CHAPTER 3

Preparing a Server for Installation

After you verify that the target server meets the requirements described in Chapter 2, “Requirements and Dependencies,” you can use these checklists to prepare and optimize your server for installation:

- Best Practices for Enhanced Server Performance and Security, page 3-1
- Readiness Checklist for Installation, page 3-4

Best Practices for Enhanced Server Performance and Security

A framework of best practices, recommendations, and other preparatory tasks can enable your Security Manager server to run faster and more reliably than it might do otherwise.

⚠ **Caution** We do not make any assurances that completing the tasks in this checklist improves the performance of every server. Nonetheless, if you choose not to complete these tasks, Security Manager might not operate as designed.

You can use this checklist to track your progress while you complete the recommended tasks.

✓	Task
❑	1. **Find and organize the installer applications for any recommended updates, patches, service packs, hot fixes, and security software to install on the server.**
❑	2. **Upgrade the server BIOS if an upgrade is available.**
❑	3. **If you plan to install Security Manager on a server that you have used for any other purpose, first back up all important server data, then use a boot CD or DVD to wipe all data from the server.** We do *not* support installation or coexistence on one server of Security Manager 4.0.1 and any release of Common Services earlier than 3.3. Nor do we support coexistence with any third-party software or other Cisco software, unless we state explicitly otherwise in this guide or at http://www.cisco.com/go/csmanager.
❑	4. **Perform a clean installation of only the baseline server OS, without any manufacturer customizations for server management.**
❑	5. **Install any required OS service packs and OS patches on the target server.** To check which service packs or updates are required for the version of Windows that you use, select **Start > Run**, then enter **wupdmgr**.

✓	Task
□	6. **Install any recommended updates for drivers and firmware on the target server.**
□	7. **Scan the system for malware.** To secure the target server and its OS, scan the system for viruses, Trojan horses, spyware, key-loggers, and other malware, then mitigate all related problems that you find.
□	8. **Resolve security product conflicts.** Study and work to resolve any known incompatibilities or limitations among your security tools, such as popup blockers, antivirus scanners, and Cisco Security Agent or similar products from other companies. When you understand the conflicts and interactions among those products, decide which of them to install, uninstall, or disable temporarily, and consider whether you must follow a sequence. For example: • If your organization uses any host-based intrusion prevention utility from a company other than Cisco, you *must not* install that utility on the target server until *after* you install Security Manager. Otherwise, it might interfere with the installation of Cisco Security Agent, which is installed automatically in most cases as part of the Security Manager installation. If you want to use a server where another IPS utility is installed, uninstall it, then install Security Manager, then uninstall Cisco Security Agent, and then re-install the utility. • If any version of Cisco Security Agent is installed on a Security Manager server, the server relies on a set of agent policies specific to Security Manager servers. However, the customized, standalone agent that includes those policies is installed only if the target server has no pre-existing installation of the full version of Cisco Security Agent. The full agent version does not include the specific policies that a Security Manager server requires. If you prefer the full agent to the standalone agent, you must import into your full agent all the exported agent policies that you find on the Security Manager installation DVD (in its \csm<*version*>_win_server\CSA subfolder). We recommend that you do not uninstall the standalone agent until or unless you obtain equivalent server security through another method that you trust. If you import policies from the file on the DVD, you must reconcile those imported policies with any conflicting policies that your organization has configured generally for its managed agents.
□	9. **“Harden” user accounts.** To protect the target server against brute force attacks, disable the guest user account, rename the administrator user account, and remove as many other user accounts as is practical in your administrative environment.
□	10. **Use a strong password for the administrator user account and any other user accounts that remain.** A strong password has at least eight characters and contains numbers, letters (both uppercase and lowercase), and symbols. **Tip** You can use the Local Security Settings tool to require strong passwords. Select **Start > Administrative Tools > Local Security Policy**.

✓	Task
❑	**11. Remove unused, unneeded, and incompatible applications.** For example: • Microsoft Internet Information Server (IIS) is not compatible with Security Manager. If IIS is installed, you must uninstall it before you install Security Manager. • We do not support the coexistence of Security Manager with any third-party software or other Cisco software (including any CiscoWorks-branded “solution” or “bundle,” such as the LAN Management Solution (LMS)), unless we state explicitly otherwise in this guide or at http://www.cisco.com/go/csmanager. We do support the installation of Security Manager, AUS, Performance Monitor and RME on the same server, but we recommend that configuration only for very small networks; also, you must install CiscoWorks Common Services before installing any of those products. • We do not support the installation or coexistence of this version of Security Manager on a server with any release of Common Services earlier than 3.3. • We do not support the coexistence of Security Manager on a server with any CD-ONE components (including CiscoView Device Manager) that you do not receive when you purchase Security Manager. • We do not support the coexistence of Security Manager on the same server with Cisco Secure ACS for Windows. • We do not support the coexistence of Security Manager on the same server with the full version of Cisco IPS Event Viewer.
❑	**12. Disable unused and unneeded services.** At a minimum, Windows requires the following services to run: DNS Client, Event Log, Plug & Play, Protected Storage, and Security Accounts Manager. Check your software and server hardware documentation to learn if your particular server requires any other services.
❑	**13. Disable all network protocols except TCP and UDP.** Any protocol can be used to gain access to your server. Limiting the network protocols limits the access points to your server.
❑	**14. Avoid creating network shares.** If you must create a network share, secure the shared resources with strong passwords. **Note** We strongly discourage network shares. We recommend that you disable NETBIOS completely.
❑	**15. Configure server boot settings.** Set a zero-second startup time, set Windows to load by default, and enable automatic reboot in cases of system failure.

Readiness Checklist for Installation

You must complete the following tasks before you install Security Manager.

✓	Readiness Factor
❑	⚠ **Caution** A server can be vulnerable to attack when you uninstall or disable security applications. 1. **Disable security applications temporarily.** For example, you must temporarily disable any antivirus software on the target server before you install Security Manager. Installation cannot run while these programs are active.
❑	**Tip** You will invalidate the SSL certificate on your server if you set the server date and time outside the range of time in which the SSL certificate is valid. If the server SSL certificate is invalid, the DCRServer process cannot start. 2. **Carefully consider the date and time settings that you apply to your server.** Ideally, use an NTP server to synchronize the server date and time settings with those of the devices you expect to manage. Also, if you use Security Manager in conjunction with a Cisco Security Monitoring, Analysis, and Response System (Cisco Security MARS) appliance, the NTP server that you use should be the same one that your Cisco Security MARS appliance uses. Synchronized times are especially important in Cisco Security MARS because timestamp information is essential to accurately reconstruct what transpires on your network. **Tip** If a change to the date and time settings on your server invalidates the SSL certificate, a “java.security.cert.CertificateNotYetValidException” error is visible in your *NMSROOT*\log\DCRServer.log file, where *NMSROOT* is the path to the Security Manager installation directory. The default is **C:\Program Files\CSCOpx**.
❑	3. **Confirm that required services and ports are enabled and available for use by Security Manager.** See Required Services and Ports, page 2-1.
❑	4. **If Terminal Services is enabled in Application Mode, disable Terminal Services and reboot the server.** Installation of Security Manager on a system with Terminal Services enabled in Application Mode is not supported. Terminal Services enabled in Remote Administration Mode is supported. If Terminal Services is enabled on the target server in Application mode when you try to install Security Manager, an error will stop the installation.
❑	5. **Disable any domain controller service (primary or backup) that is running.**
❑	6. **Confirm that the target directory for installation is not encrypted.** Any attempt to install Security Manager in an encrypted directory will fail.
❑	7. **If you are performing a fresh install, you should place your license file on the target server before installation.** You will be prompted to select this file during installation.
❑	8. **If you have not done so already, uninstall IIS.** It is not compatible with Security Manager.
❑	9. **Disable every active instance of Sybase on your server, including Cisco Secure ACS for Windows if it is present.** You can choose whether to re-enable or restart Sybase after you install Security Manager, but remember we do not support the coexistence of Security Manager on the same server with Cisco Secure ACS for Windows.

✓	Readiness Factor
❑	10. **If the Cisco Security Manager client is already installed on the server, the client needs to be stopped.** This condition is checked during installation.
❑	11. **Disable FIPS-compliant encryption.** Federal Information Processing Standard (FIPS)-compliant encryption algorithms sometimes are enabled for group security policy on Windows Server 2008. When FIPS compliance is turned on, the SSL authentication may fail on CiscoWorks Server. You should disable FIPS compliance for CiscoWorks to work properly. **Procedure** To enable or disable FIPS on Windows Server 2008, follow these steps: 1. Go to **Start > Administrative Tools > Local Security Policy**. The Local Security Policy window appears. 2. Click **Local Polices > Security Options**. 3. Select **System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing**. 4. Right-click the selected policy and click **Properties**. 5. Select **Enabled** or **Disabled** to enable or disable FIPS compliant algorithms. 6. Click **Apply**. You must reboot the server for the changes to take effect.