Post-Installation Server Tasks

The following topics are tasks to complete after you install Security Manager or its related applications on a server.

- Server Tasks To Complete Immediately , on page 1
- Verifying that Required Processes Are Running , on page 2
- Configuration of Heap Sizes for Security Manager Processes using MRF, on page 3
- Best Practices for Ongoing Server Security , on page 8
- Verifying an Installation or an Upgrade , on page 8
- (Optional) Changing the Hostname of the Security Manager Server, on page 9
- Verifying and Validating CSM Log Viewer, on page 10
- Where To Go Next , on page 11

Server Tasks To Complete Immediately

Make sure that you complete the following tasks immediately after installation.

✓	Task
❑	1. **Re-enable or re-install antivirus scanners and similar products.** If you uninstalled or temporarily disabled any server security software, such as an antivirus tool, re-install or restart that software now, then restart your server if required.Make sure to exclude the NMSROOT directory and the eventing folder from scanning as long as Security Manager is installed on the server. **Note** If you see that your antivirus software is reducing the efficiency or responsiveness of a Security Manager server, see your antivirus software documentation for recommended settings.
❑	1. **Re-enable the services and server processes that you disabled for installation.** Do not re-enable IIS.
❑	1. **On the server, add a self-signed certificate to the list of trusted certificates.** To learn how, see your browser documentation.
❑	1. **Check for updates on Cisco.com for Security Manager and its related applications.** If you learn that updates are available, install the ones that are relevant to your organization and network.

Verifying that Required Processes Are Running

You can run the **pdshow** command from a Windows command prompt window to verify that all required processes are running correctly for the Cisco server applications that you choose to install. Process requirements differ among the applications.

Tip To learn more about **pdshow**, see the Common Services documentation.

Use Table 7-1 to understand which applications require which processes.

Table 1: Application Process Requirements

This application:	Requires these Daemon Manager processes:
Common Services	Apache CmfDbEngine CmfDbMonitor CMFOGSServer CSRegistryServer DCRServer diskWatcher EDS EDS-GCF ESS EssMonitor jrm LicenseServer Proxy Tomcat TomcatMonitor NameServer NameServiceMonitor EventFramework
Cisco Security Manager	AthenaOGSServer ccrWrapper CsmReportServer rptDbEngine rptDbMonitor VmsBackendServer vmsDbEngine vmsDbMonitor VmsEventServer CsmHPMServer ProcessManager

Configuration of Heap Sizes for Security Manager Processes using MRF

Memory Reservation Framework (MRF), a feature introduced in Security Manager 4.1, provides Cisco Security Manager administrators the capability to modify heap sizes of key processes; doing so can enhance the performance of the server. MRF enables processes to adjust heap sizes on the basis of the RAM installed on the server.

The Security Manager processes that can be configured using MRF are listed in Table 7-2.

Table 2: Security Manager Processes that Can Be Configured by Using MRF

Process	Name as shown in pdshow	Description
Backend Process	VmsBackendServer	Performs device discovery and deployment operations.
Tomcat	Tomcat	Hosts applications responsible for editing and validating policies, etc.
Report Server	CsmReportServer	Generates reporting data.
Event Server	VmsEventServer	Collects events being sent from devices.

Note Based on your configuration load, it is always recommended to find Tomcat & Backend Server heap size according to your environment for better performance.

Note There is no MRF configuration for the HPM (Health and Performance Monitor) server.

Note You can learn more about the pdshow command in the previous section, Verifying that Required Processes Are Running , on page 2, and in the Common Services documentation.

Default Configuration

The processes listed in Table 7-3, which are the Security Manager processes that can be configured by using MRF, are pre-configured with default values for heap sizes. Table 7-3 lists the default minimum and maximum heap sizes in megabytes for different amounts of RAM available to the server for each Security Manager process that can be configured by using MRF.

Table 3: Default Heap Sizes Preconfigured for Security Manager Processes

Physical RAM on server (GB)	VmsBackendServer	Tomcat	CsmReportServer	VmsEventServer	CsmHPMServer
< 8	1024, 2048	512, 1024	1024, 1024	1024, 2048	512, 1024
8	1024, 3072	1024, 2048	1024, 1024	1024, 3072	512, 1024
12	2048, 4096	2048, 3072	1024, 2048	2048, 4096	512, 1024
16	2048, 4096	2048, 4096	1024, 4096	4096, 4096	512, 1024
24	4096, 8192	4096, 4096	1024, 4096	4096, 8192	512, 1024
>= 28	8192, 8192	4096, 4096	1024, 4096	4096, 8192	512, 1024

Some RAM is reserved for the operating system and for other processes and is not listed here. For example, consider the case of 16 GB RAM in Table 7-3. The total maximum heap size for all 4 processes is (4096 + 4096 + 1024 + 4096) = 13312 Mb or 13 Gb. There is 3 GB additional RAM available for the operating system and for other processes.

Note Please refer the deployment model guide and use the respective RAM for your environment. You can fine tune the above parameters for better performance if memory-related slowness is observed.

Configuration Commands

MRF provides a command and a set of sub-commands to read and modify heap sizes for Security Manager server processes. Minimum and maximum heap sizes can be set for the process by using the mrf command. Information on using of this command is displayed by executing this command as follows:

```
> mrf
mrf help
           Prints this message.
mrf backup
           Backup existing configuration
mrf revert
           Restores backed up configuration
mrf set_heap_params process X-Y [min],[max]
           Sets minimum and maximum heap sizes
           process -> process name
           X-Y -> Memory Range in MB to which heap sizes apply
           [min],[max] -> minimum and maximum heap sizes in MB. These are optional but
atleast one should be specified.
mrf get_heap_params process [memory]
           Prints minimum and maximum heap sizes in MB
           process -> process name
```

```
          [memory] -> memory size in MB for which heap sizes are to be printed. If not
specified heap sizes are to be printed for current system memory.
```

Make sure that only valid process names are used while running **mrf** commands. No error is thrown when an invalid process name is specified. Valid process names are listed in Table 7-2. Process names are case-sensitive.

Configuring Heap Sizes for Processes

Configuring heap sizes for Security Manager processes can be thought of as consisting of the following three major steps:

1. Save Existing Configuration

2. Read Existing Configuration

3. Modify Configuration , on page 6

1. Save Existing Configuration

Configuring a process heap size is a critical procedure that can affect the performance of Security Manager, so Cisco recommends that it be done only under the guidance of application experts.

Also, as a precautionary measure, Cisco recommends that you save your existing memory configurations for processes before changing them, and MRF provides two methods for doing so.

1. The first method can be used if you are testing the configuration changes. In this case the old configuration can be saved, and new modifications can be reverted to old configurations, by using the two commands listed below, respectively:

   ```
   mrf backup
   mrf revert
   ```

2. The second method is useful if you would like to revert to old values after you have used the new configuration for a significant period. There are two ways of doing this; you can use one or the other of the following ways:

   a. You can run mrf revert, provided you have not run mrf backup after you did the configuration changes.

   b. You will be taking a backup of your Cisco Security Manager Server before you make configuration changes. If you want to revert the changes, then restore the backup. In this case, data changes done after backup was taken will be lost.

2. Read Existing Configuration

Now that you have saved your data, you can query existing values for the processes by using the following command:

mrf get_heap_params *[process name] [memory]*

If memory is not specified in this command, the current RAM size will be used. Usually you are interested in the current RAM size. The parameter *[process name]* has one of the values listed in Table 7-2. Process names are case-sensitive.

The output of the command appears as shown below. Values are in MB.

```
Minimum Heap Size = 1024
Maximum Heap Size = 2048
```

3. Modify Configuration

After you have verified the current configuration, you can proceed to modify the configuration as described in this section.

To configure the heap sizes, use the following command:

mrf set_heap_params *[process name] [X-Y] [min] ,[max]*

The parameter *[process name]* can be any of the processes listed in Table 7-2. Process names are case-sensitive.

You need to restart the Security Manager server after executing this command for the changes to take effect.

Note Changes made by using **mrf set_heap_params** can be lost if the backup that was taken before modifying heap parameters is restored. In this case, if you want to retain the new values, you can follow these steps:

1. Run, mrf backup
2. Do application restore.
3. Run, mrf revert

This command uses the following syntax:

mrf set_heap_params *[process name] [X-Y] [min],[max]*

Sets minimum and maximum heap sizes

[X-Y[: memory range in MB to which heap sizes apply

[min],[max]: minimum and maximum heap sizes in MB. These are optional but at least one should be specified.

The parameter *[process name]* has one of the values listed in Table 7-2. Process names are case-sensitive.

Examples of Modify Configuration

The following examples illustrate how you can modify heap size configurations:

- mrf set_heap_params Tomcat 7372-8192 2048,4096

Sets minimum and maximum heap sizes to 2048 MB and 4096 MB, respectively, for the Tomcat process when the RAM size is in the range of 7372 MB to 8192 MB

- mrf set_heap_params Tomcat 7372-8192 2048

Sets the minimum heap size to 2048 MB for the Tomcat process when the RAM size is in the range of 7372 MB to 8192 MB

- mrf set_heap_params Tomcat 7372-8192,4096

Sets the maximum heap size to 4096 MB for the Tomcat process when the RAM size is in the range of 7372 MB to 8192 MB

- mrf set_heap_params Tomcat 8080-8080 2048,4096

Sets the minimum and maximum heap sizes to 2048 MB and 4096 MB, respectively, for the Tomcat process when the RAM size is 8080 MB. You can execute the **getramsize** command to get the existing RAM size in MB.

Verification of Modify Configuration

After heap parameters are set, you can verify the changes by executing the **mrf get_heap_params** command.

Summary of Configuring Heap Sizes for Processes

The three major steps described in this section for configuring heap sizes for Security Manager processes can be summarized by the following commands, listed in their order of execution:

```
mrf backup
mrf get_heap_params process
mrf set_heap_params Tomcat 7372-8192 2048,4096
mrf revert #if required to revert changes
```

Typical scenarios in which the User Might Have to Reconfigure Heap Sizes

Scenario 1

A Security Manager 4.0 user potentially may be using a maximum heap size of 4 GB for the Backend Process (VmsBackendServer). This is more than the default maximum heap size of 3 GB allocated in Security Manager 4.1 for 8 GB RAM. In this scenario, the user may have to reconfigure the Backend Process heap size to 4 GB. The user can choose to do this in case Event Management, which uses the Event Server process (VmsEventServer) is not enabled.

Scenario 2

Suppose Security Manager is being used in configuration-only mode (Event Management and reporting are disabled). In this scenario, the Backend Process and Tomcat heap sizes can be increased.

Scenario 3

Suppose Security Manager is being used in configuration-only mode (Event Management and reporting are disabled) and Event Management needs to be enabled. In this scenario, the Backend process and Tomcat heap sizes should be decreased, before enabling Event Management, so that the total of all heap sizes of Security Manager processes does not exceed the RAM size available to the server.

Scenario 4

Event Management and the Backend process are memory-intensive and need higher RAM allocation. (If event Management is unused, that RAM could be allocated for the Backend process by increasing its maximum heap size.)

Best Practices for Ongoing Server Security

The least secure component of a system defines how secure the system is. The steps in the following checklist can help you to secure a server and its OS after you install Security Manager:

✓	Task
❑	1. **Monitor server security regularly.** Log and review system activity. Use security tools such as the Microsoft Security Configuration Tool Set (MSCTS) and Fport to periodically review the security configuration of your server. Review the log file for the standalone version of Cisco Security Agent that is installed sometimes on a Security Manager server. **Tip** You can obtain MSCTS from the Microsoft web site and Fport from the Foundstone/McAfee web site.
❑	1. **Limit physical access to your server.** If your server contains removable media drives, set the server to boot from the hard drive first. Your data can be compromised if someone boots your server from a removable media drive. You can typically set the boot order in the system BIOS. Make sure you protect the BIOS with a strong password.
❑	1. **Do not install remote access or administration tools on the server.** These tools provide a point of entry to your server and are a security risk.
❑	1. **Set a virus scanning application to run automatically and continuously on the server.** Virus scanning software can prevent trojan horse applications from infecting your server. Update the virus signatures regularly.
❑	1. **Back up your server database frequently.** Store all backups in a secure location with restricted access. **Note** Remove the logs/ database backup files regularly in order to maintain sufficient free space on your hard disk at all times. It is recommended to have a minimum of 10GB hard disk space free.
❑	1. **Back up your Security Manager Server regularly.** If regular backups have not been made, or if several changes have been made to your Security Manager installation, back up your Security Manager server before running any Windows Update.

Verifying an Installation or an Upgrade

You can use Common Services to verify that you installed or upgraded Security Manager successfully. If you are trying to verify the installation because the Security Manager interface does not appear or is not displayed correctly, see XREF.

Procedure

Step 1 Use a browser on the client system to log in to the Security Manager server using either of the following:

- For HTTP service—**http://**<*server_name* >**:1741**
- For SSL service—**https://**<*server_name* >**:443**

To learn which browsers and browser versions are supported, see Client Requirements.

Step 2 From the Cisco Security Management Suite page, click the **Server Administration** panel to open Common Services at the **Server > Admin** page.

Step 3 To display the Process Management page, click **Processes**.

The resulting list names all the server processes and describes the operational status of each process. The following processes must be running normally:

- vmsDbEngine
- vmsDbMonitor
- EDS

(Optional) Changing the Hostname of the Security Manager Server

If you are required to change the hostname of the Security Manager Server, follow the steps below:

Procedure

Step 1 Change the hostname in the OS:

a) Right-click **Computer** and select **Properties** or open **Control Panel** and select **System**.
b) Under **Computer Name, Domain and Workgroup Settings**, click **Change Settings**.
c) Click **Change** to modify the **Computer Name** (hostname).
d) Restart the computer.

Step 2 Stop the Security Manager Daemon Manager by entering **net stop crmdmgtd** in the command window.

Step 3 Execute the Security Manager Server hostname change script by running the following command in a command window:

Example:

```
NMSROOT\bin\perl NMSROOT\bin\hostnamechange.pl
```

In this command, NMSROOT is the path to the Security Manager installation directory.

Tip

hostnamechange.pl is a utility that updates the hostname changes in the Common Services- related directories, files, database entries and registry entries after the hostname is changed in the OS.

Step 4 Restart the computer.

Note
In this step, you must restart the computer. Restarting the Security Manager Daemon Manager is not sufficient.

Verifying and Validating CSM Log Viewer

From Cisco Security Manager 4.24 onwards, post CSM software installation or upgrade, you can use the CSM Log Viewer to verify and validate the supported options.

Procedure

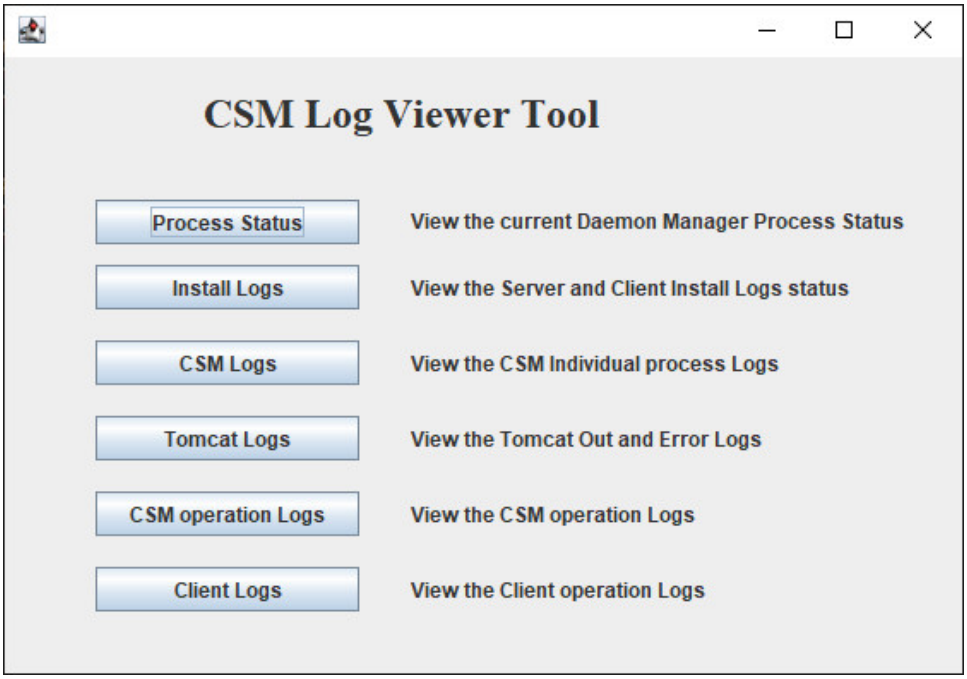
Step 1 Navigate to the following location: **C:\ProgramFiles(x86)\CSCOpx\bin**

Step 2 Run the batch file **CsmLogViewer**

You can view the CSM Log Viewer tool with all the following supported options:

- Process Status
- Install Logs
- CSM Logs
- Tomcat Logs
- CSM operation Logs
- Client Logs

Figure 1: CSM Log Viewer



Step 3 From the CSM log viewer drop down box, select the log you want to check the information or error and validate the data.

Where To Go Next

If you want to:	Do this:
Understand the basics	See the interactive *JumpStart* guide that opens when you start Security Manager.
Get up and running with the product quickly	See the "Getting Started with Security Manager" topic in the online help, or see Chapter 1 of *User Guide for Cisco Security Manager* .
Complete the product configuration	See the "Completing the Initial Security Manager Configuration" topic in the online help, or see Chapter 1 of *User Guide for Cisco Security Manager* .
Manage user authentication and authorization	See the following topics: • User Permissions • Integrating Security Manager with Cisco Secure ACS

If you want to:	Do this:
Bootstrap your devices	See the "Preparing Devices for Management" topic in the online help, or see Chapter 2 of *User Guide for Cisco Security Manager 4.30*, available at http://www.cisco.com/en/us/support/security/security-manager/products-user-guide-list.html