



Upgrading to VMS 2.3

This section assumes you want to upgrade VMS in its entirety including all components on Disk 1 and Disk 2 as listed in [Chapter 1, “VPN/Security Management Solution Overview.”](#) VMS upgrade takes approximately one hour.

This chapter includes the following upgrade information:

- [Backing Up Your Existing VMS Database](#)
- [Order of Upgrade](#)
- [Upgrading Common Services and Management Centers](#)
- [Upgrading RME \(Disk 4\)](#)



Note

If you are downloading components from Cisco.com, see [Chapter 1, “Preparing to Install or Upgrade VMS.”](#)

Before You Begin

- Verify that all system requirements are met as listed in [Chapter 1, “VPN/Security Management Solution Overview.”](#)
 - Perform all proper system checks and safety measures as listed in [Chapter 1, “Preparing to Install or Upgrade VMS.”](#)
 - Back up your existing VMS database. See [“Backing Up Your Existing VMS Database”](#) in this chapter.
-

Backing Up Your Existing VMS Database

VMS backup occurs by backing up the Common Services and RME databases from the CiscoWorks server desktop, and by using the backup utility to backup all of the Management Center components. We recommend that you back up all system and database files now to establish a system baseline, and to avoid having to reinstall any VMS components if data becomes corrupted.

Common Services and RME Database Backup

To back up the Common Services system files and databases, use the backup data command, described ahead, and in *Installation and Setup Guide for CiscoWorks Common Services 2.2 on Solaris* at:

http://www.cisco.com/en/US/docs/net_mgmt/cisoworks_common_services_software/2.2/cd_one/installation/solaris/guide/InstallSetupGuideForComSerCVSol.pdf. Make sure the backed up data is stored on tape or CD-ROM.

To backup your data:

-
- Step 1** Access the CiscoWorks desktop and log in. For information, see [Chapter 1, “Upgrading to VMS 2.3.”](#)
- Step 2** Select **Server Configuration > Administration > Database Management > Back Up Data Now**.

The Back Up Data Now dialog box appears.

- Step 3** Enter the pathname of the target directory.



Note We recommend that you use a different directory from the directory where VMS files are located, for example, /cw/backups.

- Step 4** To begin the backup, click **Finish**.
- This process may take a few minutes to complete.
-

Management Center Backup

To back up all Management Center system files and databases, use the backup database command.

To backup your database:

-
- Step 1** Access the CiscoWorks desktop and log in. For information, see [Chapter 1, “Preparing to Use VMS 2.3.”](#)
- Step 2** Select **VPN/Security Management Solution > Administration > Common Services > Backup Database**.

The Back Up Database dialog box appears.

- Step 3** Enter the pathname of the target directory.



Note We recommend that you use a different directory from the directory where VMS files are located, for example, /cw/backups.

- Step 4** To begin the backup, click **Finish**.
- This process may take a few minutes to complete.
-

Order of Upgrade



Caution

IPS MC 1.2.3 and Security Monitor 1.2.3 require upgrade to an intermediary version (2.0.1 found on Disk4 before you can use the VMS installer found on Disk 1. For this reason, we strongly recommend selecting **Server Configuration > About the Server > Applications and Version** to determine precise component version numbers before you upgrade.

Because backups of IPS MC 1.2.3 and Security Monitor 1.2.3 data cannot be restored directly onto a IPS MC/SecMon 2.1 system, you should perform a backup for future use after successfully upgrading.

As with a new VMS installation, the components in an upgraded installation require that Common Services and VMS Service Pack 3 be installed first.

To upgrade to VMS 2.3:

-
- Step 1** Select **Server Configuration > About the Server > Applications and Versions** to determine precise component version numbers before you upgrade.
- Step 2** Follow one of the following two sets of steps:
- a. If you have IDS MC 1.2.3 or Security Monitor 1.2.3 installed, you must:
 1. Install Common Services with Service Pack 3 on Disk 1 as described in [Upgrading Common Services with Service Pack 3, page 1-5](#).
 2. Upgrade to IDS MC 2.0.1 and Security Monitor 2.0.1 on Disk 4 as described in [Upgrading IDS MC 1.2.3 and Security Monitor 1.2.3, page 1-7](#).
 3. Upgrade remaining components using the installer beginning starting with Disk 1 as described in [Upgrading VMS Configuration Components \(Disk 2\), page 1-10](#) and [Upgrading VMS Monitoring Components \(Disk 3\), page 1-11](#).
 - b. If you have IDS MC 2.0.1 or Security Monitor 2.0.1 installed:
 1. Install Common Services with Service Pack 3 on Disk 1 as described in [Upgrading Common Services with Service Pack 3, page 1-5](#).
 2. Upgrade remaining components using the installer beginning starting with Disk 1 as described in [Upgrading VMS Configuration Components \(Disk 2\), page 1-10](#) and [Upgrading VMS Monitoring Components \(Disk 3\), page 1-11](#).
-

Upgrading Common Services and Management Centers

See the following for upgrade procedures:

- [Upgrading Common Services with Service Pack 3](#)
- [Upgrading IDS MC 1.2.3 and Security Monitor 1.2.3](#)
- [Upgrading VMS Configuration Components \(Disk 2\)](#)
- [Upgrading VMS Monitoring Components \(Disk 3\)](#)

Upgrading Common Services with Service Pack 3

**Note**

Even if you have Common Services 2.2 with Update 1 installed, you *must* reinstall Common Services from VMS 2.3 Disk 1.

To upgrade Common Services (mandatory in all cases) with Service Pack 3 (embedded):

Step 1 Log in as root on the Solaris server.

Step 2 Mount the CD-ROM. See [Appendix A, “Troubleshooting Installation.”](#)

Step 3 Start the installation program by entering:

```
cd /cdrom/cdrom0/  
./setup.sh
```

The License agreement page appears.

Step 4 Do one of the following:

- Press **Enter** to view the license agreement page.
- Enter **q** to quit. The following message appears:

```
You must accept this License agreement for the installation to  
proceed.
```

```
Do you accept all the terms of the preceding License agreement? (y/n)  
[y]
```

Step 5 Enter **y** to accept the agreement, or **n** to quit.

Step 6 Determine whether an Express, Typical or Custom installation is required. There is a brief description of each type of installation next to the number indicating its option.



Note For more details about the different types of Common Services installation, see the *Installation and Setup Guide for CiscoWorks Common Services 2.2 (Includes CiscoView 5.5) on Solaris* at: http://www.cisco.com/en/US/docs/net_mgmt/cisoworks_common_services_software/2.2/cd_one/installation/solaris/guide/InstallSetupGuideForComSerCVSol.pdf.

Step 7 Enter one of the following:

1 for an Express installation that installs the product using the default settings.
2 for a Typical installation, which is recommended for most computers.
3 for a Custom installation, which is recommended to customize the setup option.
q to quit the installation

Step 8 Enter the location where you are installing Common Services if it differs from the default /opt/CSCOpx.

The Disk 1 components are listed in detail (including Cisco View and Integration Utility) and you are asked to select the ones you are installing. You are also given the option to select all (recommended).

Step 9 Enter the number(s) corresponding to the components you are installing or 4 to install all VMS Disk 1 components.

The installation program displays the details of your available system resources against the product requirements.



Caution If your system does not meet the disk space or memory requirements, exit the installation and make the necessary system adjustments.

The installation program will continue.

Step 10 Follow the prompts that ask you to enter an admin password or accept one that is randomly generated. Installation completes.

Upgrading IDS MC 1.2.3 and Security Monitor 1.2.3

System Parameters

During installation, IDS MC sets the following system parameters in the `/etc/system` file on Solaris:

```
set shmsys:shminfo_shmmax=4294967295
set shmsys:shminfo_shmmin=1
set shmsys:shminfo_shmmni=100
set shmsys:shminfo_shmseg=10
set semsys:seminfo_semmsl=160
set semsys:seminfo_semopm=100
set semsys:seminfo_sevmx=32767
set semsys:seminfo_semaem=16384
set semsys:seminfo_semmap=66
set semsys:seminfo_semume=20
set semsys:seminfo_semuns=510
set semsys:seminfo_semuni=170
set semsys:seminfo_semmnu=120
set rlim_fd_cur=120
```

If you are running other applications that use these parameters, you must increment them according to application documentation. If you change these parameters, you must reboot the system for the changes to take effect.

You can find general information about tuning the system parameters on the Sun Microsystems website:

<http://docs.sun.com/>

Before you begin



Note Verify that you have root privileges on the server.

This section describes how to upgrade to IDS MC 2.0.1 and Security Monitor 2.0.1. If IDS MC and Security Monitor are installed on the same server, you must upgrade both. If only one component is installed on the server, you can optionally install the current version of the other component on the same server during the upgrade process.

To upgrade IDS MC, Security Monitor, or both from version 1.2.3 to 2.0.1, or to upgrade one component while installing the other, follow these steps:

Step 1 Log in as root.

Step 2 To run the installation program, enter:

```
# cd tempdir
# ./setup.sh
```

where *tempdir* is the location where you extracted the installation files.

The following message appears:

```
Press Enter to read/browse the following license agreement:
```

Step 3 Press **Enter** to read the license agreement.

The following message appears at the end of the license agreement:

```
You must accept this License agreement for the installation to
proceed.
```

```
If you enter N/n, the installation will exit.
```

```
Do you accept all the terms of the preceding License Agreement? (y/n)
[y]
```

Step 4 To accept the terms of the license agreement and proceed with the installation, enter **y**.



Note If you do not accept the terms of the license agreement, enter **n** to stop the installation.

One of the following applies depending on which components are installed on your server:

- If both IDS MC and Security Monitor are installed on your server, the installation application upgrades both components. Skip to [Step 8](#).
- If only IDS MC is installed on your server, the following message appears:


```
(1) IDS Management Center
(2) Both IDS Management Center and Security Monitor
```
- If only Security Monitor is installed on your server, the following message appears:


```
(1) Security Monitor
```

(2) Both IDS Management Center and Security Monitor

- Step 5** Enter 1 to upgrade the component that is installed on the server or enter 2 to upgrade the component and to install the other component.



Note If only one component (IDS MC or Security Monitor) is installed on the server, and you want to install the other component on the same server, you should wait and install it using the 2.0.1 installer.

The following message appears:

NOTE: Security Monitor attack records will be archived on disk. See online help to import archived records, if desired.
IMPORTANT: You are performing an upgrade, it is strongly recommended that you first make a VMS backup. Enter y if you have a backup and are ready to proceed.

- Step 6** Do one of the following:
- To cancel this upgrade and perform a VMS backup, enter **n** and then back up the database.
After you have completed the VMS backup, restart this procedure.
 - To proceed with the upgrade, enter **y**.

- Step 7** If you are installing IDS Management Center while upgrading Security Monitor, enter the following details:
- Database password
 - Database location
 - Host IP address

The installation proceeds.

- Step 8** Verify that the upgrade was successful and reboot the system if required.

During installation, a warning message appears if the `/etc/system` file is modified for tuning system parameters. You should reboot the system for the changes to the `/etc/system` file to take effect. If you do not reboot the system, IDS MC and Security Monitor may not work as expected.

You should enable and configure `syslogd` service for `IDS_Receiver` to receive `syslog` events from remote hosts.

After the installation is completed, Daemon Manager starts.



Note Error messages or warning messages appear if the required and recommended Solaris patches are not present on your system. Before running Security Monitor and IDS MC, download and install the most recent recommended patches from <http://www.sunsolve.sun.com>.

If errors occurred during installation, check the installation log file: `/var/tmp/ciscoinstall.log`. Each installation appends to this file.

Upgrading VMS Configuration Components (Disk 2)

This procedure assumes you have installed Common Services with Service Pack 3.

To install any or all VMS Disk 2 components:

-
- Step 1** Follow [Step 1](#) through [Step 5](#) in “Upgrading Common Services and Management Centers”.
- Step 2** Enter the number(s) corresponding to the components you want to install or enter **5** to install all VMS Disk 2 components: Firewall MC, Router MC, IDS MC, and AUS.
- Step 3** Enter the location where you are installing Disk 2 components if it differs from the host IP address displayed.
- You will be prompted for VMS database and Lock Manager passwords. These passwords, if different from database passwords already installed will only be applied to those components being installed or upgraded now. They will not be applied to installed components that are not being upgraded.
- The installation program displays the Lock Manager (LM) Port configuration information. The default is port number 1272.
- Step 4** To accept the default port, press **Enter**. To specify a different port, enter that port number, then press **Enter**. If the port number that you provide is not available, it will ask for another port number. Port number parameters (1 to 65535) are displayed.

Installation progress is displayed while files are copied and components are configured.

Upgrading VMS Monitoring Components (Disk 3)

This procedure assumes you have installed Common Services with Service Pack 3.

To install any or all VMS Disk 3 components:

- Step 1** Follow [Step 1](#) through [Step 5](#) in “[Upgrading Common Services and Management Centers](#)”.
- Step 2** Enter the number(s) corresponding to the components you want to install, or enter **3** to install Performance Monitor and Security Monitor.
- Step 3** Enter the location where you want to install Disk 2 components if it differs from the host IP address displayed.

You will be prompted for a VMS database password. We recommend using the same password as you did in “[Upgrading VMS Configuration Components \(Disk 2\)](#)”, [Step 10](#).

Installation progress is displayed while files are copied and components are configured.

Upgrading RME (Disk 4)

It is very likely that if you are upgrading from a previous version of VMS, you already having RME 3.5 installed on your server, in which case you can install IDU 12 and proceed by upgrading CSA MC to complete your upgrade to VMS 2.3.

Before You Begin

- Verify all system requirements are met as listed in [Chapter 1](#), “[VPN/Security Management Solution Overview](#).”

- Perform all proper system checks and safety measures as listed in [Chapter 1, “Preparing to Install or Upgrade VMS.”](#)

**Caution**

If you already have RME 3.5 installed, you still must install the RME VMS Update for RME to work with this version of VMS. If you are upgrading from an earlier version of RME, you must install RME 3.5 followed by IDU 12 provided on Disk 2.

This procedure assumes you have installed Common Services with Service Pack 3.

To upgrade VMS Disk 4 components (RME 3.5 and the VMS RME update):

-
- Step 1** Follow [Step 1](#) through [Step 5](#) in “[Upgrading Common Services and Management Centers](#)”, but substitute the change directory commands to navigate to the RME directory (as opposed to the VMS RME update directory).

The installation program checks for required patches and other dependencies and displays:

```
1) Typical ("Typical installation is recommended for all computers.")
2) Custom ("Custom installation can be selected if you want to
customize the setup options.")
Select one of the installation modes using its number or enter q to
quit [1]
```



Note If you choose the Typical installation mode, the RME database password is randomly generated for you. You can view the password at the end of installation. If you choose the Custom installation mode, you are prompted to enter the Essentials database password.

- Step 2** Do one of the following:
- If you want the Typical installation mode, see “[New Installation—Typical](#)” in the following section.
 - If you want the Custom installation mode, see “[New Installation—Custom](#)” in the following section.
-

New Installation—Typical

For a Typical Installation:

Step 1 Enter 1 and press **Return**.

Step 2 The installation program checks dependencies and system requirements.

If your system does not meet the requirements a warning appears:

```
System memory is less than the minimum requirement, which may affect
performance.
```

If the drive does not have enough space, an error message appears:

```
There is not enough space in drive drive name.
```

Step 3 Make necessary changes to your system to ensure that they meet the system requirements if needed.

If the drive does not have enough space, an error message appears:

```
There is not enough space in drive drive name.
```

Step 4 Select another drive, or free some space on drive *drive name*.

The installation proceeds without displaying more questions. The following message appears:

```
Do you want to see the passwords that were entered/randomly generated?
If yes, please remember that passwords are security sensitive data and
hence make sure they are kept secure. [y/n]
```

If you enter **y**, the password appears in clear text on the console. If you enter **n**, the password does not appear.

The following message appears:

```
To ensure that you retain the latest device support and bug fixes,
please install the latest Incremental Device Update (IDU) for Resource
Manager Essentials 3.5. You can download the latest IDU from
http://www.cisco.com/cgi-bin/tablebuild.pl/cw2000-rme Please refer to
the Installation and Setup Guide for details.
```



Note All IDUs necessary for the VMS version of RME are included in the VMS RME update on VMS Disk 4. You do not need to download or install any IDUs from Cisco.com.

The installation completes without displaying more questions.

Step 5 Restart your system.

New Installation—Custom

For a Custom Installation:

Step 1 Enter **2** and press **Return**.

Step 2 The installation program checks dependencies and system requirements.

If your system does not meet the requirements a warning appears:

```
System memory is less than the minimum requirement, which may affect
performance.
```

If the drive does not have enough space, an error message appears:

```
There is not enough space in drive drive name.
```

Step 3 Make necessary changes to your system to ensure that they meet the system requirements if needed.

If the drive does not have enough space, an error message appears:

```
There is not enough space in drive drive name.
```

Step 4 Select another drive, or free some space on drive *drive name*.

The installation program displays the following message:

```
Enter RME database password:
```

Step 5 Enter a new password.

The following message appears:

```
Confirm Password.
```

Step 6 Enter the password again to confirm.

The installation proceeds without displaying more questions. The following message appears:

To ensure that you retain the latest device support and bug fixes, please install the latest Incremental Device Update (IDU) for Resource Manager Essentials 3.5. You can download the latest IDU from <http://www.cisco.com/cgi-bin/tablebuild.pl/cw2000-rme> Please refer to the Installation and Setup Guide for details.



Note All IDUs necessary for the VMS version of RME are included in the VMS RME update on VMS Disk 4. You do not need to download or install any IDUs from Cisco.com.

Step 7 Restart your system.

Installing IDU 12

This procedure assumes you have installed Common Services with Service Pack 3 and RME 3.5.

-
- Step 1** Follow [Step 1](#) through [Step 5](#) in “[Upgrading Common Services and Management Centers](#)”, but substitute the change directory commands to navigate to the VMS RME update directory (as opposed to the RME component directory).
- Step 2** The installation proceeds with IDU and VMS update messages appearing.
- Step 3** Restart your system.
- For uninstallation instructions see [Chapter 1, “Installing and Uninstalling VMS.”](#)

