



## 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](#)
- [Migrating AUS and Configuration Engines, page 5-5](#)
- [Obtaining Service Packs and Point Patches, page 5-6](#)
- [Downgrading Server Applications, page 5-6](#)

## Upgrading Server Applications

CSM 3.2.1 will support upgrades from older releases (major, minor, or maintenance release). You can upgrade to CSM 3.2.1 from CSM 3.1, 3.1.1 and 3.2. You can upgrade Security Manager using any one of the following methods:

- **Inline method:** 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. Refer the section [Upgrading to Security Manager 3.2.1 Using Inline Method, page 5-1](#) for more information.
- **Backing up and restoring of data method:** 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. Refer the section [Upgrading to Security Manager 3.2.1 by Backing Up and Restoring the Database, page 5-3](#) for more information.



### Note

---

Security Manager 3.2.1 requires that you use Common Services 3.1.1. Therefore, if you upgrade from an earlier Security Manager version, the installed Common Services version is also upgraded.

---

## Upgrading to Security Manager 3.2.1 Using Inline Method

CSM 3.2.1 upgrade will not support pending data. You will have to approve or discard pending activities before upgrading. The following procedure describes how to use the inline method to upgrade to Security Manager 3.2.1 on a server where Security Manager 3.1, 3.1.1 and 3.2 is installed.

---

**Step 1** Before you can successfully upgrade to Security Manager 3.2.1, you must ensure that the existing Security Manager database does not contain any pending data, meaning data that has not been committed to the database.

**Step 2** 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 3** To upgrade in place, simply run the installer for Security Manager 3.2.1. For step-by-step instructions, see [Installing Server Applications, page 4-1](#).

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 5-5](#) to import these servers into Security Manager after upgrade.

**Step 4** After you upgrade Security Manager, overwrite the existing version of the Security Manager client on your client system by running the 3.2.1 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 3.2.1 version of the client is already available on your system.

---

## Checking for Pending Data during Inline Upgrade

When you upgrade to CSM 3.2.1 using the Inline upgrade method, CSM 3.2.1 will check for pending data first. If it finds pending data in the database tables, installer will pop up an error message and abort the installation.

A connection is established to the CSM database and the database tables are checked to ensure that there is no pending data. Since CSM 3.2, every database connection needs to be authorized. Therefore, the database connection used to check pending data has to be authorized. The authorization can be done through API provided by Common Services 3.1.1. The following Common Services 3.1.1 API is used for authorization:

```
perlDbEncrypt::perlDbSystemCall(\@dbStringSQL)
(\@dbStringSQL: an array of strings that store SQL parameters.)
```

## Upgrading to Security Manager 3.2.1 by Backing Up and Restoring the Database

The following procedure describes how to back up the database on a server where Security Manager 3.1, 3.1.1 and 3.2 (or any of its related applications) is installed and restore it after installing Security Manager 3.2.1 on the server.

**Step 1** Before you can successfully upgrade to Security Manager 3.2.1, 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 3.1, 3.1.1 and 3.2 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 3.1, 3.1.1 and 3.2. See [Uninstalling Server Applications, page 4-6](#).
- If you want to restore the backed up database on a different server than the one running Security Manager 3.1, 3.1.1 and 3.2, 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 3.2.1. 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 Data, page 5-4](#).
- 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 5-5](#) to import these servers into Security Manager after upgrade.

## Restoring the Security Manager Data

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. Ensure you have the required permissions to perform the activity:

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

```
net stop crmdmgt
```

- Step 2** Restore the database by entering:

```
$NMSROOT\CSCOpX\bin\perl $NMSROOT\CSCOpX \bin\backup.pl <BackupDirectory> [LogFile]
[Num_Generations]
```

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*.

- **-a BKP**—(Required) The backup directory to use.
- **-h**—(Optional) Provides help. When used with **-a BackupDirectory**, shows correct syntax along with available suites and generations.

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

```
$NMSROOT\CSCOpX\bin\perl $NMSROOT\CSCOpX\bin\restorebackup.pl <-d backup directory>
[-gen GenerationNumber] [-t TempDirector] [-help]
```

where:

**GenerationNumber**—The latest generation number of the backup. If “-gen” option is not specified, the default value “0” will be considered.

For example, to restore CSM data from C:\backup\100 folder, you would enter the following:

```
C:\Progra~1\CSCOpX\bin\perl C:\Progra~1\CSCOpX\bin\restorebackup.pl -d C:\backup -gen 100
```

**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
```

## Migrating AUS and Configuration Engines

When you upgrade from a version of Security Manager earlier than 3.2 to 3.2.1, the Auto Update Servers (AUS) and Configuration Engines that are configured in the earlier versions of Security Manager are not available in the 3.2.1 database. Although devices managed by AUS and CNS are migrated after the upgrade to 3.2.1, 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.
- 

## 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 3.2.1 to release 3.1, 3.1.1, or 3.2 (including 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 3.2.1 and AUS 3.2.1. See [Uninstalling Server Applications, page 4-6](#).
- Step 2** Install Security Manager 3.1, 3.1.1, or 3.2 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 Data, page 5-4](#).



---

**Note** Your downgraded copy of Security Manager includes only the information that you saved *before* you upgraded to release 3.2.1.

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.

---

