version of Security Manager, you must revert them to a version supported by Security Manager. Otherwise, such devices are treated as unmanaged devices.
