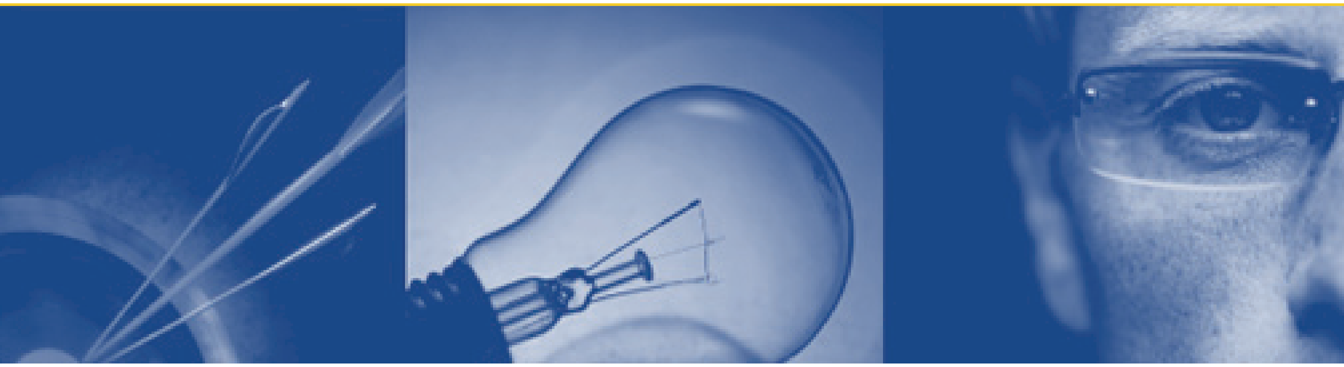
Quest Management Xtensions 2.2

CONFIGURATION MANAGER 2007 EDITION

Installation Guide



If you have any questions regarding your potential use of this material, contact:

Quest Software World Headquarters
LEGAL Dept.
5 Polaris Way
Aliso Viejo, CA 92656 USA
www.quest.com
email: legal@quest.com

Refer to our Web site for regional and international office information.

TRADEMARKS

Disclaimer

The information in this document is provided in connection with Quest products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Quest products. EXCEPT AS SET FORTH IN QUEST'S TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, QUEST ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL QUEST BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF QUEST HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Quest makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Quest does not make any commitment to update the information contained in this document.

QMX - Configuration Manager 2007 Installation Guide
Updated - September 2009
Software Version - 2.2

Contents

About this Guide

- Overview
- Conventions
- About Quest System Center Solutions Group
- About Quest Software, Inc.
- Contacting Quest Software, Inc.

Overview

IT professionals can now leverage their preferred tool for managing configuration changes and system updates for Windows and non-Windows systems alike. Quest® Management Xtensions - Configuration Manager 2007 Edition (*QMX - Configuration Manager 2007*) extends the power of Microsoft System Center Configuration Manager 2007 (*System Center Configuration Manager 2007*) to UNIX, Linux, Mac OS X and VMware ESX systems. Thus, Quest enables *System Center Configuration Manager 2007* to be the single, end-to-end platform for managing desktops, servers, and devices in both physical and virtual environments.

This guide is intended for Windows, UNIX, Linux, and Mac OS X system administrators who will be installing *QMX - Configuration Manager 2007* for the first time. By following the instructions presented in this guide, a system administrator will be ready to begin managing non-Windows systems from within the Configuration Management console.

Conventions

Quest Software, Inc. products support a number of different implementations of UNIX-like operating systems that include Solaris, HP-UX, Linux, Mac OS X, and AIX. To refer to all of these platforms, the term “Unix” will be used for conciseness and consistency.

About Quest System Center Solutions Group

With a comprehensive set of solutions that extend the powerful capabilities of the Microsoft System Center family to heterogeneous environments, Quest Software enables IT professionals to leverage System Center as the single, end-to-end platform for managing physical and virtual IT environments across data centers, desktops and devices. For more information on Quest’s System Center Solutions group, please visit http://www.quest.com/system-center/change-configuration.aspx.

About Quest Software, Inc.

Quest Software, Inc., a leading enterprise systems management vendor, delivers innovative products that help organizations get more performance and productivity from their applications, databases, Windows infrastructure and virtual environments. Quest also provides customers with client management through its ScriptLogic subsidiary and server virtualization management through its Vizioncore subsidiary. Through a deep expertise in IT operations and a continued focus on what works best, Quest helps more than 100,000 customers worldwide meet higher expectations for enterprise IT. Quest's System Center solutions enable the Microsoft System Center platform to serve as the comprehensive systems management platform for organizations managing heterogeneous environments. Together, an integrated platform improves IT productivity, increases return on IT investments, and ensures compliance and service levels to help drive business profitability. Quest Software creates and supports systems management products-helping our customers solve everyday IT challenges faster and easier. Visit Quest's System Center solutions at www.quest.com/system-center. Quest Software can be found in offices around the globe and at www.quest.com.

Contacting Quest Software, Inc.

Phone	949.754.8000 (United States and Canada)
Email	info@quest.com
Mail	Quest Software, Inc. World Headquarters 5 Polaris Way Aliso Viejo, CA 92656 USA
Web site	www.quest.com
SupportLink	www.quest.com/support
Email at	support@quest.com

Please refer to our Web site for regional and international office information.

Contacting Quest Support

Quest Support is available to customers who have a trial version of a Quest product or who have purchased a commercial version and have a valid maintenance contract. Quest Support provides around the clock coverage with SupportLink, our web self-service. Visit SupportLink at http://support.quest.com/

From SupportLink, you can do the following:

- Quickly find thousands of solutions (Knowledgebase articles/documents).
- Download patches and upgrades.
- Seek help from a Support engineer.
- Log and update your case, and check its status.

View the Global Support Guide for a detailed explanation of support programs, online services, contact information, and policy and procedures. The guide is available at: http://support.quest.com/pdfs/Global Support Guide.pdf.

Joining the Community

Get the latest product information, find helpful resources, and join a discussion with the QMX - Configuration Manager 2007 team and other community members at: http://vintela.inside.quest.com/category.jspa?categoryID=34

1

Introducing QMX - Configuration Manager 2007

- Installation Overview
- System Requirements
- Solaris 10 Zones Support
- VMware Support

Installation Overview

Quest® Management Xtensions - Configuration Manager 2007 Edition (*QMX - Configuration Manager 2007*) provides tools and extensions to the Configuration Manager Console that let you manage your enterprise's non-Windows resources. To enable Microsoft System Center Configuration Manager 2007 (*System Center Configuration Manager 2007*) to manage non-Windows systems, you must install the following components:

1. The **Configuration Manager Console Extensions**, which includes the Wizards and Remote Tools.
2. The **Collections and Queries** which allow you to manage the resources on your network.
3. The **QMX - Configuration Manager 2007 License.**
4. The **QMX - Configuration Manager 2007 Agent**, which is installed on non-Windows systems and is designed to work and act like the System Center Configuration Manager 2007 client. It is based upon a Unix-based implementation of Web-Based Enterprise Management / Common Information Model (WBEM/CIM) standards defined by the Distributed Management Task Force (DMTF) just as Windows Management Instrumentation (WMI) is a Windows-based implementation of the same standards.

   Through the use of the Quest Configuration Manager Console Extensions, the non-Windows systems work much the same as the Windows systems. They show up in collections, the hardware and software information is exposed by the Resource Explorer, the data works in standard System Center Configuration Manager 2007 reports, and so forth.

Briefly, these are the steps you must take to install QMX - Configuration Manager 2007:

1. Preparing for Installation
2. Installing the Console Extensions
3. Installing the Collections and Queries
4. Installing the License
5. Installing the Agent

System Requirements

System Center Requirements

For the hardware and software requirements necessary to implement and maintain Microsoft System Center Configuration Manager 2007 in your environment, refer to: http://technet.microsoft.com/en-us/library/bb680717.aspx#SiteServerSystemRequirements. Quest Software, Inc. maintains the same requirements.

Before you introduce QMX - Configuration Manager 2007 to your environment, you must be certain that System Center Configuration Manager 2007 is installed and working properly. Install at least one Windows client in the Configuration Manager Console and ensure that it is fully functional.

You must select **Allow clients to connect anonymously (Required for mobile device clients)** on the *ConfigMgr distribution point Properties* dialog (for mixed mode only). Navigate to Site Management/<site-code> - <site-name>/Site Settings/Site Systems/<*Distribution point server*> and double click **ConfigMgr distribution point** to open the *Properties* dialog.

QMX Requirements

QMX - Configuration Manager 2007 supports the following:

Management Point

- System Center Configuration Manager 2007 SP1, SP2, and R2
- Windows Server 2003 (including R2) 32-bit and 64-bit (for Mixed mode only.)

  Note • In native mode, QMX - Configuration Manager 2007 Management Point Proxy supports *only* Windows Server 2003 32-bit. (See also Native Mode Requirements.)

- Windows Server 2008 SP1 and SP2 32-bit and 64-bit; and R2
- IIS 6 or IIS 7

Configuration Manager Console Extensions

- Windows XP, Windows 7
- Windows Server 2003 (including R2) 32-bit and 64-bit support

- Windows Server 2008 SP1 and SP2 32-bit and 64-bit; and R2
- 10 MB of available hard disk space
- Display resolution of 1024x768 or greater

Agent System Requirements

Agent system minimum requirements

- Processor: 400 MHz or higher CPU
- Memory: 256 MB or more recommended

Hard drive space requirements for supported operating systems:

QMX - CONFIGURATION MANAGER 2007 AGENT REQUIREMENTS

PLATFORM	PROCESSOR	VERSION	/OPT SPACE	/VAR SPACE	INSTALL TEMP SPACE	APPROX TOTAL INSTALLED SIZE
Apple Mac OS X[5]	PPC	Server & Desktop 10.4, 10.5	190 MB	22 MB + 40 MB for longs	160 MB	250 MB
Apple Mac OS X	x86	Server & Desktop 10.4, 10.5, 10.6	190 MB	11 MB + 40 MB for logs	160 MB	250 MB
CentOS	x86 & x86-64	4, 5	80 MB	11 MB + 40 MB for logs	64 MB	130 MB
Hewlett Packard HP-UX	pa-risc	11i, 11i v2 (11.23), v3 (11.31)	190 MB	10 MB + 40 MB for logs	140 MB	240 MB
Hewlett Packard HP-UX	Itanium	v2 (11.23), v3 (11.31)	190 MB	10 MB + 40 MB for logs	140 MB	240 MB

PLATFORM	PROCESSOR	VERSION	/OPT SPACE	/VAR SPACE	INSTALL TEMP SPACE	APPROX TOTAL INSTALLED SIZE
IBM AIX	ppc/Power	5.1, 5.2, 5.3, 6.1	560 MB	10 MB + 40 MB for logs	800 MB	610 MB
Red Hat Enterprise Linux (RHEL)[5]	x86 & x86-64	AS/ES/ WS & Desktop 3.0, 4.x	80 MB	11 MB + 40 MB for logs	64 MB	130 MB
Red Hat Enterprise Linux (RHEL)	x86 & x86-64	Server & Desktop 5.x[3]	80 MB	11 MB + 40 MB for logs	64 MB	130 MB
SUSE Linux Enterprise Server (SLES)[5]	x86 & x86-64	9, 10, 11	80 MB	15 MB + 40 MB for logs	64 MB	135 MB
SUSE Novell Linux Desktop	x86 & x86-64	9	80 MB	15 MB + 40 MB for logs	64 MB	135 MB
SUSE Linux Enterprise Desktop (SLED)	x86 & x86-64	10, 11	80 MB	22 MB + 40 MB for logs	64 MB	140 MB
Sun Solaris	Sparc	8, 9, 10	240 MB	11 MB + 40 MB for logs	160 MB	300 MB
Sun Solaris	x86	9, 10	240 MB	11 MB + 40 MB for logs	160 MB	300 MB
VMware ESX[4 & 5]	x86	3.0.x, 3.5	80 MB	10 MB + 40 MB for logs	64 MB	130 MB

Notes:

Note[1]: Files in /var will grow as new policy is downloaded and data is collected, etc. Quest recommends that you allocate sufficient space to the /var filesystem to assure enough space to store package files during software distribution.

Note[2]: You can choose /tmp or another directory of your choice for temporary files. Temporary Space is used when the QMX - Configuration Manager 2007 Agent Installation Wizard installs QMX - Configuration Manager 2007 on the target client machines. **During an upgrade, Quest recommends that you triple the size of this directory until the upgrade is complete.** If you use a directory other than the /tmp directory, you must add the sticky bit to the directory.

Note[3]: The AS, ES and WS variants provided by prior releases of Red Hat Enterprise Linux are not available for version 5. Replacements for all these products are provided with version 5. (see http://www.redhat.com/rhel/ for more information.)

Note[4]: QMX - Configuration Manager 2007 supports running inside any VMware virtual machine guest operating system that is one of the supported operating systems. See the QMX - Configuration Manager 2007 Administrator's Guide for information regarding limitations to running Hardware Inventory in a virtual environment.
Note[5]: QMX - Configuration Manager 2007 no longer supports Mac OS X 10.3, or Red Hat Enterprise Linux (RHEL) 2.1.

- Minimum memory requirements for supported operating systems is 256 MB; however, increasing the memory will enhance your overall performance. Quest recommends that you allocate from 512 MB to 1 GB of memory.
- Space required for `/etc` is 1 MB for all supported platforms.

Patch Requirements:

Before you begin the installation make sure that you have the latest patches for your operating system version. The following is a list of required patch levels:

- AIX 5.1: Maintenance level 4 (5100-04) and 9
- AIX 5.2: Maintenance level 4 (5200-04)
- AIX 5.3: Maintenance level 1 (5300-01)
- HP-UX: Patch PHSS_35379
- HP-UX: Patch PHCO_35732
- Solaris 8: Patch 110934-05, 110380-04, 108993 and 111368-01

- Solaris 9 SPARC: Patch 117480, 113713-04, 112874-37 or greater, and 113319-22-1
- Solaris 9 x86: Patch 114568-24 and 114432
- Solaris 10: Patch 120664

Quest recommends that you keep each platform up to date with the recommended patch set for that platform. To get the latest patches from IBM for all versions of AIX, go to http://www-933.ibm.com/support/fixcentral/main/System+p/AIX. Standard HP-UX Patch Bundles are listed at the following link: http://docs.hp.com/en/5992-0674/ch05s02.html?jumpid=reg_R1002_USEN

For additional platform support, please contact Sales@Quest.com.

Remote Tools Requirements:

You must have an X Server running in order to launch some X-based tools. A Windows-based X Server enables the UI to show the non-Windows tools on your Windows desktop. Some choices might be StarNet X-Win32 X Window Server, a platform-independent, network-transparent windowing system that provides a client/server interface between display hardware and the desktop environments. Or, you might use Cygwin/XFree86, an open-source implementation of the X Window system. There is also a Hummingbird product.

Quest cannot provide support for any of these third-party products.

In order to use Remote Tools, you must have an X Server installed and running on the Configuration Manager Console. (See the *QMX - Configuration Manager 2007 Administrator's Guide* for more information about Remote Tools.)

Native Mode Requirements

Native mode is a new security site mode added to System Center Configuration Manager 2007 which provides a more reliable infrastructure. To run QMX - Configuration Manager 2007 in native mode there are a few additional requirements:

- System Center Configuration Manager 2007 SP1
- IIS 6 or newer configured to run 32-bit ASP.net applications.

  Note ● If you are installing the MP Proxy on Windows 2008 with IIS 7, then you must also install the "IIS 6 Management

Compatibility” component. (You cannot put IIS 7 on Windows 2003.)

- .NET framework 2.0
- Visual Studio 2005 SP1 C++ Runtime Libraries
- Management Point API
- ASP.NET

The proxy management point (MP Proxy) installer checks for .NET 2.0, Visual Studio 2005 SP1 C++ Runtime Libraries, and the MP API. If it does not detect these components, `setup.exe` downloads and installs them. Then starts a GUI version of the `mp_proxy.msi` and runs the MP Proxy installation. If you plan to perform an “unattended” MP Proxy installation, you must manually install these components first.

- BITS must be installed and enabled on the Management Point and Distribution Point servers. (See Internet Information Server for how to enable BITS.)
- WebDav must be installed and enabled on the Management Point and Distribution Point servers. (See Ensure WebDav is Installed.)

The proxy management point (MP Proxy) installer adds a new virtual directory to the default Web site and a new application pool that corresponds to the virtual directory.

See Installing the MP Proxy for more information about running QMX - Configuration Manager 2007 in native mode.

Solaris 10 Zones Support

Sun introduced Zones in Solaris 10. Zones is a partitioning technology used to virtualize operating system services and provide an isolated and secure environment for running applications. There are two types of non-global zone root file system models:

- sparse root
- whole root

The sparse-root zone model optimizes the sharing of objects while the whole-root zone model provides the maximum configurability. Additional information on Solaris 10 and Zones can be found at www.sun.com.

Solaris 10 Zones Installation Guidelines

Here are some general guidelines for installing QMX - Configuration Manager 2007 into a Solaris 10 Zones configuration:

- No QMX - Configuration Manager 2007 files can be shared between zones.
- QMX - Configuration Manager 2007 can be installed into a whole-root zone.
- QMX - Configuration Manager 2007 can be installed into a sparse-root zone provided that none of the QMX - Configuration Manager 2007 files are shared. The files are stored under the following directories:

`/opt/quest/qmxcm`

`/opt/quest/umi`

`/etc/opt/quest/qmxcm`

`/etc/opt/quest/umi`

`/var/opt/quest/qmxcm`

`/var/opt/quest/umi`

`/tmp`

- The install or upgrade process must be performed in every zone. Always use the provided script. Attempting to manually upgrade the packages will result in a non-functional installation.
- QMX - Configuration Manager 2007 requires a network interface configured for IPv4.

General Zone Guidelines

When using QMX - Configuration Manager 2007 with systems configured with Zones, be aware of the following:

- You can join sparse-root zones to Active Directory if the sparse-root zone does not share `/opt`, `/etc`, or `/var` with the Global Zone.

  Note • If you do not have the sparse-root zone configured properly, do not select the **Join Unix clients to Active Directory by using vastool** option during installation. This will cause the installation to fail.

- Some hardware inventory data is obtained by querying device files normally found in `/dev`. By default non-global zones do not have any of these devices, so QMX - Configuration Manager 2007 Agents in these zones will not report hardware inventory data on Disk Drives, SCSI Controllers, or IDE Controllers. Creating the appropriate devices will enable the collection of the data.
- When distributing software to Solaris systems with zones, you must be aware of the state of the Zone (either global or non-global zone) and how `pkgadd` is being invoked. See chapter 24 of the Sun document "*System Administration Guide: Solaris Containers-Resource Management and Solaris Zones*" (http://docs.sun.com/app/docs/doc/817-1592/6mhahuosa)

- If the QMX - Configuration Manager 2007 Agent is installed in a global zone which is later copied into a new non-global zone, the new QMX - Configuration Manager 2007 Agent will have the same unique ID as the original. To rectify this situation, run the following command as root in the new zone:

  ```
  # /opt/quest/umi/bin/owexecwql -u localhost:owipc/vmx -w
  "delete from Vintela_VMXData where Name='ClientID'"
  ```

  This command deletes the previous ID, and the QMX - Configuration Manager 2007 Agent will generate a new one.

VMware Support

There are two VMware-based virtual models: Hosted Architecture and ESX Server Architecture, also referred to as “Bare-Metal” (Hypervisor) Architecture. For more information about these models, see the following VMware datasheet: http://www.vmware.com/pdf/esx_datasheet.pdf and the VMware whitepaper: http://www.vmware.com/pdf/virtualization.pdf.

Whichever model you use, in order to perform management tasks on the complete system, you must have a QMX - Configuration Manager 2007 Agent installed on both the physical machine and on each virtual machine.

A license is required for each QMX - Configuration Manager 2007 Agent installed whether it is on a virtual or physical machine.

In both models, the QMX - Configuration Manager 2007 Agent collects data either from the virtual host or physical host depending upon where the QMX - Configuration Manager 2007 Agent is installed. If it is installed on the physical host it collects data from the physical machine and if it is installed on the virtual host it collects data from the virtual machine.

You can use Custom Inventory Collection to extend Hardware Inventory to collect additional data. (See *Associating Virtual Machines with Physical Hosts* in the *QMX - Configuration Manager 2007 Administrator’s Guide* for more information about associating virtual machines with a particular physical host.)

2

Preparing for Installation

- Preparing Configuration Manager for QMX
- Preparing the Client for QMX
- Running QMX in Native Mode

Preparing Configuration Manager for QMX

Before you attempt to install and deploy QMX - Configuration Manager 2007, make sure that your System Center Configuration Manager 2007 environment is configured properly.

Please refer to the *Known Issues* section of the Release Notes for information about concerns and limitations at the time of release.

Verify that all components in your system are properly configured and functioning correctly. The System Center Configuration Manager 2007 Site Server, Management Point, Distribution Point and all other components must be running and error free for proper functioning of QMX - Configuration Manager 2007. Make sure that all system management functions perform as intended before you introduce QMX - Configuration Manager 2007 into your environment. In addition, you must have fully functioning Windows clients in your Configuration Manager console prior to installing QMX - Configuration Manager 2007. Otherwise, Management Point, Networking, or Distribution Point problems can masquerade as QMX - Configuration Manager 2007 problems which can be difficult to diagnose and resolve.

Quest recommends that you backup your system before you start the QMX - Configuration Manager 2007 installation process.

Verify the Management Point

You must resolve problems on any of the System Center Configuration Manager 2007 Management Point components *before* installing QMX - Configuration Manager 2007. Errors in the Management Point components can cause a breakdown in communications between System Center Configuration Manager 2007 and the QMX Agent.

Check the Management Point component status in the Configuration Manager Console to verify that the System Center Configuration Manager 2007 Management Point Control Manager and other System Center Configuration Manager 2007 Management Point components are functioning correctly. In particular, it is important to verify the functionality of the Management Point components listed under the **Site Status | Component Status** section of the Configuration Manager Console.

Verify IIS and BITS Are Installed

If your System Center Configuration Manager 2007 Management Point is running Windows Server 2003, verify that Internet Information Server (IIS) is running and Background Intelligent Transfer Service (BITS) Server Extensions are properly installed and running on the Management Point Server *before* installing QMX - Configuration Manager 2007.

Internet Information Server

QMX - Configuration Manager 2007 Software Distribution requires that you have IIS installed on the Distribution Point; using a distribution point that is a server share on a machine without IIS is not supported.

ISAPI extensions are applications that run on IIS and have access to all of the functionality provided by IIS. IIS is not installed by default in Windows 2003 as it is in Windows 2000. When you install IIS, the BITS Server Extensions must be manually added to the installation.

If you are planning to run System Center Configuration Manager 2007 in native mode, the MP Proxy requires IIS 6 or newer.

Background Intelligent Transfer Service

Background Intelligent Transfer Service (or BITS) is an important part of Management Point functionality.

The BITS server component must be running on the Distribution Point server and turned on in System Center Configuration Manager 2007 for successful software distribution to the QMX Agent. This enables the QMX Agent to receive the required HTTP URL to the Distribution Point during Software Distribution. Although BITS must be turned on (per Distribution Point) inside System Center Configuration Manager 2007 for the QMX Agent to get the proper HTTP URL, the QMX Agent does not make use of BITS throttling technology during file download.

Within the Configuration Manager Console, there is an *Enable BITS* check box associated with each Distribution Point.

To turn BITS on in the Configuration Manager Console

1. Navigate to **Site Database | Site Management | <site code> - <site name> | Site Settings | Site Systems**.
2. Select the site that contains the Distribution Point.

3. Right-click **ConfigMgr distribution point** and choose **Properties**.
4. Select **Allow clients to transfer content from this distribution point using BITS, HTTP, and HTTPS (required for device clients and Internet-based clients)**.
5. Select **Allow clients to connect anonymously (Required for mobile device clients)**.

   Note ● Anonymous Connections is for mixed mode only.

6. Click **OK**.

NOTES:

- If BITS is installed and running on the Distribution Point server, and turned on in System Center Configuration Manager 2007, the QMX - Configuration Manager 2007 Software Distribution process should conclude successfully.
- BITS is dependent on IIS (Internet Information Service) and WinHTTP. Please be sure to read and follow Microsoft instructions and notes to install and configure BITS correctly.
- BITS is not installed by default with Windows 2000 Server. It may be necessary to download and install BITS on Windows 2000 Servers designated as Distribution Points for QMX Agents.
- If you plan to run QMX in native mode, you must install and enable BITS on the Management Point and Distribution Point servers.

Ensure WebDav is Installed

Web-based Distributed Authoring and Versioning (WebDAV) is required for the management point and distribution point site system roles and must be enabled on the Distribution Point for successful Software Distribution and for the successful recursive search of any subdirectories within the base HTTP URL returned by BITS. Ensure that WebDav is installed, running, and properly configured on the Distribution Point Server.

If you plan to run QMX in native mode, you must install WebDav on the Management Point servers, as well.

The WebDAV component is not included in Windows Server 2008 operating system. You must download, install, and configure WebDAV manually on BITS-enabled distribution points running Windows Server 2008. For more information, see "How to Configure Windows Server 2008 for Site System Roles" at:
http://technet.microsoft.com/en-us/library/cc431377(printer).aspx

Ensure Site Security Rights

System administrators must have the correct security rights in order to run the Software Distribution Wizard to create packages, programs, and advertisements or to run Remote Tools. QMX - Configuration Manager 2007 applies standard System Center Configuration Manager 2007 security rights, so a System Center Configuration Manager 2007 user must have at least “read” access to the Site Control file.

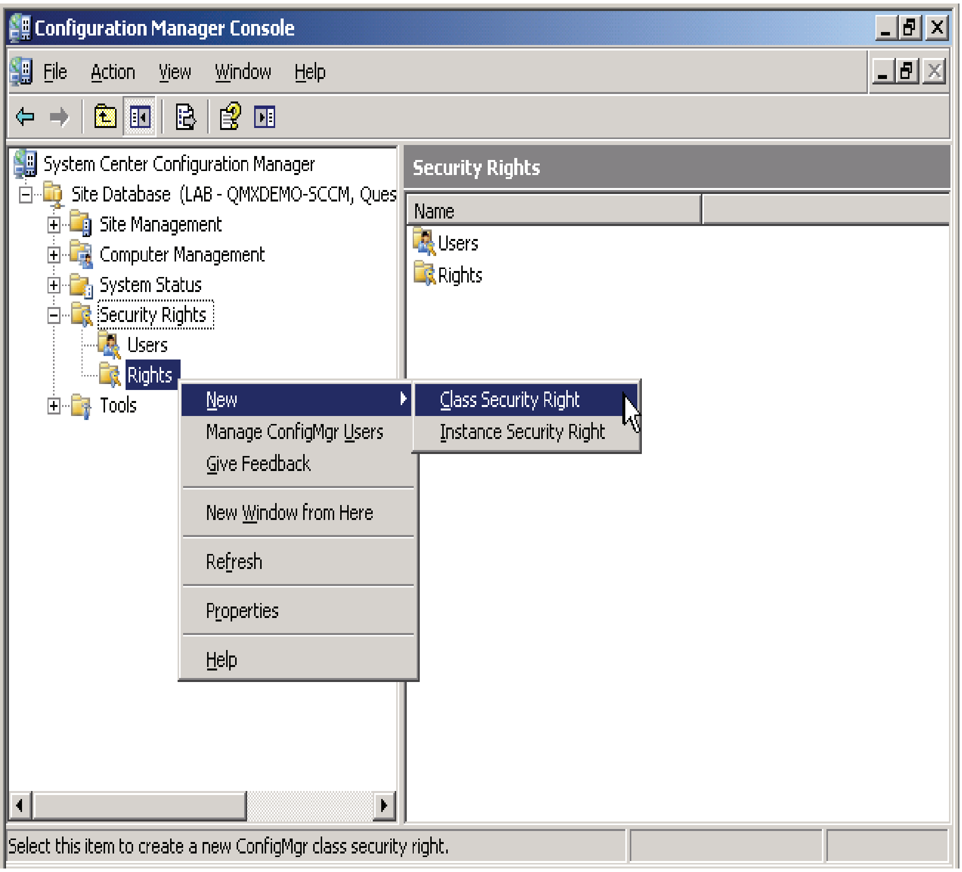
QMX - Configuration Manager 2007 supports System Center Configuration Manager 2007 permissions and security for site databases without any changes to the normal functionality. You can assign specific permissions to Users and Groups, just as you would with System Center Configuration Manager 2007.

There are two ways to assign permissions: through the *Collections Properties* dialog or through Security Rights.

To set user rights

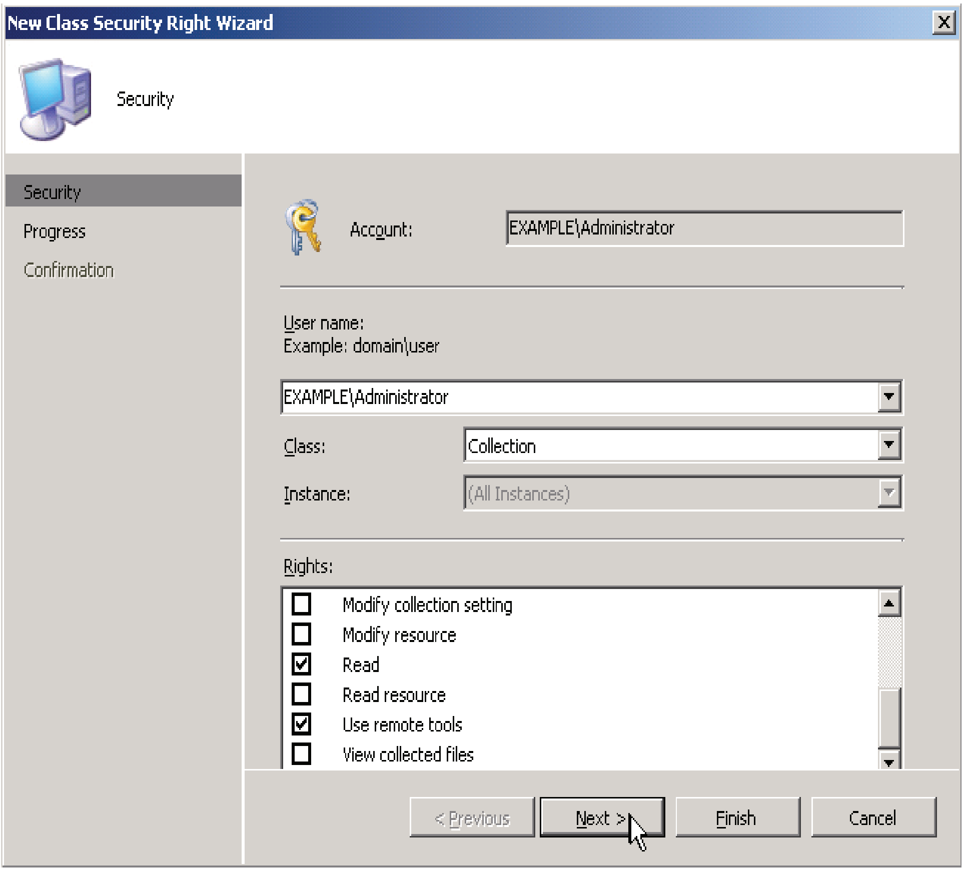
1. In the Configuration Manager Console, navigate to **System Center Configuration Manager | Site Database**.

2. Expand **Security Rights**.



Select this item to create a new ConfigMgr class security right.

3. Right-click **Rights** and choose **New | Class Security Right**.



Account: EXAMPLE\Administrator

User name:
Example: domain\user

EXAMPLE\Administrator

Class: Collection

Instance: (All Instances)

Rights:

- □ Modify collection setting
- □ Modify resource
- ☑ Read
- □ Read resource
- ☑ Use remote tools
- □ View collected files

4. Enter the **User name**.
5. Select the **Class**.
6. Check the **Read** Rights.

   Note ● You must have at least "read" access to the Site Control file. Select other Permissions, as needed.

7. Click **Next**.

   System Center Configuration Manager 2007 adds the new name, class, instance and permissions for that user.

For more information about System Center Configuration Manager 2007 Object Security, see *How to Assign Rights for Objects to Users and Groups* at: http://technet.microsoft.com/en-us/library/bb680648.aspx

Preparing the Client for QMX

Before you install the QMX - Configuration Manager 2007 Agent, verify the following:

- Ensure Site Codes Resolve to a Primary Site
- Verify the Site Code
- Verify Firewalls
- Ensure SSH Access and Root Privileges
- Ensure that the SSH Server is Running
- Verify the Port Number
- Resolve Hostnames
- Prepare Installation Files for Install
- Supply the Trusted Root Key

Ensure Site Codes Resolve to a Primary Site

Site codes for QMX Agent clients must resolve to a Primary Site. Do not use Secondary Sites for client Site Codes when installing the QMX Agent. If you enter a Secondary Site site code during the QMX Agent installation, the client does not display correctly in the Configuration Manager Console.

If you manage a client from a Secondary Site, enter the site code from the Parent Site when the install process requests it.

For example, imagine this simple System Center Configuration Manager 2007 configuration:

- Primary Site name = STORE, site code = ST1
- Secondary Site: name = DEPT, site code = DT1
- Secondary Site's management point = DT1MP1
- Client (managed from DT1MP1)

If you manage the client from the secondary site (DT1) using the secondary site’s management point (DT1MP1), enter the following values for Site Code and Management Point when installing the QMX Agent:

- Site Code: **ST1** (the Parent Site’s site code)
- Management Point: **DT1MP1** (the Secondary Site's management point)

Alternatively, if you manage a QMX Agent client from a Primary Site, enter the site code from that primary site when the install process requests it.

Consider the following System Center Configuration Manager 2007 configuration:

- Primary Site site code = PS1
- Primary Site's management point = PS1MP1
- Client (managed from PS1MP1)

The site code and management point entries to set during QMX Agent installation for this configuration would be:

- Site Code: **PS1** (The Primary Site's site code)
- Management Point: **PS1MP1** (Primary Site's management point)

Verify the Site Code

To verify the site code entered during the QMX Agent Installation

1. Open `qmxcm.conf`, the QMX Agent configuration file and look for the Site Code setting, as follows:
2. In a command window, enter:

   ```
   cd /etc/opt/quest/qmxcm
   ```

3. To display the contents of the configuration file on the screen, enter:

   ```
   more qmxcm.conf
   ```

4. Look for the value associated with `qmxcm.site_code` and verify it with the System Administrator.
5. If the Site Code in this file is NOT correct, you must change it.

   Note • You can change the site code directly in the `qmxcm.conf` file, but it is easier and less risky to use the `clienttool`, as shown in the next procedure.

To change the client's Site Code setting

1. In a command window, enter:

   ```
   /opt/quest/qmxcm/bin/clienttool --set-site-code <arg>
   ```

   No restart is necessary.

Verify Firewalls

The existence of a firewall between the QMX Agent and System Center Configuration Manager 2007 Sites could be a source of problems if the respective ports are not opened to communication between them; the QMX Agent uses the following ports:

- TCP 22 (SSH port): This port is used by the QMX - Configuration Manager 2007 Agent Installation Wizard to setup the clients remotely from the Configuration Manager Console. Remote Tools and the Policy Spy also use this port. This type of connection is initiated on the Configuration Manager Console side, however, the SSH port only needs to be open on the client's firewall.
- TCP 80 (HTTP port): This port is used for all communication between QMX Agent and System Center Configuration Manager 2007 Site Servers once the QMX Agent has been installed. This type of connection is initiated from the QMX Agent.

  Note: By default the QMX Agent uses port 80 to communicate with the Management Point and Distribution Point. However, it is possible to change the port that System Center Configuration Manager 2007 uses to handle requests. (See Verify the Port Number for more information.)
- TCP 464 and UDP 88 (vastool join): Use these ports if you plan to install the QMX Agent with the wizard (see Installing the Agent with the Wizard) and wish to join the QMX Agents to Active Directory (see Active Directory Settings).
- UDP 389 and UDP 123 (vastool timesync): Use these ports if you plan to install the QMX Agent with the wizard and wish to synchronize the clocks of both systems (see Active Directory Settings).

You must add rules to the firewall to open the communication between the QMX Agent and System Center Configuration Manager 2007. Please refer to your firewall documentation to accomplish this task.

Ensure SSH Access and Root Privileges

To deploy the QMX Agent using the QMX - Configuration Manager 2007 Agent Installation Wizard, you need Secure Shell (SSH) access and root privileges using either sudo or su or by using a user account that has root permissions. You must ensure that root can execute all the files in the QMX - Configuration Manager 2007 source folders.

You must have root privileges to run the install script either by means of `sudo` or `su` or by using a user account that has root permissions. If you do not have root privileges you will not be able to install QMX - Configuration Manager 2007 successfully.

If you are installing as a sudo user, you need to make sure you have access to the `/tmp` directory. If you have set up a different directory other than `/tmp`, make sure you have root privileges to it and that the sticky bit is set.

Ensure that the SSH Server is Running

The QMX - Configuration Manager 2007 Agent Installation Wizard makes use of Secure Shell (SSH) for security when installing the QMX Agent. You must have the SSH Daemon running on the target systems.

You must have the SSH daemon running on the systems. However, SSH is only installed by default on Solaris 9 (or higher), Mac, Red Hat Linux, and SUSE Linux. You must manually install SSH on AIX, HP-UX, and older versions of Solaris clients manually. While Mac comes with SSH, you need to enable it because it is turned off by default. See Enable SSH on Target Mac OS X Computers.

Enable SSH on Target Mac OS X Computers

When using the QMX - Configuration Manager 2007 Agent Installation Wizard to install the QMX Agent on Mac OS X machines, you need to enable SSH on the target Macintosh machine(s). In previous versions of QMX - Configuration Manager 2007, root access had to be enabled as well, but the QMX - Configuration Manager 2007 Agent Installation Wizard can now make use of sudo, thus eliminating the need to enable root on your Macintosh.

To enable SSH on the target Mac OS X machines

1. Navigate to **System Preferences | Sharing | Remote Login** (select **Remote Login**).

2. When the QMX - Configuration Manager 2007 Agent Installation Wizard has successfully installed the QMX Agent on your Mac OS X machine, in the Configuration Manager Console, trigger an **Update collection membership** and a **Refresh Collection** on the Macintosh collection to see the new clients in the Configuration Manager Console.
3. Install the provided Collections and Queries before installing the QMX Agent. If you have not installed these (or created your own), the Macintosh client appears only in the “All Systems” collection.

Verify the Port Number

By default the QMX Agent uses port 80 to communicate with the Management Point and Distribution Point. However, it is possible to change the port that System Center Configuration Manager 2007 uses to handle requests.

Ensure your firewall is not blocking the port.

The default is port 80, and this is also the default port for the QMX Agent. If you have changed your System Center Configuration Manager 2007 port to something else (for example, port 8088) then you will need to tell the QMX Agent to use port 8088 as well.

If you install the client manually using `install_client.sh` (the QMX Agent installation script) you can use the `-p` option to set the port number.

To change the client’s Management Point Port setting

1. In a command window, enter:

   ```
   /opt/quest/qmxcm/bin/clienttool --set-mp <arg>
   ```

   No restart is necessary.

   This changes the `qmxcm.mpe.port=<arg>` line in the `qmxcm.conf` file.

Resolve Hostnames

Before you attempt to install the QMX Agent onto your non-Windows systems, make sure the hostnames of the System Center Configuration Manager 2007 Management Point and Distribution Point resolve from the intended QMX Agent system as well as from the Server. The System Center Configuration Manager

2007 Server and the QMX Agent must be able to communicate both directions by means of the hostname, not IP address. The managed client system must be able to ping the Management Point and the Distribution Point by using the Fully Qualified Domain Name (FDQN) and the Management Point and the Distribution Point must be able to resolve the managed client system through DNS.

To test network name resolution, ping the following

- The IP address of the server that is your System Center Configuration Manager 2007 Management Point.
- The hostname of the server that is your System Center Configuration Manager 2007 Management Point.
- The Fully Qualified Domain Name (for example, `server.example.com`) of the server that is your System Center Configuration Manager 2007 Management Point.
- Do the same for the Distribution Point.

It is not sufficient to test a one-way ping from your Windows Systems. In many cases the ping will work from one direction and not the other. You must verify that the intended host system can successfully ping both the System Center Configuration Manager 2007 Management Point hostname and the Distribution Point hostname.

If any of the pings fail, you must resolve the problem of network hostname resolution *before* attempting the install. You may need to make entries on your DNS server, or perhaps even entries in your local `/etc/hosts` file.

To verify Management Point and QMX Agent Communication

From the Management Point Server:

1. Go to **Start | Administrative tools | Internet Information Services (IIS) Manager**.
2. Expand the *Web Sites* directory.
3. Right click *Default Web Site* and select **Properties**.
4. On the *Web Site* tab, select the *TCP Port* setting. (The default setting is 80)
5. Go to the QMX Agent and verify the port number that the client uses for communication with the Management Point and Distribution Points by opening the following configuration file:

   ```
   /etc/opt/quest/qmxcm/qmxcm.conf
   ```

   Verify that `qmxcm.mpe.port=80`.

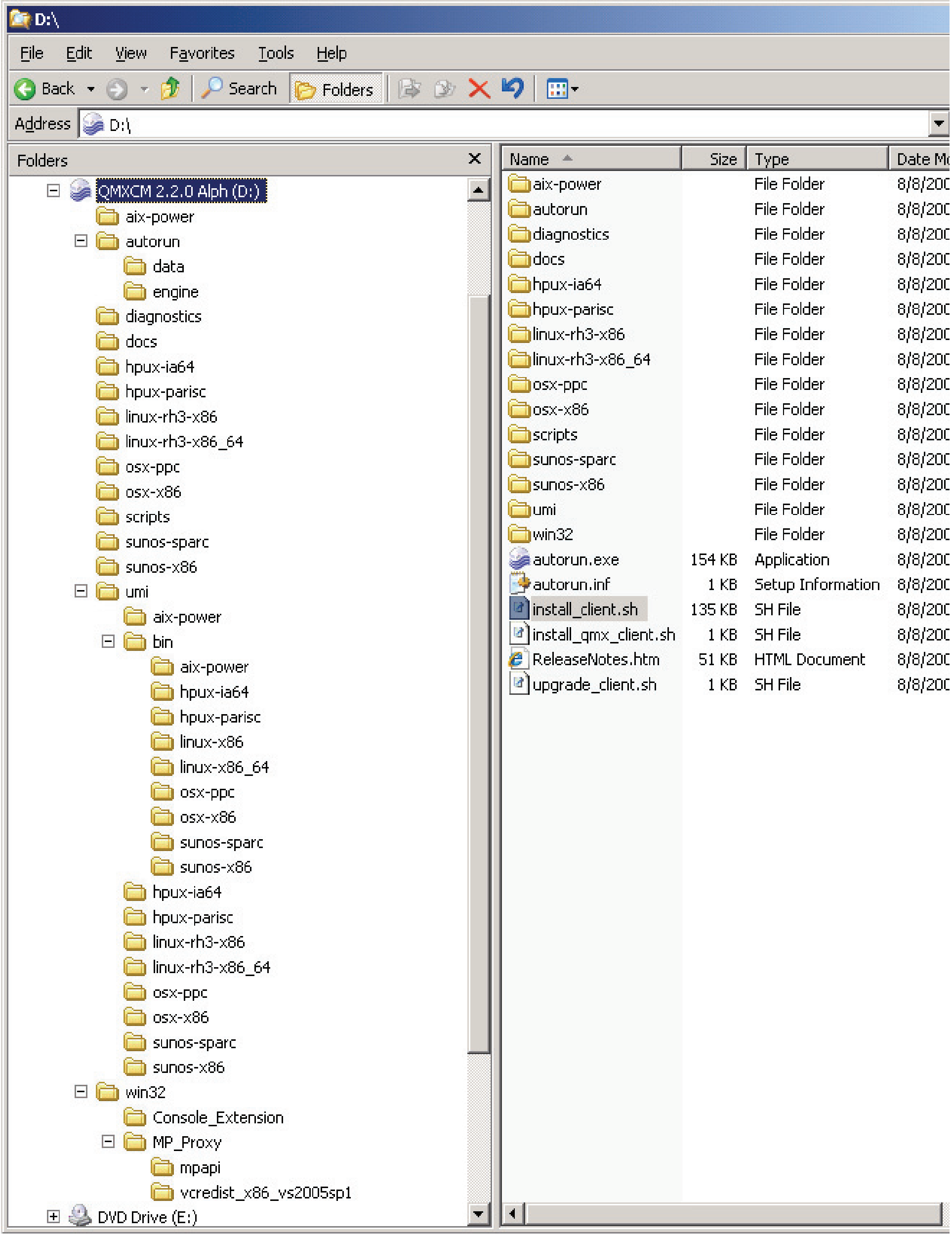
   If this setting is incorrect, use the `clienttool` to change it. (See *Using clienttool to Change the Site Settings*.)

Prepare Installation Files for Install

To save bandwidth for the software distribution, you can optionally copy only the platform-specific files that you need to a convenient location on your system; that is, you can create a directory containing only the upgrade script and the directories for your operating system platform. If you opt to do this, however, it is important to know that the installation script expects to find certain files in specific locations, so you must be careful to maintain the directory structure.

Because the QMX - Configuration Manager 2007 Software Distribution Wizard must have write access to the Source Directory, if you plan to use the wizard to install the QMX Agent, you *must* copy the installation files from the distribution media to your hard drive as described in this section.

The `install_client.sh` and the `upgrade_client.sh` scripts are at the root of the product distribution CD. Under that are folders for the individual operating systems. You must also copy `umi` folder and the individual operating system folders under `umi`, as well as the `bin` folder and the individual operating system folders under `bin`:



```
QMXCM 2.2.0 Alph (D:)
    aix-power
    autorun
        data
        engine
    diagnostics
    docs
    hpux-ia64
    hpux-parisc
    linux-rh3-x86
    linux-rh3-x86_64
    osx-ppc
    osx-x86
    scripts
    sunos-sparc
    sunos-x86
    umi
        aix-power
        bin
            aix-power
            hpux-ia64
            hpux-parisc
            linux-x86
            linux-x86_64
            osx-ppc
            osx-x86
            sunos-sparc
            sunos-x86
        hpux-ia64
        hpux-parisc
        linux-rh3-x86
        linux-rh3-x86_64
        osx-ppc
        osx-x86
        sunos-sparc
        sunos-x86
    win32
        Console_Extension
        MP_Proxy
            mpapi
            vcredist_x86_vs2005sp1
DVD Drive (E:)
```

Name	Size	Type	Date Mo
aix-power		File Folder	8/8/200
autorun		File Folder	8/8/200
diagnostics		File Folder	8/8/200
docs		File Folder	8/8/200
hpux-ia64		File Folder	8/8/200
hpux-parisc		File Folder	8/8/200
linux-rh3-x86		File Folder	8/8/200
linux-rh3-x86_64		File Folder	8/8/200
osx-ppc		File Folder	8/8/200
osx-x86		File Folder	8/8/200
scripts		File Folder	8/8/200
sunos-sparc		File Folder	8/8/200
sunos-x86		File Folder	8/8/200
umi		File Folder	8/8/200
win32		File Folder	8/8/200
autorun.exe	154 KB	Application	8/8/200
autorun.inf	1 KB	Setup Information	8/8/200
install_client.sh	135 KB	SH File	8/8/200
install_qmx_client.sh	1 KB	SH File	8/8/200
ReleaseNotes.htm	51 KB	HTML Document	8/8/200
upgrade_client.sh	1 KB	SH File	8/8/200

To prepare installation files for manual install

1. Copy the entire content of the distribution CD over to your hard drive and delete all the platform-specific folders that you are NOT interested in, leaving the directory structure intact.

Supply the Trusted Root Key

QMX Agents installed with the QMX - Configuration Manager 2007 Agent Installation Wizard automatically receive the Trusted Root Key (TRK) and the Management Point certificates; no additional action for security is required. The wizard obtains the TRK from System Center Configuration Manager 2007 and passes it to the install script automatically and securely.

If you are installing QMX - Configuration Manager 2007 2.2 for the first time manually, you can supply the Trusted Root Key (TRK) on the command line to the QMX Agent upgrade or installation script.

To install the TRK manually

1. Enter the following at the command line:

   ```
   ./install_client.sh -s SITE_CODE -m MP_ADDRESS -trk TRK_VALUE
   ```

   – OR –

   You can use the `-trkfile` option, as follows:

   ```
   ./install_client.sh -s SITE_CODE -m MP_ADDRESS -trkfile
   /SOME/PATH/TO/TRK/FILE
   ```

If you do not supply the TRK, the QMX Agent will have to download it by means of HTTP in a potentially insecure manner.

Note: For more information, see Supplying the Trusted Root Key.

Further Information about TRKs

For more information about the Trusted Root Keys, refer to the Introduction of the *QMX - Configuration Manager 2007 Administrator's Guide*.

Running QMX in Native Mode

If you plan to run QMX - Configuration Manager 2007 with System Center Configuration Manager 2007 in native mode, there are many Microsoft-specific tasks you must do to get your Windows environment ready. Please refer to the Microsoft documentation about how to set up native mode. (For example, these links might be helpful:
http://technet.microsoft.com/en-us/library/bb680464.aspx or
http://technet.microsoft.com/en-us/library/bb633203.aspx, or
http://technet.microsoft.com/en-us/library/bb680986.aspx.)

Quest recommends that you ensure your System Center Configuration Manager 2007 system is running properly in native mode before introducing QMX - Configuration Manager 2007. In addition, Quest recommends that you have a fully functioning Windows client in your Configuration Manager Console prior to installing QMX - Configuration Manager 2007. Otherwise, Management Point, Networking, or Distribution Point problems can masquerade as QMX - Configuration Manager 2007 problems which can be difficult to diagnose and resolve.

Before you install QMX - Configuration Manager 2007 into a native mode environment, ensure the computer hosting the MP Proxy meets the required prerequisites. (See Native Mode Requirements.)

You must install the MP Proxy before you install the QMX Agent. (See Installing the MP Proxy for details.)

3

Installing the MP Proxy

- About Native Mode
- About the Proxy Management Point
- Preparing a Native Mode Environment for QMX
- Switching from Mixed to Native Mode
- Troubleshooting the MP Proxy

***Note**: If you are not installing QMX - Configuration Manager 2007 into a native mode environment, you can skip this chapter. If you are installing QMX - Configuration Manager 2007 into a native mode environment, you must install the MP Proxy before you install QMX - Configuration Manager 2007.*

About Native Mode

Native mode is a new security site mode added to System Center Configuration Manager 2007 which provides a more reliable infrastructure. QMX - Configuration Manager 2007 2.2 has designed the Agent to work in native mode.

About the Proxy Management Point

When running System Center Configuration Manager 2007 in mixed mode the QMX - Configuration Manager 2007 Agent communicates directly to the management point. But when running System Center Configuration Manager 2007 in native mode, the QMX - Configuration Manager 2007 Agent communicates to the management point proxy (*MP Proxy*). Thus, before you install QMX - Configuration Manager 2007 into a native mode environment, you must install the MP Proxy on the management point *before* you install the QMX Agent.

You can not install the MP Proxy on a Windows 2003 x64 system. Thus, you must configure IIS to run 32-bit applications.

The MP Proxy uses the System Center Configuration Manager 2007 Management Point API to communicate to and from the management point on behalf of the Agent. You configure the Agents to send information about inventory data, discovery data, and status messages to the MP Proxy. The MP Proxy forwards the client information to the management point. The MP Proxy communicates to the management point by means of DCOM in either mixed or native mode.

If the site is in mixed mode, the data is not encrypted and the MP Proxy does not authenticate the management point. If the site is in native mode, it does mutual authentication and the traffic is encrypted.

The QMX Agent is designed to automatically discover the method of communication every time it contacts System Center Configuration Manager 2007. The QMX Agent checks for these three methods of communication in this order:

1. Communicating with the MP Proxy with SSL using https (see Enable SSL in IIS for requirements)
2. Talking to the MP Proxy without SSL using http
3. Talking directly to the System Center Configuration Manager 2007 Management Point

If IIS is configured with SSL, the Agent will authenticate to the MP Proxy and use encryption; conversely, if IIS is not configured with SSL, the Agent will not authenticate to the MP Proxy and will not encrypt the traffic. That is, if SSL is enabled for the Web site, the Agent uses https instead of plain http to communicate to the MP Proxy.

Preparing a Native Mode Environment for QMX

Once you have System Center Configuration Manager 2007 running successfully in native mode, these are the steps you must take to prepare your environment for QMX - Configuration Manager 2007:

To prepare a native mode environment for QMX

1. Ensure the computer hosting the MP Proxy meets the required prerequisites (see Native Mode Requirements.)
2. Create and deploy required PKI certificates. (See PKI Certificate Requirements for Native Mode.)
3. Install the MP Proxy. (See Install the MP Proxy.)

Once you have created the PKI Certificates and installed the MP Proxy on the Management Point server, you are ready to install the QMX components:

1. Install or Upgrade the QMX Configuration Manager Console extensions. (See either Installing the Console Extensions or Upgrading the Console Extensions.)
2. Install or Upgrade your QMX Agents.

   a) Use *Non-Windows Agent Push Installation* wizard if you are installing the Agent for the first time. (See Installing the Agent with the Wizard.)

   Note • When the wizard asks you to enter the Management Point on the *Agent Installer Settings* dialog, be sure to give it the MP Proxy name and port number.

   b) Use *QMX - Configuration Manager 2007 Software Distribution Wizard* if you are upgrading an existing Agent from an earlier version. (See Upgrading the Agent or Upgrading the Client.)

PKI Certificate Requirements for Native Mode

System Center Configuration Manager 2007 requires three types of PKI certificates for native mode:

CERTIFICATE REQUIREMENT	CERTIFICATE DESCRIPTION
site server signing certificate	Installed on the System Center Configuration Manager 2007 site server; used to sign client policies.
ISV Proxy certificate	Installed on MP Proxy computers; used to authenticate the MP Proxy to site systems.
Web server certificate	Installed on System Center Configuration Manager 2007 site systems servers with roles such as the management point and distribution point; used to encrypt data and authenticate the server to clients.

Note: The site server signing certificate is an System Center Configuration Manager 2007 certificate. It is not part of QMX - Configuration Manager 2007; it is set up automatically when you setup System Center Configuration Manager 2007 in Native Mode. You only have to create and deploy the ISV Proxy certificate. You must have this certificate in place before QMX - Configuration Manager 2007 can operate in native mode.

It is not within the scope of this guide to document how to create and issue certificates. Quest recommends that you follow Microsoft's step-by-steps directions for creating and deploying the public key infrastructure (PKI) Certificates that System Center Configuration Manager 2007 requires to operating in native mode on a Windows Server 2008 (see http://technet.microsoft.com/en-us/library/bb680312.aspx.) Quest assumes that you can properly set up native mode in System Center Configuration Manager 2007. However, the following sections will draw your attention to important caveats.

Deploying ISV Proxy Certificates

System Center Configuration Manager 2007 requires that the MP Proxy has a certificate that is signed by the same certificate authority that is the root of the System Center Configuration Manager 2007 site server's certificate chain. During the MP Proxy installation process you are prompted to select a management point certificate from the Local Machine - Personal certificate store.

Do not use the wizard in IIS to generate the certificate.

There is no built-in certificate template that is sufficient, so you must create a custom template that adheres to the following custom certificate template requirements.

The following steps assume you are deploying the MP Proxy certificate on a Windows 2003 Server. If you are on a Windows 2008 Server, the steps may vary slightly.

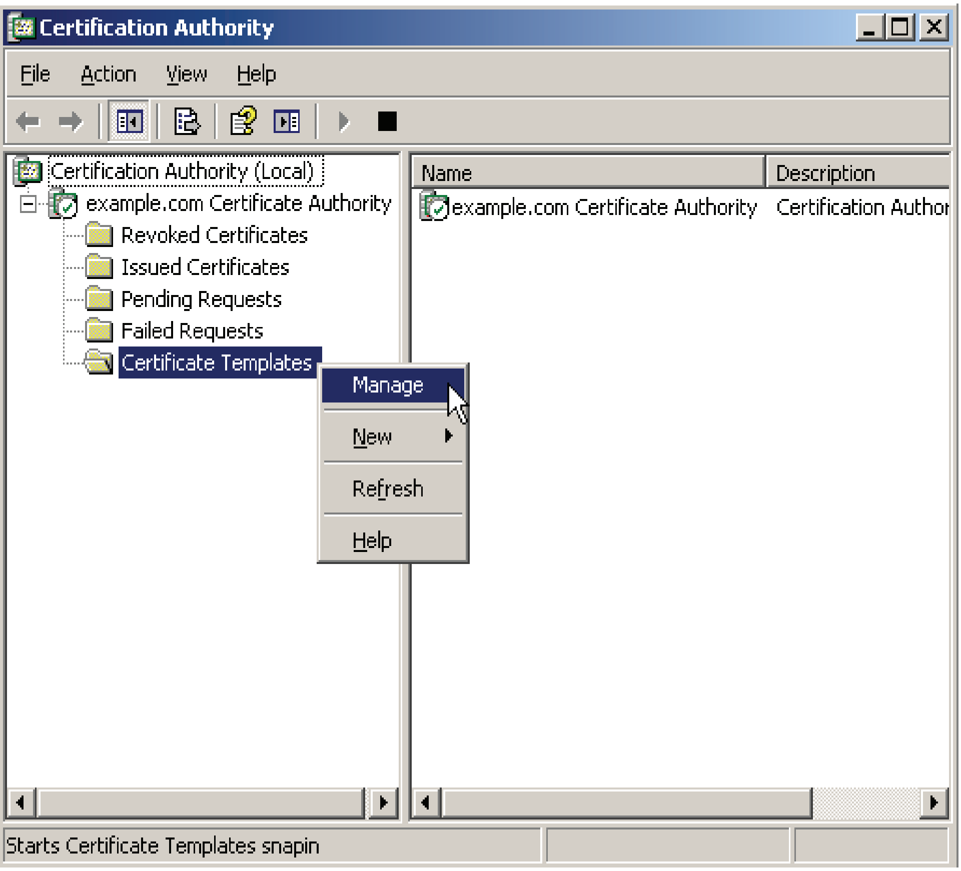
These are the high level steps for creating and deploying the MP Proxy Certificates:

- Creating the MP Proxy Certificate
- Issuing the MP Proxy Template
- Creating the Certificate Store
- Requesting the MP Proxy Certificate
- Exporting the MP Proxy Certificate
- Registering the MP Proxy Certificates

Creating the MP Proxy Certificate

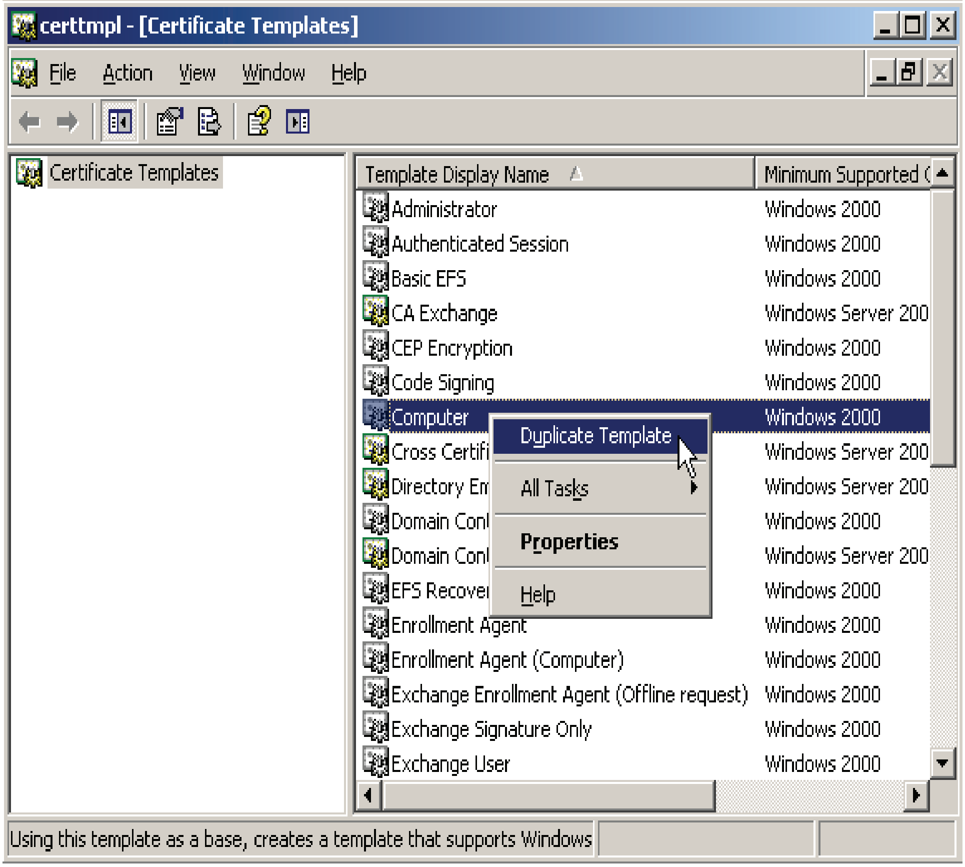
To create the MP Proxy Certificate

1. To open the certificate authority, from the Windows Desktop, navigate to **Start | Administrative Tools | Certification Authority**.
2. Expand the domain's **Certification Authority** server node.



Starts Certificate Templates snapin

3. Right-click the **Certificate Templates** folder and select **Manage** to view available templates.



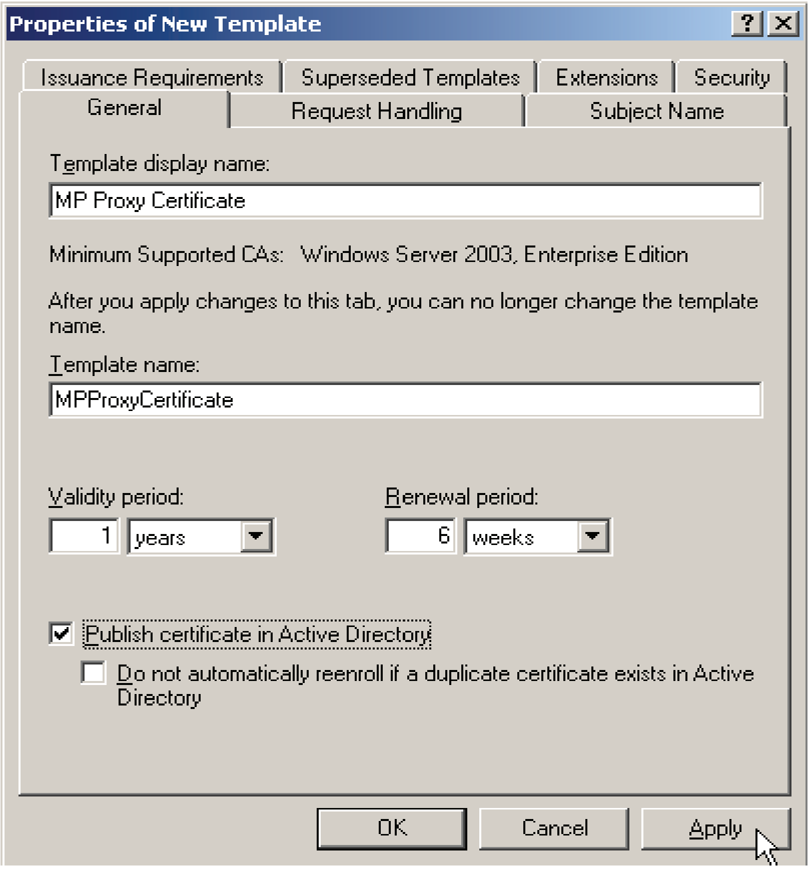
Template Display Name	Minimum Supported (
Administrator	Windows 2000
Authenticated Session	Windows 2000
Basic EFS	Windows 2000
CA Exchange	Windows Server 200
CEP Encryption	Windows 2000
Code Signing	Windows 2000
Computer	Windows 2000
Cross Certifi	Windows Server 200
Directory Em	Windows Server 200
Domain Cont	Windows 2000
Domain Cont	Windows Server 200
EFS Recover	Windows 2000
Enrollment Agent	Windows 2000
Enrollment Agent (Computer)	Windows 2000
Exchange Enrollment Agent (Offline request)	Windows 2000
Exchange Signature Only	Windows 2000
Exchange User	Windows 2000

Using this template as a base, creates a template that supports Windows

4. Right-click the **Computer** template and select the **Duplicate Template** option to open the *Properties of New Template* dialog.

Note ● If your Certificate Authority is on a Windows 2008 Server, a *Duplicate Template* dialog asks you to "select the version of Windows Server (minimum supported CAs) for the duplicate certificate template". Select **Windows 2003 Server, Enterprise Edition**. Do not select Windows 2008 Server, Enterprise Edition.

5. In the *General* tab:



Properties of New Template

Template display name: MP Proxy Certificate

Minimum Supported CAs: Windows Server 2003, Enterprise Edition

After you apply changes to this tab, you can no longer change the template name.

Template name: MPProxyCertificate

Validity period: 1 years

Renewal period: 6 weeks

☑ Publish certificate in Active Directory

□ Do not automatically reenroll if a duplicate certificate exists in Active Directory

a) Enter ***MP Proxy Certificate*** in the *Template display name* box.

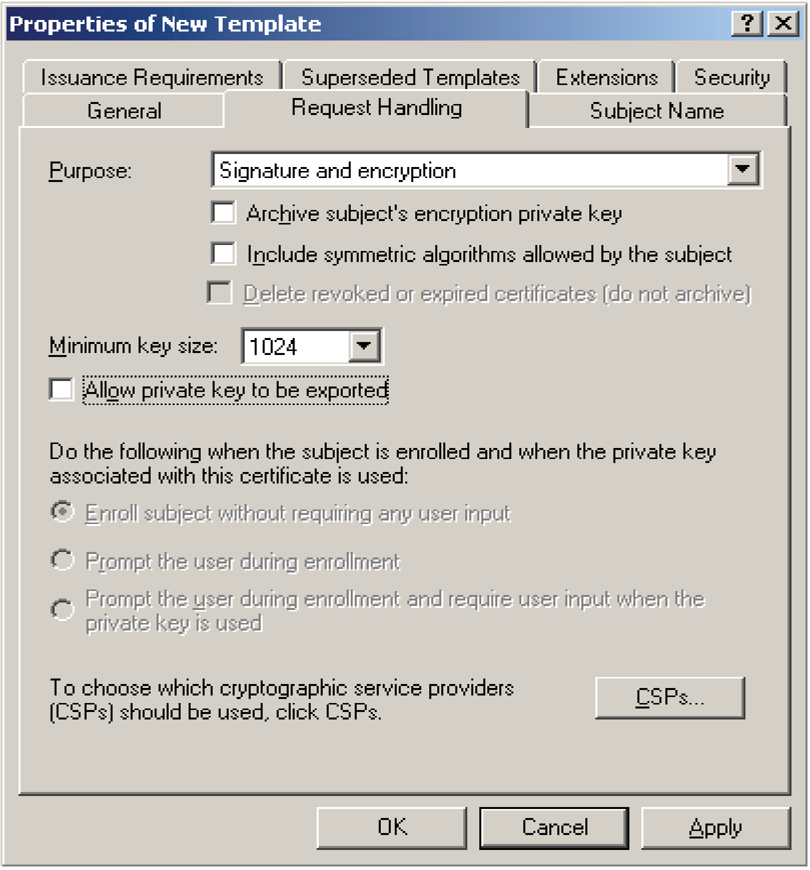
b) Enter ***MPProxyCertificate*** in the *Template name* box.

c) Enter any value in the *Validity period* fields.

d) Select the **Publish certificate in Active Directory** option.

e) Click **Apply**.

6. In the *Request Handling* tab:



Purpose: Signature and encryption

□ Archive subject's encryption private key

□ Include symmetric algorithms allowed by the subject

□ Delete revoked or expired certificates (do not archive)

Minimum key size: 1024

□ Allow private key to be exported

Do the following when the subject is enrolled and when the private key associated with this certificate is used:

● Enroll subject without requiring any user input

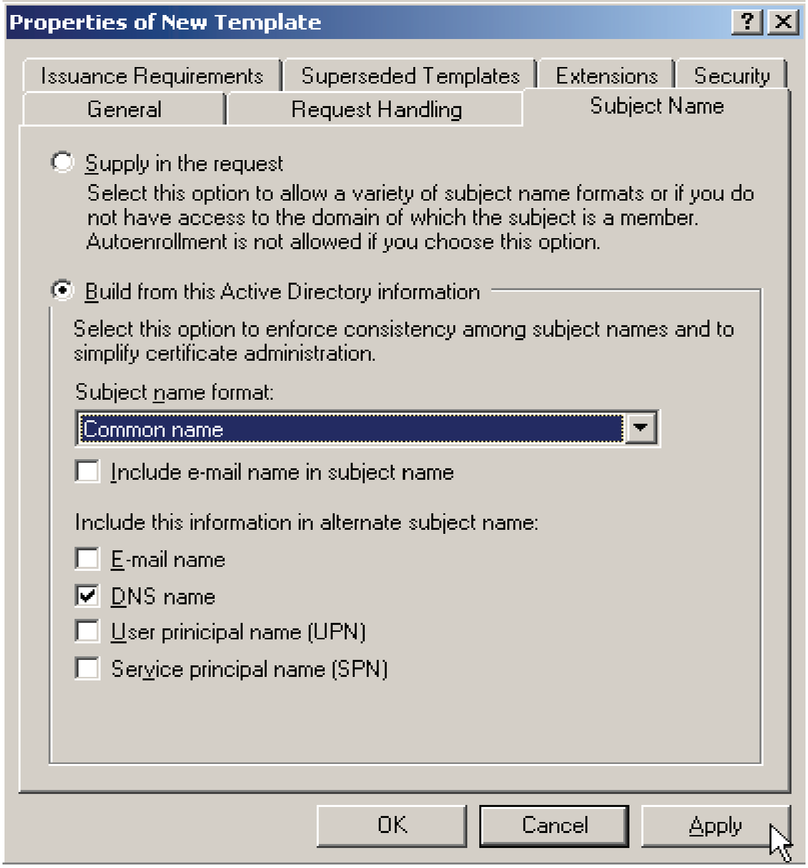
○ Prompt the user during enrollment

○ Prompt the user during enrollment and require user input when the private key is used

To choose which cryptographic service providers (CSPs) should be used, click CSPs.

a) Ensure the **Allow Private Key to be exported** option is not selected.

7. In the *Subject Name* tab:



○ Supply in the request

Select this option to allow a variety of subject name formats or if you do not have access to the domain of which the subject is a member. Autoenrollment is not allowed if you choose this option.

● Build from this Active Directory information

Select this option to enforce consistency among subject names and to simplify certificate administration.

Subject name format: Common name

□ Include e-mail name in subject name

Include this information in alternate subject name:

□ E-mail name

☑ DNS name

□ User prinicipal name (UPN)

□ Service principal name (SPN)

a) Select the **Build from this Active Directory information** option.

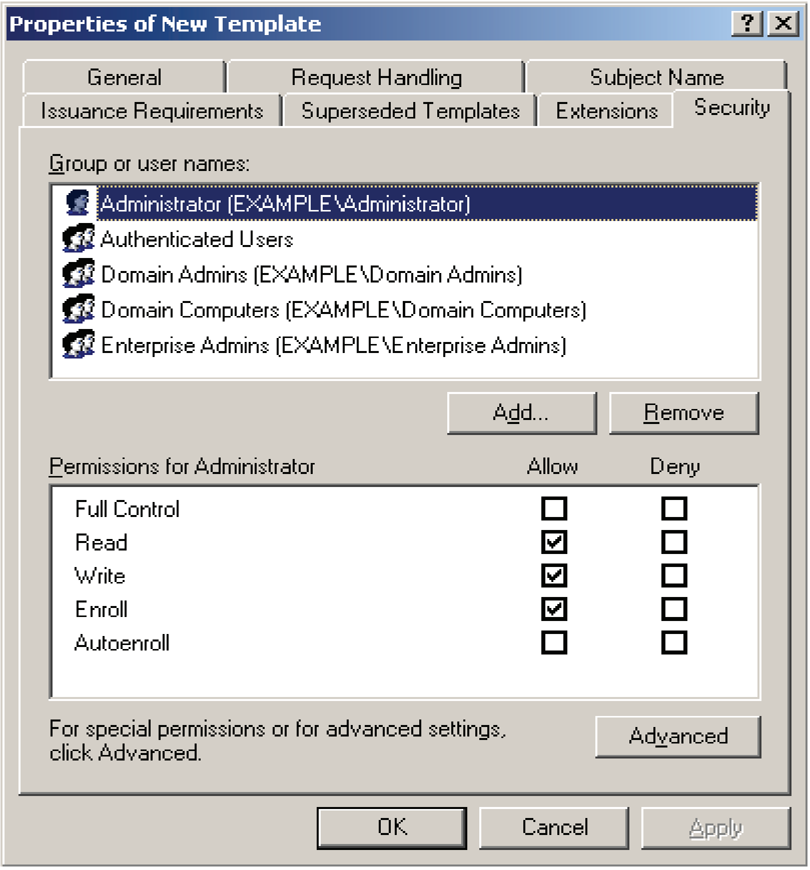
b) From the *Subject name format* drop down menu, choose **Common Name**.

c) Under *Include this information in alternate subject name*,

- Select the **DNS name** option.
  Note: This ensures that the *Subject Name* contains the hostname of the machine where you are installing the MP Proxy.
- Clear the **User principal name (UPN)** option.

d) Click **Apply**.

8. In the *Security* tab:



Group or user names:

- Administrator (EXAMPLE\Administrator)
- Authenticated Users
- Domain Admins (EXAMPLE\Domain Admins)
- Domain Computers (EXAMPLE\Domain Computers)
- Enterprise Admins (EXAMPLE\Enterprise Admins)

Permissions for Administrator	Allow	Deny
Full Control	□	□
Read	☑	□
Write	☑	□
Enroll	☑	□
Autoenroll	□	□

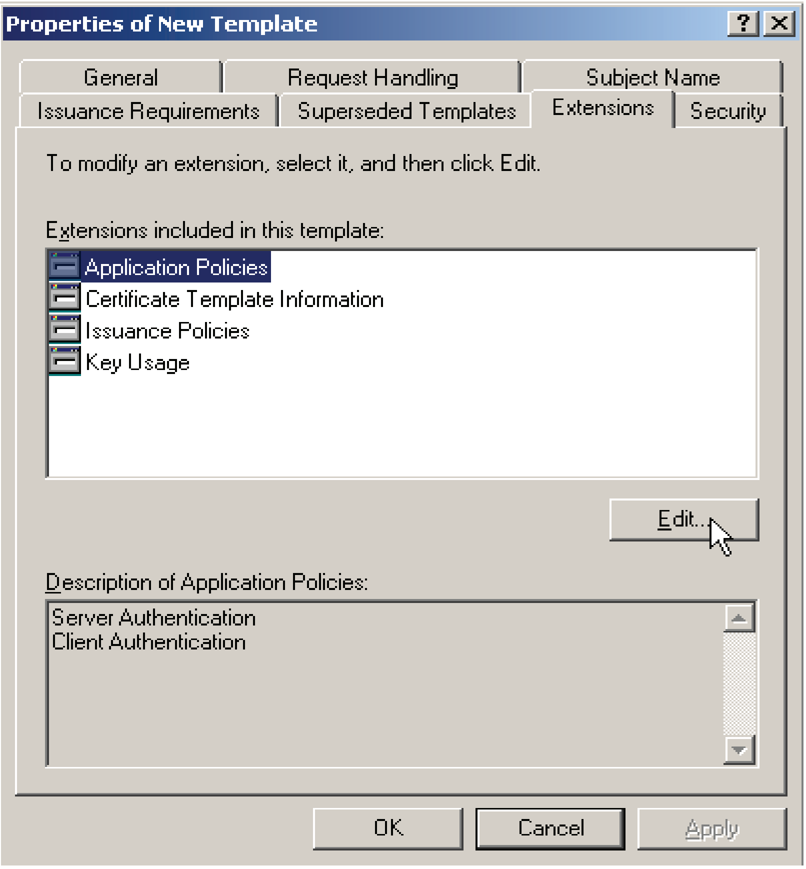
For special permissions or for advanced settings, click Advanced.

a) Set **Read**, **Write**, and **Enroll** Permissions for:

- Authenticated Users
- Administrator
- Domain Admins
- Enterprise Admins

Note ● In order to issue a certificate based on the template, the user running the MP Proxy must have **Enroll** permission for the template.

9. In the *Extensions* tab:



Properties of New Template

To modify an extension, select it, and then click Edit.

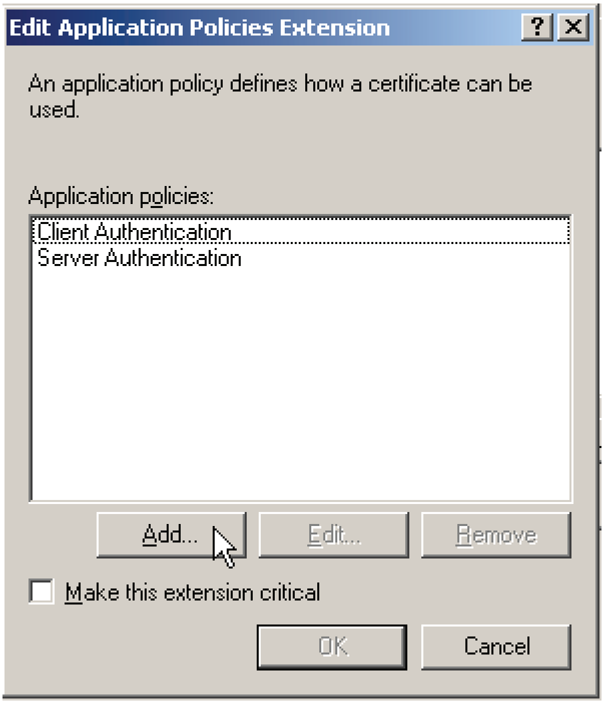
Extensions included in this template:

- Application Policies
- Certificate Template Information
- Issuance Policies
- Key Usage

Description of Application Policies:

Server Authentication
Client Authentication

a) Select **Application Policies** and click the **Edit** button.



Edit Application Policies Extension

An application policy defines how a certificate can be used.

Application policies:

Client Authentication
Server Authentication

b) Verify that only the **Client Authentication** and **Server Authentication** are listed. If they are not, click the **Add** button and add them.

Note ● The MP Proxy certificates must have "Intended Purposes" of Server Authentication and Client Authentication.

10. Click **OK** to close the *Properties of New Template* dialog.
11. Close the *Certificate Templates* window and return to the *Certification Authority* window.

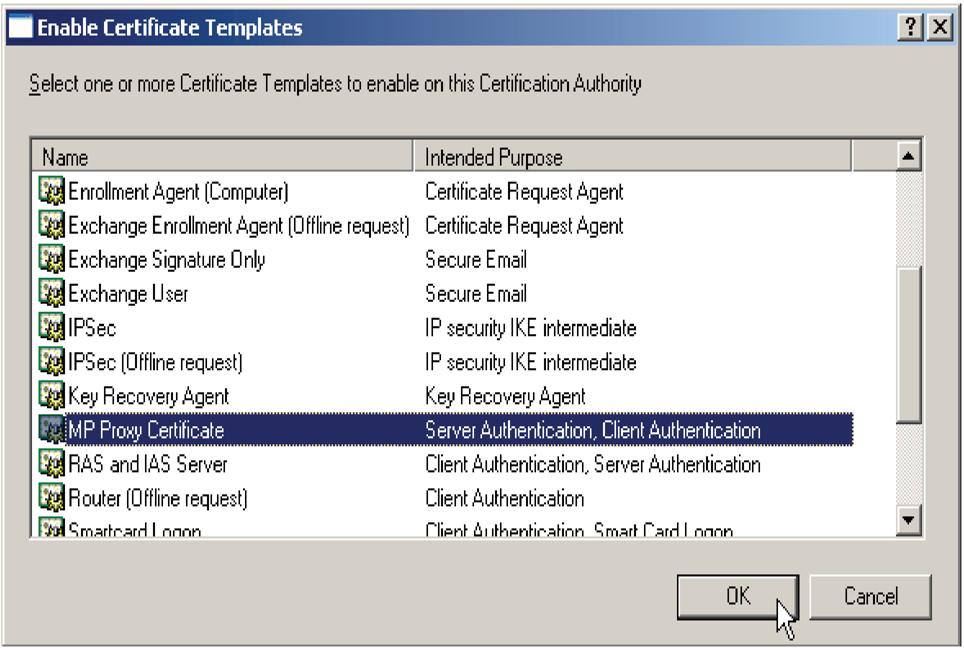
Issuing the MP Proxy Template

Issuing the template makes it available.

To issue the MP Proxy Template

1. In the **Certification Authority** window, expand the **Certification Authority** server node, if necessary.

2. Right-click the **Certificate Templates** folder and **New |Certificate Template to Issue**.



Select one or more Certificate Templates to enable on this Certification Authority

Name	Intended Purpose
Enrollment Agent (Computer)	Certificate Request Agent
Exchange Enrollment Agent (Offline request)	Certificate Request Agent
Exchange Signature Only	Secure Email
Exchange User	Secure Email
IPSec	IP security IKE intermediate
IPSec (Offline request)	IP security IKE intermediate
Key Recovery Agent	Key Recovery Agent
MP Proxy Certificate	Server Authentication, Client Authentication
RAS and IAS Server	Client Authentication, Server Authentication
Router (Offline request)	Client Authentication
Smartcard Logon	Client Authentication, Smart Card Logon

3. Select the **MP Proxy Certificate** template.
4. Click **OK**.
5. Close the *Certification Authority* window.

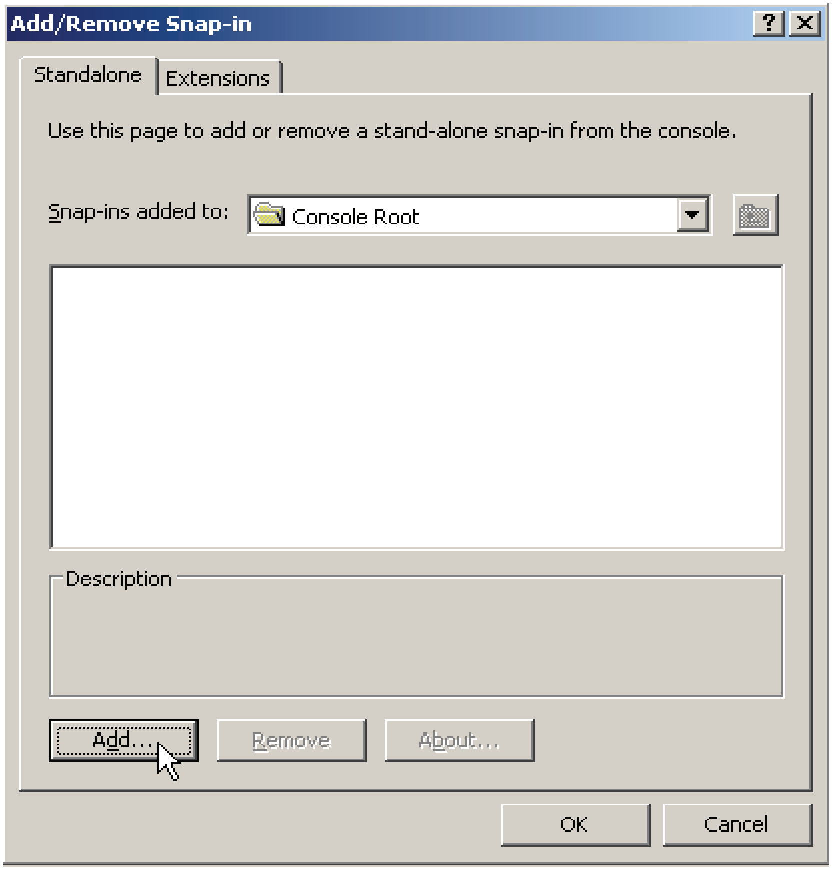
Creating the Certificate Store

To create a Certificate Store

1. From the **Start** menu select **Run** and enter ***mmc***.

   The *Console1* window opens.

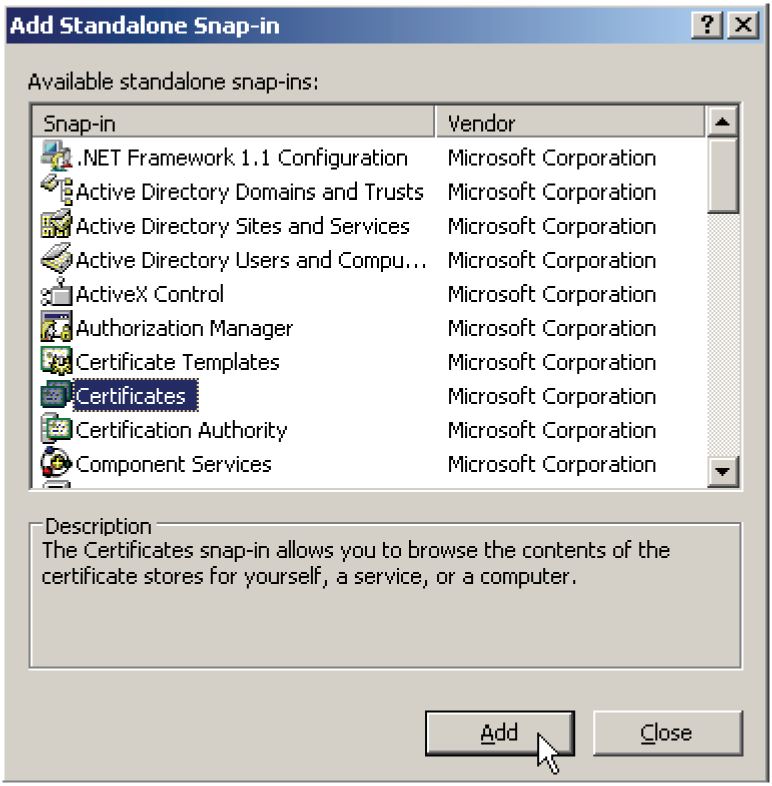
2. From the **File** menu, select **Add/Remove Snap-in**.


Add/Remove Snap-in

Use this page to add or remove a stand-alone snap-in from the console.

Snap-ins added to: Console Root

3. Click **Add**.

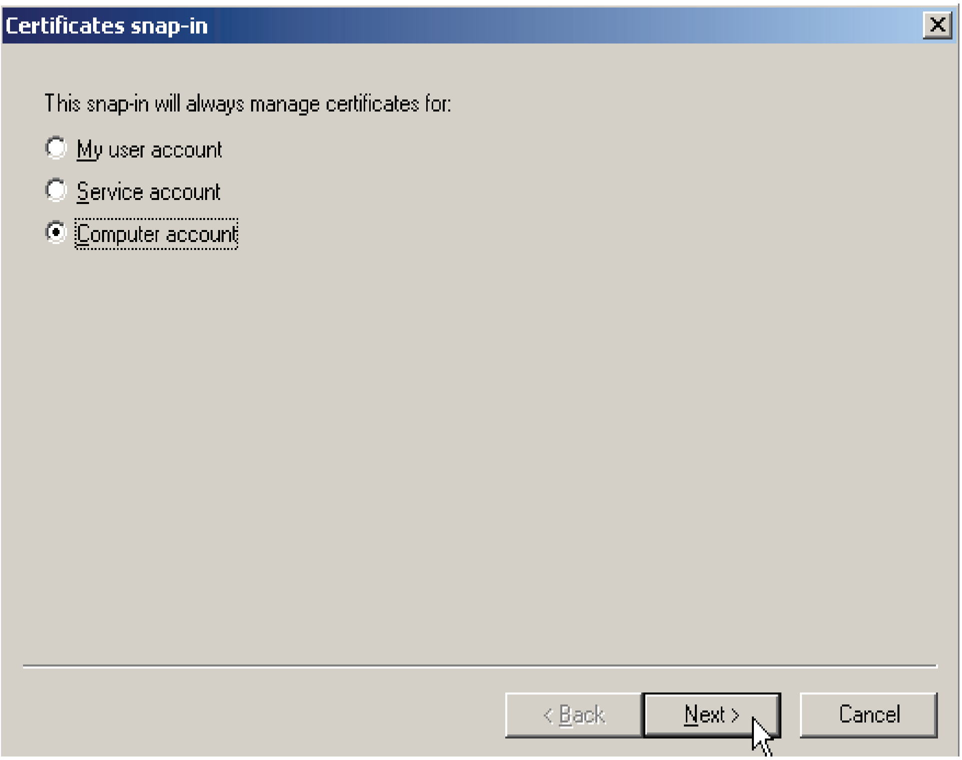


Available standalone snap-ins:

Snap-in	Vendor
.NET Framework 1.1 Configuration	Microsoft Corporation
Active Directory Domains and Trusts	Microsoft Corporation
Active Directory Sites and Services	Microsoft Corporation
Active Directory Users and Compu...	Microsoft Corporation
ActiveX Control	Microsoft Corporation
Authorization Manager	Microsoft Corporation
Certificate Templates	Microsoft Corporation
Certificates	Microsoft Corporation
Certification Authority	Microsoft Corporation
Component Services	Microsoft Corporation

Description
The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a computer.

4. Select **Certificates** and click **Add**.



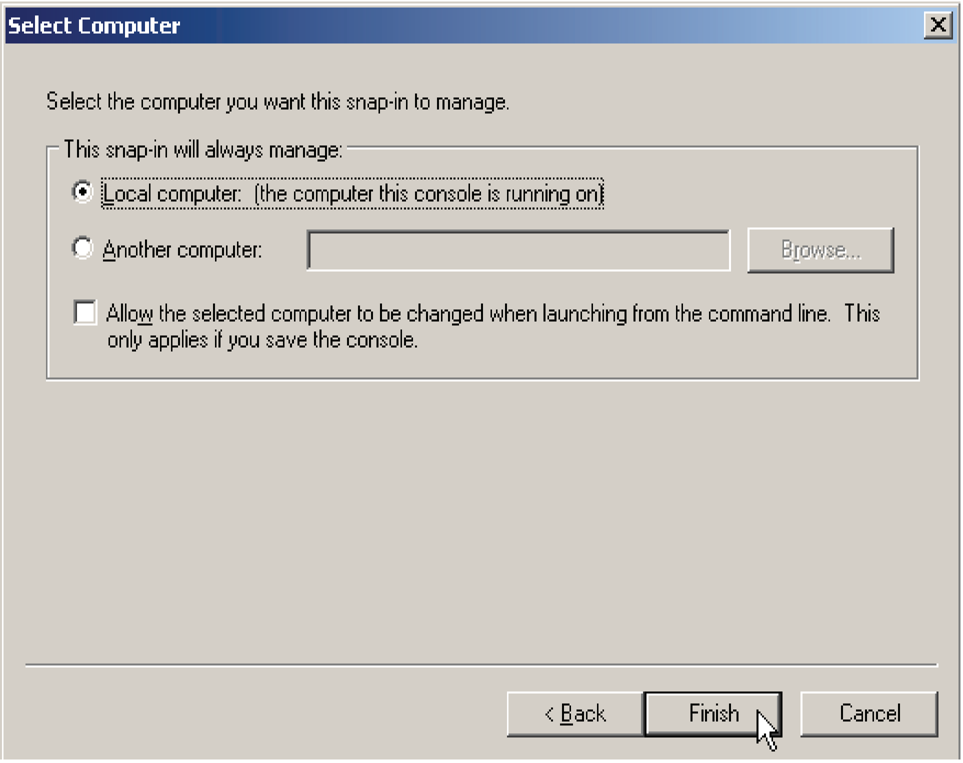
This snap-in will always manage certificates for:

○ My user account

○ Service account

● Computer account

5. Select the **Computer account** option and click **Next**.



Select Computer

Select the computer you want this snap-in to manage.

This snap-in will always manage:

● Local computer: (the computer this console is running on)

○ Another computer:

□ Allow the selected computer to be changed when launching from the command line. This only applies if you save the console.

6. Select **Local computer** and click **Finish**.
7. Close the *Add Standalone Snap-ins* dialog.
8. At the *Add/Remove Snap-in* dialog, click **OK**.
9. At the *Console1* window, open the **File** menu and choose **Save As...** and enter ***Certificate Store*** in the *File name* box.

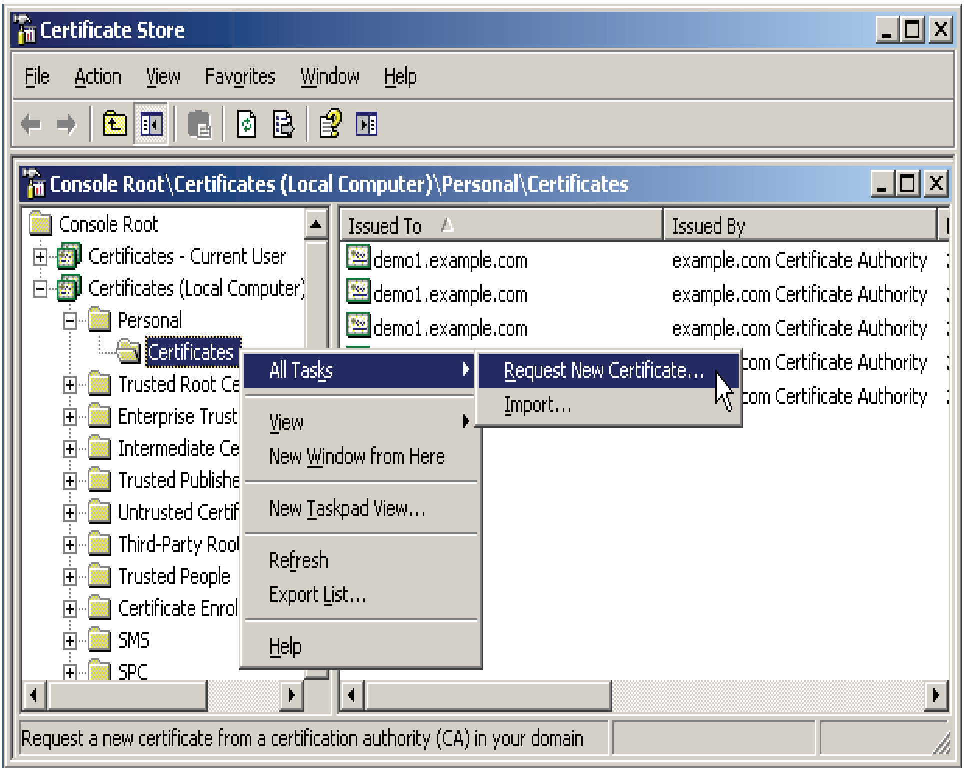
   Note • Save the ***Certificate Store*** on your Windows Desktop.

Requesting the MP Proxy Certificate

To request the MP Proxy Certificate

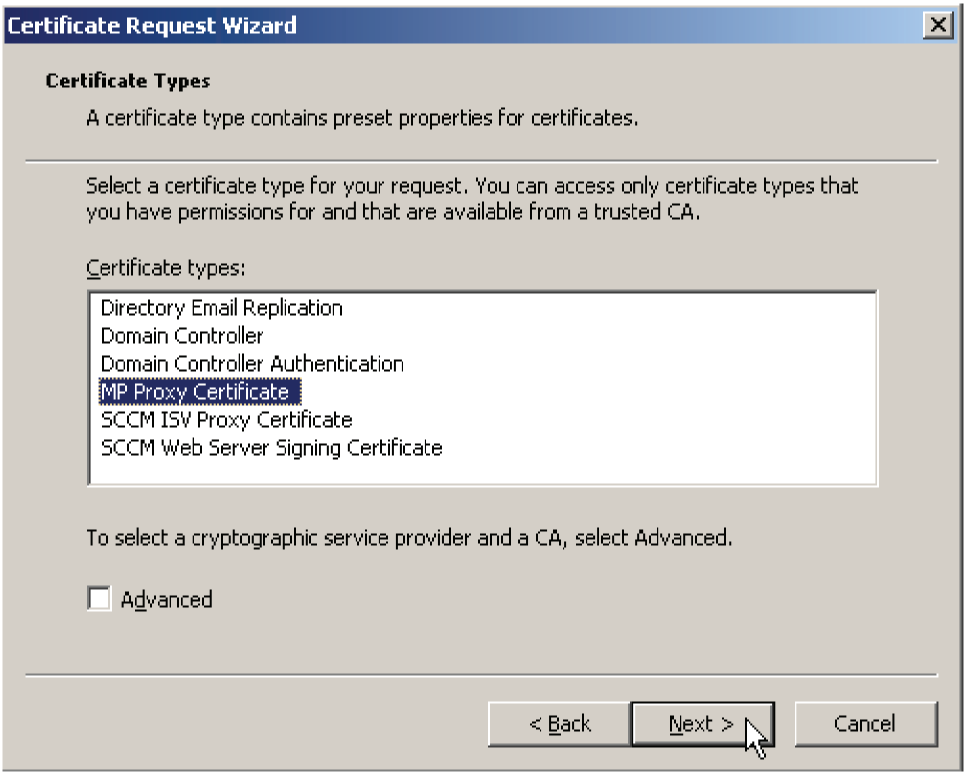
1. Double-click **Certificate Store.msc** icon from the Windows Desktop.

2. Expand **Certificates (Local Computer) | Personal** folders, if necessary.



Request a new certificate from a certification authority (CA) in your domain

3. Right-click the **Certificates** folder and select **All Tasks | Request New Certificate**.
4. Click **Next** on the Certificate Request Wizard *Welcome* page.



Certificate Request Wizard

Certificate Types

A certificate type contains preset properties for certificates.

Select a certificate type for your request. You can access only certificate types that you have permissions for and that are available from a trusted CA.

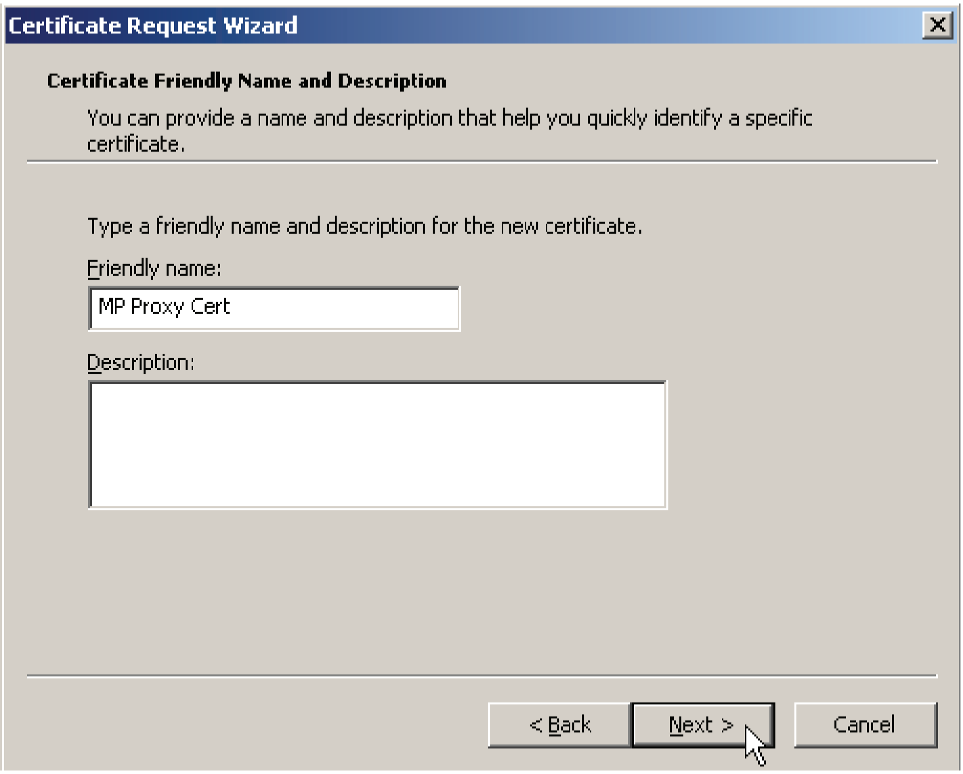
Certificate types:

- Directory Email Replication
- Domain Controller
- Domain Controller Authentication
- MP Proxy Certificate
- SCCM ISV Proxy Certificate
- SCCM Web Server Signing Certificate

To select a cryptographic service provider and a CA, select Advanced.

☐ Advanced

5. From the *Certificate types* list, select the **MP Proxy Certificate** and click **Next**.



Certificate Friendly Name and Description

You can provide a name and description that help you quickly identify a specific certificate.

Type a friendly name and description for the new certificate.

Friendly name: MP Proxy Cert

Description:

These steps assume you are deploying the MP Proxy certificate on a Windows 2003 Server. If you are on a Windows 2008 Server, the steps may vary slightly.

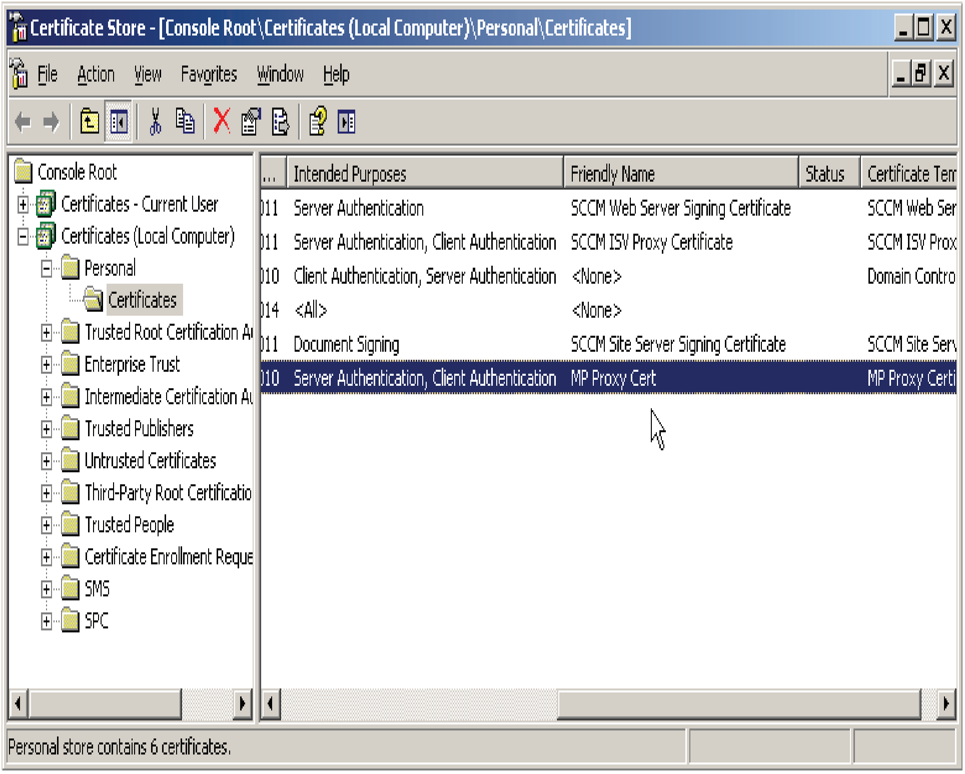
6. Enter ***MP Proxy Cert*** in the *Friendly name* box and click **Next**.
7. Click **Finish** to close the *Certificate Request Wizard*.
8. Click **OK** to return to the Certificate Store.

Exporting the MP Proxy Certificate

After you request the certificate, you must now export it from the Certificate store to a file.

To export the MP Proxy Certificate

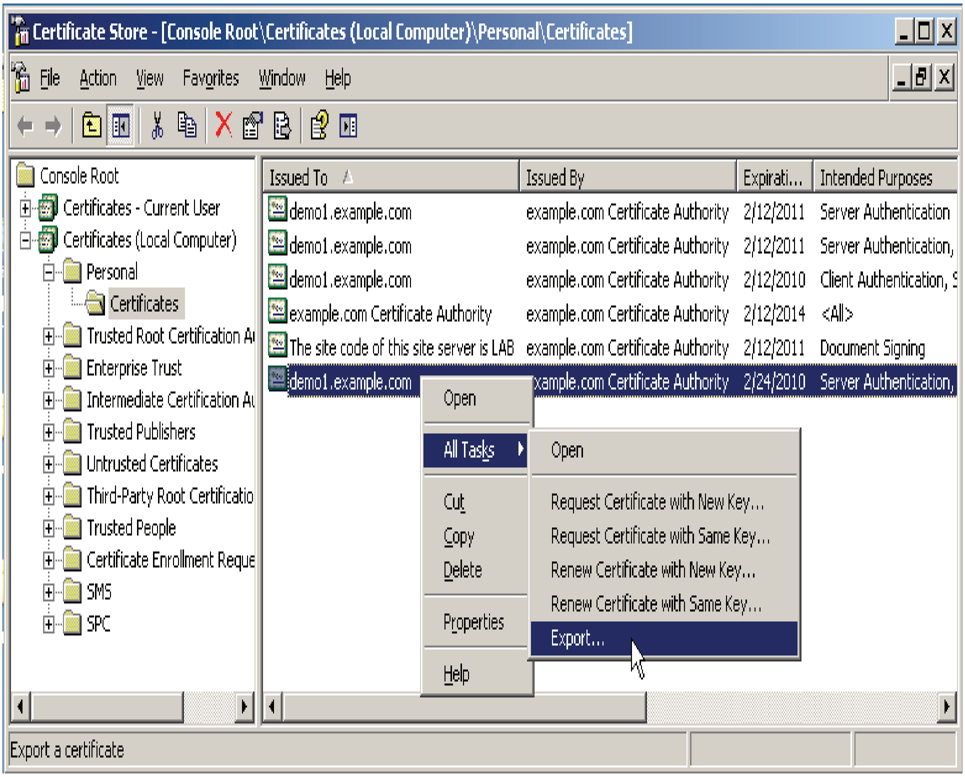
1. From the Certificate Store, navigate to **Certificates | Personal | Certificates**, if necessary.


Certificate Store - [Console Root\Certificates (Local Computer)\Personal\Certificates]
File
Action
View
Favorites
Window
Help
Console Root
Certificates - Current User
Certificates (Local Computer)
Personal
Certificates
Trusted Root Certification Au
Enterprise Trust
Intermediate Certification Au
Trusted Publishers
Untrusted Certificates
Third-Party Root Certificatio
Trusted People
Certificate Enrollment Reque
SMS
SPC

...	Intended Purposes	Friendly Name	Status	Certificate Ter
011	Server Authentication	SCCM Web Server Signing Certificate		SCCM Web Ser
011	Server Authentication, Client Authentication	SCCM ISV Proxy Certificate		SCCM ISV Prox
010	Client Authentication, Server Authentication	<None>		Domain Contro
014	<All>	<None>		
011	Document Signing	SCCM Site Server Signing Certificate		SCCM Site Serv
010	Server Authentication, Client Authentication	MP Proxy Cert		MP Proxy Certi

Personal store contains 6 certificates.

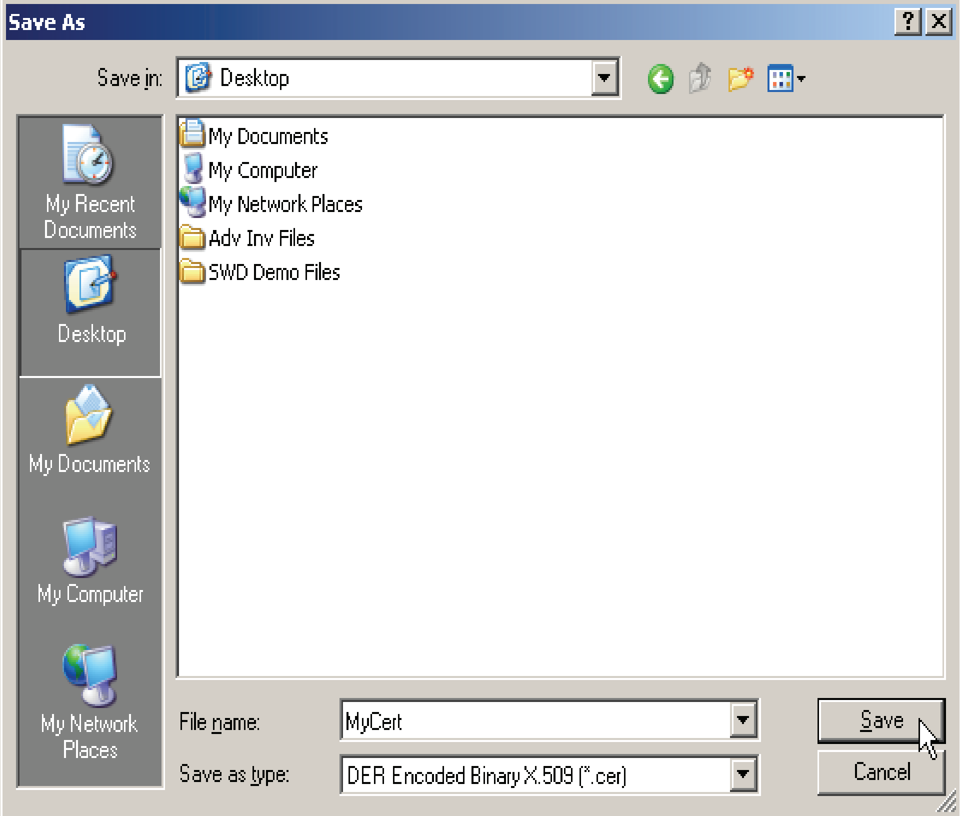
2. Scroll the window over so that you can see the *Friendly Name* column and select the *MP Proxy Cert*.


Certificate Store - [Console Root\Certificates (Local Computer)\Personal\Certificates]
File
Action
View
Favorites
Window
Help
Console Root
Certificates - Current User
Certificates (Local Computer)
Personal
Certificates
Trusted Root Certification Au
Enterprise Trust
Intermediate Certification Au
Trusted Publishers
Untrusted Certificates
Third-Party Root Certificatio
Trusted People
Certificate Enrollment Reque
SMS
SPC
Open
All Tasks
Cut
Copy
Delete
Properties
Help
Open
Request Certificate with New Key...
Request Certificate with Same Key...
Renew Certificate with New Key...
Renew Certificate with Same Key...
Export...

Issued To	Issued By	Expirati...	Intended Purposes
demo1.example.com	example.com Certificate Authority	2/12/2011	Server Authentication
demo1.example.com	example.com Certificate Authority	2/12/2011	Server Authentication,
demo1.example.com	example.com Certificate Authority	2/12/2010	Client Authentication, S
example.com Certificate Authority	example.com Certificate Authority	2/12/2014	<All>
The site code of this site server is LAB	example.com Certificate Authority	2/12/2011	Document Signing
demo1.example.com	xample.com Certificate Authority	2/24/2010	Server Authentication,

Export a certificate

3. Right-click the *MP Proxy Cert* and select **All Tasks | Export** to start the *Certificate Export Wizard*.
4. Click **Next** on the Certificate Export Wizard *Welcome* page.
5. Accept the defaults on the *Export Private Key* page and click **Next**.
6. Accept the defaults on the *Export File Format* page and click **Next**.
7. On the *File to Export* page, **Browse** to select the Windows Desktop as the location in which you want to save the certificate.



Save As

Save in: Desktop

My Documents
My Computer
My Network Places
Adv Inv Files
SWD Demo Files

File name: MyCert

Save as type: DER Encoded Binary X.509 (*.cer)

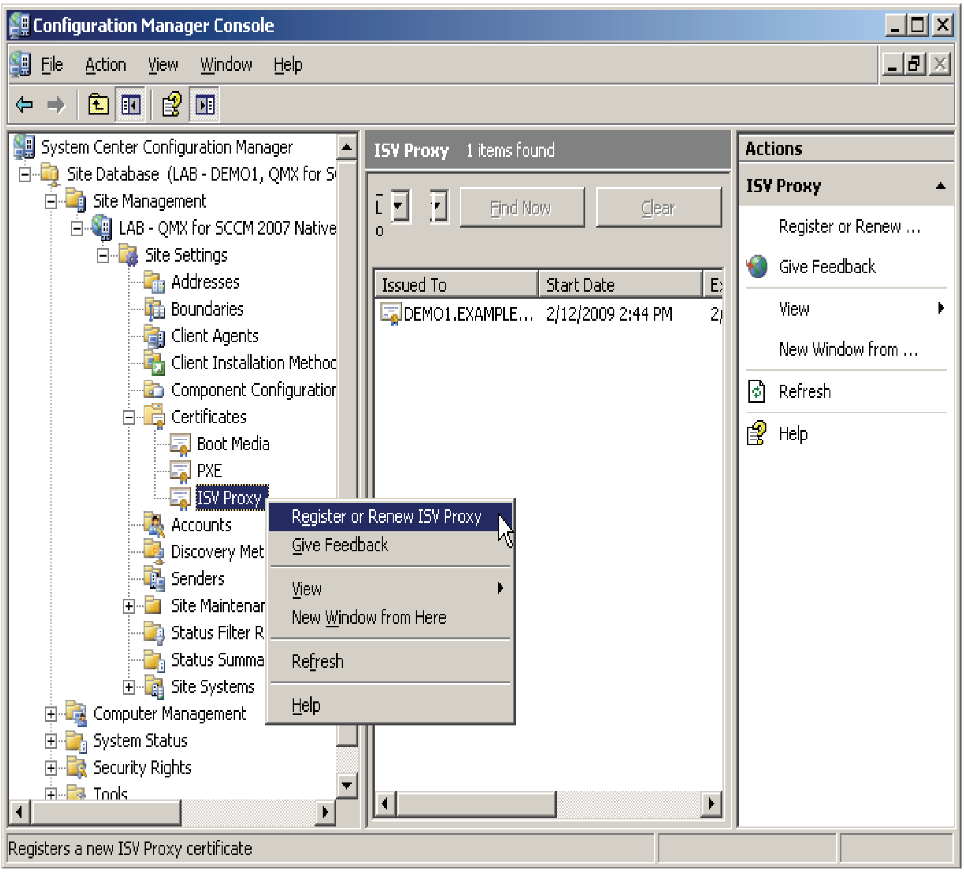
8. Enter a name for your certificate in the *File name* box and click **Save**.
9. On the *File to Export* page, click **Next**.
10. Click **Finish** on the *Completing the Certificate Export Wizard* page.
11. Click **OK** to return to the Certificate Store window.
12. Close the *Certificate Store* window.

Registering the MP Proxy Certificates

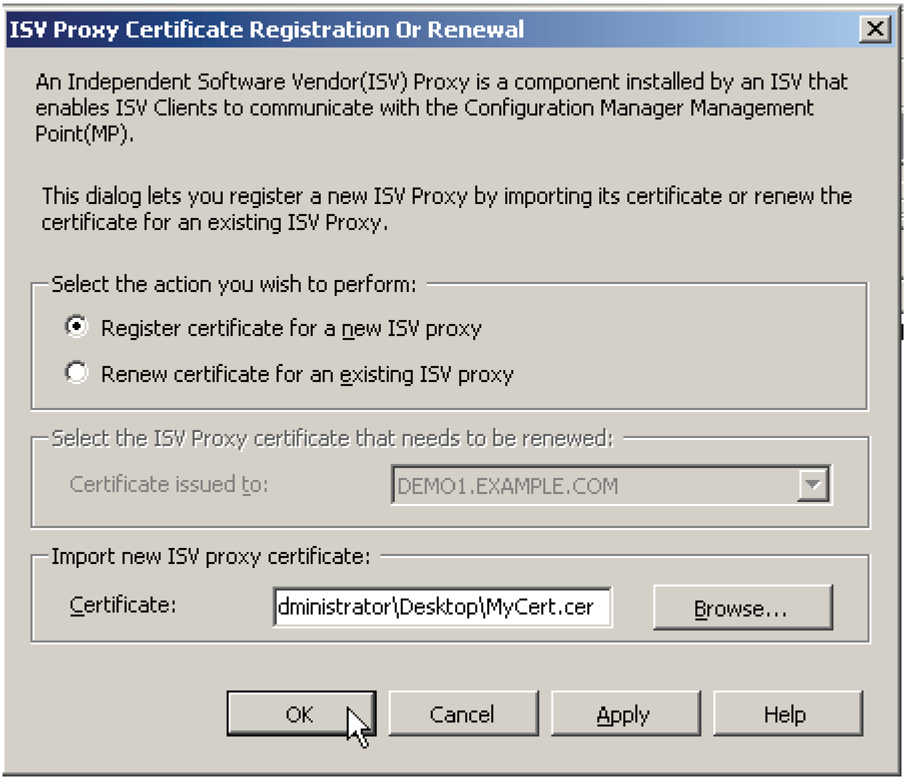
After you create the template, you need to register the MP Proxy Certificates in the Configuration Manager Console for every box that has an MP Proxy installed. You register the MP Proxy Certificate by importing it into the Configuration Manager Console by copying the certificate to the Site server where the Configuration Manager Console is installed.

To register the MP Proxy Certificates

1. Double click the **ConfigMgr Console** icon on the Microsoft Windows Virtual PC Desktop to start the Configuration Manager Console.
2. Navigate to **Site Database | Site Management | <site code> - <site name> | Site Settings | Certificates**.



3. Right-click **ISV Proxy** and choose **Register or Renew ISV Proxy**.



ISV Proxy Certificate Registration Or Renewal

An Independent Software Vendor(ISV) Proxy is a component installed by an ISV that enables ISV Clients to communicate with the Configuration Manager Management Point(MP).

This dialog lets you register a new ISV Proxy by importing its certificate or renew the certificate for an existing ISV Proxy.

Select the action you wish to perform:

● Register certificate for a new ISV proxy

○ Renew certificate for an existing ISV proxy

Select the ISV Proxy certificate that needs to be renewed:

Certificate issued to: DEMO1.EXAMPLE.COM

Import new ISV proxy certificate:

Certificate: dministrator\Desktop\MyCert.cer

4. Select **Register certificate for a new ISV proxy**.
5. **Browse** to select the certificate you created and click **Open**.
6. Click **OK** at the *ISV Proxy Certificate Registration or Renewal* dialog.
7. Close the Configuration Manager Console.

Install the MP Proxy

Once you have created the PKI Certificates, you are ready to install MP Proxy on the Management Point server. You can install the MP Proxy in either mixed or native mode.

Once you install the MP Proxy on the management point server, when you switch over to native mode, the 2.2 Agents will automatically detect the switch and start communicating by means of the MP Proxy automatically; thus, they will continue to work as usual.

The default installation directory for the MP Proxy files is: `C:\Program Files\Quest Software\QMX for ConfigMgr\MP Proxy\`.

You can use the MP Proxy installation wizard or perform an “unattended” MP Proxy installation:

- Install the MP Proxy with the Wizard
- Unattended MP Proxy Installation

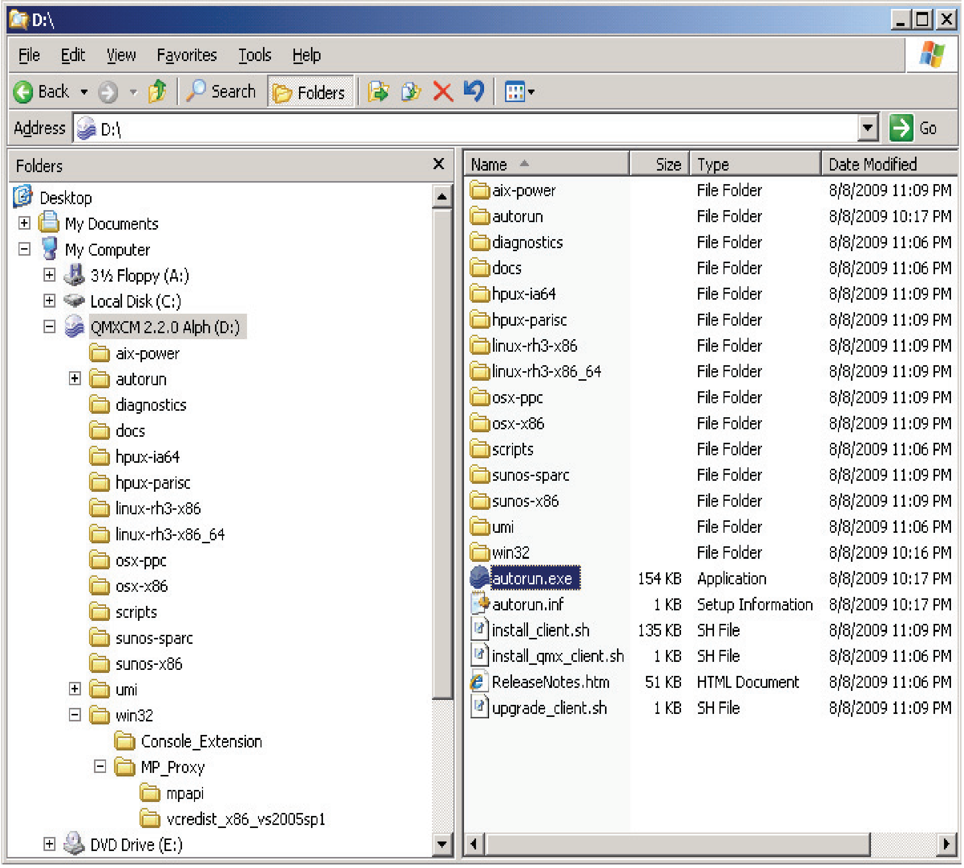
Install the MP Proxy with the Wizard

QMX - Configuration Manager 2007 2.2 includes an MP Proxy Setup Wizard.

To install the MP Proxy using the wizard

1. Ensure the computer hosting the MP Proxy meets these required pre-requisites (see Native Mode Requirements.)

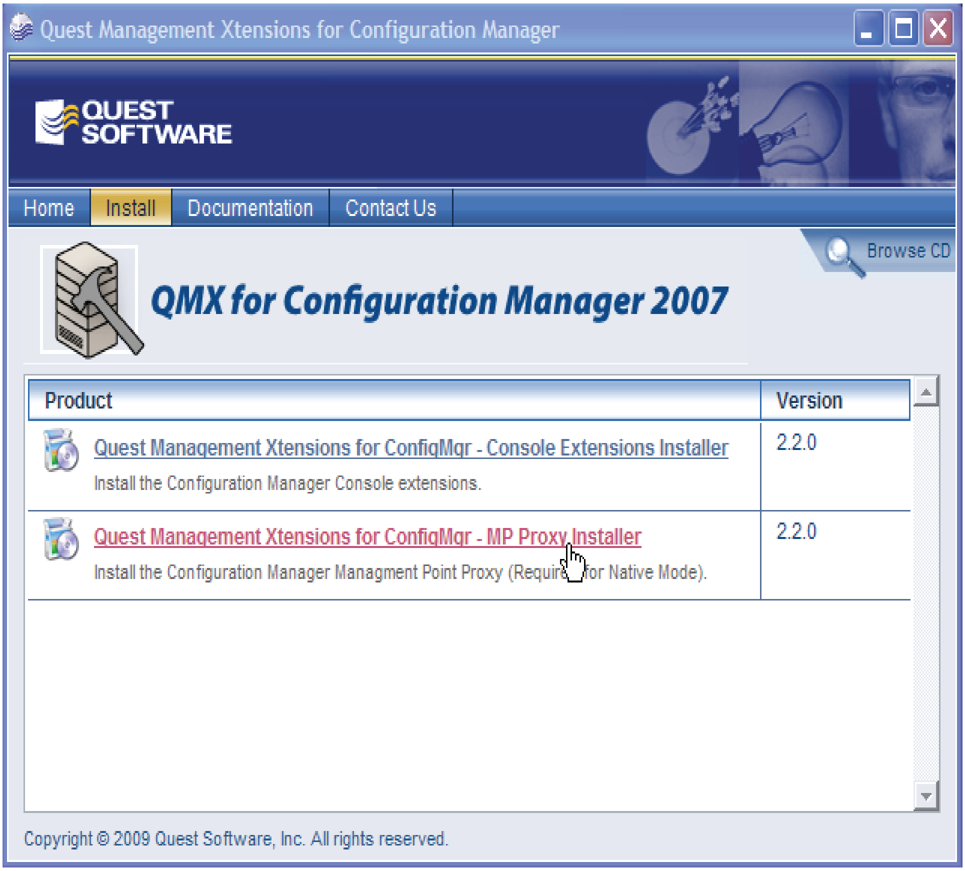
   Note ● The setup wizard checks the Management Point Server to see if it has .NET 2.0, Visual Studio 2005 SP1 C++ Runtime Libraries, and the Management Point API. If it does not detect these components, setup.exe downloads and installs them. Then it runs the MP proxy installation.



Name	Size	Type	Date Modified
aix-power		File Folder	8/8/2009 11:09 PM
autorun		File Folder	8/8/2009 10:17 PM
diagnostics		File Folder	8/8/2009 11:06 PM
docs		File Folder	8/8/2009 11:06 PM
hpux-ia64		File Folder	8/8/2009 11:09 PM
hpux-parisc		File Folder	8/8/2009 11:09 PM
linux-rh3-x86		File Folder	8/8/2009 11:09 PM
linux-rh3-x86_64		File Folder	8/8/2009 11:09 PM
osx-ppc		File Folder	8/8/2009 11:09 PM
osx-x86		File Folder	8/8/2009 11:09 PM
scripts		File Folder	8/8/2009 11:06 PM
sunos-sparc		File Folder	8/8/2009 11:09 PM
sunos-x86		File Folder	8/8/2009 11:09 PM
umi		File Folder	8/8/2009 11:06 PM
win32		File Folder	8/8/2009 10:16 PM
autorun.exe	154 KB	Application	8/8/2009 10:17 PM
autorun.inf	1 KB	Setup Information	8/8/2009 10:17 PM
install_client.sh	135 KB	SH File	8/8/2009 11:09 PM
install_qmx_client.sh	1 KB	SH File	8/8/2009 11:06 PM
ReleaseNotes.htm	51 KB	HTML Document	8/8/2009 11:06 PM
upgrade_client.sh	1 KB	SH File	8/8/2009 11:09 PM

2. From the root of the installation media, double-click **autorun.exe** to open the *QMX for Configuration Manager 2007 autorun* dialog.

3. Click the **Install** tab on the autorun dialog.



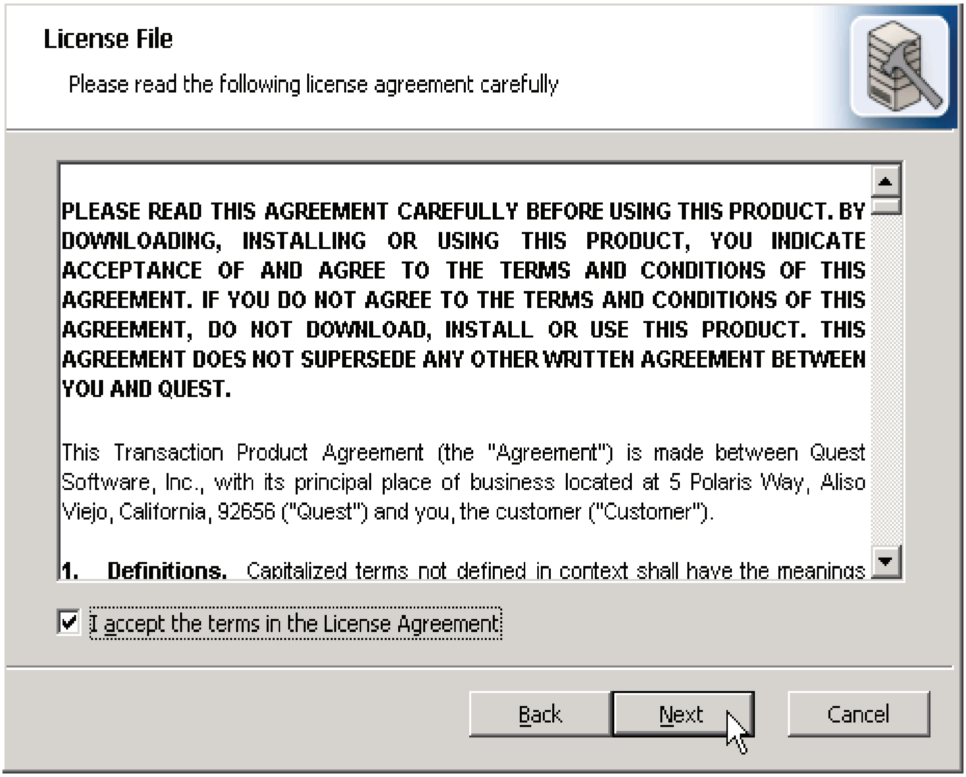
Quest Management Xtensions for Configuration Manager
QUEST SOFTWARE
Home
Install
Documentation
Contact Us
Browse CD
QMX for Configuration Manager 2007

Product	Version
Quest Management Xtensions for ConfigMgr - Console Extensions Installer Install the Configuration Manager Console extensions.	2.2.0
Quest Management Xtensions for ConfigMgr - MP Proxy Installer Install the Configuration Manager Managment Point Proxy (Requir for Native Mode).	2.2.0

Copyright © 2009 Quest Software, Inc. All rights reserved.

4. Click the **Quest Management Xtensions for ConfigMgr - MP Proxy Installer** link.
5. Click **Install** at the *mp_proxy_bootstrapper Setup* dialog.

   The *MP Proxy Setup Wizard* starts automatically.
6. At the *Welcome* dialog, click **Next**.



License File

Please read the following license agreement carefully

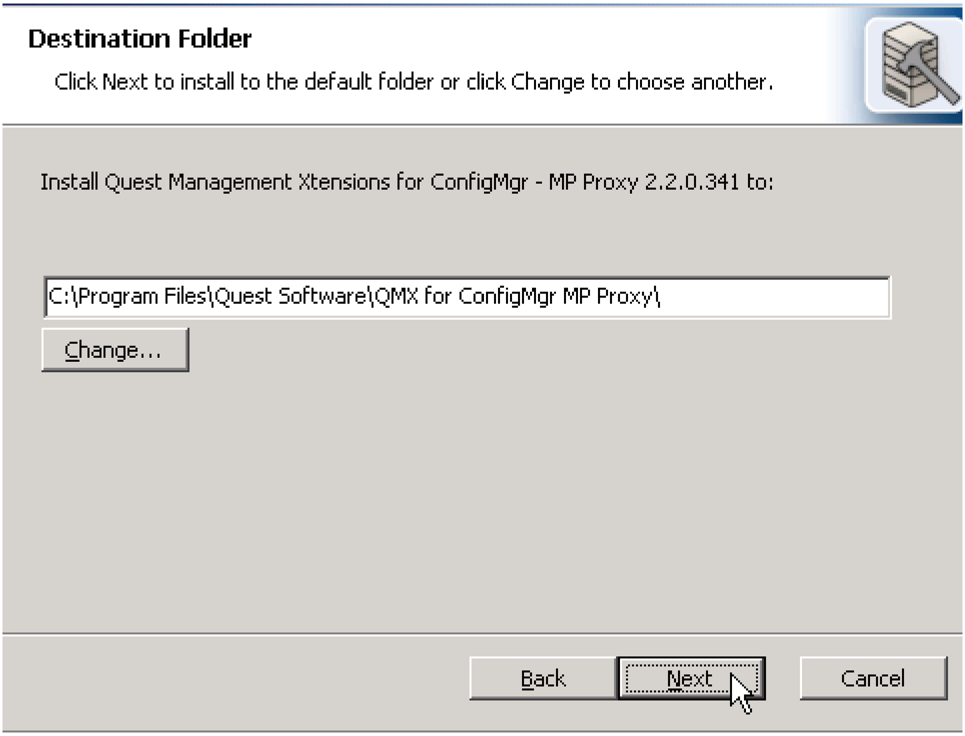
PLEASE READ THIS AGREEMENT CAREFULLY BEFORE USING THIS PRODUCT. BY DOWNLOADING, INSTALLING OR USING THIS PRODUCT, YOU INDICATE ACCEPTANCE OF AND AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT, DO NOT DOWNLOAD, INSTALL OR USE THIS PRODUCT. THIS AGREEMENT DOES NOT SUPERSEDE ANY OTHER WRITTEN AGREEMENT BETWEEN YOU AND QUEST.

This Transaction Product Agreement (the "Agreement") is made between Quest Software, Inc., with its principal place of business located at 5 Polaris Way, Aliso Viejo, California, 92656 ("Quest") and you, the customer ("Customer").

1. Definitions. Capitalized terms not defined in context shall have the meanings

☑ I accept the terms in the License Agreement

7. Select **I accept the license agreement** and click **Next**.



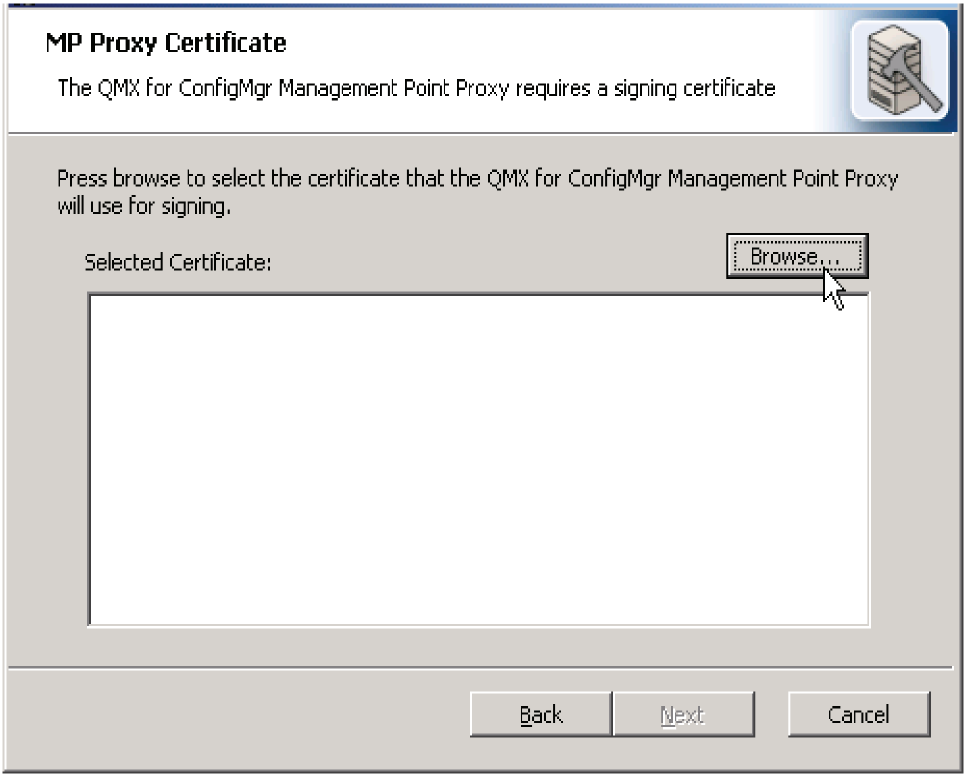
Destination Folder

Click Next to install to the default folder or click Change to choose another.

Install Quest Management Xtensions for ConfigMgr - MP Proxy 2.2.0.341 to:

C:\Program Files\Quest Software\QMX for ConfigMgr MP Proxy\

8. Accept the defaults and click **Next** or click **Change** to choose another path.



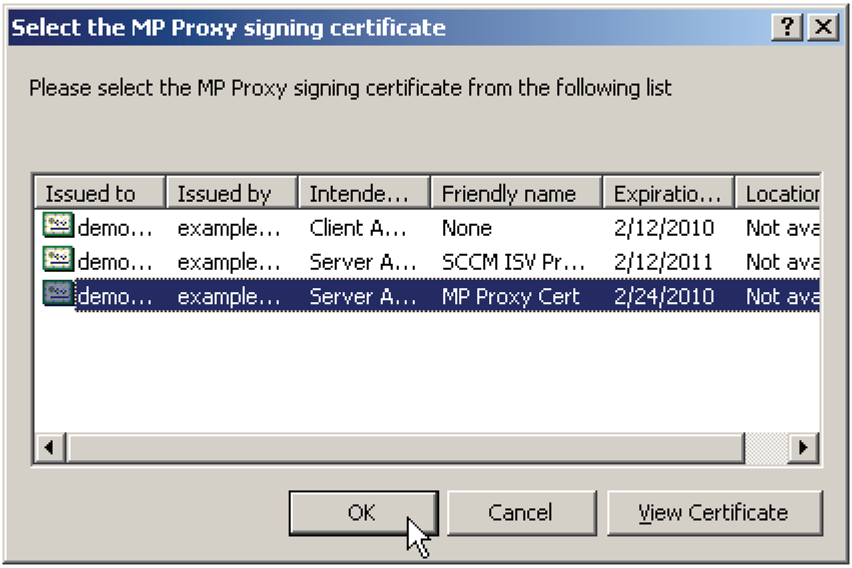
MP Proxy Certificate

The QMX for ConfigMgr Management Point Proxy requires a signing certificate

Press browse to select the certificate that the QMX for ConfigMgr Management Point Proxy will use for signing.

Selected Certificate:

9. **Browse** to select the MP Proxy Certificate.

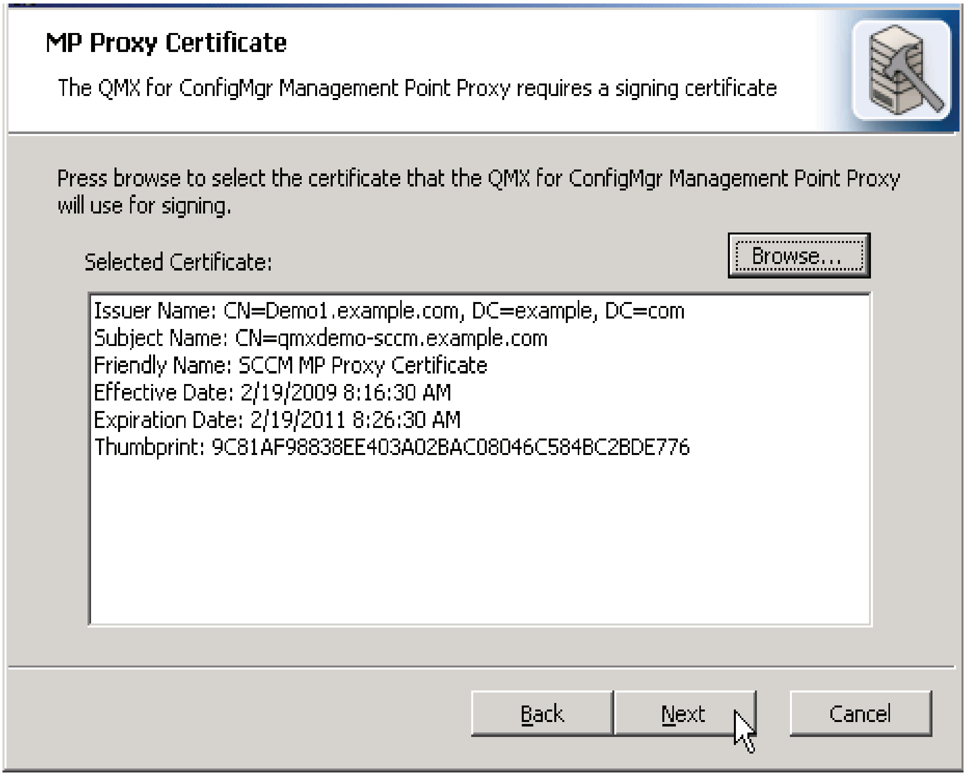


Select the MP Proxy signing certificate

Please select the MP Proxy signing certificate from the following list

Issued to	Issued by	Intende...	Friendly name	Expiratio...	Locatior
demo...	example...	Client A...	None	2/12/2010	Not ava
demo...	example...	Server A...	SCCM ISV Pr...	2/12/2011	Not ava
demo...	example...	Server A...	MP Proxy Cert	2/24/2010	Not ava

10. Scroll the window over so that you can see the *Friendly Name* column, select the **MP Proxy Cert** certificate and click **OK**.



MP Proxy Certificate

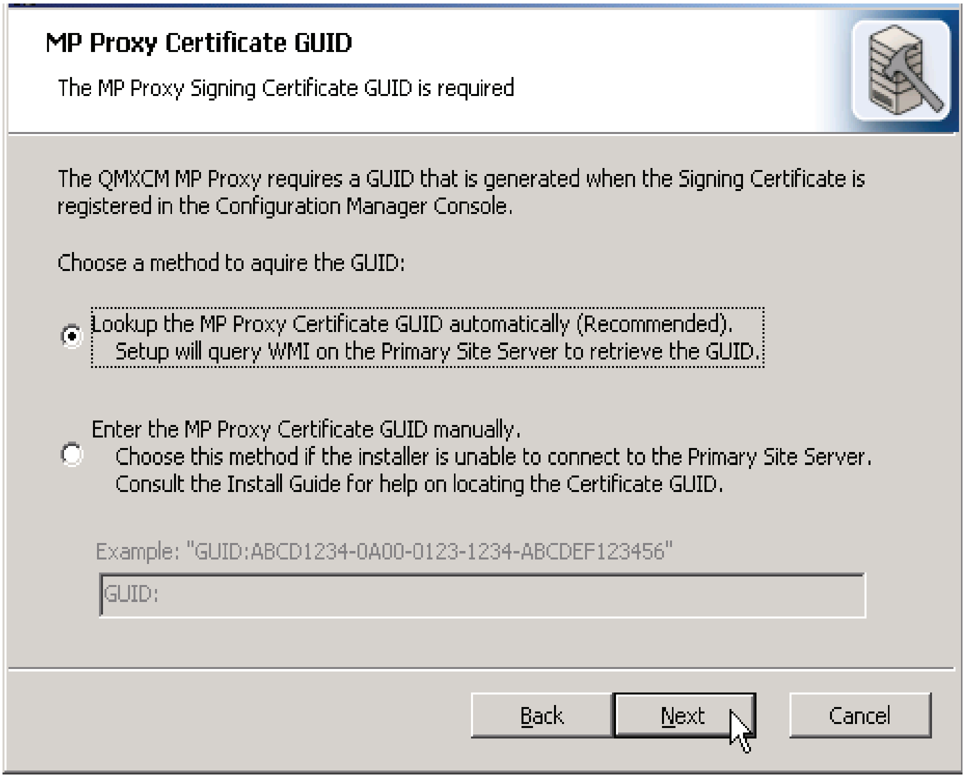
The QMX for ConfigMgr Management Point Proxy requires a signing certificate

Press browse to select the certificate that the QMX for ConfigMgr Management Point Proxy will use for signing.

Selected Certificate:

```
Issuer Name: CN=Demo1.example.com, DC=example, DC=com
Subject Name: CN=qmxdemo-sccm.example.com
Friendly Name: SCCM MP Proxy Certificate
Effective Date: 2/19/2009 8:16:30 AM
Expiration Date: 2/19/2011 8:26:30 AM
Thumbprint: 9C81AF98838EE403A02BAC08046C584BC2BDE776
```

11. Click **Next**.



MP Proxy Certificate GUID

The MP Proxy Signing Certificate GUID is required

The QMXCM MP Proxy requires a GUID that is generated when the Signing Certificate is registered in the Configuration Manager Console.

Choose a method to aquire the GUID:

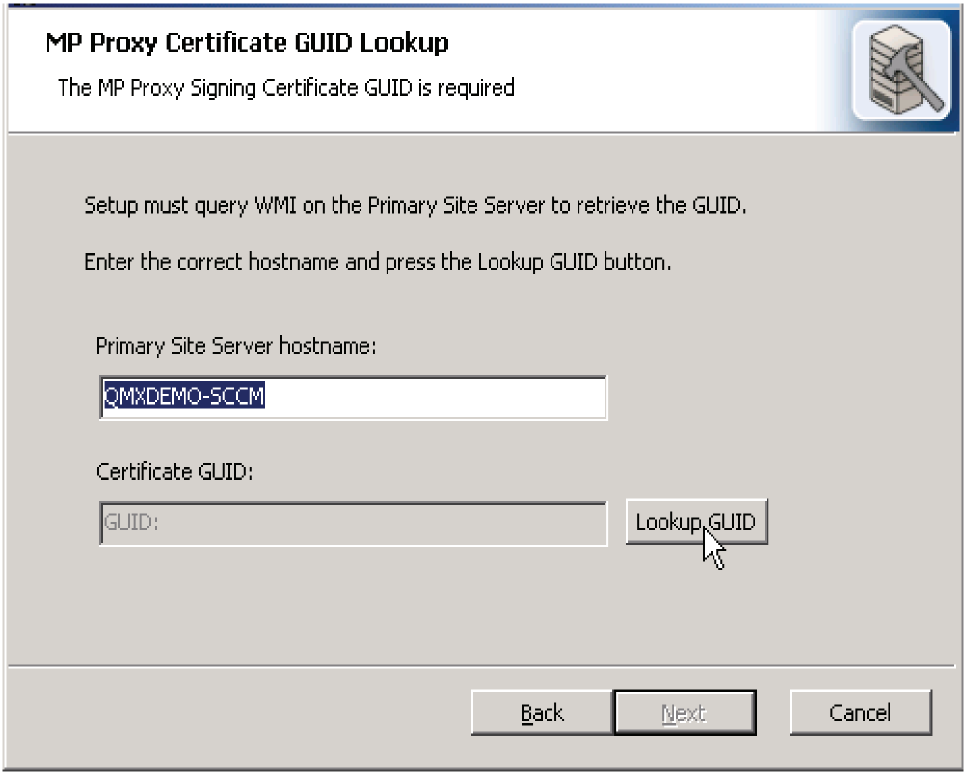
● Lookup the MP Proxy Certificate GUID automatically (Recommended).
Setup will query WMI on the Primary Site Server to retrieve the GUID.

○ Enter the MP Proxy Certificate GUID manually.
Choose this method if the installer is unable to connect to the Primary Site Server.
Consult the Install Guide for help on locating the Certificate GUID.

Example: "GUID:ABCD1234-0A00-0123-1234-ABCDEF123456"

GUID:

12. Choose a method to acquire the GUID.
    a) If you choose to enter the MP Proxy Certificate GUID manually, when you click Next, the wizard takes to directly to the “Ready to install” page.
    b) If you choose to have the wizard retrieve the GUID for you, when you click Next, it opens the MP Proxy Certificate GUID Lookup page:



MP Proxy Certificate GUID Lookup

The MP Proxy Signing Certificate GUID is required

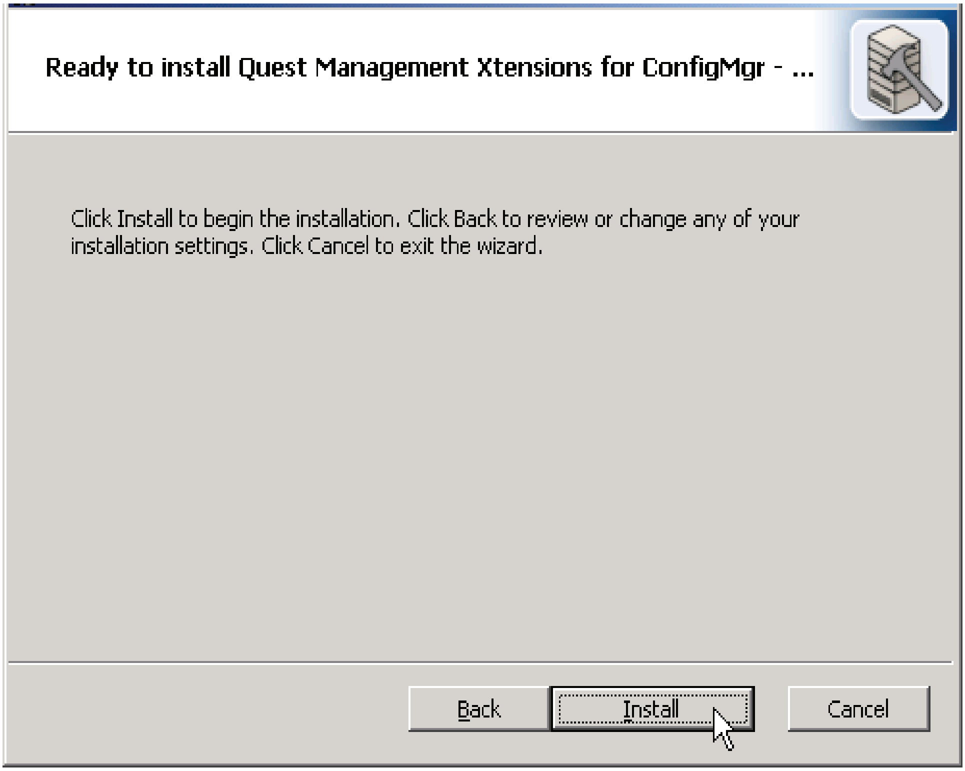
Setup must query WMI on the Primary Site Server to retrieve the GUID.

Enter the correct hostname and press the Lookup GUID button.

Primary Site Server hostname: QMXDEMO-SCCM

Certificate GUID: GUID:

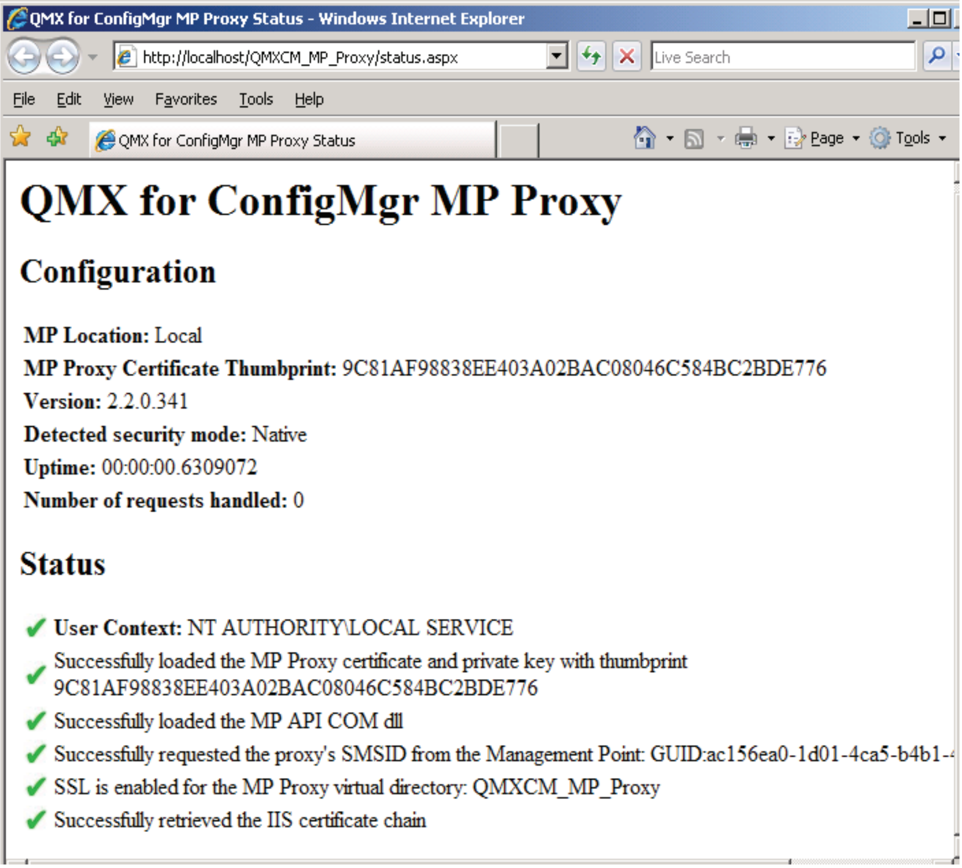
13. Click **Lookup GUID** and the wizard will retrieve it for you.
14. Click **Next** after it populates the *Certificate GUID* box.



Ready to install Quest Management Xtensions for ConfigMgr - ...

Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.

15. Click **Install**.
16. Click **Finish** when the MP Proxy Setup wizard completes the installation.


QMX for ConfigMgr MP Proxy Status - Windows Internet Explorer
http://localhost/QMXCM_MP_Proxy/status.aspx
Live Search
File
Edit
View
Favorites
Tools
Help
QMX for ConfigMgr MP Proxy Status
Page
Tools

QMX for ConfigMgr MP Proxy

Configuration

MP Location: Local
MP Proxy Certificate Thumbprint: 9C81AF98838EE403A02BAC08046C584BC2BDE776
Version: 2.2.0.341
Detected security mode: Native
Uptime: 00:00:00.6309072
Number of requests handled: 0

Status

- ✓ **User Context:** NT AUTHORITY\LOCAL SERVICE
- ✓ Successfully loaded the MP Proxy certificate and private key with thumbprint 9C81AF98838EE403A02BAC08046C584BC2BDE776
- ✓ Successfully loaded the MP API COM dll
- ✓ Successfully requested the proxy's SMSID from the Management Point: GUID:ac156ea0-1d01-4ca5-b4b1-
- ✓ SSL is enabled for the MP Proxy virtual directory: QMXCM_MP_Proxy
- ✓ Successfully retrieved the IIS certificate chain

The installation process automatically opens the *QMX for ConfigMgr MP Proxy* window showing you the status of the MP Proxy. At this point, if you have not changed the site mode to *native* in the Configuration Manager Console, it will detect that System Center Configuration Manager 2007 is in *mixed mode*. (See Troubleshooting the MP Proxy for more information about the *QMX for ConfigMgr MP Proxy* window.)

17. After you review the information that the *QMX for ConfigMgr MP Proxy* window provides, close the window. (See Troubleshooting the MP Proxy for more information about the status page.)
18. Close the autorun dialog, if it is still open.

Unattended MP Proxy Installation

You perform an "unattended" installation from the Windows command line.

To perform an "unattended" MP Proxy installation

1. Ensure the computer hosting the MP Proxy meets the required pre-requisites (see Native Mode Requirements.)

   Note ● If you plan to perform an "unattended" MP Proxy installation, you must manually install these components first.

2. Run `msiexec` on the command line with the correct parameters.
   - If you install the MP Proxy on a machine that is a management point, execute the following command:

     ```
     msiexec /passive /i mp_proxy.msi INSTALLDIR="C:\Some
     Other\Path" CERT_THUMBPRINT="b7 a2 47 00 ca b0 b2 e7 19
     26 fc 37 eb 48 a6 ba 25 af ae b8"
     ```

Obtaining the CERT_THUMBPRINT

When doing an "unattended" MP Proxy installation, you must supply the certificate thumbprint on the command line.

To obtain the certificate thumbprint

1. Run `mmc.exe` and add the Certificates (Local Computer) snap in.
2. Browse to **Personal | Certificates**.
3. Double-click the certificate that will be used by the MP Proxy.
4. Select the **Details** tab.
5. Click the Thumbprint.
6. Copy the certificate thumbprint from here in the format "93 79 16 44 e9 d7 01 eb 50 03 fd f5 ec bb 12 57 92 f0 8a ec" and paste it into the command line.

   – OR –

7. Specify it without spaces like this:

   `"93791644e9d701eb5003fdf5ecbb125792f08aec".`

   Note ● The letters may be lowercase or uppercase.

The installer adds the MP Proxy virtual directory into an existing IIS Web site. If a Web site named "Default Web Site" exists it will be used, otherwise it uses the first Web site it finds.

Registry Keys

The MP Proxy installer prompts you for configuration and saves it in the registry during the MP Proxy installation. You can verify the registry key settings and change their values, if necessary.

The MP Proxy installer adds the following registry keys under:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Quest Software\QMX for ConfigMgr MP
Proxy
```

REGISTRY KEY	TYPE	DESCRIPTION
InstallDir	REG_SZ	Installation directory.
CertThumbprint	REG_BINARY	A byte array containing the MP Proxy's certificate thumbprint.
SMSID	REG_SZ	Stores the MP Proxy’s SMS ID.
SiteCode	REG_SZ	Stores the ConfigMgr Site Code

Keys that always exist when the MP Proxy is installed:

- **InstallDir** - Installation path for the MP Proxy
- **CertThumbprint** - The thumbprint/hash for the certificate that the MP Proxy is using to sign data sent to System Center Configuration Manager 2007.
- **SMSID** - The MP Proxy’s SMS ID.
- **SiteCode** - The System Center Configuration Manager 2007 Site Code.

Enable SSL in IIS

These are the requirements for the QMX Agent to use SSL when communicating with the MP Proxy in native mode using https:

1. SSL must be enabled in IIS.
2. The IIS certificate must have a valid certificate chain.
3. The `qmxcm.mpe` item in the `qmxcm.conf` file must contain a Fully Qualified Domain Name (FDQN).

Note • Previous versions of QMX - Configuration Manager 2007 only required a hostname or IP address for the Management Point. While the QMX Agent will still work with just a hostname or IP address without using SSL, it must have a FQDN when using SSL! It uses the FQDN for validation of the MP Proxy certificate chain and is therefore required to use SSL securely. If you need to change the `qmxcm.mpe` setting, use the `clienttool`. (See *Using clienttool to Change the Site Settings*.)

It is not within the scope of this guide to document how to enable SSL in IIS. You must consult Microsoft documentation for specifics. (Go to: http://www.microsoft.com/technet/prodtechnol/WindowsServer2003/Library/IIS/56bdf977-14f8-4867-9c51-34c346d48b04.mspx?mfr=true for procedures.)

Switching from Mixed to Native Mode

If you are switching from mixed to native mode, QMX - Configuration Manager 2007 has some `clienttool` options that can help you to verify that your system is ready for native mode:

- `clienttool --run-native-mode-readiness-check`
- `clienttool --run-native-mode-ssl-check`

To run the native mode readiness checker

1. From the client command line, enter the following:

```
/opt/quest/qmxcm/bin/clienttool
--run-native-mode-readiness-check
```

Note • If any Agents are not communicating to the MP Proxy, consult the error message, fix the problem, and rerun the *Native Mode Readiness Checker*.

Rather than running this command on each client individually, you can use the QMX - Configuration Manager 2007 Software Distribution Wizard’s *Script or Custom Command* software distribution package type, to push a script out to each client agent to run the `clienttool --run-native-mode-readiness-check` or `clienttool --run-native-mode-ssl-check` options to verify that all your Agents are communicating to the MP Proxy and your system is ready for you to switch from mixed to native mode.

For more information about the `clienttool` options, see the *Using the Client Tool* section of the *QMX - Configuration Manager 2007 Administrator's Guide* which is located in the "docs" directory of the distribution media (navigate to: **Program Files | Quest Software | QMX for ConfigMgr | Docs**.)

Switching from mixed to native mode creates a new Client Id for each managed host. Thus, you will see duplicate clients in your collections. Enable the "Delete Obsolete Client Discovery Data" Site Maintenance Task to automatically purge the obsolete clients.

After you switch from mixed to native mode, verify all the MP Proxies have detected native mode using the *QMX for ConfigMgr MP Proxy* window. (See Troubleshooting the MP Proxy for information about using the *QMX for ConfigMgr MP Proxy* window.)

Troubleshooting the MP Proxy

The MP Proxy installer creates a folder under **Start | Programs** that contains a link to the *QMX for ConfigMgr MP Proxy* window which shows you the status of the MP Proxy. This is useful for troubleshooting issues with the MP Proxy. It is located at:

```
http://<MPProxyHostName>/QMXCM_MP_Proxy/Status.aspx
```

To open the QMX for ConfigMgr MP Proxy window

1. From the **Start** menu, navigate to **All Programs | Quest Management Xtensions for ConfigMgr | MP Proxy Status page**.

This page gives you the following information about the MP Proxy:

- Configuration:
  - MP Proxy Certificate Thumbprint
  - MP Proxy version
- Status
  - User context (must be LOCAL SERVICE)
  - If the MP Proxy is able to communicate to the management point, it displays the SMSID.
  - If the MP Proxy fails to get the SMSID, it displays the following:
    - If it can resolve the hostname, it displays the IP addresses.

  - Indicates if the http(s) ports can be opened
    Note: this might fail because of a firewall issue, or wrong MP hostname.
  - Indicates if the MP Proxy certificate was loaded; if not, it displays an error message.
  - Indicates if the management point API COM dll was loaded; if not, it displays an error message.
  - Indicates if there was an error communicating to the management point; if so, it displays the error message.
  - Indicates if communication to the management point was successful, but no ID was retrieved. (See Common Errors for more information about this error message.)
    Note: If this happens, examine the MP Proxy logs (see Logging).
- Identifies the security mode: *Native*, *Mixed*, or *Unknown*.
- Indicates if the certificate chain was loaded; if not, it displays an error message.
- If any Agent requests have failed, it lists the last 10 failures.
- Indicates the length of time (uptime) the MP Proxy has been running.
- Indicates the number of requests the MP Proxy has handled since it has been running.

Common Errors

The following some errors you might see on the QMX for ConfigMgr MP Proxy Status page and some steps you can take to resolve the situation.

Failed to retrieve the MP Proxy SMS ID. Exception: System.Runtime.InteropServices.COMException (0x80004005)

There are many things that could cause this error message.

To Troubleshooting this error

1. Verify that the MP Proxy is using the correct certificate.
2. Verify that the MP Proxy certificate has been registered in the Configuration Manager Console.
3. Verify that the MP Proxy certificate registered in the Configuration Manager Console has the same thumbprint as the one the MP Proxy is using. You can see the MP Proxy certificate thumbprint on the MP Proxy Status page, and in the registry at HKLM\SOFTWARE\Quest Software\QMX for ConfigMgr MP Proxy\CertThumbprint.

4. Verify that the MP Proxy certificate was created using a Template that meets the MP Proxy certificate requirements. (See PKI Certificate Requirements for Native Mode.)
5. Verify that the System Center Configuration Manager 2007 Windows clients are working.
6. Verify that SSL is enabled on the Management Point IIS Web site.
7. If SSL is enabled on the Web site, verify that it has the correct Web Server certificate and that the template used to create it matches the Microsoft specifications. (See http://technet.microsoft.com/en-us/library/bb694035.aspx.)
8. This error can indicate that the Management Point returned an error to the MP Proxy (by means of the MP API). Check the log files (especially `MP_RegistrationManager.log`) at `C:\Program Files\SMS_CCM\Logs`.

Failed to retrieve the MP Proxy SMS ID. Exception: System.Runtime.InteropServices.COMException (0x8009000F): Object already exists. (Exception from HRESULT: 0x8009000F)

In this case, the MP Proxy log just says: "System.Runtime.InteropServices.COMException (0x8009000F): Object already exists. (Exception from HRESULT: 0x8009000F)". You might find some useful information for this problem in the Management Point logs.

If the `MP_RegistrationManager.log` file says "Rejecting the registration request because Agent Type is ISV Proxy and registration hint was either not supplied in the request or verified" it means that there is something wrong with the MP Proxy Certificates.

To Troubleshooting this error

1. Verify that the MP Proxy is using the correct certificate.
2. Verify that the MP Proxy certificate has been registered in the Configuration Manager Console.
3. Verify that the MP Proxy certificate registered in the Configuration Manager Console has the same thumbprint as the one the MP Proxy is using. You can see the MP Proxy certificate thumbprint on the Mp Proxy Status page, and in the registry at `HKEY_LOCAL_MACHINE\SOFTWARE\Quest Software\QMX for ConfigMgr MP Proxy\CertThumbprint`.
4. Verify that the MP Proxy certificate was created using a template that meets the MP Proxy certificate requirements. (See PKI Certificate Requirements for Native Mode.)

5. If everything looks correct with the MP Proxy certificate then System Center Configuration Manager 2007 might be having a problem with the certificate so you will have to create a new MP Proxy certificate:
   a) Issue a new certificate.
   b) Renew the ISV Proxy certificate in the Configuration Manager Console.
   c) Reinstall the QMX MP Proxy with the new certificate.
   d) Check the MP Proxy Status page again.

Logging

The MP Proxy installer creates a directory named "log" under the MP Proxy installation directory, located at `C:\Program Files\Quest Software\QMX for ConfigMgr MP Proxy\log`. This directory grants full control permissions to the LOCAL SERVICE user in order to allow the MP Proxy Web site to write log files. By default the MP Proxy logging is disabled.

To enable MP Proxy logging

1. Navigate to the MP Proxy installation directory (C:\Program Files\Quest Software\QMX for ConfigMgr MP Proxy).
2. Double-click the `web.config` file to open it for editing.
3. Read the comment and change the value of the "General" switch to the desired level.

   Note • The values are documented in the file.

Note: After you modify `web.config`, you do not need to manually restart the MP Proxy, ASP.NET will detect the change and restart it automatically.

Management Point Log Files

System Center Configuration Manager 2007 creates the Management Point log files at: `C:\Program Files\SMS_CCM\Logs.`

The `MP_RegistrationManager.log` contains information about client registration. The MP Proxy uses client registration to determine its SMSID, so this log can contain useful information if the MP Proxy Status page says "Failed to retrieve the MP Proxy SMS ID."

Enabling Debug Logging

To enable debug logging for System Center Configuration Manager 2007

1. Stop the SMS Agent Host service.

a) From the **Start** menu, navigate to **Programs** | **Administrative Tools** | **Services**.

b) In the *Services* screen, locate the *SMS Agent Host service*.

c) Right-click the **SMS Agent Host** service, and click **Stop**.

2. Add a *DebugLogging* key to the registry:

   a) From the **Start** menu, choose **Run** and enter ***Regedit*** to open the Registry Editor.

   b) Navigate to **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CCM**.

   c) Right-click **Logging** and choose **New** | **Key**.

   d) Enter ***DebugLogging*** as the name of the new key.

3. Add a new String Value to the *DebugLogging* Key:

   a) Right-click the **DebugLogging** key and choose **New** | **String Value**.

   b) Enter ***Enabled*** as the subkey name.

   c) Double-click **Enabled** to open the *Edit String* dialog.

   d) Enter ***True*** in the *Value data* box and click **OK**.

Enable Verbose Logging for Management Point Logs

To enable verbose logging for System Center Configuration Manager 2007

1. From the **Start** menu, choose **Run** and enter ***Regedit*** to open the Registry Editor.
2. Navigate to **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CCM**.
3. Right-click the **@GLOBAL** Key and choose **Permissions**.
4. Add “Full Control” for Administrators.
5. Select the **@GLOBAL** key, then double-click **LogLevel** to open the Edit DWORD Value dialog.
6. Change the *Value data* to 0 and click **OK**.

Note ● The System Center Configuration Manager 2007 Management Point Logs are located at `C:\Program Files\SMS_CCM\Logs`.

4

Installing the Console Extensions

- About the Configuration Manager Console Extensions
- Installing the Console Extensions

About the Configuration Manager Console Extensions

The Quest Configuration Manager Console extensions provide integrated menus, wizards, property pages, and remote administration tools that enable you to seamlessly manage non-Windows systems from the Configuration Manager Console.

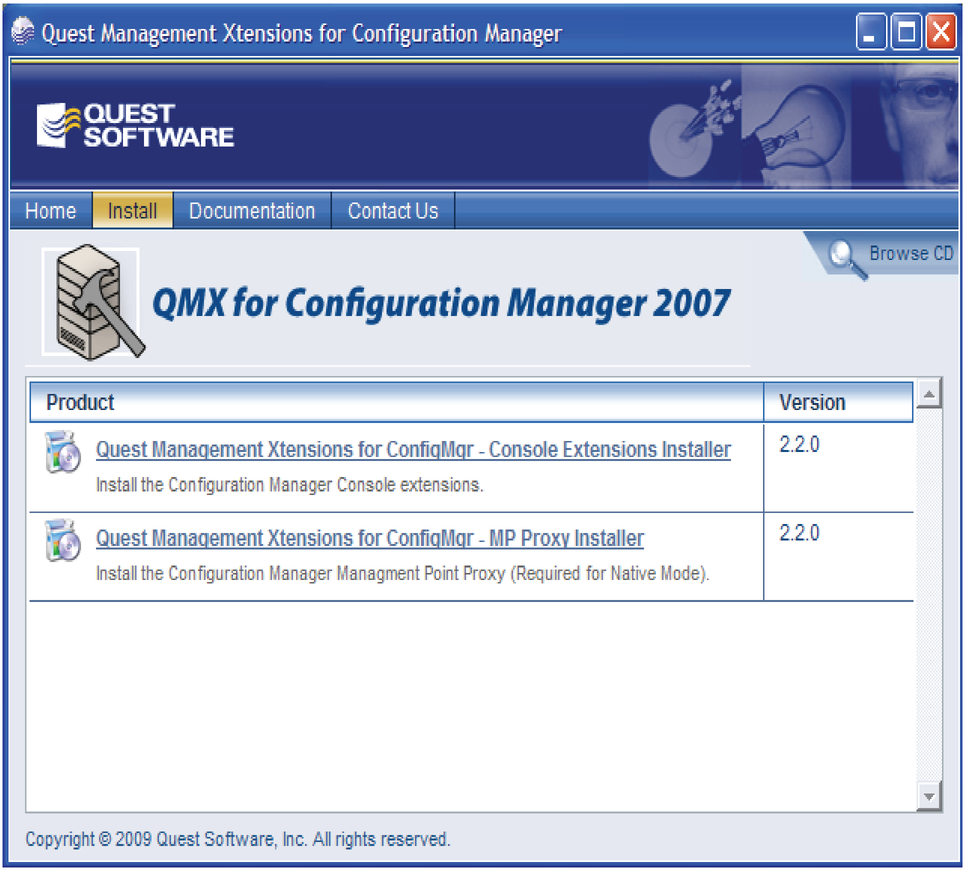
Installing the Console Extensions

You must install the Quest Configuration Manager Console extensions on all servers and workstations that run the Configuration Manager Console. Installing these extensions makes non-Windows management tasks available through the Configuration Manager Console.

You must have Administrator privileges in order to install the Configuration Manager Console extensions.

To install the Configuration Manager Console extensions

1. Insert the installation CD into the CD-ROM drive of the target machine to open the Autorun dialog:



QMX for Configuration Manager 2007

Product	Version
Quest Management Xtensions for ConfigMgr - Console Extensions Installer Install the Configuration Manager Console extensions.	2.2.0
Quest Management Xtensions for ConfigMgr - MP Proxy Installer Install the Configuration Manager Managment Point Proxy (Required for Native Mode).	2.2.0

2. Click the **Install** tab on the autorun dialog.
3. Click the **Quest Management Xtensions for ConfigMgr - Console Extensions Installer** link. (See Installing the MP Proxy for information about the MP Proxy Installer.)

   The *Configuration Manager Console Extensions Setup Wizard* starts automatically to lead you through the following dialogs:

   a) “Welcome” dialog

   b) License File

   c) Destination Folder

   d) Ready to Install

   e) "Finish" dialog.

4. Close the autorun dialog and open the Configuration Manager Console.

If you open the Configuration Manager Console during the installation, you must close and reopen it before the Quest Configuration Manager Console extensions display.

Unattended MMC Extension Installation

An unattended installation is a hands-free method of installing the Quest Configuration Manager Console extensions. This is convenient for system administrators who want to install the MMC extensions using the System Center Configuration Manager 2007 Distribute Software Wizard to a collection of Windows computers.

To install the console extensions into the default directory

1. Start the System Center Configuration Manager 2007 *Distribute Software* Wizard.
2. On the *Package* page, select **Create a new package and program without a definition file**.
3. On the *Source Files* page, select **Create a compressed version of the source files**.
4. On the *Source File Compression* page, select **Local drive on site server** and enter the following in the *Source directory* box: **D:\win32**.
5. On the *Program identification* page, enter the following into the *Command Line* box to install the MMC extensions to the default directory (C:\Program Files\Quest Software\QMX for ConfigMgr):

   ```
   msiexec /passive /i qmxcm.msi
   ```

   – OR –

   ```
   msiexec /silent /i qmxcm.msi
   ```

   Note ● The `/passive` switch shows a progress bar.

6. to install the MMC extensions to a specified directory, enter the following into the *Command Line* box:

```
msiexec /passive /i qmxcm.msi INSTALLDIR="C:\Some
other\install path"
```

Instead of using the *Distribute Software Wizard* to do an unattended MMC extension install, you can also use the *Create Package from Definition Wizard*.

5

Installing the Collections and Queries

- About Collections and Queries
- Installing Collections
- Installing Queries

About Collections and Queries

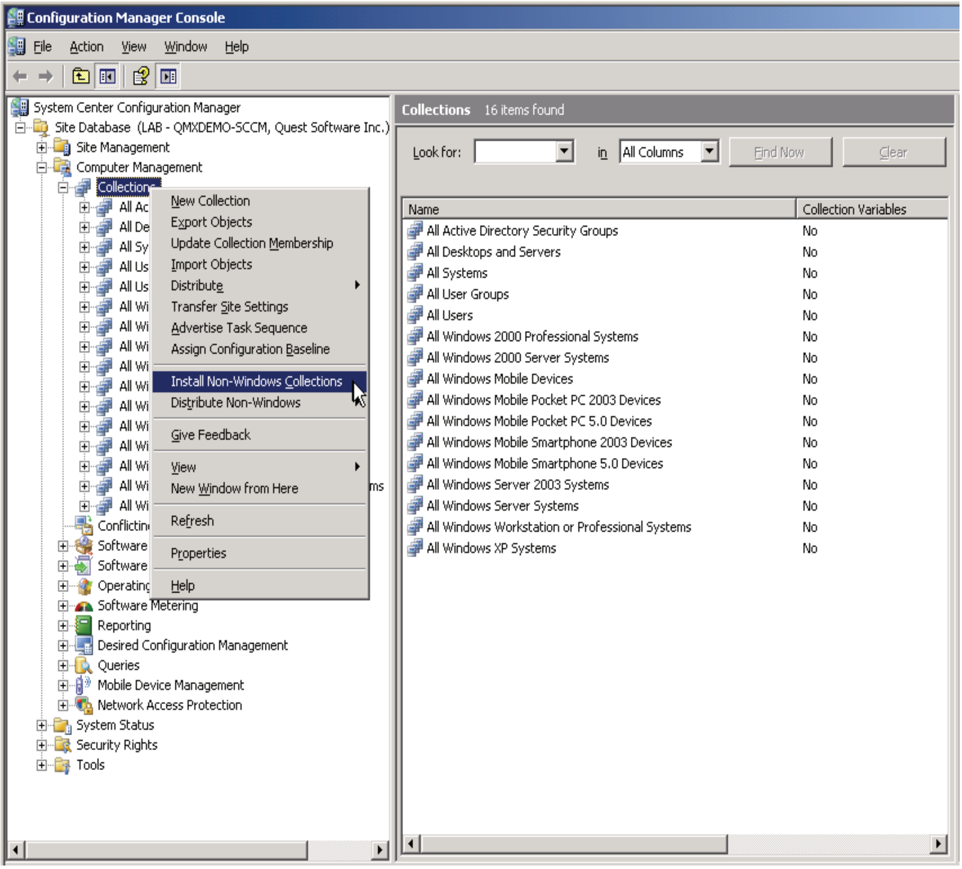
You use collections and queries to manage the resources on your network. You can install default QMX - Configuration Manager 2007 Agent-based collections and queries for the non-Windows operating systems you need. These will help you manage the non-Windows resources on your network. If you opt to install the collections and queries, be sure you are logged into Windows as a user with permission to create collections and queries in System Center Configuration Manager 2007. We recommend that you run it from the top-level site server.

Collections are automatically propagated down from higher to lower level sites; queries are not. Thus, you can install the collections once on your top-level site server and they propagate throughout your hierarchy. In contrast, you must install the queries individually on any site server where you want them to be available.

Installing Collections

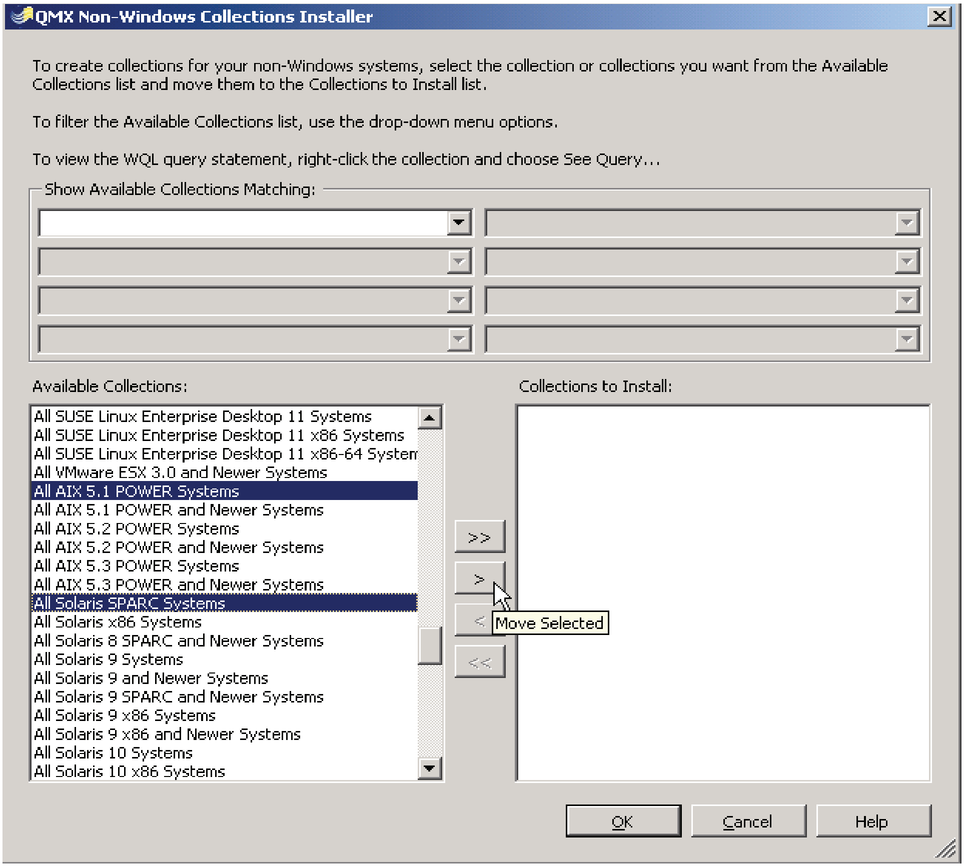
To install Collections

1. From the Configuration Manager console, navigate to **System Center Configuration Manager | Site Database | Computer Management**.



Name	Collection Variables
All Active Directory Security Groups	No
All Desktops and Servers	No
All Systems	No
All User Groups	No
All Users	No
All Windows 2000 Professional Systems	No
All Windows 2000 Server Systems	No
All Windows Mobile Devices	No
All Windows Mobile Pocket PC 2003 Devices	No
All Windows Mobile Pocket PC 5.0 Devices	No
All Windows Mobile Smartphone 2003 Devices	No
All Windows Mobile Smartphone 5.0 Devices	No
All Windows Server 2003 Systems	No
All Windows Server Systems	No
All Windows Workstation or Professional Systems	No
All Windows XP Systems	No

2. Right-click **Collections** and choose **Install Non-Windows Collections**.



QMX Non-Windows Collections Installer

To create collections for your non-Windows systems, select the collection or collections you want from the Available Collections list and move them to the Collections to Install list.

To filter the Available Collections list, use the drop-down menu options.

To view the WQL query statement, right-click the collection and choose See Query...

Show Available Collections Matching:

Available Collections:

All SUSE Linux Enterprise Desktop 11 Systems
All SUSE Linux Enterprise Desktop 11 x86 Systems
All SUSE Linux Enterprise Desktop 11 x86-64 Systen
All VMware ESX 3.0 and Newer Systems
All AIX 5.1 POWER Systems
All AIX 5.1 POWER and Newer Systems
All AIX 5.2 POWER Systems
All AIX 5.2 POWER and Newer Systems
All AIX 5.3 POWER Systems
All AIX 5.3 POWER and Newer Systems
All Solaris SPARC Systems
All Solaris x86 Systems
All Solaris 8 SPARC and Newer Systems
All Solaris 9 Systems
All Solaris 9 and Newer Systems
All Solaris 9 SPARC and Newer Systems
All Solaris 9 x86 Systems
All Solaris 9 x86 and Newer Systems
All Solaris 10 Systems
All Solaris 10 x86 Systems

Collections to Install:

3. Select the collection(s) you want in the *Available Collections* list and click the “**>**” button to move it to the *Collections to Install* list.

   Note ● Click the "**>>**" button to move all collections.

4. To filter the *Available Collections* list, use the drop-down menu options in the *Show Available Collections Matching* box.
5. To view the WQL query statement, right-click the Collection and choose **See Query...**
6. Click **OK** to create the collections listed in the *Collections to Install* list.

To update the collection membership

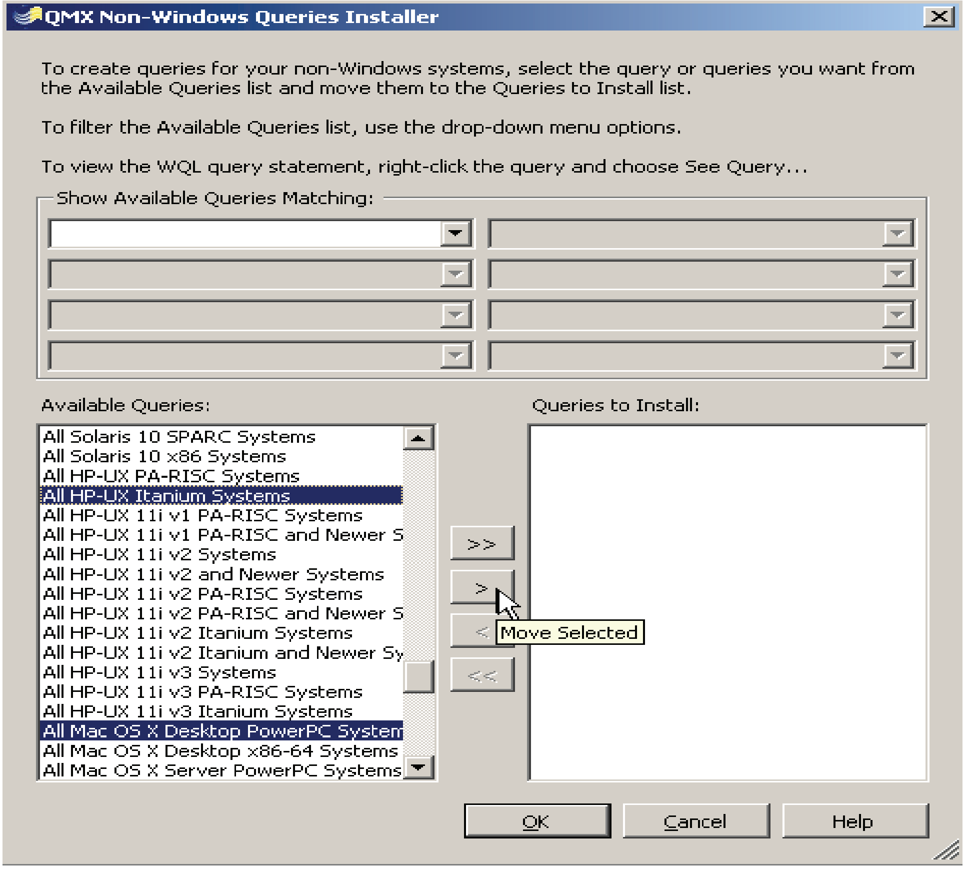
1. Right-click **Collections** and choose **Update Collection Membership**.
2. Click **Yes** at the *Update Collections* verification dialog.

Installing Queries

Installing the Queries is similar to installing the Collections.

To install Queries

1. Right-click **Queries** and choose **Install Non-Windows Queries**.


QMX Non-Windows Queries Installer

To create queries for your non-Windows systems, select the query or queries you want from the Available Queries list and move them to the Queries to Install list.

To filter the Available Queries list, use the drop-down menu options.

To view the WQL query statement, right-click the query and choose See Query...

Show Available Queries Matching:

Available Queries:

All Solaris 10 SPARC Systems
All Solaris 10 x86 Systems
All HP-UX PA-RISC Systems
All HP-UX Itanium Systems
All HP-UX 11i v1 PA-RISC Systems
All HP-UX 11i v1 PA-RISC and Newer S
All HP-UX 11i v2 Systems
All HP-UX 11i v2 and Newer Systems
All HP-UX 11i v2 PA-RISC Systems
All HP-UX 11i v2 PA-RISC and Newer S
All HP-UX 11i v2 Itanium Systems
All HP-UX 11i v2 Itanium and Newer Sy
All HP-UX 11i v3 Systems
All HP-UX 11i v3 PA-RISC Systems
All HP-UX 11i v3 Itanium Systems
All Mac OS X Desktop PowerPC System
All Mac OS X Desktop x86-64 Systems
All Mac OS X Server PowerPC Systems

Queries to Install:

2. To create queries for your non-Windows systems, select the query or queries you want in the *Available Queries* list and click the "**>**" button to move them to the *Queries to Install* list.

   Note • Click the "**>>**" button to move all queries.

3. To filter the *Available Queries* list, use the drop-down menu options in the *Show Available Queries Matching* box.
4. To view the WQL query statement, right-click the Query and choose **See Query...**
5. Click **OK** to create the queries listed in the *Queries to Install* list.

6

Installing the License

- About Licensing
- Managing Licenses for Multiple Central Sites
- Using the License Manager

About Licensing

When you purchase QMX - Configuration Manager 2007 you will receive an email that contains one License file and Serial Number. You must import the license using the License Manager.

If your system only has one Central Site, then proceed to Using the License Manager. If you have more than one Central Site server, refer to Managing Licenses for Multiple Central Sites for information on how to obtain and install multiple licenses.

The license file can only be installed by the Administrator or a user who has Read and Modify security rights to the site security class.

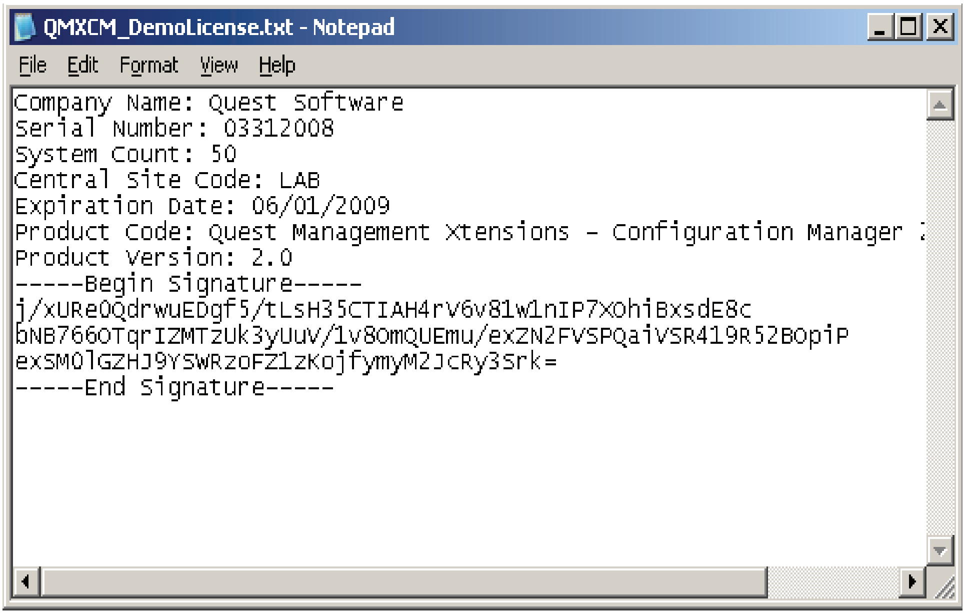
Managing Licenses for Multiple Central Sites

Quest Software, Inc. allows you to allocate your total license count among one or multiple System Center Configuration Manager 2007 Central Sites. To help you maintain license compliance within your organization, you can generate unique license keys for each Central Site and track the number of servers and workstations for each. To allocate the number of systems among Central Sites and generate the resulting new license keys, open the Quest Customer License Web site located at: http://java.quest.com/tims/licenseFileEntry.do?licenseNumber=.

You will need your three-character System Center Configuration Manager 2007 Central Site codes to which you will allocate your licenses. If you decide to add Central Sites later or make any other changes, you can revisit the Quest Customer License Web site to re-allocate your licenses and generate new license files to install on each Central Site server. When you generate new license files, you will receive a new email with the newly generated license files attached.

Using the License Manager

You will receive a license file from Quest that looks similar to this:



```
Company Name: Quest Software
Serial Number: 03312008
System Count: 50
Central Site Code: LAB
Expiration Date: 06/01/2009
Product Code: Quest Management Xtensions - Configuration Manager 2
Product Version: 2.0
-----Begin Signature-----
j/xURe0QdrwuEDgf5/tLsH35CTIAH4rV6v81w1nIP7XOhiBxsdE8c
bNB766OTqrIZMTzUk3yUuV/1v8OmQUEmu/exZN2FVSPQaiVSR419R52BOpiP
exSM0lGZHJ9YSWRzoFZ1zKojfymyM2JcRy3Srk=
-----End Signature-----
```

QMX - Configuration Manager 2007 manages its own licenses. The License Manager imports the license file, validates the data, and enters it into the Site Control File. The total number of licenses is compared to the number of clients on your site. The total number of client systems is based on a WQL query against the System Center site database.

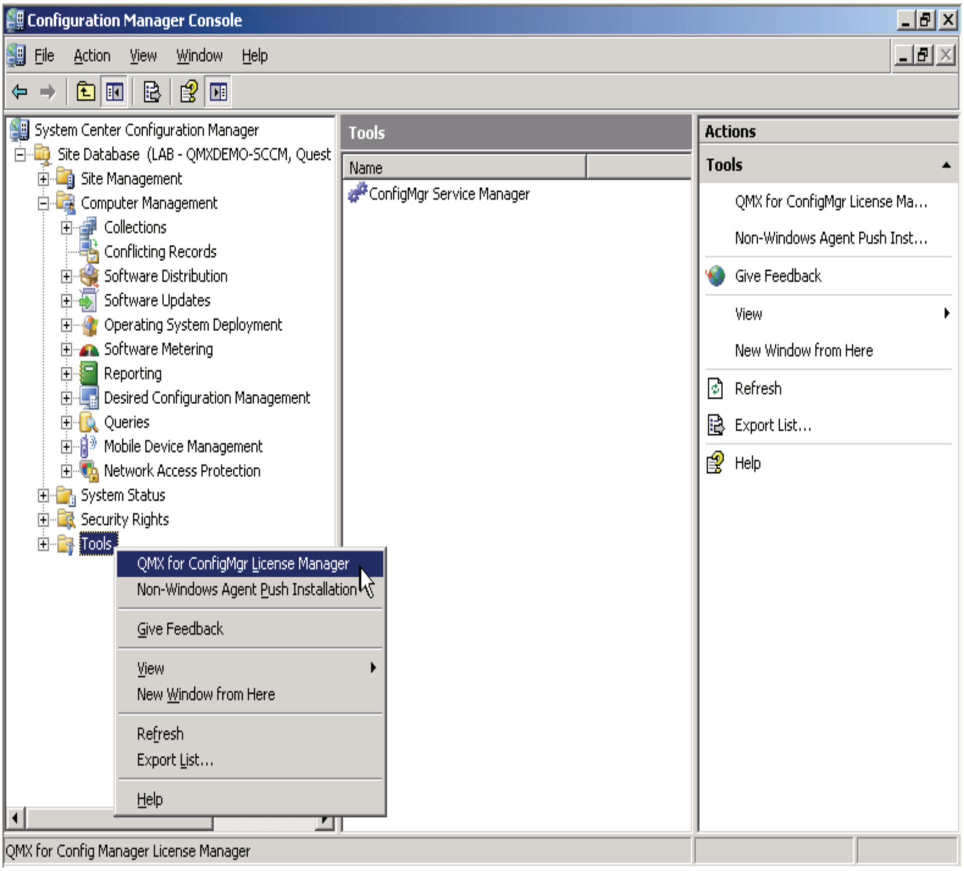
The QMX - Configuration Manager 2007 License Manager uses the System Center Configuration Manager 2007 Site Control File. The license must be installed on the top-level site server. QMX - Configuration Manager 2007 then propagates the license down to the other site servers.

Adding a License

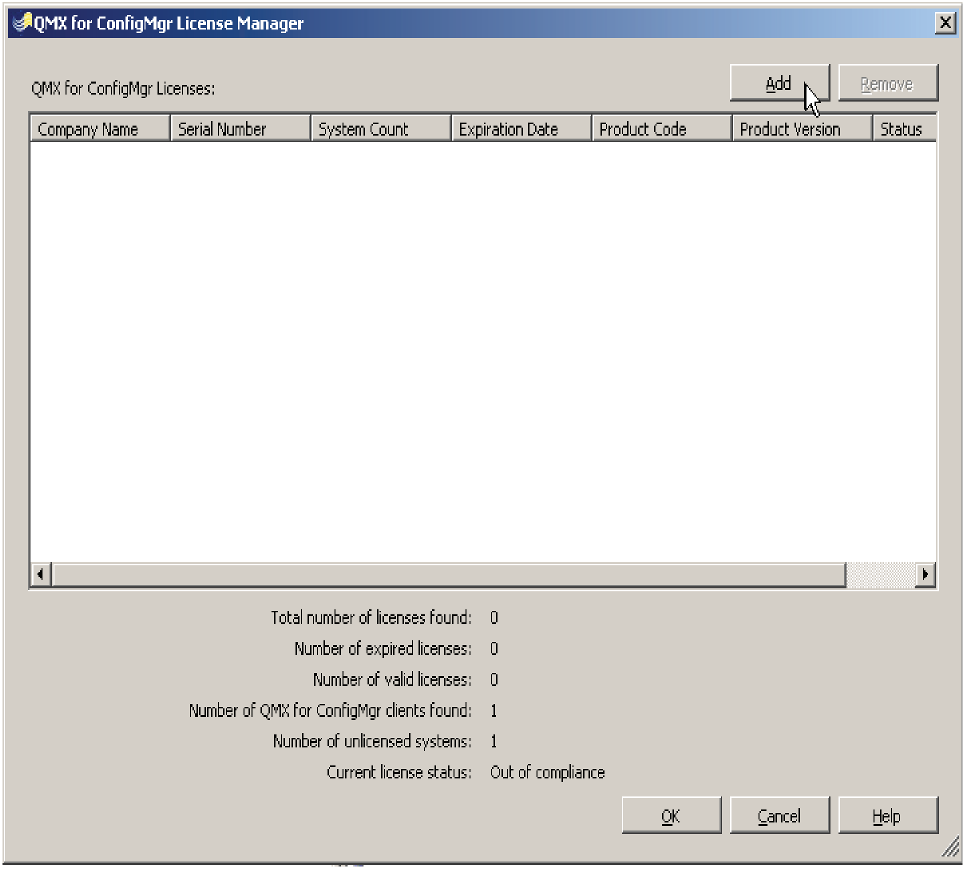
In order to add or remove a license, you must start the License Manager from the Central Site server.

To add a new license key

1. Download the license file you received from Quest to a convenient location.
2. Navigate to your top-level site server in the Configuration Manager Console.
3. From the Configuration Manager Console, navigate to **System Center Configuration Manager | Site Database**.


Configuration Manager Console
File Action View Window Help
System Center Configuration Manager
Site Database (LAB - QMXDEMO-SCCM, Quest
Site Management
Computer Management
Collections
Conflicting Records
Software Distribution
Software Updates
Operating System Deployment
Software Metering
Reporting
Desired Configuration Management
Queries
Mobile Device Management
Network Access Protection
System Status
Security Rights
Tools
QMX for ConfigMgr License Manager
Non-Windows Agent Push Installation
Give Feedback
View
New Window from Here
Refresh
Export List...
Help
Tools
Name
ConfigMgr Service Manager
Actions
Tools
QMX for ConfigMgr License Ma...
Non-Windows Agent Push Inst...
Give Feedback
View
New Window from Here
Refresh
Export List...
Help
QMX for Config Manager License Manager

4. Right-click **Tools** and choose **QMX for ConfigMgr License Manager** to open the *License Manager* dialog:



QMX for ConfigMgr License Manager

QMX for ConfigMgr Licenses:

Company Name	Serial Number	System Count	Expiration Date	Product Code	Product Version	Status

Total number of licenses found:	0
Number of expired licenses:	0
Number of valid licenses:	0
Number of QMX for ConfigMgr clients found:	1
Number of unlicensed systems:	1
Current license status:	Out of compliance

The License Manager connects to the Central Site server site control file and lists all of the existing QMX - Configuration Manager 2007 licenses.

5. Click **Add** to add a new license key to the License Manager.
6. Navigate to the license file.
7. Click **Open** to select the license file.
8. Click **OK** at the *License Manager* dialog.

   System Center Configuration Manager 2007 propagates the information down to the site control files of each child sites.

Removing a License

To remove a license from the License Manager

1. Open the License Manager (see Adding a License)
2. Select the license you want to remove.
3. Click **Remove** to delete a Quest license from the License Manager.
4. Click **OK** if you are sure you want to delete the license key.

   The *License Removed* dialog displays, confirming the removal of that license key.

7

Installing the Agent

- Important Agent Installation Considerations
- Installing the Agent with the Wizard
- Installing the Agent Manually
- Installing a QMX Agent in an Image
- Using the RedHat Linux KickStart System
- Using the SUSE AutoYaST System
- Using the HP-UX Mount All Filesystems Option

Important Agent Installation Considerations

You must install the QMX - Configuration Manager 2007 Agent on each non-Windows resource you want to manage with System Center Configuration Manager 2007. You can manually install the QMX - Configuration Manager 2007 Agent or use the QMX - Configuration Manager 2007 Agent Installation Wizard as explained in these topics:

- Using the Agent Installation Wizard
- Installing the Agent Manually

To rapidly install the QMX - Configuration Manager 2007 Agent to large numbers of identical clients, QMX - Configuration Manager 2007 also works with the RedHat Linux KickStart system and the SUSE's AutoYaST. See Using the RedHat Linux KickStart System and Using the SUSE AutoYaST System for those details.

Before you attempt to install the QMX - Configuration Manager 2007 Agent review these pre-installation verification steps discussed in Preparing for Installation:

- Ensure Site Codes Resolve to a Primary Site
- Verify the Site Code
- Ensure WebDav is Installed
- Ensure SSH Access and Root Privileges
- Ensure that the SSH Server is Running
- Enable SSH on Target Mac OS X Computers
- Verify the Port Number
- Resolve Hostnames
- Prepare Installation Files for Install
- Supply the Trusted Root Key
- Running QMX in Native Mode

Installing the Agent with the Wizard

In order to make installing the QMX - Configuration Manager 2007 Agent on multiple clients as easy as possible, includes a wizard that “pushes” the Agent out to non-Windows clients.

The QMX - Configuration Manager 2007 Agent Installation Wizard can install the Agent on more than one operating system in one operation. For example, it can install the Agent to a collection containing Mac OS X, Solaris, and Linux machines. The wizard installs the correct version of the QMX - Configuration Manager 2007 Agent on each operating system.

You must have the SSH daemon running on the systems. However, SSH is only installed by default on Solaris 9 (or higher), HP-UX, Mac, Red Hat Linux, and SUSE Linux. You must manually install SSH on AIX, and older versions of Solaris clients manually. While Mac comes with SSH, you need to enable it because it is turned off by default. See Enable SSH on Target Mac OS X Computers.

The wizard steps you through the process of entering the data it needs to connect to the managed hosts, send the files, and provide the QMX - Configuration Manager 2007 Agent installation options.

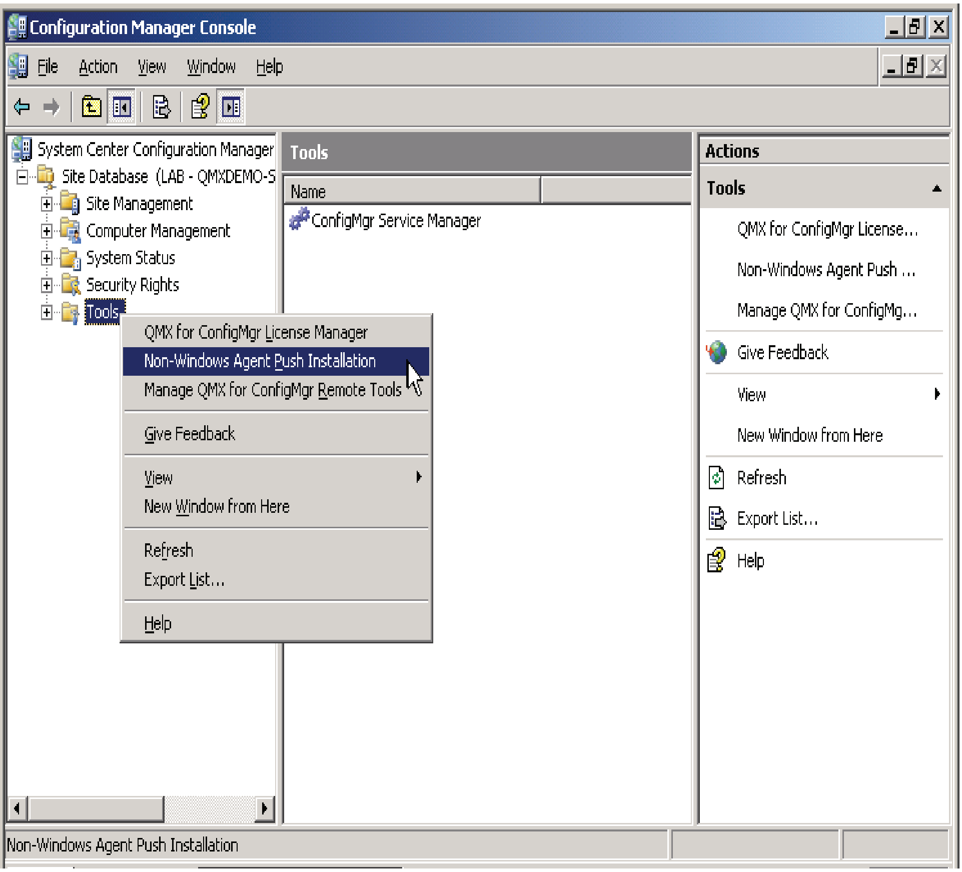
The wizard enables you to select the following QMX - Configuration Manager 2007 Agent Installation parameters:

- Agent Installer Settings
- SSH Connection Settings
- Root Privileges Settings
- Active Directory Settings
- Identified Non-Windows Systems
- Ready to Install the Agent
- Installation Status
- Agent Installation Completed

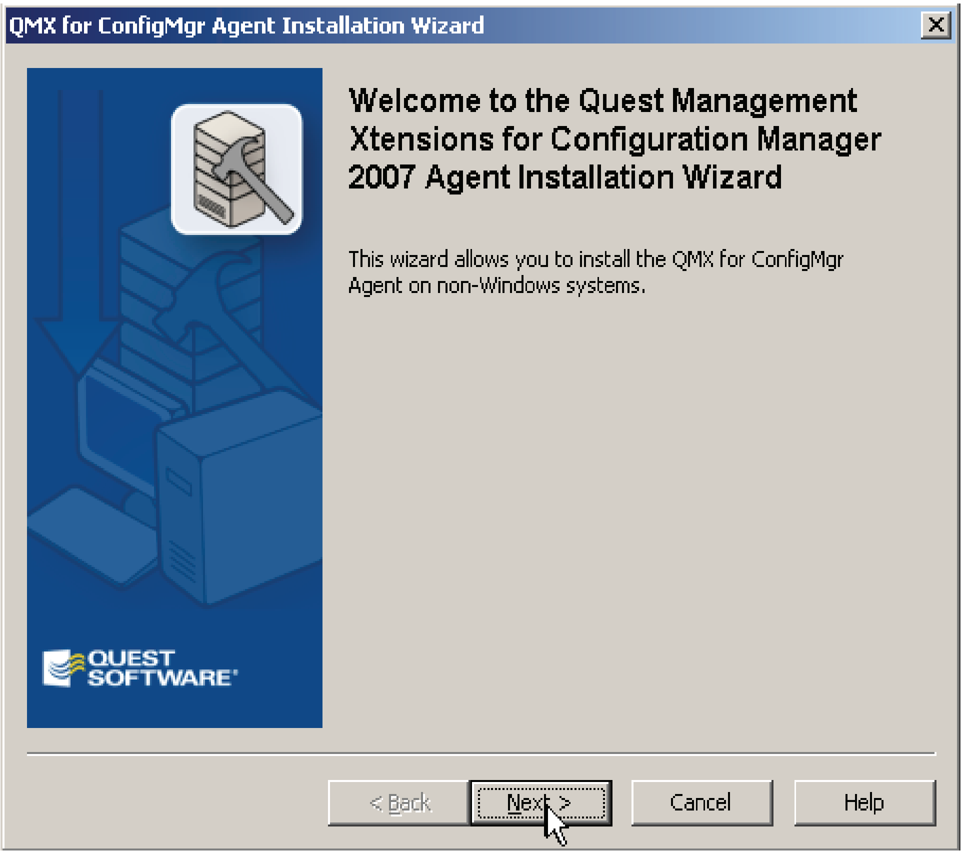
Using the Agent Installation Wizard

To start the QMX - Configuration Manager 2007 Agent Installation Wizard

1. From the Configuration Manager Console, right-click **Tools** and choose **Non-Windows Agent Push Installation**.


Configuration Manager Console
File
Action
View
Window
Help
System Center Configuration Manager
Site Database (LAB - QMXDEMO-S
Site Management
Computer Management
System Status
Security Rights
Tools
Tools
Name
ConfigMgr Service Manager
QMX for ConfigMgr License Manager
Non-Windows Agent Push Installation
Manage QMX for ConfigMgr Remote Tools
Give Feedback
View
New Window from Here
Refresh
Export List...
Help
Actions
Tools
QMX for ConfigMgr License...
Non-Windows Agent Push ...
Manage QMX for ConfigMg...
Give Feedback
View
New Window from Here
Refresh
Export List...
Help
Non-Windows Agent Push Installation

The QMX - Configuration Manager 2007 Agent Installation Wizard starts:



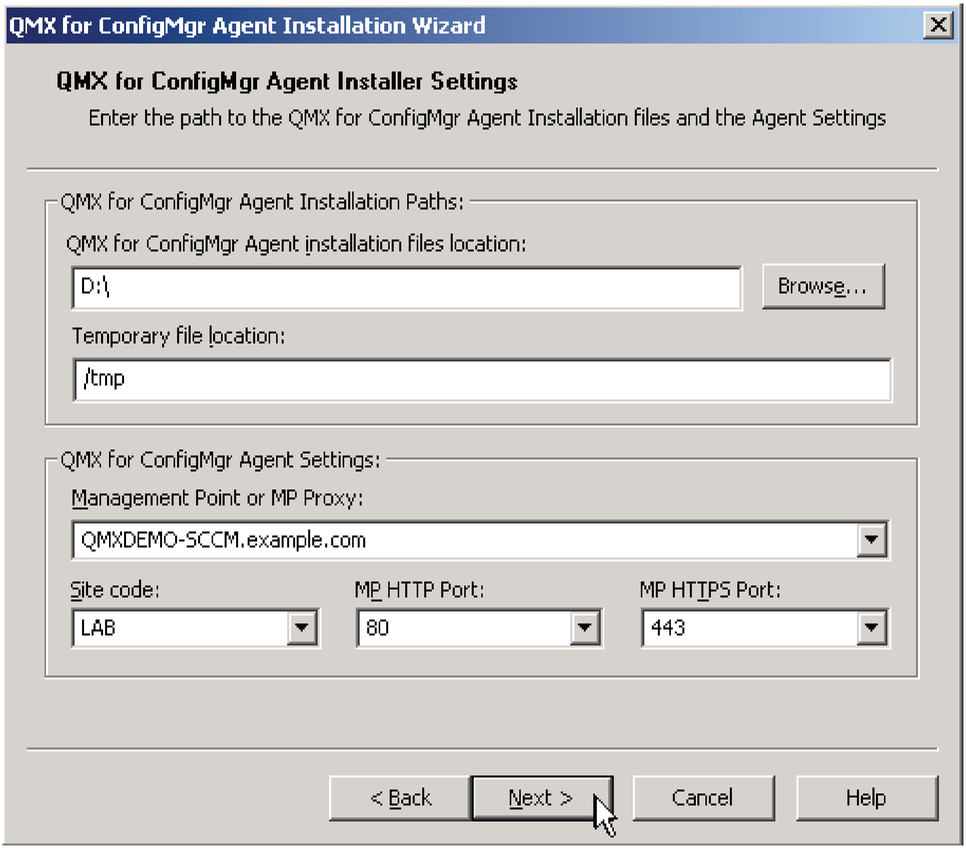
QMX for ConfigMgr Agent Installation Wizard

Welcome to the Quest Management Xtensions for Configuration Manager 2007 Agent Installation Wizard

This wizard allows you to install the QMX for ConfigMgr Agent on non-Windows systems.

2. Click **Next** to open the Agent Installer Settings dialog.

Agent Installer Settings



QMX for ConfigMgr Agent Installation Wizard

QMX for ConfigMgr Agent Installer Settings

Enter the path to the QMX for ConfigMgr Agent Installation files and the Agent Settings

QMX for ConfigMgr Agent Installation Paths:

QMX for ConfigMgr Agent installation files location: D:\

Temporary file location: /tmp

QMX for ConfigMgr Agent Settings:

Management Point or MP Proxy: QMXDEMO-SCCM.example.com

Site code: LAB

MP HTTP Port: 80

MP HTTPS Port: 443

To connect and send files to the clients

1. Under *QMX for ConfigMgr Agent Installation Paths*,

   a) Enter or **Browse** to select to the Installation media or the directory containing the installation files.

   b) Enter the path to the temporary file location on the client.

   Note • This directory will need to temporarily hold large installation files during the QMX - Configuration Manager 2007 Agent installation. Most people use `/tmp`, a temporary file system on most non-Windows clients. However, you can use any file system on which you do not mind storing temporary files. For example, you can use the `/opt filesystem`. In most cases there are no problems if you use `/tmp` for this field. Check with your System Administrator for the correct directory to use on the target system.

2. Under *QMX for ConfigMgr Agent Settings*,

   a) Enter the Fully Qualified Domain Name for the System Center Configuration Manager 2007 Management Point (or, MP Proxy, if you are installing the Agent for native mode.)

   Note ● You must install the MP Proxy before you install the QMX Agent if you are installing QMX - Configuration Manager 2007 into a native mode environment. (See Installing the MP Proxy.)

   b) Select or enter the Site Code.

   Note ● The Management Point and Site Code you select on this dialog will be applied to all systems you select to install the QMX - Configuration Manager 2007 Agent on unless you manually edit the hostnames. See Identified Non-Windows Systems for information about editing an entry from the list of Systems to Install.

   c) Enter the Management Point HTTP Port number. (The default port is 80.)

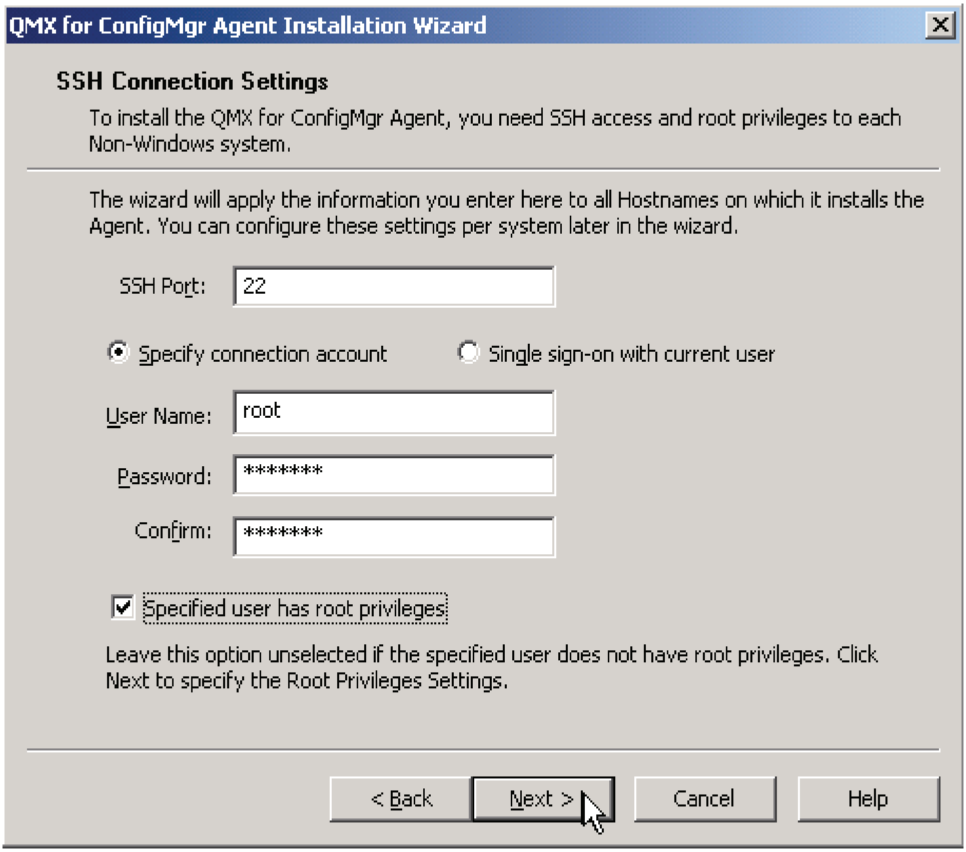
   Note ● The Agent communicates to the management point by means of http when in mixed mode and https when in native mode. When in native mode, if the MP Proxy is not installed on the same machine as the MP, this must be set to the MP's http port. Typically port 80.

   d) Enter the Management Point HTTPS Port number. (The default port is 443; optional in mixed mode.)

   Note ● When in native mode, if SSL is enabled for the Web site, the Agent uses https instead of plain http to communicate to the MP Proxy. If the MP Proxy is not installed on the same machine as the Management Point, this must be set to the MP's https port. If System Center Configuration Manager 2007 is in mixed mode, the https port will not be active. This value should be set to the value the https port will have once native mode is enabled. Typically port 443.

3. Click **Next** to open the SSH Connection Settings dialog.

SSH Connection Settings



QMX for ConfigMgr Agent Installation Wizard

SSH Connection Settings

To install the QMX for ConfigMgr Agent, you need SSH access and root privileges to each Non-Windows system.

The wizard will apply the information you enter here to all Hostnames on which it installs the Agent. You can configure these settings per system later in the wizard.

SSH Port: 22

● Specify connection account ○ Single sign-on with current user

User Name: root

Password: *******

Confirm: *******

☑ Specified user has root privileges

Leave this option unselected if the specified user does not have root privileges. Click Next to specify the Root Privileges Settings.

1. Enter the **SSH Port** number.

   Note • Port 22 is the usual default and will probably not need to change.

To install the QMX - Configuration Manager 2007 Agent, you need SSH access and root privileges to each non-Windows system. There are two ways to obtain SSH access, either by specifying a user that has SSH privileges to the target system or by allowing the current user to authenticate to the target systems using Single Sign-On.

2. Select one of the following radio buttons:
   - **Specify connection account** to specify a user name account.

  - Enter the User Name of a user that has SSH privileges to the target system.
  - Enter the Password of a user that has SSH privileges to the target system and confirm it.

– OR –

- **Single Sign-on with current user** to authenticate access to the target systems using Active Directory.

Note ● When you select *Single sign-on with current user*, the *User Name*, *Password,* and *Confirm* fields are de-selected. This makes it possible for someone without root access to install the QMX - Configuration Manager 2007 Agent. However, you must have it set up correctly and have proper access rights.

The Single Sign-On capabilities use Active Directory authentication using Vintela Authentication Services from Quest Software. Vintela Authentication Services (VAS) is another Quest Software product that uses Active Directory for cross-platform identity integration and authentication. (See What is VAS?for more information.)

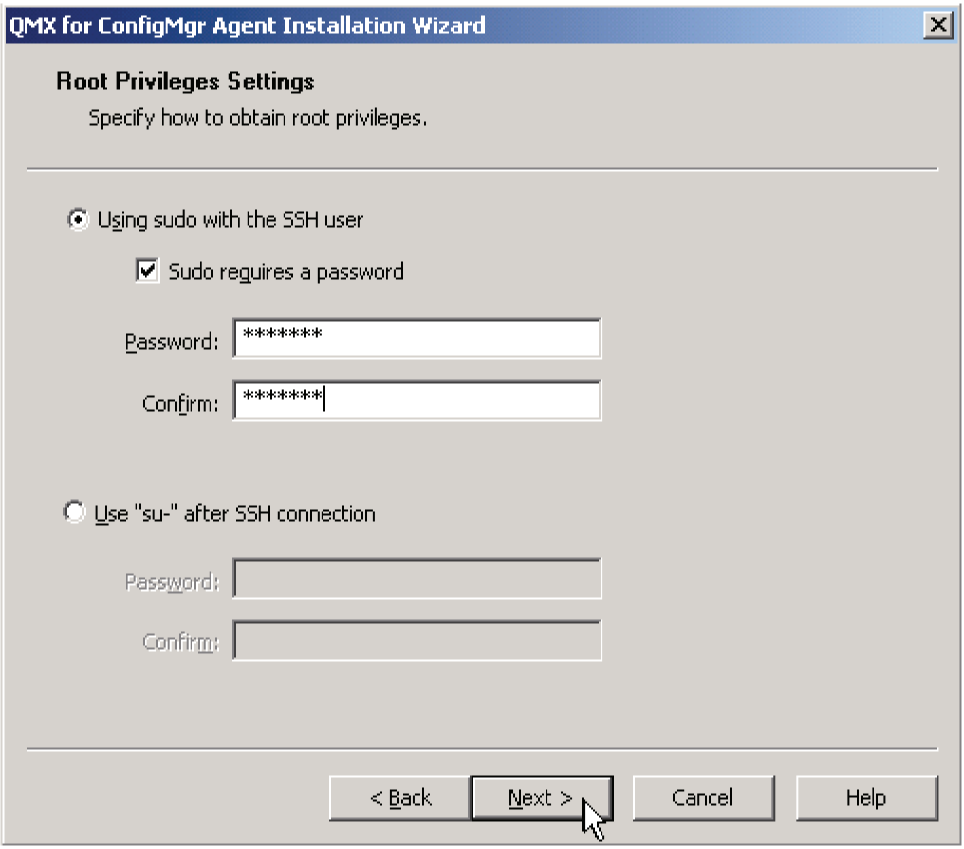
To authenticate with VAS, you must be logged in as a Unix-enabled user and you must have a version of the SSH client and server that supports GSSAPI. Go to http://rc.quest.com/topics/openssh/ to download the latest release of OpenSSH. The Quest version of OpenSSH defaults to authenticating users by means of the GSSAPI-with-MIC mechanism, and authenticating hosts using GSSAPI-KEX. Quest-OpenSSH works in conjunction with Vintela Authentication Services (VAS), to allow secure shell single sign-on to non-Windows hosts that have been joined to Active Directory domains.

3. Select *Specified user has root privileges*, if applicable.

   Note ● If the specified user does not have root privileges, leave this option unselected.

4. Click **Next**.
   - If the *Specified user has root privileges* option is un-selected when you click **Next**, it opens the Root Privileges Settings dialog where you can specify the root privilege settings.
   - If the *Specified user has root privileges* option is selected when you click **Next**, it opens the Active Directory Settings dialog.

Root Privileges Settings



QMX for ConfigMgr Agent Installation Wizard

Root Privileges Settings

Specify how to obtain root privileges.

● Using sudo with the SSH user

☑ Sudo requires a password

Password: ********

Confirm: ********

○ Use "su-" after SSH connection

Password:

Confirm:

There are two ways to obtain root privileges, either by using `sudo` with the SSH user or by using `su` after the SSH connection.

To specify how to obtain root privileges

1. Select one of the following radio buttons:
   - **Using sudo with the SSH user** to run processes with super user privileges.

   Note • This option uses the UNIX-based utility sudo and is the preferred method to the "su –" option as it provides for much finer grained privilege granting than using the all-powerful root account. It does, however, need to be configured properly before attempting to install, and is therefore somewhat more inconvenient.

- Select **Sudo requires a password** option if sudo is configured to require one. When you check this option, it enables the Password and Confirm boxes. Enter the password of the specified user and confirm it.

– OR –

- **Use "su-" after SSH connection** to log into the root account after establishing the initial connection. Many machines have SSH configured so that the root account cannot log in remotely. When you select this option, you must enter the password of the root account and confirm it.

Note • Your system administrator has turned off remote connections for root for a reason. It might be a good idea to check with him before selecting this option.

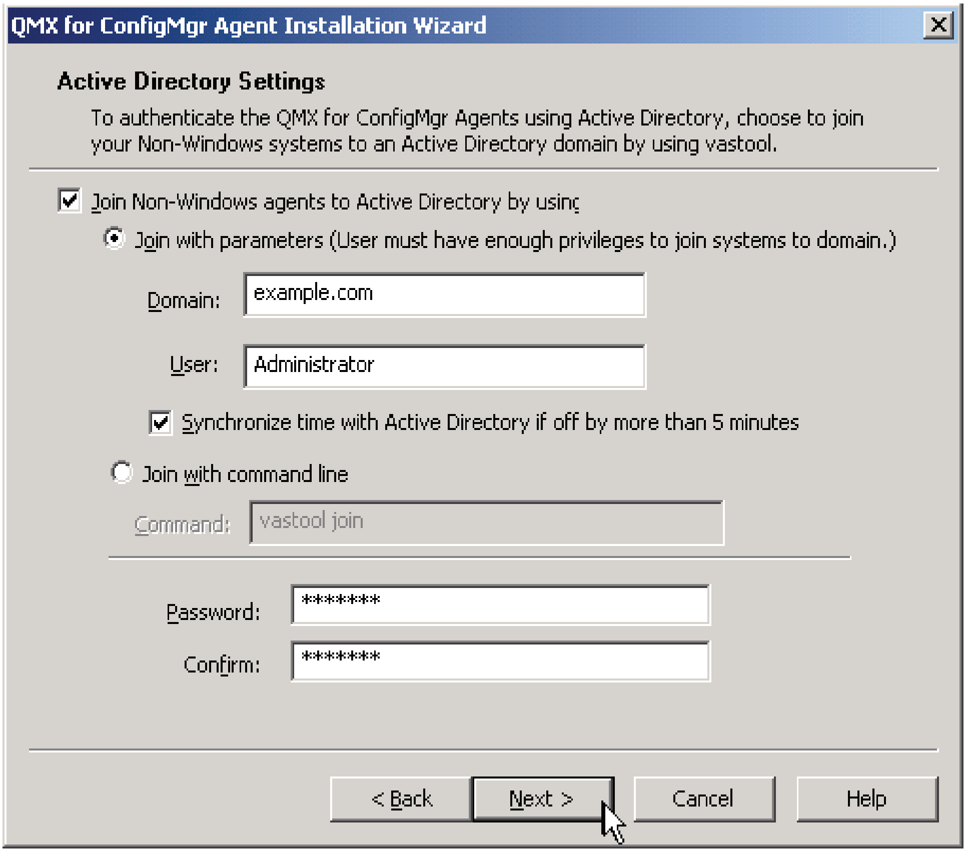
- Enter the Root Password and confirm it.

2. Click **Next** to open the Active Directory Settings dialog.

Active Directory Settings

Use the *Active Directory Setting* dialog to join your non-Windows systems to an Active Directory domain.

If you do not have Active Directory available, the QMX - Configuration Manager 2007 Agent Installation Wizard skips this dialog.



Active Directory Settings

To authenticate the QMX for ConfigMgr Agents using Active Directory, choose to join your Non-Windows systems to an Active Directory domain by using vastool.

☑ Join Non-Windows agents to Active Directory by usinc

● Join with parameters (User must have enough privileges to join systems to domain.)

Domain: example.com

User: Administrator

☑ Synchronize time with Active Directory if off by more than 5 minutes

○ Join with command line

Command: vastool join

Password: *******

Confirm: *******

Sparse-root zones cannot be joined to Active Directory; thus, do not select the **Join Non-Windows agents to Active Directory by using vastool** option during installation. This will cause the installation to fail.

1. Select **Join Non-Windows agents to Active Directory by using vastool**.
2. Select one of the following radio buttons:
   - **Join with parameters (User must have enough privileges to join systems to domain.)**
     - Enter the Domain name.
     - Enter User name.

- Select **Synchronize time with AD if off by more than 5 minutes** to synchronize the system time with Active Directory.

Note ● In order to join your non-Windows systems to your Active Directory domain, there cannot be more than a five minute disparity between the client's system time and that of the Active Directory server. If the difference is more than five minutes between the two systems, you must select this option in order to run the `vastool timesync` command. This will synchronize the clocks of both systems. If you select this option, it will only synchronize the two systems if they are more than five minutes off, otherwise the time will not be changed.

– OR –

- **Join with command line** to edit the `vastool join` command arguments in the *Command* box. The basic join command is:

```
-s -u Administrator join EXAMPLE.com
```

where *Administrator* is the user name and *EXAMPLE.com* is the domain name.

Note ● The basic `join` command works for all platforms. For more information about using the `vastool` command, please see the `vastool.html` file in the docs directory.

- Enter the Password for the user specified in the join command and confirm it.

3. Once you have entered the Active Directory Settings, click **Next** to open the Identified Non-Windows Systems dialog.

If your clients do not already have a licensed version of Vintela Authentication Services (or VAS) installed on them, the QMX - Configuration Manager 2007 Agent Installation Wizard automatically installs a VAS client agent. However, without purchasing and installing the license for VAS, QMX - Configuration Manager 2007 only enables the VAS features that are directly relevant to Active Directory domain joins and some additional security benefits. To enable the full feature set of VAS, you must purchase and install a license.

Vintela Authentication Services (or VAS) is another Quest Software product that uses Active Directory for cross-platform identity integration and authentication. (See What is VAS? for more information.)

What is VAS?

The QMX - Configuration Manager 2007 Agent installation automatically installs Vintela Authentication Services from Quest Software. Vintela Authentication Services (VAS) is another Quest Software product that uses Active Directory for cross-platform identity integration and authentication. For more information about VAS. See *Integrating with VAS* in the *QMX - Configuration Manager 2007 Administrator's Guide* or http://www.quest.com/Vintela-Authentication-Services for more information about VAS.

While QMX - Configuration Manager 2007 2.2 installs a full version of VAS, it will have limited functionality unless you purchase a license for it. QMX - Configuration Manager 2007 installs VAS specifically to enable Single Sign-On capabilities using Active Directory authentication.

How Upgrading QMX - Configuration Manager 2007 Affects VAS

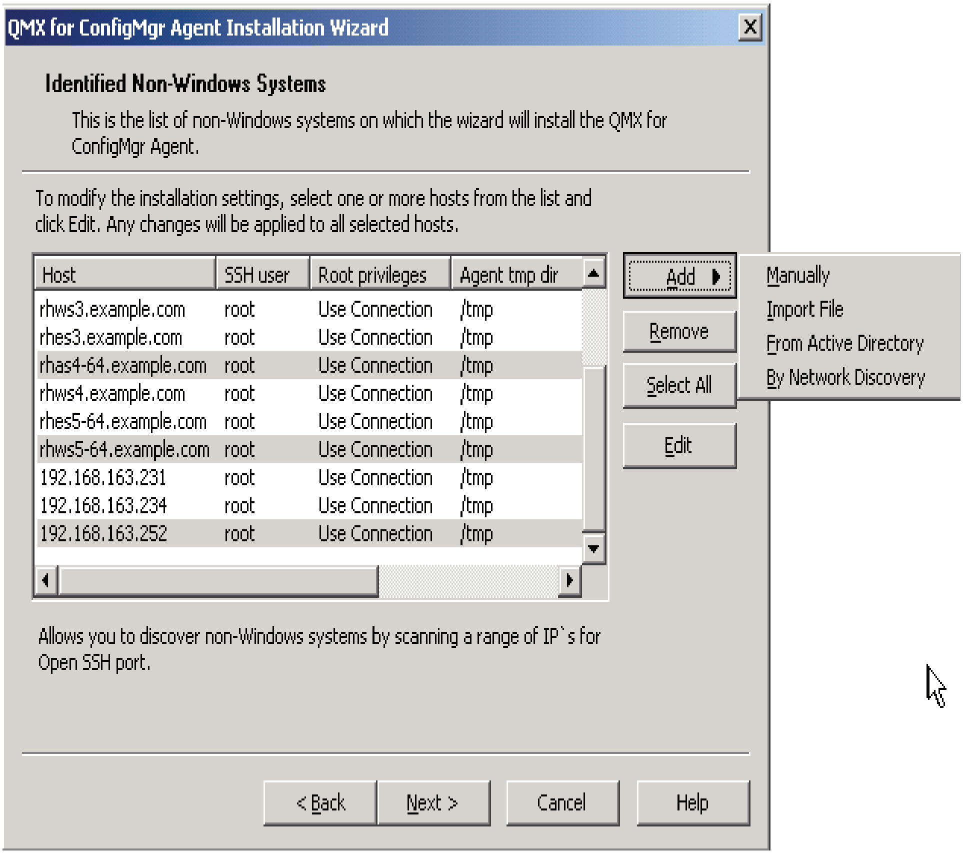
When upgrading QMX - Configuration Manager 2007 to version 2.2, the installation process does not automatically upgrade `vashost` to VAS 3.5.1.

- If you already have a licensed version of VAS installed, the upgrade to QMX - Configuration Manager 2007 2.2 will not upgrade your current version of VAS. If you want to upgrade VAS, you must do it manually. (See the "*Upgrading VAS*" section of the *Integrating with VAS* chapter in the *QMX - Configuration Manager 2007 Administrator's Guide*.)
- If you have `vashost` or the limited, unlicensed version of VAS on your client and your system is not joined to the Active Directory domain, the upgrade to QMX - Configuration Manager 2007 2.2 will automatically upgrade `vashost` or VAS to VAS 3.5.1.
- If you have `vashost` or the limited, unlicensed version of VAS on your client and your system is joined to the domain, the upgrade to QMX - Configuration Manager 2007 2.2 will not upgrade `vashost` or VAS. To upgrade `vashost` or VAS to VAS 3.5.1, Quest Software, Inc. recommends that you use the *Script or Custom Command* distribution method to distribute a software package that includes the updated version of the VAS client as described in Using the Wizard to Upgrade the Client.

Go to: https://support.quest.com/SUPPORT/index?page=home to download the VAS 3.5.1 client.

Identified Non-Windows Systems

This dialog allows you to build a list of non-Windows systems on which to install the QMX - Configuration Manager 2007 Agent.



Identified Non-Windows Systems

This is the list of non-Windows systems on which the wizard will install the QMX for ConfigMgr Agent.

To modify the installation settings, select one or more hosts from the list and click Edit. Any changes will be applied to all selected hosts.

Host	SSH user	Root privileges	Agent tmp dir
rhws3.example.com	root	Use Connection	/tmp
rhes3.example.com	root	Use Connection	/tmp
rhas4-64.example.com	root	Use Connection	/tmp
rhws4.example.com	root	Use Connection	/tmp
rhes5-64.example.com	root	Use Connection	/tmp
rhws5-64.example.com	root	Use Connection	/tmp
192.168.163.231	root	Use Connection	/tmp
192.168.163.234	root	Use Connection	/tmp
192.168.163.252	root	Use Connection	/tmp

Allows you to discover non-Windows systems by scanning a range of IP`s for Open SSH port.

To add systems to the list

1. See Identifying Hostnames for information about the various methods of adding systems to the list.

To delete systems from the list

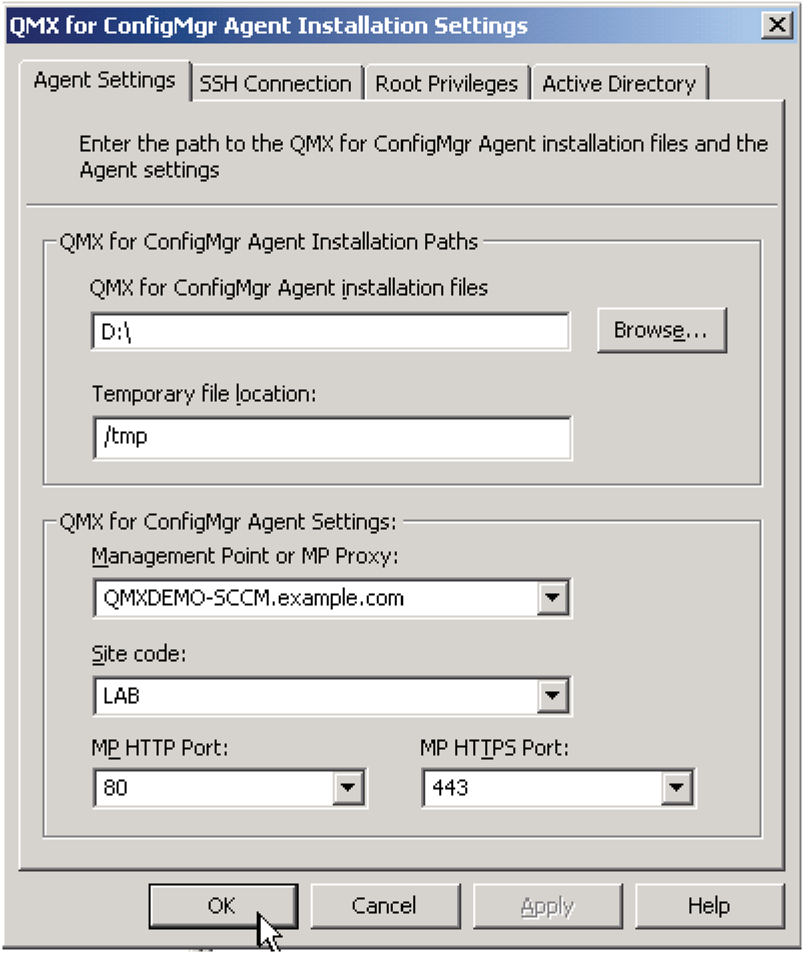
1. Select one or more individual system(s) or click **Select All**.
2. Click **Remove**.

To edit an entry in the list of systems

The settings you selected on the Agent Installer Settings, the SSH Connection Settings, the Root Privileges Settings, and the Active Directory Settings dialogs will be applied to all Hostnames on which you install the QMX - Configuration Manager 2007 Agent unless you manually change the settings for a specific system. For example, you may want to apply a unique Computer name to a specific system before you install the QMX - Configuration Manager 2007 Agent on all the systems listed on the Identified Non-Windows Systems dialog.

1. Select the Hostname(s) or IP Address(s) in the list and click **Edit** to open the Agent Installation Settings dialog.

Agent Installation Settings



Enter the path to the QMX for ConfigMgr Agent installation files and the Agent settings

QMX for ConfigMgr Agent Installation Paths

QMX for ConfigMgr Agent installation files: D:\

Temporary file location: /tmp

QMX for ConfigMgr Agent Settings:

Management Point or MP Proxy: QMXDEMO-SCCM.example.com

Site code: LAB

MP HTTP Port: 80

MP HTTPS Port: 443

2. Customize any settings for the selected hostname(s).
3. Click **OK** to return to the Identified Non-Windows Systems dialog.
4. Once the list of non-Windows systems is built, click **Next** to open the Ready to Install the Agent dialog.

Identifying Hostnames

There are several methods of identifying systems. You can identify systems manually, by importing a text file listing hostnames and IP addresses of the systems, by searching for VAS-enabled systems in a list of Active Directory containers, or by scanning IP address ranges for open SSH ports.

To add Hostnames

1. Click **Add**.

   The QMX - Configuration Manager 2007 Agent Installation Wizard allows you to add systems to the list using the following methods:

   - **Manually** allows you to enter a specific Hostname or IP Address. (See Identify Non-Windows Systems Manually.)
   - **Import File** allows you to specify a text file which the wizard uses to import resolvable hostnames or IP addresses. (See Identify Non-Windows Systems Using a Text File.)

   Note ● If for some reason the QMX - Configuration Manager 2007 Agent fails to install successfully, the wizard allows you to save a text file listing those hostnames. You can import this file using the *Import File* method of non-Windows system identification next time you run the QMX - Configuration Manager 2007 Agent Installation Wizard. (See Agent Installation Completed.)

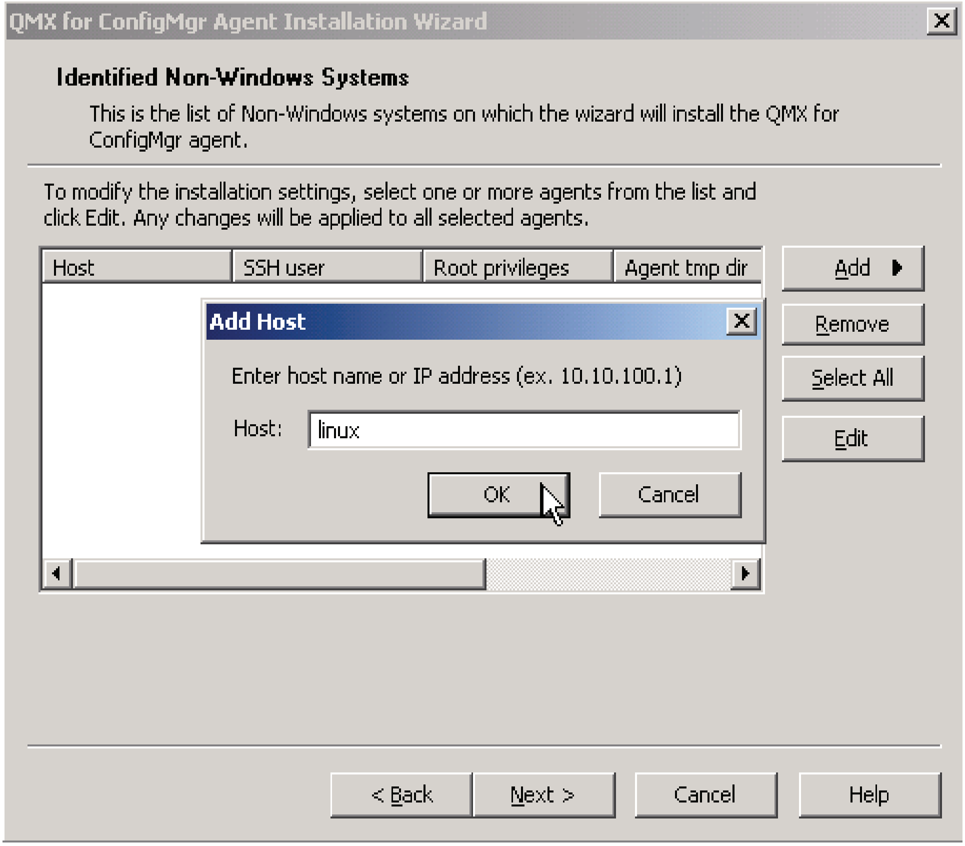
   - **From Active Directory** allows you to install the Agent to VAS-enabled systems found in a list of Active Directory containers. (VAS-enabled systems are systems that have Vintela Authentication Services installed and are already joined to the domain. Vintela Authentication Services is another Quest Software product that uses Active Directory for cross-platform identity integration and authentication and joins non-Windows systems to Active Directory Domains.) (See Identify Non-Windows Systems From a List of Active Directory Containers.)
   - **By Network Discovery** enables QMX - Configuration Manager 2007 to select non-Windows target systems by scanning a range of IP addresses for open SSH ports. (Use this option with caution!) (See Identify Non-Windows Systems From a Range of IP Addresses.)

   Note ● QMX - Configuration Manager 2007 does not use System Center Configuration Manager 2007 network discovery.

Identify Non-Windows Systems Manually

To add a hostname or IP address manually

1. Click **Manually**.



QMX for ConfigMgr Agent Installation Wizard

Identified Non-Windows Systems

This is the list of Non-Windows systems on which the wizard will install the QMX for ConfigMgr agent.

To modify the installation settings, select one or more agents from the list and click Edit. Any changes will be applied to all selected agents.

Host	SSH user	Root privileges	Agent tmp dir

Add Host

Enter host name or IP address (ex. 10.10.100.1)

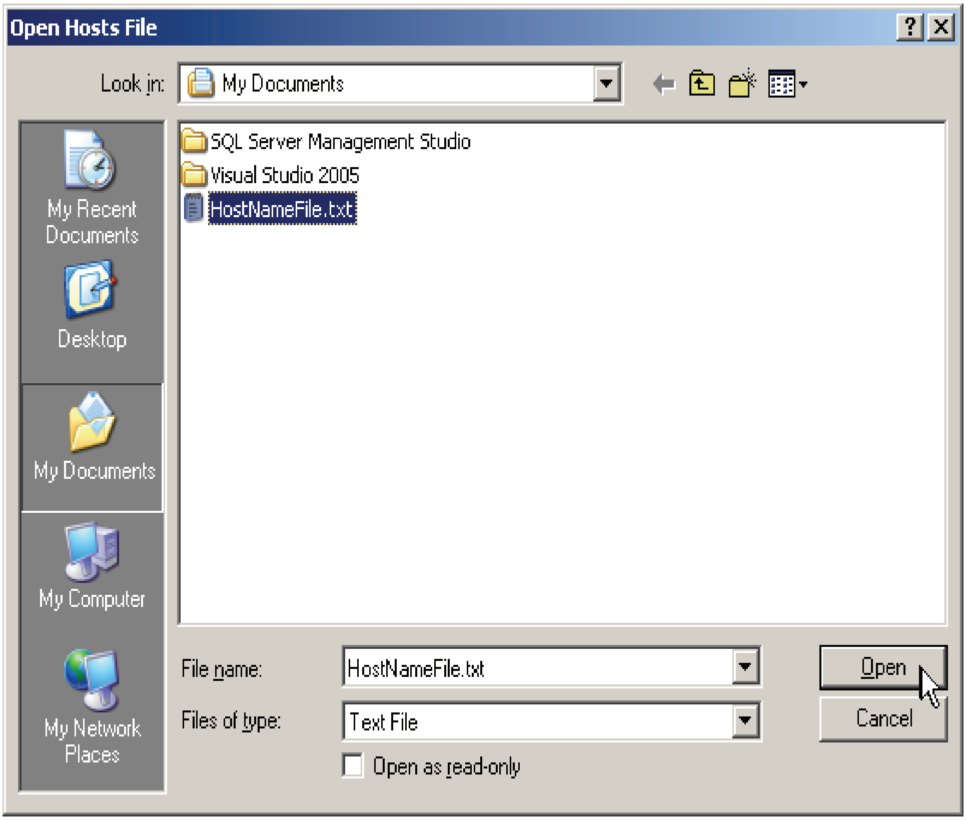
Host: linux

2. Enter the host name or IP address in the *Host* box and click **OK**.
3. Once the list of non-Windows systems is built, click **Next** to open the Ready to Install the Agent dialog.

Identify Non-Windows Systems Using a Text File

To import a list of host names or IP addresses from a text file

1. Click **Import File**.



Open Hosts File

Look in: My Documents

SQL Server Management Studio

Visual Studio 2005

HostNameFile.txt

File name: HostNameFile.txt

Files of type: Text File

□ Open as read-only

2. Select the text file and click **Open**.

   You can create this file either manually or you can generate it from a SSH port scan. For example, you can use a tool like `nmap` to create this file. But, the file must take the following form:

```
Hostname
Hostname
IP address
Hostname
IP address
IP address
```

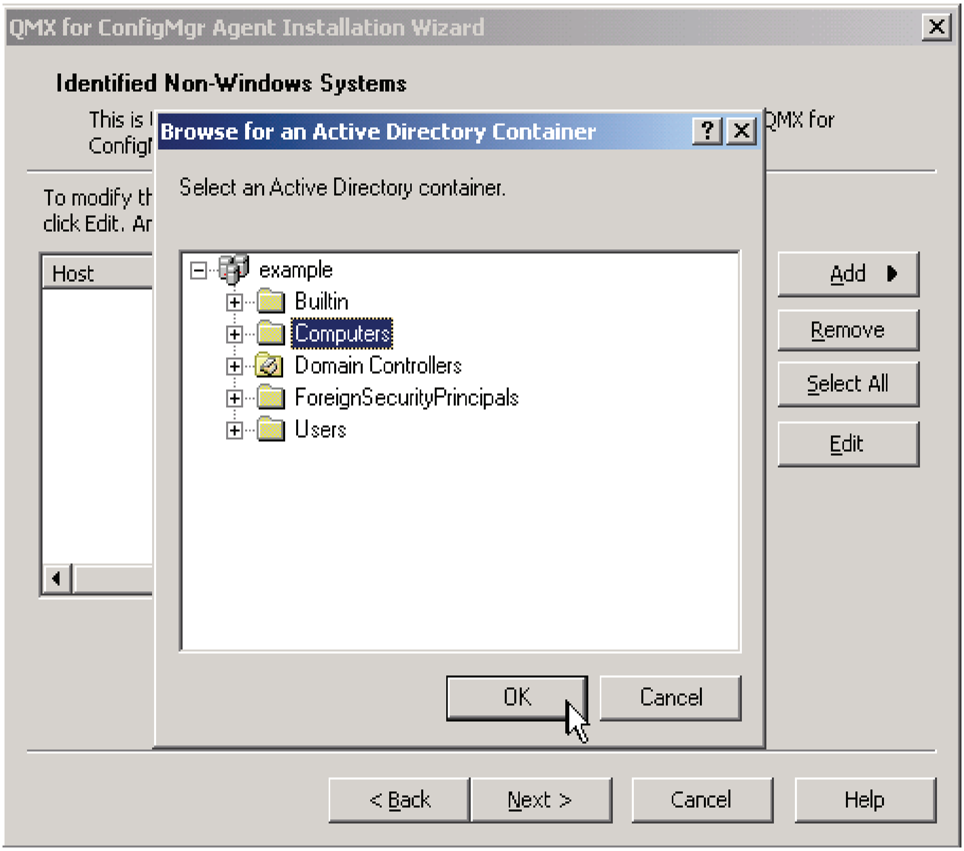
It does not matter what order you list the hostnames and IP addresses, but you must only list one hostname or IP address per line.

3. Once the list of non-Windows systems is built, click **Next** to open the Ready to Install the Agent dialog.

Identify Non-Windows Systems From a List of Active Directory Containers

To list the VAS-enabled systems

1. Click **From Active Directory**.


QMX for ConfigMgr Agent Installation Wizard
Identified Non-Windows Systems
This is l
Configl
QMX for
To modify tl
click Edit. Ar
Host
Browse for an Active Directory Container
Select an Active Directory container.
example
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Users
OK
Cancel
Add
Remove
Select All
Edit
< Back
Next >
Cancel
Help

2. Select an Active Directory container.

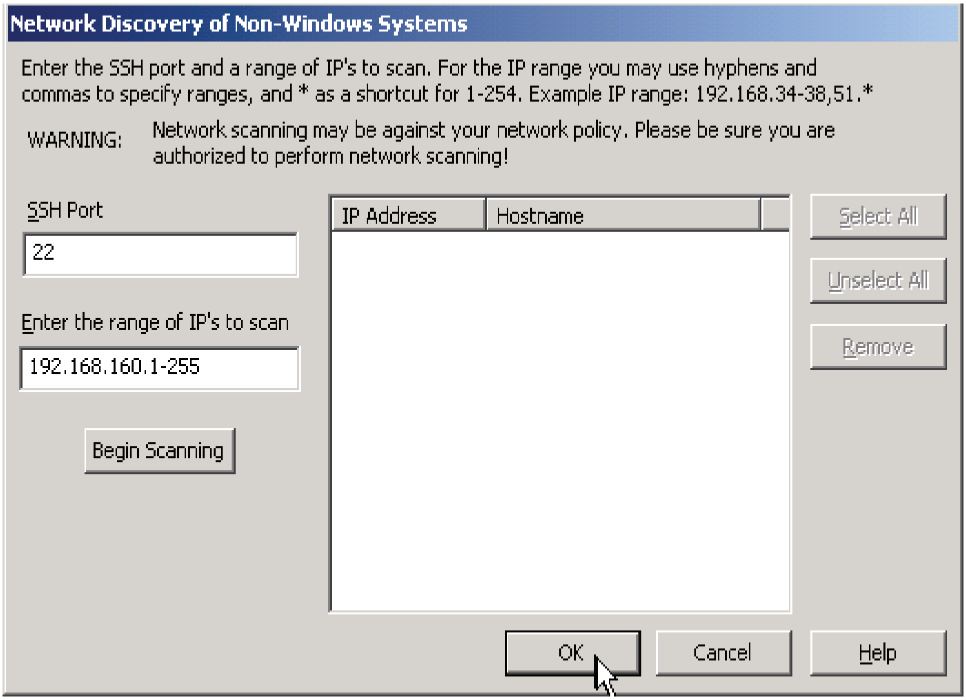
The wizard searches for VAS-enabled systems in this list of containers and adds them to the list of systems on which to install the QMX - Configuration Manager 2007 Agent. (VAS-enabled systems are systems that already have Vintela Authentication Services installed and are joined to the domain.)

3. Click **Remove** to delete a container name form the list.
4. Once the list of non-Windows systems is built, click **Next** to open the Ready to Install the Agent dialog.

Identify Non-Windows Systems From a Range of IP Addresses

To identify non-Windows systems from a range of IP addresses

1. Click **By Network Discovery**.



Network Discovery of Non-Windows Systems

Enter the SSH port and a range of IP's to scan. For the IP range you may use hyphens and commas to specify ranges, and * as a shortcut for 1-254. Example IP range: 192.168.34-38,51.*

WARNING: Network scanning may be against your network policy. Please be sure you are authorized to perform network scanning!

SSH Port: 22

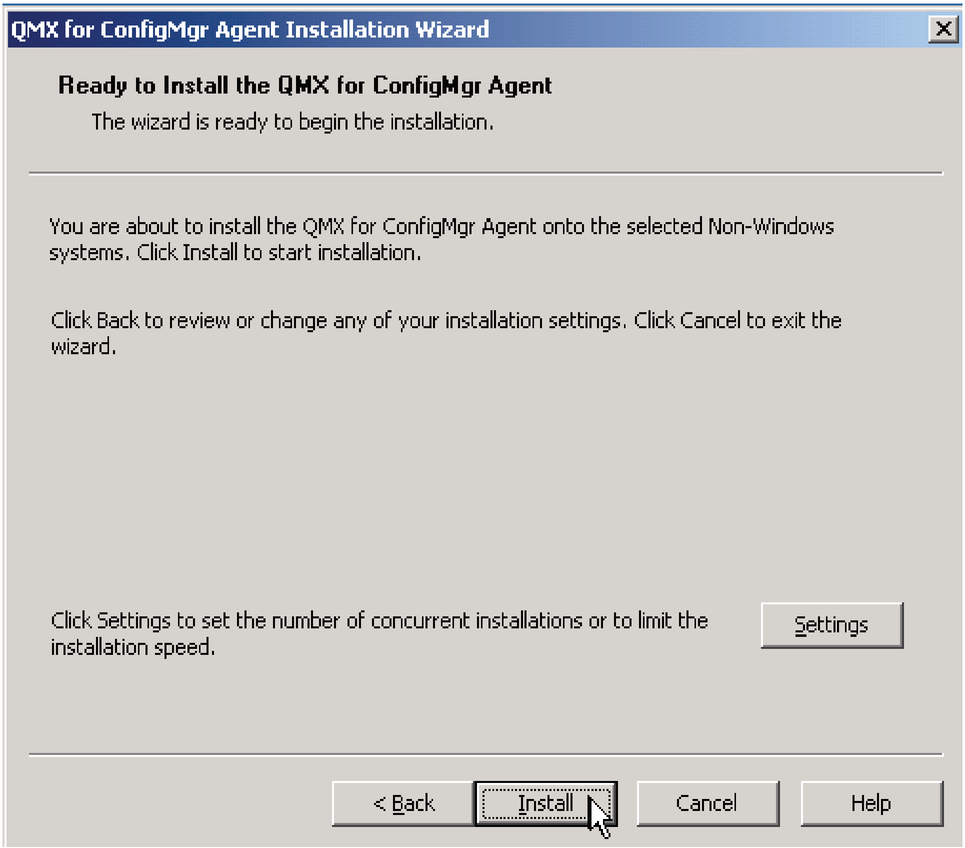
Enter the range of IP's to scan: 192.168.160.1-255

2. Enter a range of IP’s to scan and the SSH port number. For the IP range, you can use hyphens and commas to specify ranges, and * as a shortcut for 1-255. For example: 10.5.7-9.*.
3. Click **Begin Scanning** to list the available IP addresses.
4. Select the IP addresses of the machines onto which you want to install the QMX - Configuration Manager 2007 Agent. You can **Select All** or select specific systems using the **Ctrl** key and your mouse, or you can **Unselect All** or **Remove** specific systems from the list.

5. Once the list of non-Windows systems is built, click **Next** to open the Ready to Install the Agent dialog.

Many organizations prohibit the use of port scanning! Before initiating any port scans, be sure you are authorized to do so.

Ready to Install the Agent



QMX for ConfigMgr Agent Installation Wizard

Ready to Install the QMX for ConfigMgr Agent

The wizard is ready to begin the installation.

You are about to install the QMX for ConfigMgr Agent onto the selected Non-Windows systems. Click Install to start installation.

Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.

Click Settings to set the number of concurrent installations or to limit the installation speed.

6. Click **Install** to begin the installation.

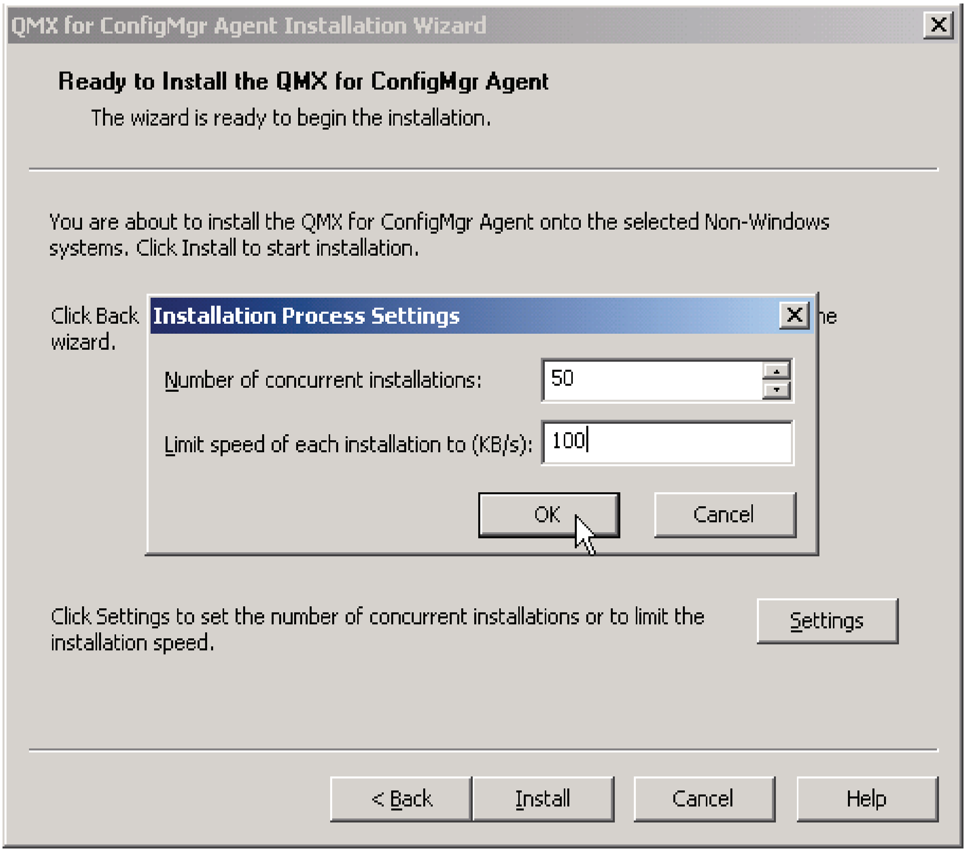
Note ● The installation starts immediately and opens the Installation Status dialog.

Installation Process Settings

Once the list of non-Windows systems is built, you are ready to start the QMX - Configuration Manager 2007 Agent installation process. But before you do, you may want to set the installation process settings.

To set the installation process settings

1. Click **Settings** on the Ready to Install the Agent dialog.



QMX for ConfigMgr Agent Installation Wizard

Ready to Install the QMX for ConfigMgr Agent

The wizard is ready to begin the installation.

You are about to install the QMX for ConfigMgr Agent onto the selected Non-Windows systems. Click Install to start installation.

Click Back he wizard.

Installation Process Settings

Number of concurrent installations: 50

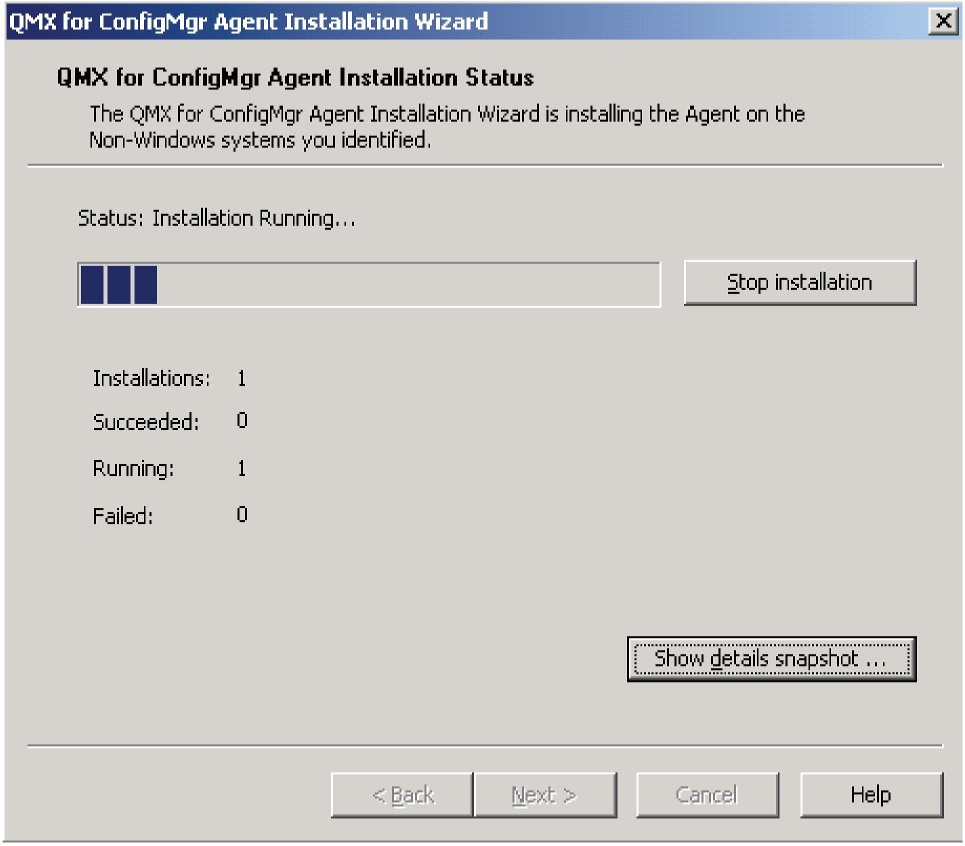
Limit speed of each installation to (KB/s): 100

Click Settings to set the number of concurrent installations or to limit the installation speed.

2. Enter the number of installations that you want the QMX - Configuration Manager 2007 Agent Installation Wizard to “push” concurrently. By default it will push the Agent out to 50 machines simultaneously. If you are pushing the Agent out to many machines, this helps speed up the processing.

3. Enter the speed limit for each installation. If the available bandwidth in your network, or the performance of the target machines are concerns, the Agent Push Installer allows you to enter the throttle speed for the file transfers. This is the average number of kilobytes per second you want the wizard to transfer each of the listed hostnames over the network. If you leave this field blank, it defaults to the fastest speed.

Installation Status


QMX for ConfigMgr Agent Installation Wizard

QMX for ConfigMgr Agent Installation Status

The QMX for ConfigMgr Agent Installation Wizard is installing the Agent on the Non-Windows systems you identified.

Status: Installation Running...

Installations: 1

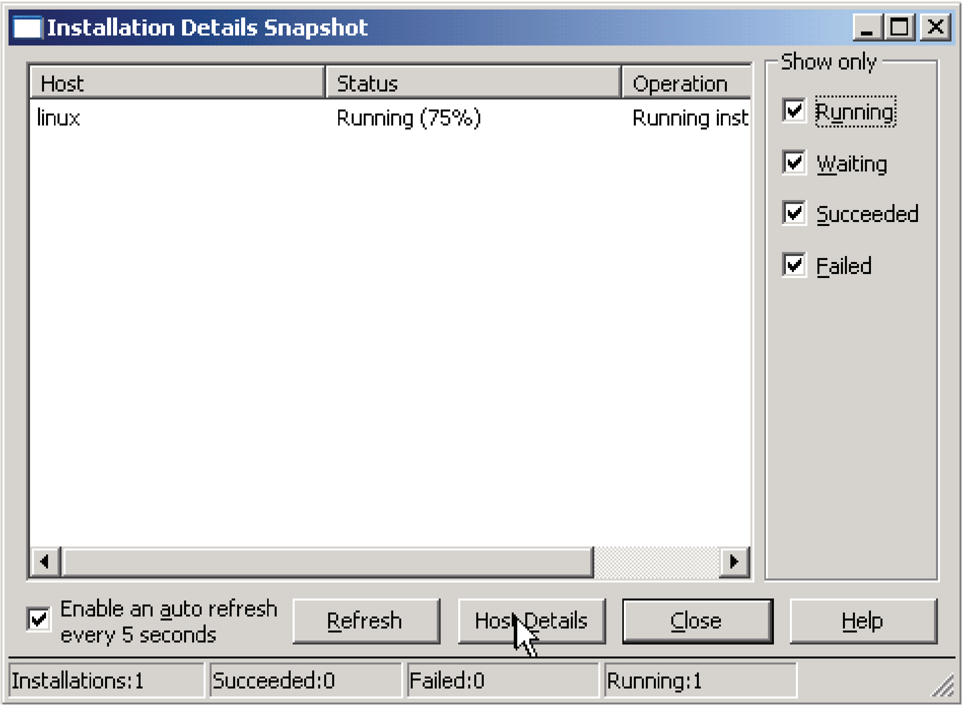
Succeeded: 0

Running: 1

Failed: 0

4. Click **Stop installation** to stop the installation process.
5. Click **Show details snapshot** to open the Installation Details Snapshot dialog so that you can view the details of the installation.

Installation Details Snapshot



Host	Status	Operation
linux	Running (75%)	Running inst

Show only

☑ Running

☑ Waiting

☑ Succeeded

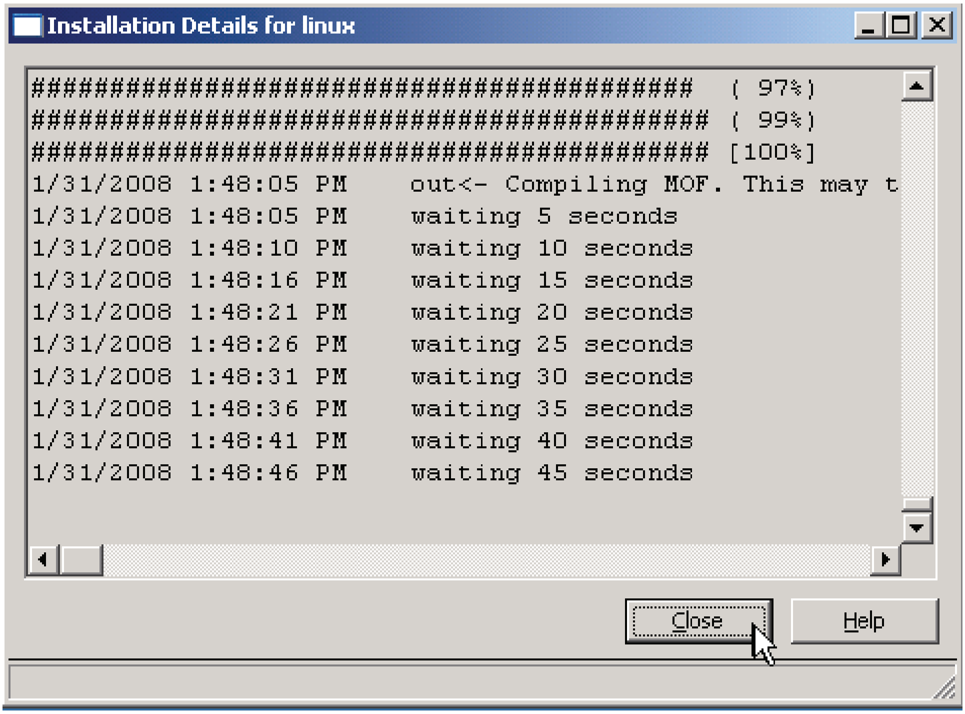
☑ Failed

☑ Enable an auto refresh every 5 seconds

Installations:1 Succeeded:0 Failed:0 Running:1

6. Select the desired **Show only** options to filter the list of displayed system by status: Running, Waiting, Succeeded, or Failed.
7. Select a Host and click **Host Details** to open the Installation Details dialog to view all the detailed information about the install for the selected Hostname.
8. Click **Refresh** to reload the data into the *Installation Details Snapshot* window.
9. Click **Close** to return to the Installation Status dialog.

Installation Details



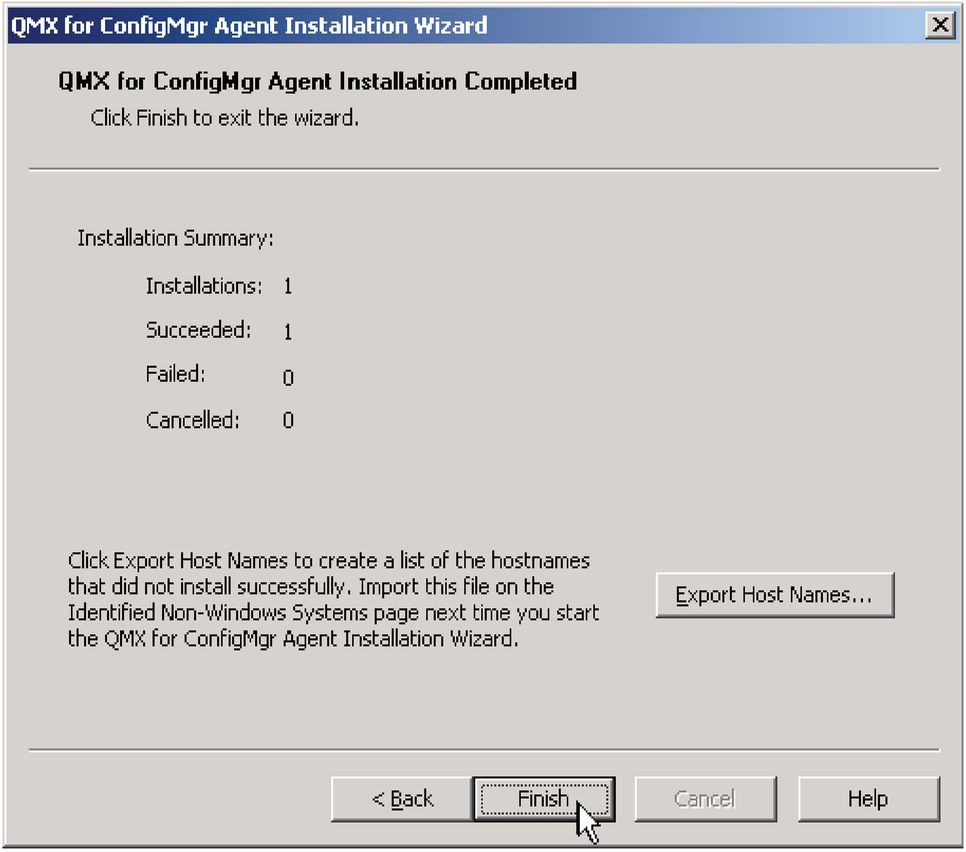
```
##########################################  ( 97%)
########################################### ( 99%)
########################################### [100%]
1/31/2008 1:48:05 PM    out<- Compiling MOF. This may t
1/31/2008 1:48:05 PM    waiting 5 seconds
1/31/2008 1:48:10 PM    waiting 10 seconds
1/31/2008 1:48:16 PM    waiting 15 seconds
1/31/2008 1:48:21 PM    waiting 20 seconds
1/31/2008 1:48:26 PM    waiting 25 seconds
1/31/2008 1:48:31 PM    waiting 30 seconds
1/31/2008 1:48:36 PM    waiting 35 seconds
1/31/2008 1:48:41 PM    waiting 40 seconds
1/31/2008 1:48:46 PM    waiting 45 seconds
```

If you have any installation issues you can copy content from this dialog and paste it into a text file. In this way you can eMail the log to Quest Support who can help you troubleshoot an installation problem.

You can also send Quest Support the `push_installer.log` file located in the C:\Program Files\Quest Software\QMX for ConfigMgr directory.

Agent Installation Completed

When the Status changes to “Installation Complete” on the Installation Status dialog, click **Next** to open *Agent Installation Completed* dialog:



QMX for ConfigMgr Agent Installation Wizard
QMX for ConfigMgr Agent Installation Completed
Click Finish to exit the wizard.

Installation Summary:

Installations: 1

Succeeded: 1

Failed: 0

Cancelled: 0

Click Export Host Names to create a list of the hostnames that did not install successfully. Import this file on the Identified Non-Windows Systems page next time you start the QMX for ConfigMgr Agent Installation Wizard.

Export Host Names...
< Back
Finish
Cancel
Help

To Export Host Names

1. Click **Export Host Names...** save a file listing the hostnames of the systems that did not install successfully. You can import this file using the *Import File* method of non-Windows identification next time you run the QMX - Configuration Manager 2007 Agent Installation Wizard. (See Identify Non-Windows Systems Using a Text File.)

Installing the Agent Manually

You must be logged in with “root” privileges to install the QMX - Configuration Manager 2007 Agent.

The instructions that follow are for a Red Hat Linux 4 operating system. The commands may vary for your system.

To install the QMX - Configuration Manager 2007 Agent manually

1. Insert the installation CD into the CD-ROM drive of the target machine.

   Note • You can install from the network file system if you don’t have a physical CD by mounting the image or copying the files to your network mount.

2. Open a terminal.
3. Change to the *root* user, if necessary.
4. Navigate to the CD directory.

   Linux usually displays the CD on the desktop. On other systems, you might need to mount the CD in order to navigate to it. If so, use the following steps (your system may vary).

5. As *root* user, enter this command at a terminal window prompt:

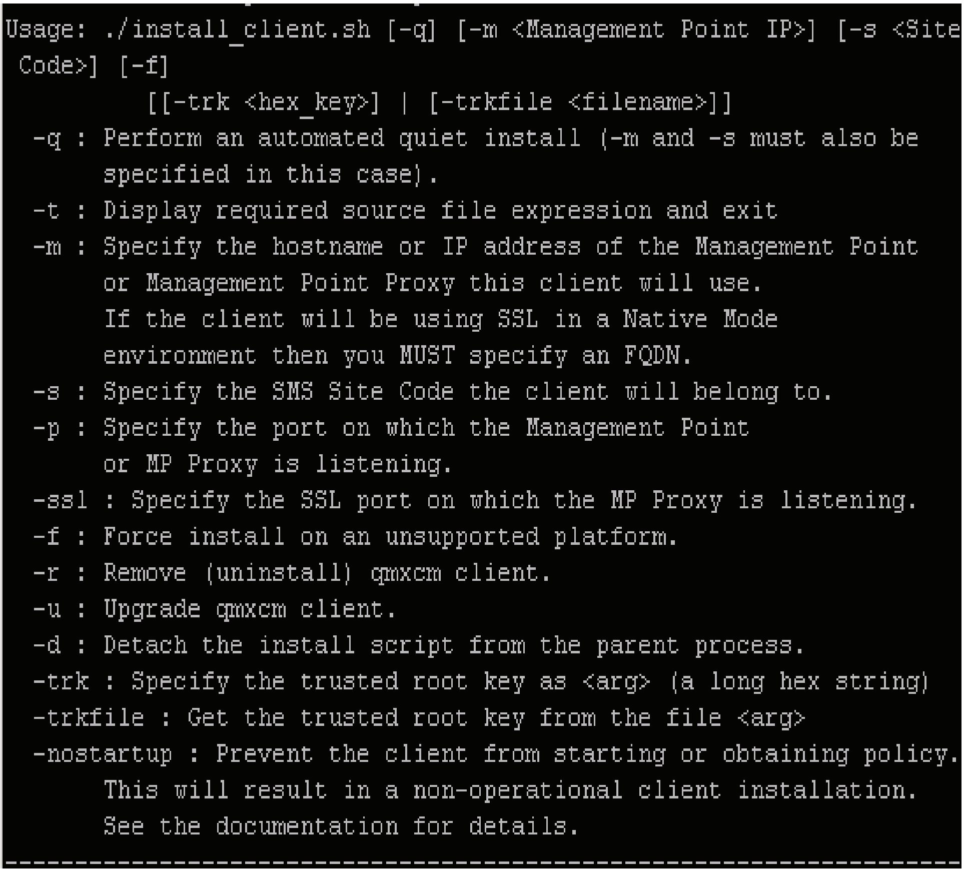
   mount /dev/cdrom /<*mount_point*>

   Note • The mount point can vary, but the CD-ROM device (link) is normally `/dev/cdrom`.

6. Click **Enter**.

   The system mounts the CD and may automatically display a GUI browser for your use. You can either browse to the CD using the GUI browser or browse to it from the terminal window.

7. From the mount point, enter **./install_client.sh --help** to see the various options available.

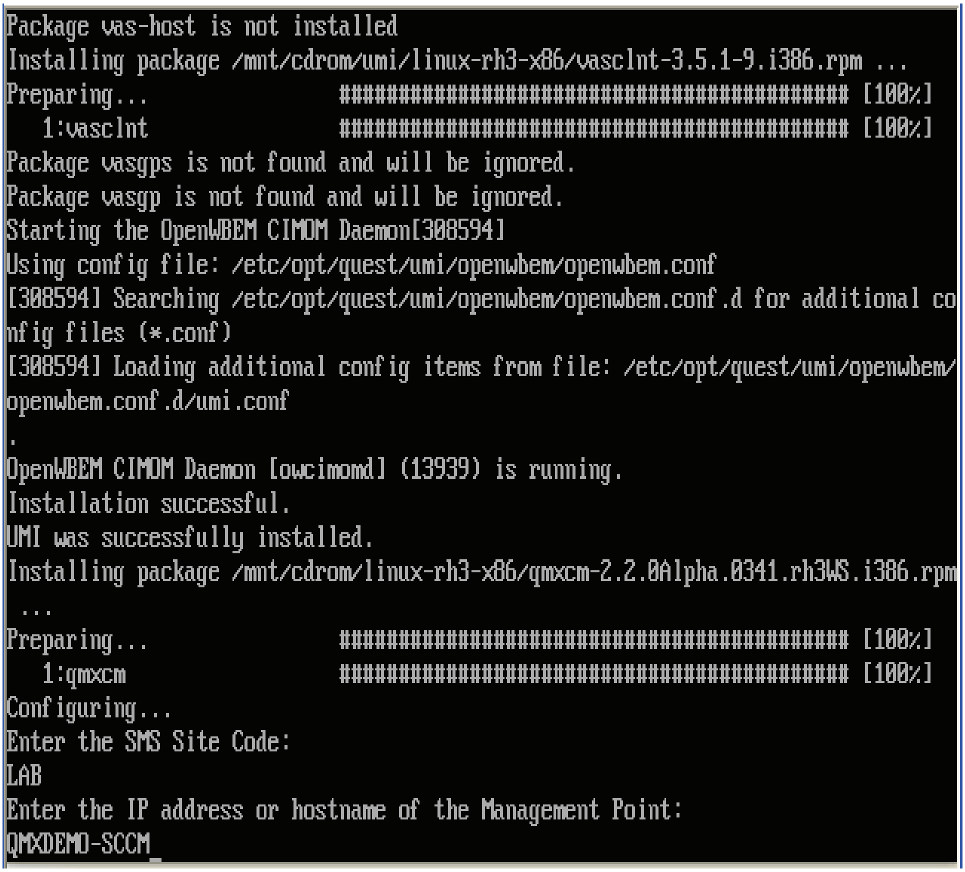


```
Usage: ./install_client.sh [-q] [-m <Management Point IP>] [-s <Site
 Code>] [-f]
          [[-trk <hex_key>] | [-trkfile <filename>]]
  -q : Perform an automated quiet install (-m and -s must also be
       specified in this case).
  -t : Display required source file expression and exit
  -m : Specify the hostname or IP address of the Management Point
       or Management Point Proxy this client will use.
       If the client will be using SSL in a Native Mode
       environment then you MUST specify an FQDN.
  -s : Specify the SMS Site Code the client will belong to.
  -p : Specify the port on which the Management Point
       or MP Proxy is listening.
  -ssl : Specify the SSL port on which the MP Proxy is listening.
  -f : Force install on an unsupported platform.
  -r : Remove (uninstall) qmxcm client.
  -u : Upgrade qmxcm client.
  -d : Detach the install script from the parent process.
  -trk : Specify the trusted root key as <arg> (a long hex string)
  -trkfile : Get the trusted root key from the file <arg>
  -nostartup : Prevent the client from starting or obtaining policy.
       This will result in a non-operational client installation.
       See the documentation for details.
---------------------------------------------------------------------
```

8. Enter **./install_client.sh** to start the installation.

Note • If you are installing QMX - Configuration Manager 2007 manually using `install_client.sh`, the QMX - Configuration Manager 2007 Agent installation script, you can use the `-p` option to indicate a port number that is different than the standard port 80 which it uses by default.

9. The installer prompts you for your System Center Configuration Manager 2007 Site Code and Management Point.



```
Package vas-host is not installed
Installing package /mnt/cdrom/umi/linux-rh3-x86/vasclnt-3.5.1-9.i386.rpm ...
Preparing...                ########################################### [100%]
   1:vasclnt                ########################################### [100%]
Package vasgps is not found and will be ignored.
Package vasgp is not found and will be ignored.
Starting the OpenWBEM CIMOM Daemon[308594]
Using config file: /etc/opt/quest/umi/openwbem/openwbem.conf
[308594] Searching /etc/opt/quest/umi/openwbem/openwbem.conf.d for additional co
nfig files (*.conf)
[308594] Loading additional config items from file: /etc/opt/quest/umi/openwbem/
openwbem.conf.d/umi.conf
.
OpenWBEM CIMOM Daemon [owcimomd] (13939) is running.
Installation successful.
UMI was successfully installed.
Installing package /mnt/cdrom/linux-rh3-x86/qmxcm-2.2.0Alpha.0341.rh3WS.i386.rpm
 ...
Preparing...                ########################################### [100%]
   1:qmxcm                  ########################################### [100%]
Configuring...
Enter the SMS Site Code:
LAB
Enter the IP address or hostname of the Management Point:
QMXDEMO-SCCM_
```

Note • If you are installing QMX - Configuration Manager 2007 into a native mode environment, use the `-m` option to specify the Management Point Proxy the client will use. If the client communicates with the MP Proxy using SSL in native mode, then you must specify a Fully Qualified Domain Name, not just the a hostname or IP address for the Management Point.

10. After processing the Site Code and Management Point entries, the install script:

- Compiles the MOF (this may take a while).
- Starts the OpenWBEM CIMOM Daemon.
- Exits to a command prompt.

Note ● The Managed Object Format (MOF) syntax is a way to describe object definitions. The MOF file is basically made up of a series of class and instance declarations. After it creates the class instances and class definitions in the MOF file, it compiles it.

11. Wait for the “QMXCM installation successful” message.

Supplying the Trusted Root Key

If you are installing the QMX - Configuration Manager 2007 Agent from the command line, you can optionally supply the Trusted Root Key (TRK) in hex-encoded form. Since most people won't want to type out the full TRK in hex-encoded form, you can copy it from a file using the backquoting feature of shells:

You can find the TRK at one of these locations:

- In the registry at: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SMS\MP\Certificates\TrustedRootKey.
- It is also located in the site control file under the property: TrustedRootKey.

Once you copy it, put it into a new file of your choice and location. Then use the following command:

```
./install_client.sh -s SITE_CODE -m MP_ADDRESS -trkfile
/SOME/PATH/TO/TRK/FILE`.
```

This causes the file located at `/SOME/PATH/TO/TRK/FILE` to be read and included on the command line for the Agent install script.

You can also supply the TRK using this command:

```
./install_client.sh -s SITE_CODE -m MP_ADDRESS -trk TRK_VALUE
```

Supplying the TRK to the command line is not required. If you do not opt to supply the TRK, then the QMX - Configuration Manager 2007 Agent will obtain the key from either Active Directory (if configured properly), or from the Management Point itself (which is not very secure).

Installing a QMX Agent in an Image

Many customers want to replicate their core image, including the QMX - Configuration Manager 2007 Agent, to other systems. To avoid duplicating the System Center Configuration Manager 2007 Client ID onto the other systems, Quest provides a `-nostartup` option to the Install Script.

The first time you start the QMX - Configuration Manager 2007 Agent, it creates a unique System Center Configuration Manager 2007 Client ID so if you plan to capture your core image and copy it to other machines, add the `-nostartup` option to the installation command line as in the following example:

```
./install_client.sh -nostartup
```

The `-nostartup` option disables the QMX - Configuration Manager 2007 Agent's initial startup and prevents subsequent startups by creating the `QMXCM.nostartup` file. Setting the `-nostartup` option also bypasses the policy update and management point check that normally occurs at the end of the QMX - Configuration Manager 2007 installation.

Before you attempt to start a copied or cloned QMX - Configuration Manager 2007 Agent, navigate to `/etc/opt/quest/qmxcm` and delete the `QMXCM.nostartup` file created by the `-nostartup` option. Deleting the `QMXCM.nostartup` file ensures the QMX - Configuration Manager 2007 Agent will start properly when the init script executes. You can delete this file before you clone the images as long as you do not allow the client to start before you copy the image. When you deploy the images, they will boot up automatically. When the QMX - Configuration Manager 2007 Agent starts up it will proceed with a policy update and will create a unique System Center Configuration Manager 2007 Client ID.

To clone the QMX Agent image

1. From the mount point, enter:

   ```
   ./install_client.sh -nostartup
   ```

2. Once the QMX Agent installation is complete, and before clone QMX Agent image, go to the following directory:

   ```
   /etc/opt/quest/qmxcm
   ```

3. Delete the `QMXCM.nostartup` file.
4. Copy the image to the other computers.

   When you deploy the images they should boot up automatically. When the QMX Agent starts it create a unique Client ID.

Using the RedHat Linux KickStart System

To rapidly install large numbers of identical Linux boxes you can use the RedHat Linux KickStart system. KickStart makes it possible for you to script the regular installation process by putting the information you would normally type at the keyboard into a configuration file. KickStart allows you to install multiple groups of packages without causing problems. You may also specify a sequence of shell-level commands that you want to execute after the main installation (disk partitioning, package installation, and so on) is complete. KickStart simply automates the normal steps involved in a RedHat installation.

To learn more about KickStart for RedHat Enterprise Linux, click here: http://www.redhat.com/docs/manuals/enterprise/RHEL-3-Manual/sysadmin-guide/ch-kickstart2.html.

The following is a sample of a post-install script for RedHat Linux KickStart:

```
%post


mkdir /mnt/share
mount <NFS_SERVER_IP_ADDRESS>:/share /mnt/share


echo "qmxcm installation in process..."
cd /mnt/share/qmxcm
./install_client.sh -q -s <SITECODE> -m <MP_IP_ADDRESS>


echo "qmxcm installation completed..."
```

Using the SUSE AutoYaST System

AutoYaST is the system for installing one or more SUSE Linux systems automatically and without user intervention. Using AutoYaST, you can create a configuration for a single system or a set of systems to control automated installations. The control file can be provided to YaST2 during installation in different ways.

For version 8.0 and higher, it is possible to perform the installation automatically with YaST. For more information on this subject, click here: http://www.suse.de/~nashif/autoinstall/index.html.

The following is a sample of a post-install script for SUSE AutoYaST:

```
<script>
      <chrooted config:type="boolean">true</chrooted>
   qmxcm.sh
      <interpreter>shell</interpreter>
      <location> </location>
      <source> <![CDATA]
#!/bin/sh

hostname labsuse
mkdir /mnt/share
mount 192.168.0.11:/share /mnt/share
echo "Quest Management Xtensions Installation in progress..."
cd /mnt/share/qmxcm
./install_client.sh -q -s <SITECODE> -m <MP_IP_ADDRESS>
#ps -ef | grep ow
echo "qmxcm Installation complete."

   ]]></source>
   </script>
```

Using the HP-UX Mount All Filesystems Option

The HP-UX documentation for `swinstall` says the following about `mount_all_filesystems`:

- Normally set to "true," the commands automatically attempts to mount all filesystems in the file system table (`/etc/checklist`) or the `/etc/fstab` file at the beginning of the analysis phase to ensure that all listed file systems are mounted before proceeding. This policy helps to ensure that files are not loaded into a directory that may be below a future mount point.
- When set to "false," no additional file systems are mounted, the mount operation is not attempted, and no check of the current mounts is performed.
- Applies only to `swinstall`, `swcopy`, `swverify`, `swremove`, `swconfig`.

QMX - Configuration Manager 2007 does not specify the value for the `mount_all_filesystems` option, so `swinstall` uses the system default.

To disable the mount_all_filesystems option

1. Change the default setting in either one of the following files:

   a) The system-wide default values:

   ```
   /var/adm/sw/defaults
   ```

   b) The user-specific default values:

   ```
   $HOME/.swdefaults
   ```

Note ● In addition to the `mount_all_filesystems` option, you can change several other software distribution behaviors and policy options by editing the default values found in either one of these files.

8

Post Installation Checklist

- Verifying the Agent Installation
- Enabling Client Signing and Encryption
- Uninstalling the Agent
- Reinstalling the Agent
- Getting Started with Inventory

Verifying the Agent Installation

QMX - Configuration Manager 2007 discovers non-Windows systems and adds them to the System Center Configuration Manager 2007 System Inventory.

To verify that the client displays in the Configuration Manager Console

1. From the Configuration Manager Console, navigate to **System Center Configuration Manager | Site Database | Computer Management**.
2. Right-click **Collections** and choose **Update Collection Membership**.
3. Click **Yes** at the *Update Collections* verification dialog.
4. Select the **All Systems** collection.

   The QMX - Configuration Manager 2007 Agent client should now display in the right-hand details pane.

   Note ● The Discovery Process may take a few minutes; you may need to press F5 to refresh.

To verify the installation from the client console

1. Enter **/opt/quest/qmxcm/bin/ -v** at the command line.

   This command displays the version number of QMX - Configuration Manager 2007.

   Note ● For more information about the other `clienttool` options, see *Using the Client Tool* in the *QMX - Configuration Manager 2007 Administrator Guide*.

To verify the status of the Agent

1. Enter this command:

   ```
   /opt/quest/qmxcm/sbin/qmxcmd_init status
   ```

   This command displays the current service status: running or not running; enabled or not enabled; or, dead.

   Note ● For more information about the other options to the `qmxcmd_init` script, see *Agent Init Script*.)

To verify the site code entered during the Agent installation

1. In a command window, enter:

   ```
   cd /etc/opt/quest/qmxcm
   ```

2. To display the contents of the file on the screen, enter:

   ```
   more qmxcm.conf
   ```

3. Look for:

   ```
   The Management Point: qmxcm.mpe = yourHostName

   The Site Code: qmxcm.site_code = yourSiteCode
   ```

4. If either of these settings is incorrect, use the `clienttool` to change them. (See *Using clienttool to Change the Site Settings*.)

Hardware and software inventory data is collected automatically right after each new QMX - Configuration Manager 2007 Agent discovers (or, reports) itself into System Center Configuration Manager 2007 as a valid Agent. However, there may be a delay before System Center Configuration Manager 2007 recognizes the objects. See Getting Started with Inventory for information about sending hardware and software information up to System Center Configuration Manager 2007 immediately.

Enabling Client Signing and Encryption

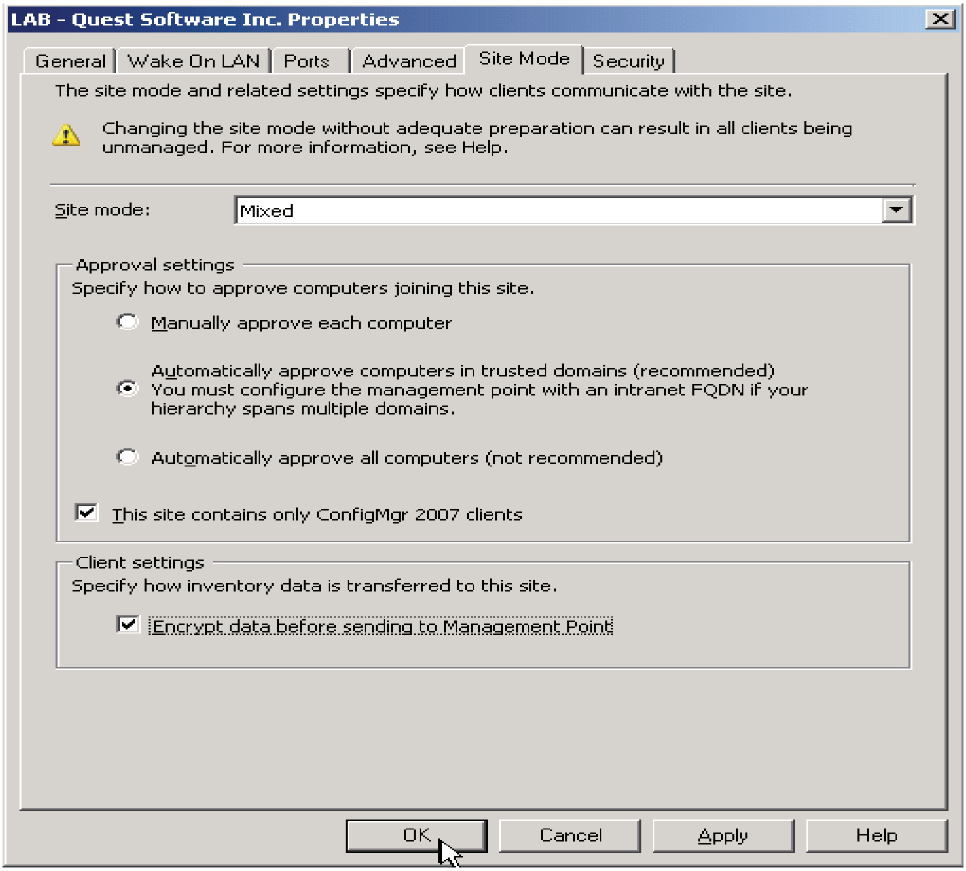
Client authentication and encryption are not enabled by default. If you enable these features, you need to enable client authentication and encryption on every site in the hierarchy to avoid problems with roaming clients having their inventory rejected. To prevent clients from injecting invalid data into the System Center site database, you must enable client authentication. And, to encrypt inventory messages sent from the client to a Management Point, you must enable client encryption.

After client inventory signing is enabled, you cannot disable it.

To enable inventory protection

1. In the Configuration Manager Console, navigate to **System Center Configuration Manager | Site Database | Site Management | <site code> - <site name>**.
2. Right-click **<site code> - <site name>** and choose **Properties**.

3. Click the **Site Mode** tab.



LAB - Quest Software Inc. Properties

The site mode and related settings specify how clients communicate with the site.

Changing the site mode without adequate preparation can result in all clients being unmanaged. For more information, see Help.

Site mode: Mixed

Approval settings

Specify how to approve computers joining this site.

○ Manually approve each computer

● Automatically approve computers in trusted domains (recommended) You must configure the management point with an intranet FQDN if your hierarchy spans multiple domains.

○ Automatically approve all computers (not recommended)

☑ This site contains only ConfigMgr 2007 clients

Client settings

Specify how inventory data is transferred to this site.

☑ Encrypt data before sending to Management Point

4. Select **Encrypt data before sending to Management Point**.
5. Click **OK**.

Uninstalling the Agent

To uninstall the QMX - Configuration Manager 2007 Agent

1. Go to the command line terminal.
2. If you are not the "root" user, enter **su** to change to the *root* user.
3. Enter the system password at the prompt.
4. Enter `/opt/quest/qmxcm/bin/uninstall_client.sh`
5. Wait for the "qmxcm uninstallation successful" message.

6. Enter **exit** to log off root after the command has processed.

Reinstalling the Agent

To manually install (or reinstall) the QMX - Configuration Manager 2007 Agent

1. Go to the command line terminal.
2. If you are not the "root" user, enter **su** to change to the *root* user
3. Enter the system password at the prompt.
4. Mount the distribution media.
5. From the mount point, enter **./install_client.sh**.
6. Enter the System Center Configuration Manager 2007 Site Code and the name or IP address of the Management Point when prompted. These are unique to each user's network.

   The install script prints a message "Compiling MOF" (this can take 5 to 15 minutes depending on the speed of your machine). When it is finished compiling MOF, the install script exits.
7. Enter **exit** to log off root after the command processes.

Getting Started with Inventory

QMX - Configuration Manager 2007 extends the native System Center Configuration Manager 2007 functionality. For example, when you enable Hardware and Software Inventory in System Center Configuration Manager 2007, you automatically enable the equivalent QMX - Configuration Manager 2007 functionality for non-Windows systems.

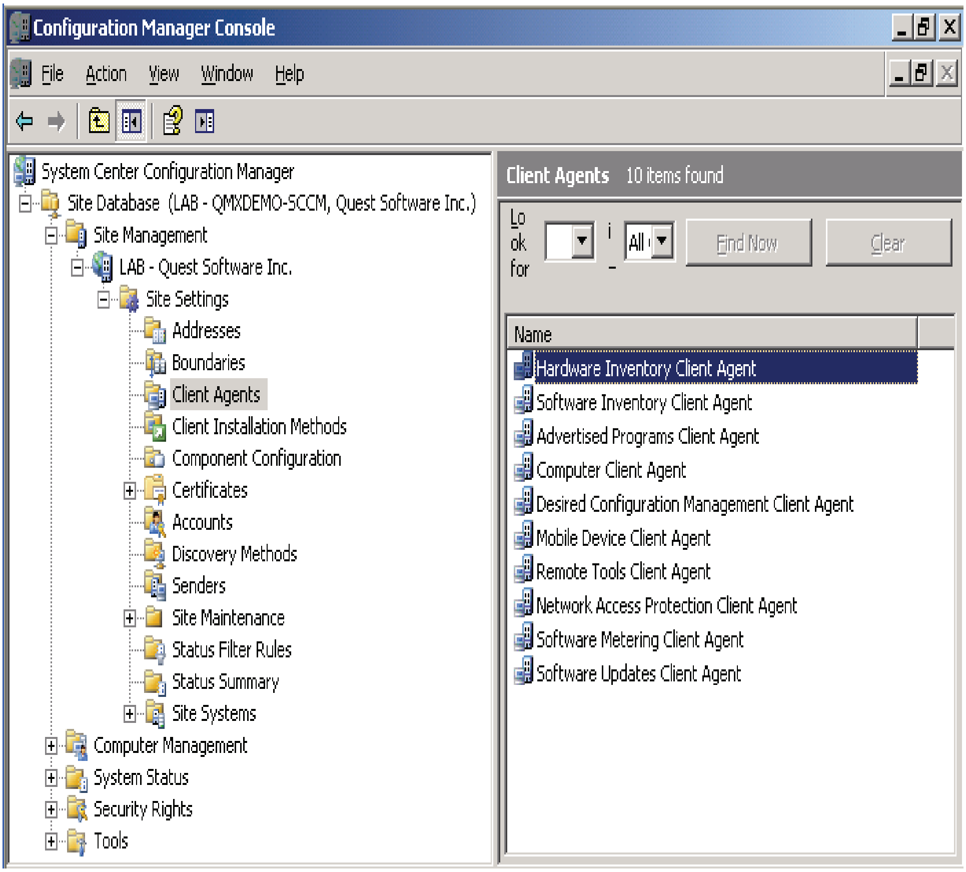
There are several System Center Configuration Manager 2007 features that use hardware and software inventory data, such as reports. This data must be collected from QMX - Configuration Manager 2007 Agents in order to build a database of information about the non-Windows computers in your organization. Please refer to http://technet.microsoft.com/en-us/library/bb632437.aspx for more information about Inventory in Configuration Manager.

After you first install QMX - Configuration Manager 2007 you need to make sure everything is configured properly before you can start managing your non-Windows systems.

Configuring the Hardware Inventory Client Agent

To configure the Hardware Inventory Client Agent

1. Navigate to **Site Management | Site Settings | Client Agent**.

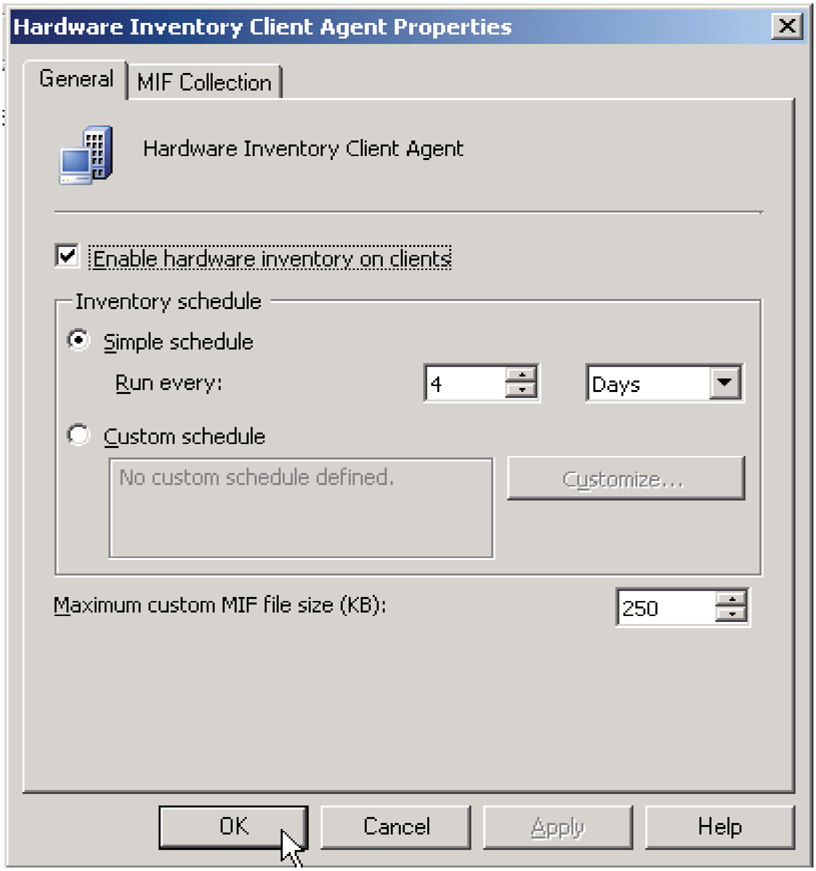


- System Center Configuration Manager
  - Site Database (LAB - QMXDEMO-SCCM, Quest Software Inc.)
    - Site Management
      - LAB - Quest Software Inc.
        - Site Settings
          - Addresses
          - Boundaries
          - Client Agents
          - Client Installation Methods
          - Component Configuration
          - Certificates
          - Accounts
          - Discovery Methods
          - Senders
          - Site Maintenance
          - Status Filter Rules
          - Status Summary
          - Site Systems
    - Computer Management
    - System Status
    - Security Rights
    - Tools

Client Agents 10 items found

- Hardware Inventory Client Agent
- Software Inventory Client Agent
- Advertised Programs Client Agent
- Computer Client Agent
- Desired Configuration Management Client Agent
- Mobile Device Client Agent
- Remote Tools Client Agent
- Network Access Protection Client Agent
- Software Metering Client Agent
- Software Updates Client Agent

2. Double click Hardware Inventory Client Agent to open its Properties window.



Hardware Inventory Client Agent Properties

Hardware Inventory Client Agent

☑ Enable hardware inventory on clients

Inventory schedule

● Simple schedule

Run every: 4 Days

○ Custom schedule

No custom schedule defined.

Maximum custom MIF file size (KB): 250

3. Select **Enable hardware inventory on clients**.
4. Set the schedule.

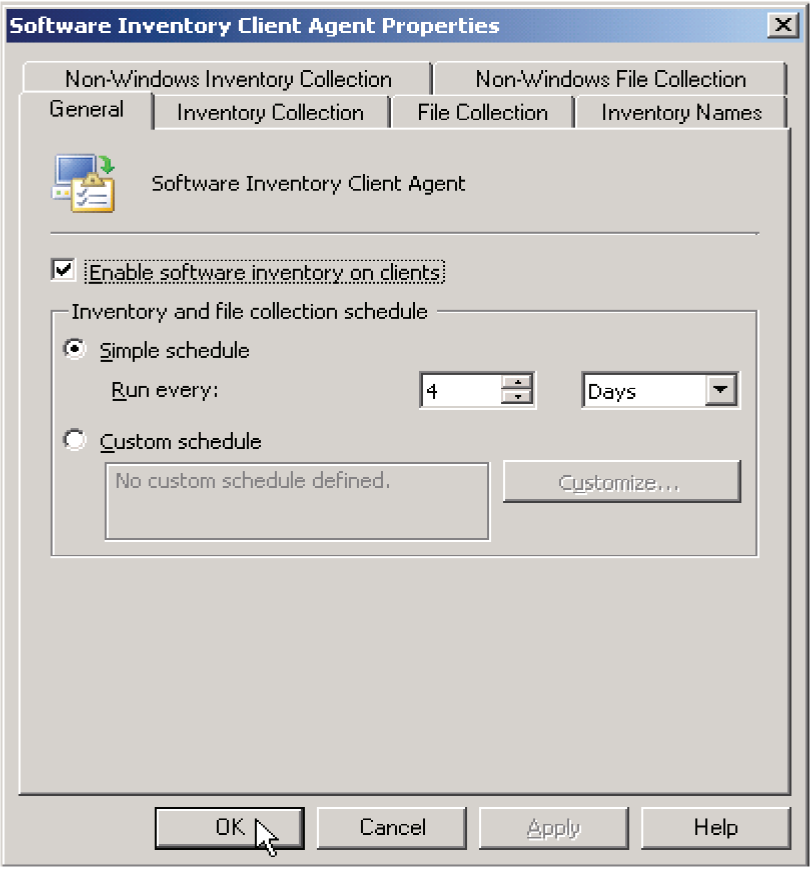
Note • QMX - Configuration Manager 2007 uses the System Center Configuration Manager 2007 policy that is already built. QMX pulls it down to the non-Windows client agents.

Configuring the Software Inventory Client Agent

To configure the Software Inventory Client Agent

1. From the Systems Management Server, navigate to **Site Database | Site Management | <site code> - <site name> | Site Settings | Client Agents**.

2. In the results pane, double-click **Software Inventory Client Agent**.



Software Inventory Client Agent Properties

Software Inventory Client Agent

☑ Enable software inventory on clients

Inventory and file collection schedule

● Simple schedule

Run every: 4 Days

○ Custom schedule

No custom schedule defined.

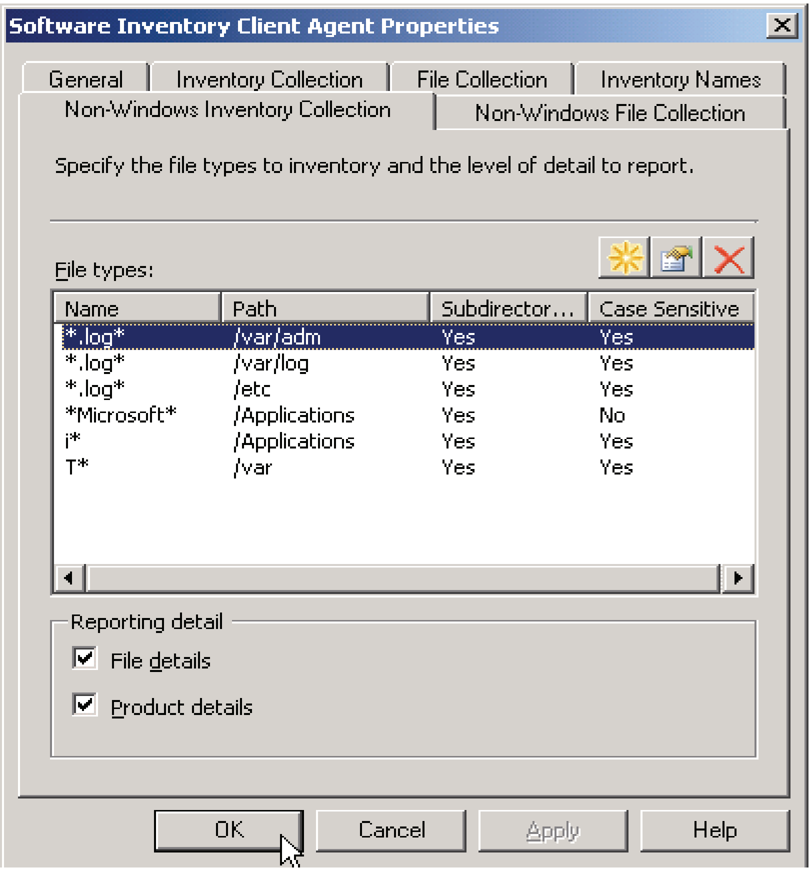
3. Select **Enable software inventory on clients**.
4. Set the schedule.

Non-Windows Inventory Collection

When you enable software inventory for a site, use the *Non-Windows Inventory Collection* tab to specify the file types to inventory and how to report the inventory in the Resource Explorer.

To create an Inventory Collection rule

1. Click the **Non-Windows Inventory Collection** tab.


Software Inventory Client Agent Properties
General
Inventory Collection
File Collection
Inventory Names
Non-Windows Inventory Collection
Non-Windows File Collection

Specify the file types to inventory and the level of detail to report.

File types:

Name	Path	Subdirector...	Case Sensitive
.log	/var/adm	Yes	Yes
.log	/var/log	Yes	Yes
.log	/etc	Yes	Yes
Microsoft	/Applications	Yes	No
i*	/Applications	Yes	Yes
T*	/var	Yes	Yes

Reporting detail

☑ File details

☑ Product details

This is where you define the rules that specify the file types you want to inventory and the level of detail you want it to capture.

Note ● See how Unix-like file paths are.

2. Click the **Create New Entry** button (the “starburst” icon) to open the *Inventoried File Properties* dialog where you can specify a new file type to inventory.

You can only add up to 64 rules to the *Files types* list. Once you meet this limit, QMX - Configuration Manager 2007 disables the *Create New Entry* button.

3. Enter a file name in the *Name* box.

Note • You can enter exact file names, or you can use wildcards such as ***.conf**. You may not use any of the following special characters: / : \ < > |

4. Click the **Set** button to indicate a particular folder or folder tree you want QMX - Configuration Manager 2007 to search.

   a) Select **All client hard disks** to scan all hard disks on the System Center Configuration Manager 2007 clients for the files to collect.

   b) Select **Variable or path name** to specify a single folder or folder tree. For example the `secure` files are in the `/var/log` path.

   c) Select **Search subdirectories** to indicate that you want to search sub folders.

   d) Click **OK** to close the *Path Properties* dialog.

5. Select **Case sensitive file matching**, if desired.

Note • Unless you select this option, System Center Configuration Manager 2007 treats files with the same name but different cases as the same file. For example, it sees no difference between `testcase.txt` and `TestCase.txt`.

6. Click **OK** to return to the Software Inventory Client Agent Properties dialog.
7. Select **File details** to display all scanned files in the Resource Explorer under **File Details**.
8. Select **Product details** to list software product manufacturer information in the Resource Explorer when it is available.

If you want Product Details for Mac OS X, you must not only select **Product details**, you must also edit the configuration file. On the command line of each client, go to: `/etc/opt/quest/qmxcm` and edit the `qmxcm.conf` file. Change the line that says: "`qmxcm.`package_cache=disabled" to "`qmxcm.`package_cache=enabled." This variable is "disabled" by default because it uses a lot of system resources.

9. Click **OK**.

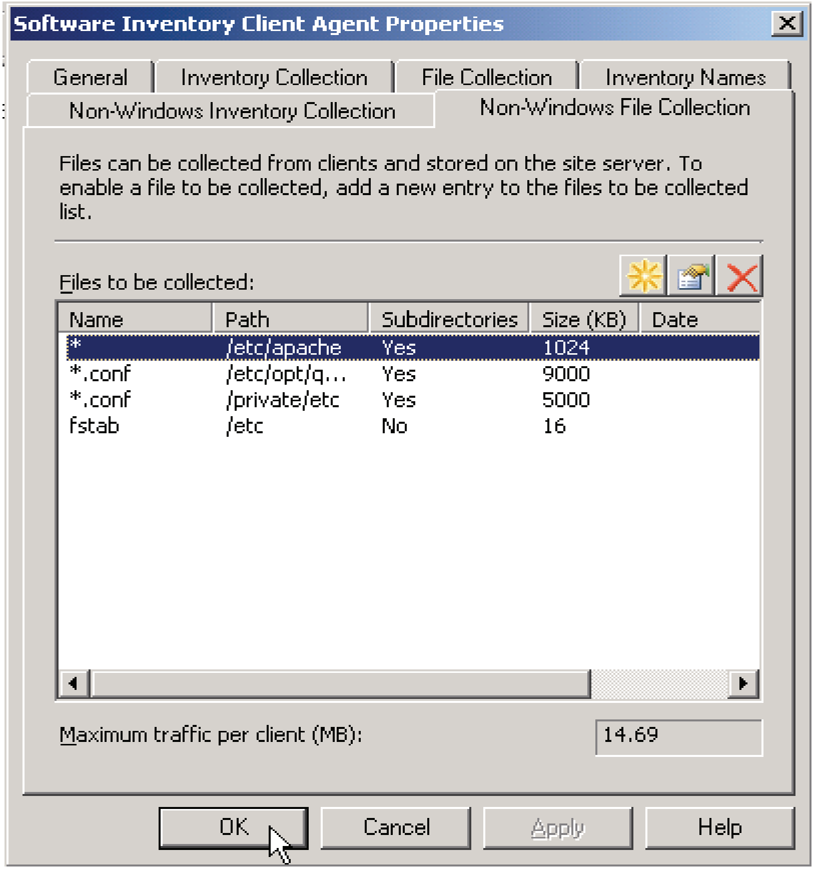
Note • Next time the inventory cycles you can view the results with the Resource Explorer under **Software | File Details** or **Product Details**.

Non-Windows File Collection

Like System Center Configuration Manager 2007, QMX - Configuration Manager 2007 can put whole files into the System Center site database for viewing. You use software inventory to collect files from non-Windows clients and store them at the primary site server to which the clients are assigned. After you create the file collection rule and propagate it to the clients, the files are collected each time software inventory runs. You must specify the files you want to collect. When you do, you can use wildcard characters or specify multiple variations of a file, such as `Status*.doc`.

To create a File Collection rule

1. Click the **Non-Windows File Collection** tab.


Software Inventory Client Agent Properties
General
Inventory Collection
File Collection
Inventory Names
Non-Windows Inventory Collection
Non-Windows File Collection
OK
Cancel
Apply
Help

Files can be collected from clients and stored on the site server. To enable a file to be collected, add a new entry to the files to be collected list.

Files to be collected:

Name	Path	Subdirectories	Size (KB)	Date
*	/etc/apache	Yes	1024	
*.conf	/etc/opt/q...	Yes	9000	
*.conf	/private/etc	Yes	5000	
fstab	/etc	No	16	

Maximum traffic per client (MB): 14.69

This is where you define the rules that specify which files you want to collect from the clients. These files are copied into the SQL Database. For example, you may want to examine a .bat, .log, or .conf file.

Note: You can limit the size of the files so that you don't fill up the database.

2. Click the **Create New Entry** button (the “starburst” icon) to open the *Collected File Properties* dialog where you can add a new entry to the *Files to be collected* list:

You can only add up to 64 rules to the *Files to be collected* list. Once you meet this limit, QMX - Configuration Manager 2007 disables the *Create New Entry* button.

3. Enter the name of a file or file type you want to collect from the clients. For example, if you want to collect security file logs from the clients, enter **secure**.

Note ● You can enter exact file names, or you can use wildcards. For example if you want to collect `secure.1`, `secure.2`, and `secure.3`, enter **secure.***. You may not use any of the following special characters: `/ : \ < >`

4. Click the **Set** button to scan a particular folder or folder tree.

By default, all hard disks on the System Center Configuration Manager 2007 clients are scanned for files to collect. If you want to scan a particular folder or folder tree, click the **Set** button to change the default.

Note ● When System Center Configuration Manager 2007 sends a large volume of collected files across the network, network performance can suffer. To minimize this problem, you can restrict the path so that you collect only copies of the files from the desired folder tree, or schedule software inventory when network traffic is lightest.

a) Select **All client hard disks** to scan all hard disks on the System Center Configuration Manager 2007 clients for the files to collect.

b) Select **Variable or path name** to specify a single folder or folder tree. For example the `secure` files are in the `/var/log/` path.

c) Select **Search subdirectories** to indicate that you want to search sub folders. If you enable this option, QMX - Configuration Manager 2007 will not search Network file systems mounted on subdirectories. You can also create a file named `skpswi.dat` and place it in a directory that you want excluded from the search.

The QMX - Configuration Manager 2007 Agent uses CPU while scanning the hard drive for files that match the rules' pattern. The more directories that need to be scanned, the longer it will take. If you wish to reduce the amount of CPU usage, you can make fewer rules or make rules more specific by not specifying the search subdirectories option or specifying a deeper subdirectory so the Agent will not have to scan as many directories.

d) Click **OK** to close the Path Properties dialog.

5. Select **Only collect files modified after the following date** and enter a date in the field provided if you desire to limit the number of files you collect. (This is a way to restrict the number of files collected.)
6. Select **Case sensitive file matching**, if you desire.

Note • In File Collection, System Center Configuration Manager 2007 treats files with the same name but different cases as different files.

7. Select an amount in the *Maximum size (KB)* box for the combined size of the files matching the rule you want to collect. This is the maximum size allowed for all files matching the rule, in kilobytes (KB), that you want System Center Configuration Manager 2007 to collect from a client during a software inventory cycle. If the combined size of the files matching the rule exceeds the *Maximum size* level, System Center Configuration Manager 2007 collects no files.
8. Collected files from each client in a site hierarchy can generate quite a bit of network traffic and require extensive storage space, especially if you choose a larger value for the combined size of the files. Test the traffic that would be generated on your network before you enable a larger combined file size.
9. Click **OK**.

Note • Next time the inventory cycles you can view the results with the Resource Explorer under **Software | Collected Files**.

Using the clienttool to Force Inventory Collection

System Center Configuration Manager 2007 collects Hardware and software Inventory data according to a schedule set in System Center Configuration Manager 2007. Therefore, there may be a delay before the QMX - Configuration Manager 2007 Agent runs the inventory. If you don’t want to wait for the inventory collection to occur, you can force inventory from the command line of the QMX - Configuration Manager 2007 Agent client using the `clienttool` command. It is a good idea to run a Policy update before forcing a Hardware Inventory cycle, particularly if new classes have been added to the `sms_def.mof` file. To do that, enter **/opt/quest/qmxcm/bin/clienttool --run-policy-update** at the command line.

To force the Hardware Inventory and Software Inventory cycles, enter **/opt/quest/qmxcm/bin/clienttool --run-hardware-inventory** or enter **/opt/quest/qmxcm/bin/clienttool --run-software-inventory**.

This process sends hardware and software information up to System Center Configuration Manager 2007 immediately.

For more information about using the `clienttool`, see *Using the Client Tool* in the *QMX - Configuration Manager 2007 Administrator’s Guide*.

After you force the inventory, refresh the Resource Explorer for the system to view the newly posted data.

9

Upgrading

- Upgrade Overview
- Upgrading From 1.6 and Newer
- Upgrading from Versions Prior to 1.6

Upgrade Overview

Quest recommends that you triple the size of your /tmp directory ***before*** you begin. (See Agent System Requirements for size requirements.) Also refer to Ensure SSH Access and Root Privileges for a caution.

There are two upgrade paths depending on which version of QMX - Configuration Manager 2007 you are upgrading.

- Upgrading From 1.6 and Newer.
- Upgrading from Versions Prior to 1.6

Quest recommends that you backup all of your systems before you start the upgrade process. For example, when you upgrade QMX - Configuration Manager 2007, you will overwrite any modification you may have made to the sms_def.mof file.

Native Mode Consideration

If you plan to run QMX - Configuration Manager 2007 2.2 with System Center Configuration Manager 2007 in native mode, you must ensure that your MP_Address is the Fully Qualified Domain Name (FQDN).

Previous versions of QMX - Configuration Manager 2007 only required a hostname or IP address for the Management Point. While the QMX Agent will still work with just a hostname or IP address without using SSL, it must have a FQDN when using SSL! It uses the FQDN for validation of the MP Proxy certificate chain and is therefore required to use SSL securely. To change the Management Point address to the FQDN, run the `clienttool --reset-stored-site-info` command.

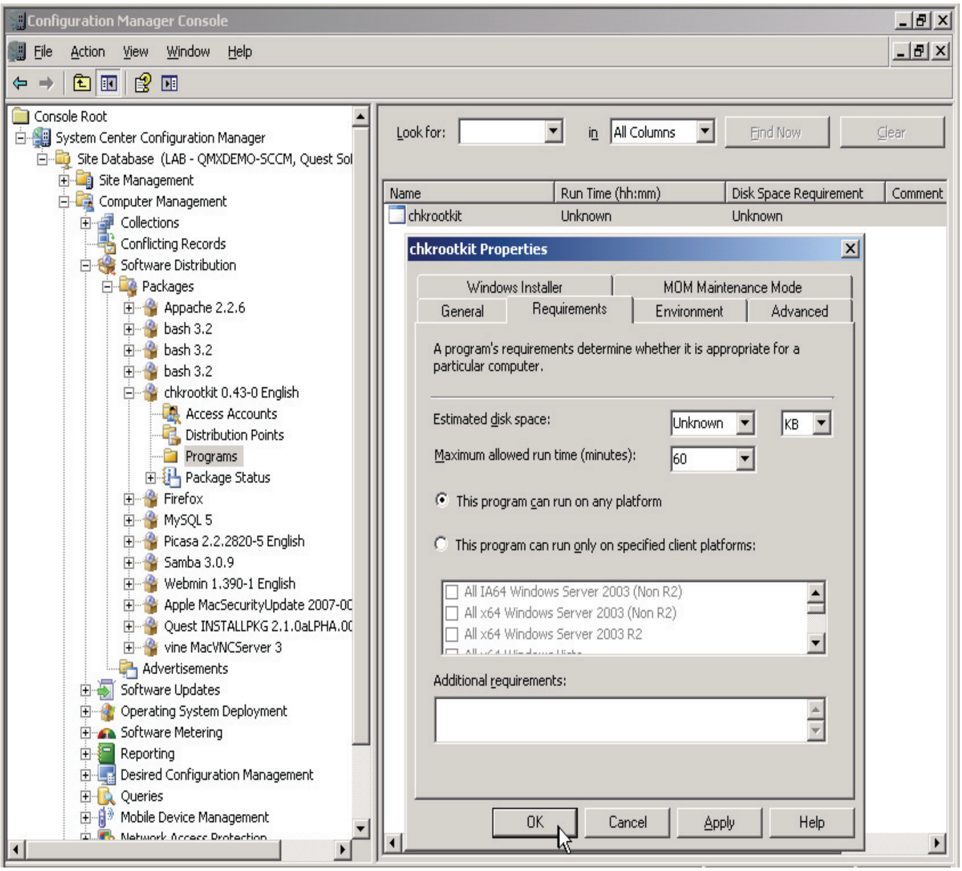
Maintenance Mode Considerations

To take advantage of Maintenance Windows, you must edit any packages and advertisements that existed before you upgraded to version 2.1. Maintenance Windows is a new feature which allows you to define a window in which to perform software distributions and software updates. The window uses an estimated time period defined in the Software Distribution wizard to execute the entire install.

To edit a Program

1. Navigate to **Software Distribution | Packages | <old package> | Programs**.

2. Open a program's *Property* dialog.



A program's requirements determine whether it is appropriate for a particular computer.

Estimated disk space: Unknown KB

Maximum allowed run time (minutes): 60

● This program can run on any platform

○ This program can run only on specified client platforms:

□ All IA64 Windows Server 2003 (Non R2)
□ All x64 Windows Server 2003 (Non R2)
□ All x64 Windows Server 2003 R2

Additional requirements:

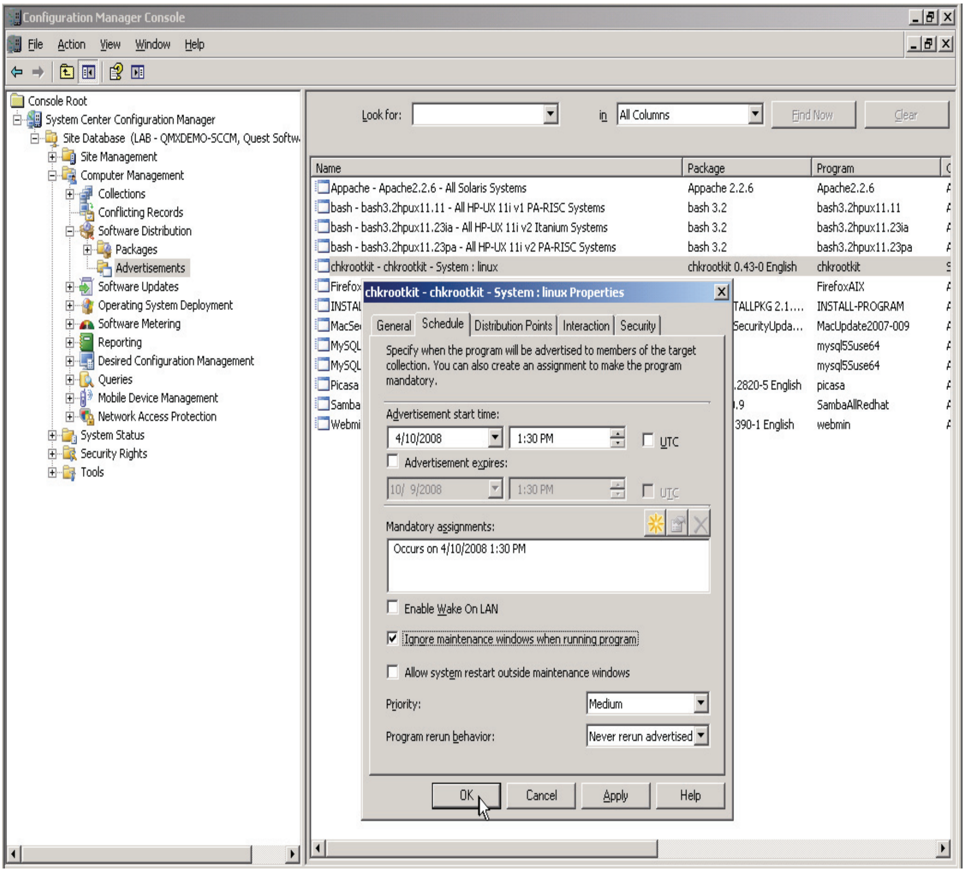
3. Select the **Requirements** tab.
4. Enter the maximum run time (in minutes) that you expect the program to run on the client computer.

   Note • Include the estimated time it will take to download the program.

To edit an Advertisement

1. Navigate to **Software Distribution | Advertisements**.
2. Open an advertisement's *Property* dialog.

3. Select the **Schedule** tab.



Name	Package	Program
Appache - Apache2.2.6 - All Solaris Systems	Apache 2.2.6	Apache2.2.6
bash - bash3.2hpux11.11 - All HP-UX 11i v1 PA-RISC Systems	bash 3.2	bash3.2hpux11.11
bash - bash3.2hpux11.23ia - All HP-UX 11i v2 Itanium Systems	bash 3.2	bash3.2hpux11.23ia
bash - bash3.2hpux11.23pa - All HP-UX 11i v2 PA-RISC Systems	bash 3.2	bash3.2hpux11.23pa
chkrootkit - chkrootkit - System : linux	chkrootkit 0.43-0 English	chkrootkit
Firefox		FirefoxAIX
INSTAL	TALLPKG 2.1....	INSTALL-PROGRAM
MacSe	SecurityUpda...	MacUpdate2007-009
MySQL		mysql5Suse64
MySQL		mysql5Suse64
Picasa	.2820-5 English	picasa
Samba	.9	SambaAllRedhat
Webmi	390-1 English	webmin

chkrootkit - chkrootkit - System : linux Properties

Specify when the program will be advertised to members of the target collection. You can also create an assignment to make the program mandatory.

Advertisement start time: 4/10/2008 1:30 PM ☐ UTC

☐ Advertisement expires: 10/ 9/2008 1:30 PM ☐ UTC

Mandatory assignments:
Occurs on 4/10/2008 1:30 PM

☐ Enable Wake On LAN

☑ Ignore maintenance windows when running program

☐ Allow system restart outside maintenance windows

Priority: Medium

Program rerun behavior: Never rerun advertised

4. Select **Ignore maintenance windows when running program**.

Note • Software Distribution expects to run rules within defined Maintenance Windows. If you have not defined any maintenance windows, no distribution rules will run unless you explicitly set them to ignore maintenance windows.

5. Set the **Program rerun behavior**: *Never rerun advertised program*, *Always rerun program*, *Rerun if failed previous attempt*, or *Rerun if succeeded on previous attempt*. QMX - Configuration Manager 2007 honors the System Center Configuration Manager 2007 rerun behavior.

Note • Setting the *Program rerun behavior* only makes sense if you have a *Mandatory assignment* set to repeat.

6. Click **OK**.

Upgrading From 1.6 and Newer

To upgrade QMX - Configuration Manager 2007 to the latest product release you must install the following components:

- **QMX - Configuration Manager 2007 Agent** (see Upgrading the Agent).
- **Microsoft Management Console Extensions**, which includes the QMX - Configuration Manager 2007 Snap-In, property pages, and remote administration tools that enable you to manage non-Windows systems from the SMS Administration Console. (See Upgrading the MMC Extensions.)

The order in which you install these components is important. Quest recommends that you upgrade the Agent before you upgrade the Management Console Extensions.

Upgrading the Agent

When you receive an upgrade for your QMX - Configuration Manager 2007 product, you can either upgrade the Agent manually or use the Software Distribution Wizard.

You can not use the Agent Installation Wizard for upgrades.

Using the Wizard to Upgrade the Agent

Because the QMX - Configuration Manager 2007 Software Distribution Wizard must have write access to the Source Directory, you must copy the installation files from the distribution media to your hard drive before you begin. Please read Prepare Installation Files for Install as the upgrade script is expecting to find certain files in particular locations.

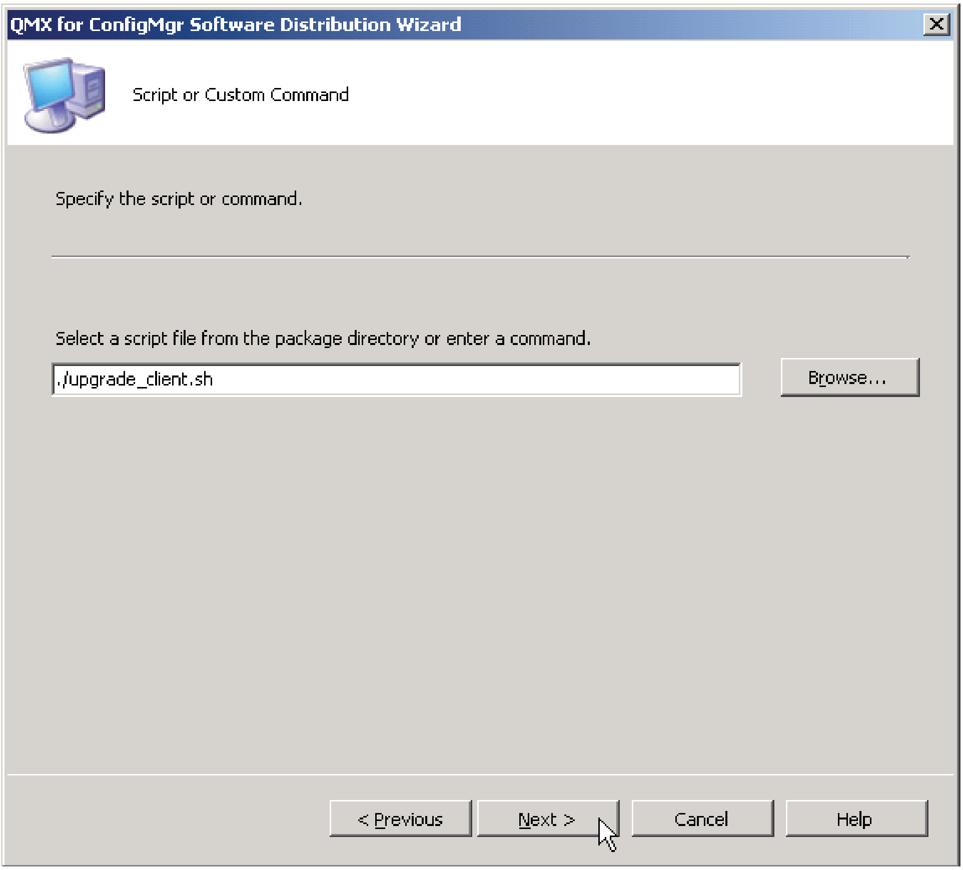
To upgrade the Agent using the wizard

1. In the Configuration Manager Console, navigate to and right-click the collection you wish to upgrade.

2. Choose **Distribute Non-Windows | Software** to start the *QMX - Configuration Manager 2007 Software Distribution Wizard*.

   The wizard steps you through the process of identifying the package, source files, and so forth.

3. When the wizard displays the *Package Type* dialog, choose **Script or Custom command**.
4. **Browse** to select a script file.



QMX for ConfigMgr Software Distribution Wizard

Script or Custom Command

Specify the script or command.

Select a script file from the package directory or enter a command.

./upgrade_client.sh

Note ● Do not use quotes in this command line.

5. Proceed through the rest of the Software Distribution Wizard screens to create an Advertisement and set the date and time when you want to assign the program.

After you create the Advertisement, System Center Configuration Manager 2007 publishes the upgrade and all the Agents in the collection will install the upgrade after the next policy update.

6. After all the Agents are upgraded, you can upgrade the Microsoft Management Console (MMC) extensions. (See Upgrading the MMC Extensions.)

Manually Upgrading the Agent

You must have "root" privileges to install QMX - Configuration Manager 2007 Agents.

To upgrade the Agent manually

1. Insert the installation CD into the CDROM drive of the target machine.

   Note ● You can install from the network file system if you do not have a physical CD by mounting the image or copying the files to your network mount. However it is important that you maintain the directory structure. (See Prepare Installation Files for Install.)

2. Open a terminal.
3. Change to the root user, if necessary.
4. Navigate to the CD directory.

   Linux usually displays the CD on the desktop. On other systems, you might need to mount the CD in order to navigate to it. If so, use the following steps (your system may vary).

   As root user, enter this command at a terminal window prompt:

   ```
   mount /dev/cdrom
   ```

   Note ● The mount point can vary, but the CD-ROM device (link) is normally `/dev/cdrom`.

5. Press **Enter**.

   The system mounts the CD and may automatically display a GUI browser for you to use. Either browse to the CD using the GUI browser or browse to it from the terminal window. If the CD-ROM is already mounted, the system indicates that the device is already mounted.

6. Change to the `cdrom` directory: **cd /media/cdrom**
7. Enter **./install_client.sh -u**

Note • Previous versions of QMX - Configuration Manager 2007 only required a hostname or IP address for the Management Point. QMX - Configuration Manager 2007 2.2 requires that you use the Fully Qualified Domain Name (FQDN), not just the Hostname for the MP_Address value.

When upgrading, if you do not provide new SITE_CODE and the MP_ADDRESS values, the system reconfigures the new Agent using the previous settings for the SMS Site Code and Management Point.

To change the Management Point address to the FQDN after installation, you can run the `clienttool --reset-stored-site-info` command.

8. After processing the Site Code and Management Point entries, the install script does these things:
   - Compiles the MOF (This may take awhile).
   - Starts the Client daemon.
   - Displays, "Upgrade successful."
   - Exits to a command prompt.
9. Enter **exit** to exit from the shell.

After all the Agents are upgraded, you can upgrade the Microsoft Management Console (MMC) extensions. (See Upgrading the MMC Extensions.)

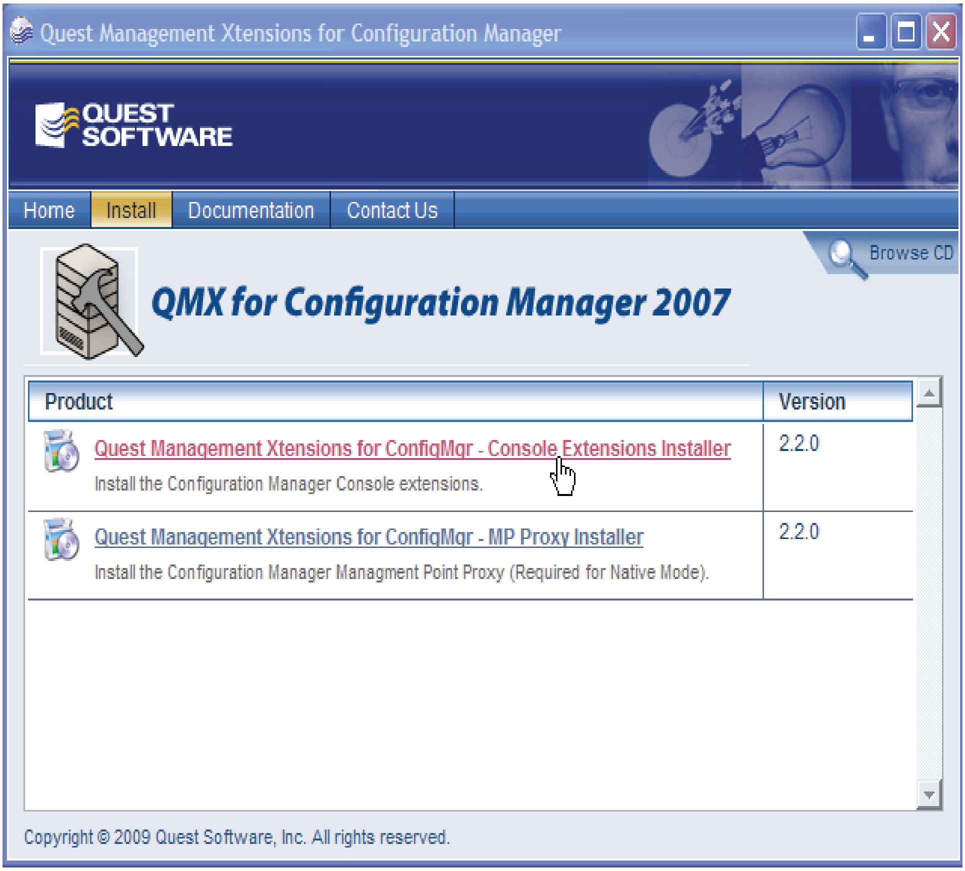
To Uninstall or Upgrade VAS, see *About Integration of VAS* in the *QMX - Configuration Manager 2007 Administrator's Guide*.

Upgrading the MMC Extensions

You must install the Microsoft Management Console Extensions upgrade on all servers and workstations that run the Configuration Manager Console. Installing these extensions makes non-Windows management tasks available through the console.

To upgrade the MMC Extensions

1. Insert the installation CD into the CD-ROM drive of the target machine:



QMX for Configuration Manager 2007

Product	Version
Quest Management Xtensions for ConfigMgr - Console Extensions Installer Install the Configuration Manager Console extensions.	2.2.0
Quest Management Xtensions for ConfigMgr - MP Proxy Installer Install the Configuration Manager Managment Point Proxy (Required for Native Mode).	2.2.0

Copyright © 2009 Quest Software, Inc. All rights reserved.

2. Click the **Install** tab on the autorun screen.
3. Click the **Quest Management Xtensions for ConfigMgr -- Console Extensions Installer** link.

   The *Management Console Extensions Setup* Wizard starts automatically and leads you through the process.

Upgrading Collections and Queries

For a list of new platforms supported in QMX - Configuration Manager 2007 2.2, please consult the “New in This Release” section of the Release Notes located at the root of the distribution media. New Collections and Queries were added and old Collections and Queries were updated to support these new platforms.

Upgrading the MMC extensions, does not automatically install collections or queries for any new client Agents supported by QMX - Configuration Manager 2007, nor does it update existing collections or queries. To upgrade collections or queries, you must first delete the old ones and then install the new ones (see Installing the Collections and Queries).

Whenever you re-install any query or collection that was previously modified, the changes will be lost.

Upgrading from Versions Prior to 1.6

If you have a version earlier the QMX for SMS 1.6, you must first upgrade to 1.6 before upgrading to the latest version of QMX - Configuration Manager 2007.

There are four stages to these upgrade procedures:

1. Upgrade the VMX or QMX for SMS Client. (see Upgrading the Client).
2. Upgrade Microsoft System Management Server (SMS) to Microsoft System Center Configuration Manager 2007.
3. Upgrade the Quest Microsoft Management Console (MMC) extensions, which include the property pages and remote administration tools that enable you to manage non-Windows systems from the Configuration Manager Console. (See Upgrading the Console Extensions.)
4. If you are upgrading from VMX for SMS 1.2.x or earlier, you must also uninstall the old Management Point Extension. (See Uninstalling the Management Point Extension for detailed steps.) However, it is important NOT to remove the MPE until you are confident your upgrade was successful.

Important Upgrade Considerations

Before you begin, please take note of the following:

1. The order in which you perform these steps is important:

a) Upgrade the VMX or QMX for SMS Client to the QMX - Configuration Manager 2007 Agent before you upgrade SMS to Microsoft System Center Configuration Manager 2007.

Quest recommends that you use a phased approach to upgrading your systems. Upgrade all of your VMX or QMX for SMS Clients for a particular site server completely, then upgrade them for the next site server, and so on.

b) After upgrading SMS to System Center Configuration Manager 2007, you must upgrade the Microsoft Management Console (MMC) extensions because the old QMX for SMS Administrator Console extensions for the Software Distribution Wizard, Remote Tools, and so forth, will not work with the new System Center Configuration Manager console. (See Upgrading the Console Extensions.)

2. Suggestions for System Management During the Interim:

a) During the interim between upgrading the Client and upgrading the MMC extensions, do not create new Software Distributions for the upgraded Agent from the older MMC extensions. (Hardware and Software Inventory will work.)

b) To manage the new Agents with the older version of the MMC extensions, create collections based on the Agent version number. Or, you can install the new MMC console extensions on a separate console to manage the new Agents during the transition period.

3. After you upgrade the QMX - Configuration Manager 2007 Agent:

a) You must re-install your non-Windows collections and queries. (see Installing the Collections and Queries). The collections and queries that you created with VMX or QMX for SMS will not work with QMX - Configuration Manager 2007. QMX - Configuration Manager 2007 provides new collections and queries that are much more refined and useful for managing non-Windows resources.

Whenever you re-install any collection or query that was previously modified, the changes will be lost.

b) For your convenience, the upgrade process creates symbolic links for the legacy product naming conventions so that any configuration files or init scripts that you have created for previous releases of QMX for SMS that depend on the “VMX” or “Vintela” names are still accessible. For example, `/opt/vintela/vmx` will link to `/opt/quest/qmxcm` unless `/opt/vintela/vmx` could not be removed due to extra files. Originally this product was named Vintela Management Extensions (VMX). It is necessary for the code base to retain some references to “VMX” or “Vintela” for upgrade and compatibility purposes.

Upgrading the Client

When you receive an upgrade for your VMX or QMX for SMS product, you can either upgrade the VMX/QMX Client manually or use the QMX for SMS Software Distribution Wizard.

If you have Vintela Management Extensions (VMX) version 1.1 or older, you must first upgrade to QMX for SMS version 1.2, 1.5, or 1.6. You can not directly upgrade the 1.1 VMX Client to the QMX - Configuration Manager 2007 Agent. It is safe to upgrade the 1.2, 1.5, or 1.6 clients to the QMX - Configuration Manager 2007 Agent provided that the version of the console extensions with which you are performing a distributed upgrade is not newer than the client's version.

Using the Wizard to Upgrade the Client

When upgrading by means of the Software Distribution Wizard, please note:

- Make sure to use the same version of the console extensions that is running on the client when you create the upgrade package. For example, if you have a client with VMX 1.2 installed, use the Admin Console with VMX 1.2 installed.
- Make sure you have plenty of space for the temporary install files! 800 MB is required in `/var/opt/quest/qmxcm` for AIX. Other platforms do not require as much space; it depends on the size of the install files.

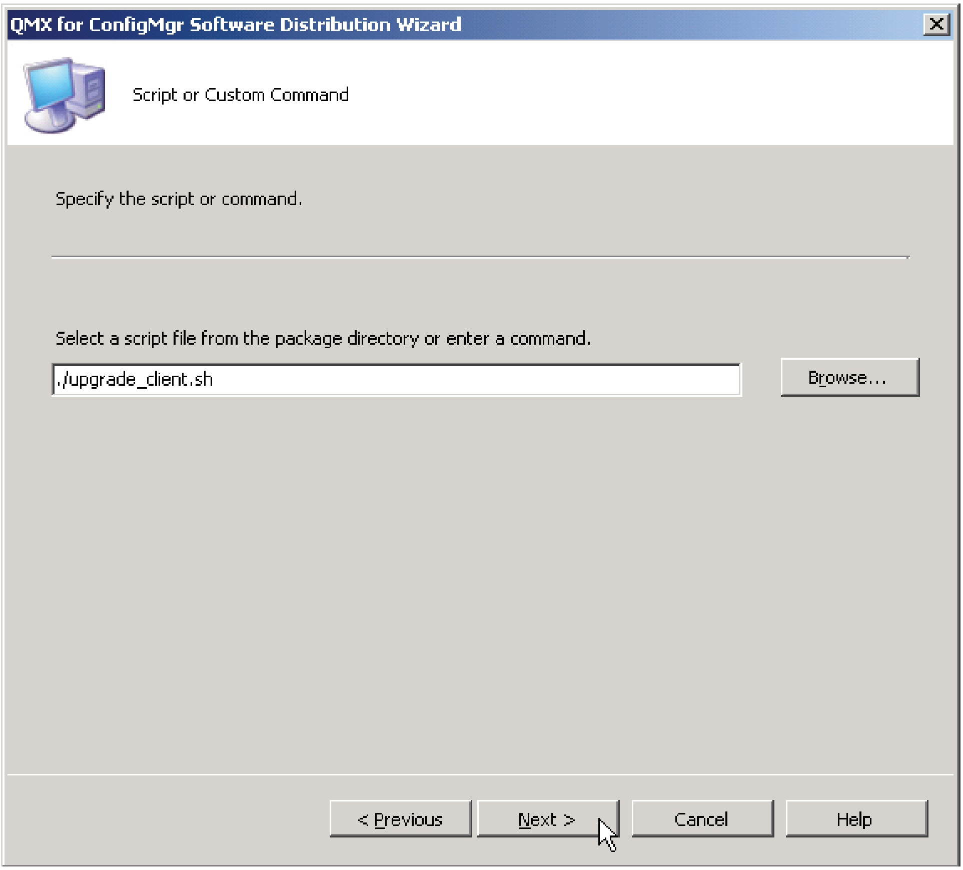
To upgrade the QMX for SMS Client using the wizard

1. In the SMS Administrator Console, navigate to and right-click the collection you wish to upgrade.
2. Choose **All Tasks | QMX for SMS Software Distribution Wizard** to start the Software Distribution Software Wizard.

   The wizard steps you through the process of identifying the package, source files, and so forth.
3. When the wizard displays the *Select Method* dialog, choose **General Unix**.

   Note ● You use the *General Unix Software Distribution* method to distribute patches and scripts.

4. **Browse** to select the `upgrade_client.sh` script:



Specify the script or command.

Select a script file from the package directory or enter a command.

./upgrade_client.sh

Note ● Do not use quotes in this command line.

5. Proceed through the rest of the Software Distribution Wizard screens to create an Advertisement and set the date and time when you want to assign the program.

After you create the Advertisement, SMS 2003 publishes the upgrade and all the clients in the collection will install the upgrade after the next policy update.

Upgrading the Client Manually

You must have “root” privileges to install the QMX - Configuration Manager 2007 Agent.

To upgrade the QMX for SMS Client manually on a Linux client

1. Insert the installation CD into the CDROM drive of the target machine.

   Note • You can install from the network file system if you do not have a physical CD by mounting the image or copying the files to your network mount. However it is important that you maintain the directory structure because the upgrade script is expecting to find certain files in particular locations. (See Prepare Installation Files for Install.)

2. Open a terminal.
3. Change to the root user, if necessary.
4. Navigate to the CD directory.

   Linux usually displays the CD on the desktop. On other systems, you might need to mount the CD in order to navigate to it. If so, use the following steps (your system may vary).

   As root user, enter this command at a terminal window prompt:

   ```
   mount /dev/cdrom
   ```

   Note • The mount point can vary, but the CD-ROM device (link) is normally `/dev/cdrom`.

5. Press **Enter**.

   The system mounts the CD and may automatically display a GUI browser for you to use. Either browse to the CD using the GUI browser or browse to it from the terminal window. If the CD-ROM is already mounted, the system indicates that the device is already mounted.

6. Change to the `cdrom` directory: **cd /media/cdrom**
7. Enter **./install_client.sh -u**

   Note • Previous versions of QMX - Configuration Manager 2007 only required a hostname or IP address for the Management Point. QMX - Configuration Manager 2007 2.2 requires that you use the Fully Qualified Domain Name (FQDN), not just the Hostname for the MP_Address value.

When upgrading, if you do not provide new SITE_CODE and the MP_ADDRESS values, the system reconfigures the new Agent using the previous settings for the SMS Site Code and Management Point.

To change the Management Point address to the FQDN after installation, you can run the `clienttool --reset-stored-site-info` command.

If you are upgrading to QMX - Configuration Manager 2007 version 2.2 and want to take advantage of the System Center Configuration Manager 2007 security features as explained in Supply the Trusted Root Key, it is important to understand how the `-u` option handles the Trusted Root Key (TRK).

- If you do NOT specify a TRK value in the upgrade command line, it will retain a TRK previously specified in an earlier install. Otherwise, you can specify a new TRK value on the command line.
- If you do NOT specify a TRK value in the upgrade command line and no TRK value previously existed, it will automatically install the TRK from your selected management point.

8. After processing the Site Code and Management Point entries, the install script does these things:
   - Compiles the MOF (This may take awhile).
   - Starts the OpenWBEM Daemon.
   - Displays, "Upgrade successful."
   - Exits to a command prompt.
9. Enter **exit** to exit from the shell.

After all the clients are upgraded, you can upgrade Microsoft System Management Server (SMS) to Microsoft System Center Configuration Manager 2007 (System Center Configuration Manager 2007). (See Upgrading SMS.)

To Uninstall or Upgrade VAS, see *Integrating with VAS* in the *QMX - Configuration Manager 2007 Administrator's Guide*.

Upgrading SMS

It is not within the scope of this guide to document how to upgrade Microsoft System Management Server (SMS) to Microsoft System Center Configuration Manager 2007 (System Center Configuration Manager 2007). The upgrade procedure is similar to a new installation, but you must consult Microsoft documentation for specifics.

After SMS is upgraded to System Center Configuration Manager 2007, you can upgrade the Microsoft Management Console (MMC) extensions. (See Upgrading the Console Extensions.)

Upgrading the Console Extensions

You can not automatically upgrade the Windows components from SMS extensions to System Center Configuration Manager extensions. You must remove the old extensions before installing the new extensions.

Use Add/Remove Programs to uninstall the old MMC extensions.

To install the new Microsoft Management Console (MMC) extensions, follow the procedures for a new installation. See Installing the Console Extensions for screen shots and step-by-step instructions. The Quest *Configuration Manager Console Extensions Setup Wizard* leads you through the process.

Enable Anonymous Connections

After you upgrade the MMC extensions, you must enable anonymous connections in the Distribution Point configuration for Software Distribution to work properly. (Note: anonymous connections is for mixed mode only.)

To enable anonymous connections in the Distribution Point

1. Navigate to **Site Database | Site Management | <site code> - <site name> | Site Settings | Site Systems**.
2. Select the site that contains the Distribution Point.
3. Right-click **ConfigMgr distribution point** and choose **Properties**.
4. Select **Allow clients to connect anonymously (Required for mobile device clients)**.
5. Click **OK**.

Upgrade Collections and Queries

Upgrading the MMC extensions, does not automatically install collections or queries for any new client Agents supported by QMX - Configuration Manager 2007, nor does it update existing collections or queries. To upgrade collections or queries, you must first delete the old ones and then install the new ones (see Installing the Collections and Queries.)

Whenever you re-install any query or collection that was previously modified, the changes will be lost.

Uninstalling the Management Point Extension

For upgrades from QMX for SMS 1.2.x and earlier, you must also uninstall the Management Point Extension (MPE). However, it is important NOT to remove the MPE until after you know you have successfully upgraded the client machines.

You can safely remove the Management Point Extensions before or after you upgrade SMS to System Center Configuration Manager 2007.

To remove the Management Point Extension manually

1. Go to **Start | Settings | Control Panel | Add or Remove Programs**.
2. Select **QMX for SMS Management Point Extensions** and click **Remove**.

To remove the Management Point Extension using Software Distribution

Note: You will need the QMX for SMS distribution CD (or the files that you used to install the Management Point Extension) for the previous version of QMX for SMS.

The following are steps to remove the MPE from Management Point Site Systems from SMS with an SMS Advanced Client installed, that is these steps assume you have not upgraded SMS to System Center Configuration Manager 2007 yet.

1. Create a new collection,

   a) Right-click the top **Collection** node and choose **New | Collection**.

b) Enter an appropriate name in the *Name* box, such as “MP Servers with SMS Client”.

c) Enter an appropriate description for this collection in the *Comment* box, such as “This collection will collect all SMS System Sites on which the SMS Advanced Client is installed and to which the Management Point Role is assigned”.

d) Click the **Membership Rules** tab.

e) Click the Query Edit button (Database Starburst) to open the *Query Rule Properties* dialog.

f) Enter an appropriate name in the *Name* box, such as “GetMPservers”.

g) Click **Edit Query Statement** to open the *Query Statement Properties* dialog.

h) Click **Show Query Language** at the bottom of the dialog to open the Query statement window.

i) Enter the following query:

```
select

* from SMS_SystemResourceList where

SMS_SystemResourceList.RoleName = 'SMS Management Point'
```

j) Click **OK** to save the query.

k) Click **OK** at the *Query Rule Properties* dialog.

l) Click **Schedule** to assign a schedule to that collection or click **OK** to create the new collection.

2. Right click the new collection you just created and select **All Tasks | Update Collection Membership**. Click **OK** to update the content of the collection.
3. Right-click the collection again and select to **All Tasks | Distribute Software**.
4. Click **Next** at the *Welcome* dialog.
5. Select the **Create a new package from a definition** option and click **Next**.
6. Click **Browse** to select the `VMXMP.msi` file in `win32` folder on the distribution CD for the previous version of QMX for SMS and click **Open**.
7. Click **Next** at the *Package Definition* dialog.
8. Select **Always obtain files from a source directory** at the *Source Files* dialog and click **Next**.
9. Select **Local drive on site server** at the *Source Directory* dialog.

10. Click **Browse** to select the `win32` folder on the distribution CD for the previous version of QMX for SMS and click **Next**.
11. Select the appropriated Distribution Points and click **Next**.
12. Select **Per-user uninstall** at the *Select a Program to Advertise* dialog and click **Next**.
13. Click **Next** at the *Advertisement Name* dialog.
14. Verify that the new collection you just created is the target for the advertisement and click **Next**.
15. Assign an appropriate schedule and click **Next**.
16. Assign the Program on an specific date and time to make it mandatory and click **Next**.
17. Review the details on the last dialog and if everything is correct click **Finish**.

10

Troubleshooting

- Basic Troubleshooting Tips
- QMX Troubleshooting Tools
- qmxcm.conf Configuration File
- qmxsms.conf Configuration File
- Changing the Log Behavior
- OpenWBEM Logs
- Agent Init Script
- Common Troubleshooting Issues
- Snapshot Script

Basic Troubleshooting Tips

Before you call Support

1. Review the steps in Preparing for Installation.
2. Review the steps in Important Agent Installation Considerations.
3. Verify that the Management Point (or MP Proxy, if in native mode) and the QMX Agent client can communicate with each other, that is, can you ping back and forth? (See Verify the Port Number.)
4. Verify that the Management Point server port (or MP Proxy server port, if in native mode) and the port the QMX - Configuration Manager 2007 Agent uses for communications are the same. (See Resolve Hostnames.)
5. Restart the QMX Agent by entering:

   ```
   /opt/quest/qmxcm/sbin/qmxcmd_init restart
   ```

If the QMX - Configuration Manager 2007 Agent installation fails, you must run the `/opt/quest/qmxcm/bin/uninstall_client.sh` script to uninstall the QMX Agent before you try to reinstall it. (For more information about the other options to the `qmxcmd_init` script, see Agent Init Script.)

6. Examine the Log files. (See Log Files.)

Try Uninstalling the Agent and Reinstalling the Agent.

QMX Troubleshooting Tools

QMX - Configuration Manager 2007 provides the following to help you troubleshoot issues you might encounter:

- Log Files
- Configuration Files
- clienttool

Log Files

QMX - Configuration Manager 2007 is instrumented with rich logging capabilities. Log files are text files that contain messages generated by the software. You use configuration files to customize the behavior of the log files. Some of the log files are found at the following locations on the QMX Agent client machine:

- /var/opt/quest/qmxcm/logs/qmxcmd.log

- /var/opt/quest/qmxcm/owlogs/qmx_status.log
- /var/opt/quest/qmxcm/owlogs/qmxlog.txt
- /var/opt/quest/umi/logs/owcimomd.log
- /var/opt/quest/umi/owcimomd.monitor.log

Agent Push Installer Log

The `push_install.log` can help you troubleshoot issues you might have when installing the QMX - Configuration Manager 2007 Agent with the QMX - Configuration Manager 2007 Agent Installation Wizard. It logs debug information from the push installer code more than one machine. That is, if you push the Agent out to multiple clients, it logs the data from all of those installations. Quest Support may ask you to send them this log file. It is located at: `C:\Program Files\Quest Software\QMX for ConfigMgr`.

You can configure this log to use one of the standard logging levels. (See Levels for information about the available logging levels.) The configuration file for this log is: `C:\Program Files\Quest Software\QMX for ConfigMgr\log.properties`.

Configuration Files

You use certain configuration files to manage the various QMX - Configuration Manager 2007 Agent logs. For example, you can change the logging levels, format, and destinations by editing the configuration file. Here is a list of configuration files and the various log files they affect.

AGENT LOG FILES

CONFIGURATION FILE	LOG FILE IT AFFECTS
/etc/opt/quest/qmxcm/**qmxcm.conf**	**Log file**: qmxcmd.log **Location**: /var/opt/quest/qmxcm/logs/qmxcmd.log **Description**: Logs operations only within the QMX - Configuration Manager 2007 polling daemon.

CONFIGURATION FILE	LOG FILE IT AFFECTS
/etc/opt/quest/umi/openwbem/openwbem.conf.d/**qmxsms.conf** This configuration file controls three log files: • qmx_status.log • qmxlog.txt • qmxlog.xml	**Log file**: qmx_status.log **Location**: /var/opt/quest/qmxcm/owlogs/qmx_status.log **Description**: Logs when various QMX - Configuration Manager 2007 processes start and stop. It is much easier to find the history/status of the QMX Agent when checking this log than checking the qmxlog.txt because it does not grow very fast. Use this log within the System Center Configuration Manager 2007 log reader, SMS Trace, with the exception of the source line number. (Access SMS Trace by opening a log file.)
Note: This is the most important log file!	**Log file**: qmxlog.txt **Location**: /var/opt/quest/qmxcm/owlogs/qmxlog.txt **Description**: Logs everything that happens in the providers and cimom. `qmxsms.conf` controls the log file settings. **Note**: The log file directory must be writable by the owcimomd user and must not have the sticky bit set.
	Log file: qmxlog.xml **Location**: /var/opt/quest/qmxcm/owlogs/qmxlog.xml **Description**: Contains the same data as qmxlog.txt. Use an xml viewer to read this log.

Quest Support may ask you to send one or more of these log files to them for analysis.

The QMX Agent Debug Log

The `qmxlog.txt` file will be your most useful log file. However, this file grows dynamically. If you wait too long before you open it, the error messages you are most interested in may have rolled by. Quest recommends that you re-create any errors seen on the client just before opening this log file. This will help ensure that the debug messages surrounding the error have not "rolled out" of the log file. You can "capture" the log by saving it to a location of your choice at any point.

clienttool

Quest has provided the `clienttool` to help you perform maintenance tasks on the QMX Agent. You can use it to force policy update, run hardware inventory and to run software distribution before its regularly scheduled process time.

To list the clienttool's options

1. At the client command line, enter:

```
/opt/quest/qmxcm/bin/clienttool -h
```

To force a policy update

1. At the client command line, enter

```
/opt/quest/qmxcm/bin/clienttool --run-policy-update
```

qmxcm.conf Configuration File

The `qmxcm.conf` file controls the `qmxcmd.log` file which logs operations within the QMX polling daemon. It is located at: `/etc/opt/quest/qmxcm` and holds the values for the Site Code and the Management Point, among other values, used by the QMX Agent. You can modify the following site variables in this configuration file:

QMX Agent Site Variables

SITE VARIABLE	DESCRIPTION
qmxcm.mpe=	The FQDN of the Management Point or MP Proxy.
qmxcm.site_code=	The site code.

SITE VARIABLE	DESCRIPTION
qmxcm.mpe.port=	The external Management Point HTTP port. (Default is 80)
qmxcm.mpe.secureport=	The external Management Point HTTPS port. (Default is 443)
qmxcm.package_cache=	Default value is “disabled” to save memory. Set to “enabled” to see product details in software inventory or software metering on Mac OS X.
qmxcm.osx.use_pachages_search=	Default is “false”. Set to “true” to scan filesystem for installed packages on the Mac OS X.
qmxcm.osx.use_spotlight_search=	Default is “true”. Enables Spotlight to query for installed packages (supported only on Mac OS X 10.4 and above).
qmxcm.poll_interval=	Default is 60 seconds. Use only if no policy is available.
qmxcm.connect_timeout=	The time-out value for connections with the MP, DP or MP Proxy. (Default is 60 seconds.)

To view the site code in the qmxcm.conf configuration file

1. At the command line navigate to:

   ```
   # cd /etc/opt/quest/qmxcm
   ```

2. Open the `qmxcm.conf` configuration file for editing.
3. Find the site code variable. It is a line that looks like this:

   ```
   qmxcm.site_code=LAB
   ```

   Note • Do not change the site code right now, as that would “break” QMX's connection to the Site Server.

Using clienttool to Change the Site Settings

You can modify the site variable values directly in `qmxcm.conf` configuration file, however it is easier to use the following `clienttool` options:

CLIENTTOOL OPTIONS

OPTIONS	DESCRIPTION
--reset-stored-site-info	Deletes the client settings (Management Point Certificates, Trusted Root Key, etc.) in the repository, installs fresh copies, and re-registers the client with the Management Point. You can run this option in combination with --set-site-code, --set-mp, --set-port, or --set-ssl-port to reset specific client settings. This enables you to switch to a new site. Or, you can use any of these options as stand-alone commands. **Note**: Use this option to clean up your site settings before switching from mixed to native mode. This option purges all of the site-specific information in the repository. It deletes certificates, removes the current Trusted Root Key (TRK) and some policy instances; then, it creates a policy update schedule, if one does not already exist, and verifies that the site is reachable using any communication settings in the `qmxcm.conf` file. This command immediately runs a discovery and, within approximately 15 minutes, it runs a policy update.
--set-site-code <arg>	Changes the Site Code to [arg] in the `qmxcm.conf` file and verifies that it is three uppercase characters.
--set-mp <arg>	Changes the Management Point to [arg] in the `qmxcm.conf` file or, if in native mode, changes the MP Proxy to [arg]. **Note**: Changes the `qmxcm.mpe` value in the `qmxcm.conf` file to the Fully Qualified Domain Name (FDQN) of the MP Proxy. This verifies that it is reachable and warns if it cannot be used securely in native mode because it is set to something other than a FQDN.
--set-port <arg>	Changes the http port to [arg] in the `qmxcm.conf` file or, if in native mode, changes the MP Proxy http port to [arg].

OPTIONS	DESCRIPTION
--set-ssl-port <arg>	Changes the MP Proxy SSL port to [arg] in the `qmxcm.conf` file and verifies that it is numeric. **Note**: 443 is the default port. The value of `qmxcm.mpe.secureport` in the `qmxcm.conf` file must match the SSL configuration of IIS for the machine on which the MP Proxy is installed. `qmxcm.mpe.secureport` is the port the Agent uses to communicate to the MP Proxy using SSL.

Example of Using --reset-stored-site-info

You can use `clienttool --reset-stored-site-info` command in combination with `--set-site-code`, `--set-mp`, `--set-port`, and `--set-ssl-port`.

For example, if you entered the following at the client command line:

```
# clienttool --reset-stored-site-info --set-site-code NAT
--set-mp css.native.qmxdev --set-port 80 --set-ssl-port 443
```

It would return the following:

```
Changed site code to NAT Changed MP Proxy SSL port to 443 Changed
MP port to 80. Changed MP to css.native.qmxdev. Detecting MP
communication method. Site successfully changed. We are now
talking to the MP Proxy using SSL.
```

qmxsms.conf Configuration File

The `qmxsms.conf` file controls log file locations and logging levels for the QMX Agent log files. It is located at: `/etc/opt/quest/umi/openwbem/openwbem.conf.d` and controls three rolling debug-logs:

- qmx_status.log
- qmxlog.txt
- qmxlog.xml

In addition, it is possible to edit `qmxsms.conf` to create a new log file focused on a specific “area” or component of the QMX Agent.

Creating a New Log

To view the qmxsms.conf configuration file

1. At the command line navigate to:

   ```
   # cd /etc/opt/quest/umi/openwbem/openwbem.conf.d
   ```

2. Open the `qmxsms.conf` configuration file for editing.
3. Notice that the "log.qmx" log and "log.qmxxml" log have lines for *components*, *level*, *format*, *type*, and so on.
   For example, the log.qmx looks like this:

   ```
   log.qmx.components = *

   log.qmx.level = DEBUG

   log.qmx.format = %d{%Y-%m-%d %H :%M :% :.%Q} (%-6r) [%5.5t]
   %-5p %20.20c - %m

   log.qmx.type = file

   log.qmx.location = /var/opt/quest/qmxcm/owlogs/qmxlog.txt

   log.qmx.max_file_size = 5000

   log.qmx.max_backup_index = 1
   ```

If you wanted to add a new log that is focused on the policy provider, for example, all you need to do is clone the log.qmx section of the `qmxsms.conf` file and change a few things.

To create a new log

1. The first thing to do is add the new log name to the *additional_logs* variable.
2. Add the name of the new log to the line that looks like this:

   ```
   owcimomd.additional_logs = qmx qmxxml qmxclientstatus
   mypolicy
   ```

3. Next, add a blank line above the log.qmx section of `qmxsms.conf`.
4. Copy and paste the log.qmx onto the new line.
5. Edit the lines until your new section looks like this: (the high-lighted words are what you need to change.)

   ```
   log.mypolicy.components = qmx.policy

   log.mypolicy.level = DEBUG

   log.mypolicy.format = %d{%Y-%m-%d %H :%M :% :.%Q} (%-6r)
   [%5.5t] %-5p %20.20c - %m

   log.mypolicy.type = file
   ```

```
log.mypolicy.location =
/var/opt/quest/qmxcm/owlogs/mypolicylog.txt

log.mypolicy.max_file_size = 5000

log.mypolicy.max_backup_index = 1
```

Note ● You have now changed the component from "everything" (*) to focus on **qmx.policy** provider and you have changed the name of the log to **mypolicylog**.

6. Save `qmxsms.conf` with these changes.
7. Restart the QMX Agent by entering:

   ```
   # /opt/quest/qmxcm/sbin/qmxcmd_init restart
   ```

8. Force debug data into the new file by entering:

   ```
   /opt/quest/qmxcm/bin/clienttool --run-policy-update
   ```

9. Verify that the policy-related debug output is now going to the newly created `policylog.txt` file by entering:

   ```
   cat /var/opt/quest/qmxcm/owlogs/mypolicylog.txt
   ```

   – OR –

10. Alternatively, you can open `mypolicylog.txt` in a text editor. It is located at cd /var/opt/quest/qmxcm/owlogs/

Changing the Log Behavior

In addition to modifying log file locations and logging levels for the QMX Agent log files, you can also change the logging behavior of any log controlled by the `qmxsms.conf` file. You can go into the `qmxsms.conf` file and change any of these settings:

- Components
- Levels
- Format
- Type
- Location
- Maximum File Size

- Maximum Backup Index

You must restart the QMX Agent for changes to take effect. Use the follow command to restart the QMX Agent. Use the qmxcmd_init script to restart the QMX Agent. For more information about the other options to the `qmxcmd_init` script, see Agent Init Script.)

Components

To create a log focused on a particular provider, set the *component* variable in any log file to one or more of the following values:

- * (all components)
- qmx.hardware
- qmx.discovery
- qmx.policy
- qmx.fiecollection
- qmx.softwaredistribution
- qmx.software (software inventory)
- qmx.qmxclientstatus
- qmx.debug
- qmx.smsinventory

The default is *. Use a space delimited list of components to specify more than one. For example:

```
log.qmxclientstatus.components = qmx.qmxclientstatus qmx.policy
```

To change the focus of the log file

1. At the command line navigate to:

   ```
   # cd /etc/opt/quest/umi/openwbem/openwbem.conf.d
   ```

2. Open the `qmxsms.conf` configuration file for editing.
3. Find the *Components* variable. It is a line that looks like this:

   ```
   log.qmx.components = *
   ```

4. Change the default *component* value from `*` (“everything”) to `qmx.policy` to focus on the Policy provider.

Levels

You can modify the amount of information sent to a log file by changing the *level* variable. For example:

```
log.qmxclientstatus.level = DEBUG
```

LOG LEVELS

LOG LEVEL	DESCRIPTION
FATAL	Severe errors that cause premature termination.
ERROR	Other runtime errors or unexpected conditions.
INFO	Interesting runtime events (startup/shutdown).
DEBUG	Detailed information on the flow through the system.

The logs output all predefined categories at and above the specified level. By default the syslog logs Agent activity at the “ERROR” level.

Format

You can specify the format of the log message by using the conversion specifiers defined in the configuration file. For example,

```
log.main.format = [%t %-5p %c] %m
```

Type

The *type* variable specifies where you want logging information written. The default *type* value is “file”. You can change the log type to *stderr*, *stdout*, but Quest does not recommend changing the *type* variable. For example,

```
log.qmx.type = file
```

Location

The *location* variable specifies the location of the log file. The QMX Agent sends log messages to syslog, the Unix equivalent of the Windows Event Logger. However, syslog is in a different location on each operating system. So, to make troubleshooting easier, redirect the output to a specific file by specifying the file path and log name in the *location* variable. The directory of the log must have *write* and *execute* permissions set so owcimond can create and delete files.

If you change the path of any log, the owcimomd user must have read, write, and execute (rwx) access to the parent folder.

For example:

```
log.qmx.location = /var/opt/quest/qmxcm/owlogs/qmxlog.txt
```

– OR –

```
monitor.log.location = /var/opt/quest/umi/owcimomd.monitor.log
```

Maximum File Size

When debugging, you will probably change the logging level to produce more information. In this case, you should also increase the size of the log file so that you do not truncate any important information.

For example,

```
log.qmxclientstatus.max_file_size = 5000000
```

Maximum Backup Index

When you are debugging, you may want to save more than one log file to preserve the logging history.

For example, to save the last three log files, change this setting to 3:

```
log.qmxclientstatus.max_backup_index = 3
```

OpenWBEM Logs

There are two OpemWBEM logs to be aware of:

```
/var/opt/quest/umi/logs/owcimomd.log
/var/opt/quest/umi/owcimomd.monitor.log
```

The configuration file that manage both of these logs is: /etc/opt/quest/umi/openwbem/openwbem.conf.d/umi.conf

OpenWBEM CIMOM Daemond Log

owcimomd.log is a very small umi log designed to find initial startup problems that arise before QMX is fully installed. This log was designed for the develoeprs to troubleshoot internal the functionality of the QMX Agent and is not really intended for customer use. This log may contain ERROR message, but these messages do not necessarily mean that the QMX Agent is not working correctly.

There are two important lines in this log:

```
;owcimomd.log_location = syslog
;owcimomd.log_level= error
```

You can change the location and level, but don't forget to remove the semicolon!

Privilege Monitor Log

owcimomd.monitor.log manages the Privilege Monitor. It logs any attempts to execute something with elevated privileges.

Agent Init Script

When troubleshooting the QMX - Configuration Manager 2007 Agent, it might be necessary for you to stop and restart the daemon in order to pick up configuration changes. Use qmxcmd_init (the Agent init script) to stop, start, restart, and check the status of the QMX Agent, as shown in this example:

```
/opt/quest/qmxcm/sbin/qmxcmd_init status
```

The options to the qmxcmd_init script are listed in this table:

THE QMXCMD_INIT SCRIPT OPTIONS

OPTION	DESCRIPTION
start	Starts the service.
stop	Stops the service.
restart	Stops and restarts the service if the service is already running, otherwise starts the service.
reload	Reloads the service configuration without actually stopping and restarting the service.
force reload	Reloads the service configuration if the service supports this, otherwise stops the service, if it is running, and then restarts it.
status	Displays the current service status: running or not running; enabled or not enabled; or, dead.

Common Troubleshooting Issues

The following sections address some of the most common troubleshooting issues:

- Hostnames Resolution
- Port Resolution
- SSH Key Resolution
- High CPU Utilization
- Remote Tools Did Not Connect

Hostnames Resolution

Failure of Hostname resolution is the number one cause of installation failure. Successful Policy Updates and Software Distribution require successful resolution of the Management Point hostname (for Policy Update) and the Distribution Point hostname (for Software Distribution).

It is possible to use an IP address for the Management Point to install the QMX - Configuration Manager 2007 Agent. However, unusual behavior (and error messages) can result. Make sure that the host name and IP address resolve on all systems.

Port Resolution

The System Center Configuration Manager 2007 IIS port and the port the QMX - Configuration Manager 2007 Agent uses for communications must be the same. If you have changed your System Center Configuration Manager 2007 port to 8088, for example, you must tell the QMX - Configuration Manager 2007 Agent to use port 8088 as well. (See Agent Installer Settings.)

You can manually change the `qmxcm.conf` file to include the following line: `qmxcm.mpe.port=8088`.The `qmxcm.conf` file is found in the following path: `/etc/opt/quest/qmxcm/qmxcm.conf`. But it is much easier to use the clienttool (see *Using clienttool to Change the Site Settings*.)

When you change the Management Point or the Site Code in the `qmxcm.conf` file, that information is loaded dynamically by the QMX - Configuration Manager 2007 Agent, so no restart is necessary. If you change the debug level, then you must restart the Agent for the configuration file changes to take affect.

SSH Key Resolution

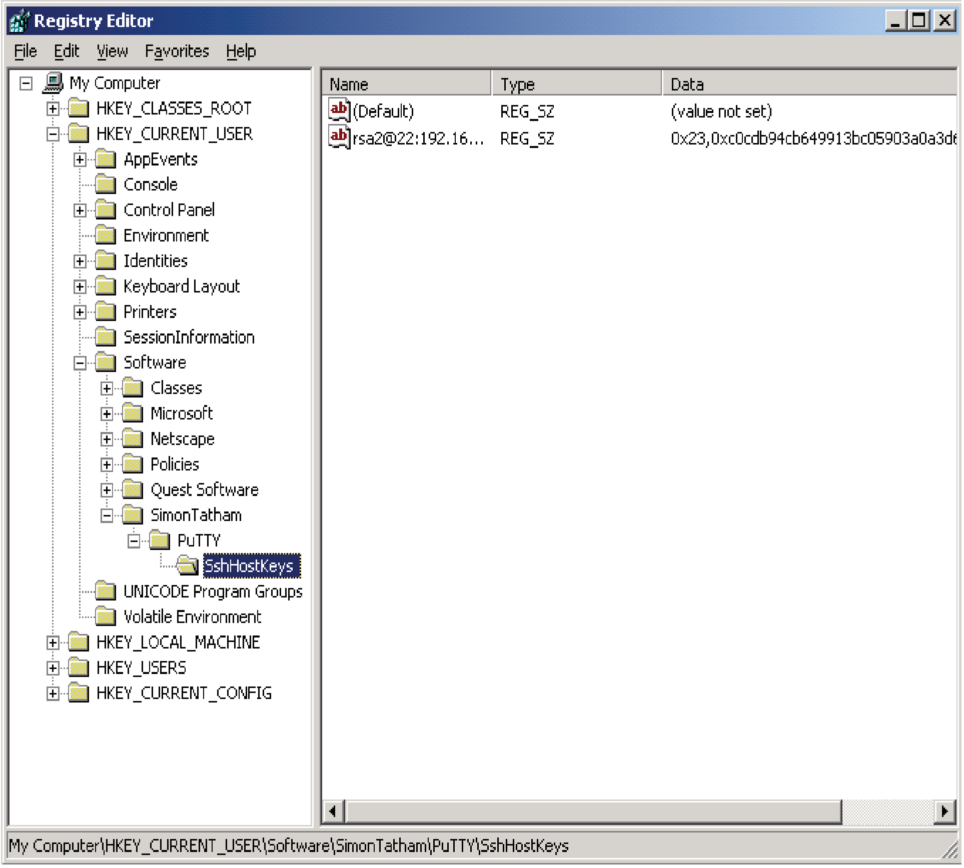
Occasionally the QMX - Configuration Manager 2007 Agent Installation Wizard hangs when the cached SSH key does not match the key sent back for the current SSH connection.

If you have previously installed the QMX Agent onto a target system, the SSH Key from that system will have been cached in the Windows Registry of the Configuration Manager Console system running the install wizard. Under normal circumstances, this caches key is expected to match the key sent up from the target system when you use the QMX Agent Installation Wizard for any subsequent installations. This matching of keys is by design -- to protect against "man-in-the-middle" security attacks. There are however, benign circumstances which can cause the key to change on the target computer. For example, if the target system has been re-installed, or re-imaged. this is because at "first start", SSH generates a new, unique key. At this point, the new key will not match the key cached in the Registry of your Configuration Manger Console computer, even though it comes form the same system, with the same IP address.

After you install the QMX - Configuration Manager 2007 Agent using the wizard, if you re-install the client operating system, the SSH Key will be different. There are two ways to update the key cached in the Registry. You can either: (1) delete the cached SSH host keys from the Registry, or (2) use PuTTY to update the SSH host keys, as explained in the next two procedures:

To delete the SSH host keys

1. Click **Start | Run**.
2. Enter **regedit** and click **OK** to display the Register Editor window:



Name	Type	Data
(Default)	REG_SZ	(value not set)
rsa2@22:192.16...	REG_SZ	0x23,0xc0cdb94cb649913bc05903a0a3d

My Computer\HKEY_CURRENT_USER\Software\SimonTatham\PuTTY\SshHostKeys

3. Navigate to **My Computer | HKEY_CURRENT_USER | Software | SimonTathum | PuTTY | SshHostKeys**.
4. Delete the Key that is causing the error.

   When you re-run the Agent Installation Wizard, it will update the Registry with the correct key.

To use PuTTY to update the SSH Key

1. Navigate to the `QMX for configMgr` folder.

   Note ● If you chose the default installation path, go to: `C:\Program Files\Quest Software\QMX for ConfigMgr`.

2. Double click **PuTTY.exe**.
3. Use the dialog launched by this file to connect to the machine in question.
4. Accept the new SSH key when prompted.

   This updates the key cached in the Registry.
5. Re-run the QMX Agent Installation Wizard.

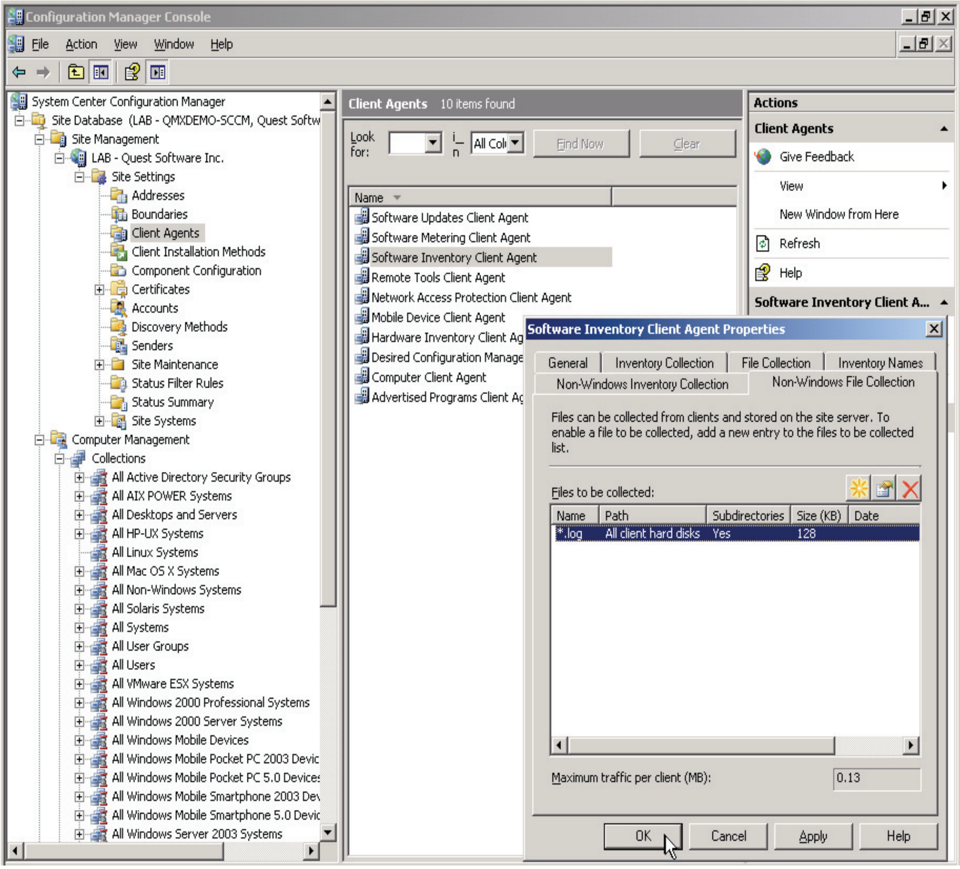
As part of the installation process QMX - Configuration Manager 2007 automatically accepts all client SSH keys rather than prompting you to accept each one. Normally this is considered a security compromise. However since prompting you to review and accept each key would be impractical and since any damage would be limited to the installation of the QMX Agent, Quest engineered QMX - Configuration Manager 2007 this way.

High CPU Utilization

Some functions require more CPU than others. For example, tasks such as Software Inventory and File collection or large and/or frequent software distributions can cause high CPU utilization and excess processing overhead on the server and client.

Here are some things you can check:

1. Check which files are you collecting under **Site Settings | Client Agents | Software Inventory Client Agent** in both the **Non-Windows Inventory Collection** tab and the **Non-Windows File Collection** tab:


Configuration Manager Console
File Action View Window Help
System Center Configuration Manager
Site Database (LAB - QMXDEMO-SCCM, Quest Softw
Site Management
LAB - Quest Software Inc.
Site Settings
Addresses
Boundaries
Client Agents
Client Installation Methods
Component Configuration
Certificates
Accounts
Discovery Methods
Senders
Site Maintenance
Status Filter Rules
Status Summary
Site Systems
Computer Management
Collections
All Active Directory Security Groups
All AIX POWER Systems
All Desktops and Servers
All HP-UX Systems
All Linux Systems
All Mac OS X Systems
All Non-Windows Systems
All Solaris Systems
All Systems
All User Groups
All Users
All VMware ESX Systems
All Windows 2000 Professional Systems
All Windows 2000 Server Systems
All Windows Mobile Devices
All Windows Mobile Pocket PC 2003 Devic
All Windows Mobile Pocket PC 5.0 Devices
All Windows Mobile Smartphone 2003 Dev
All Windows Mobile Smartphone 5.0 Devic
All Windows Server 2003 Systems
Client Agents 10 items found
Look for: in All Col Find Now Clear
Name
Software Updates Client Agent
Software Metering Client Agent
Software Inventory Client Agent
Remote Tools Client Agent
Network Access Protection Client Agent
Mobile Device Client Agent
Hardware Inventory Client Ag
Desired Configuration Manage
Computer Client Agent
Advertised Programs Client Ag
Actions
Client Agents
Give Feedback
View
New Window from Here
Refresh
Help
Software Inventory Client A...
Software Inventory Client Agent Properties
General
Inventory Collection
File Collection
Inventory Names
Non-Windows Inventory Collection
Non-Windows File Collection
OK
Cancel
Apply
Help

Files can be collected from clients and stored on the site server. To enable a file to be collected, add a new entry to the files to be collected list.

Files to be collected:

Name	Path	Subdirectories	Size (KB)	Date
*.log	All client hard disks	Yes	128	

Maximum traffic per client (MB): 0.13

a) Double click a rule to open its *Property* dialog.

b) Click the **Set** button to open the *Path Properties* dialog.

c) Select the **Variable or path name** option to specify a single folder or folder tree.

Note • Selecting the **All client hard disks** option will scan all hard disks for files to collect which could take hours and cause high CPU usage.

2. Check the software metering parameters.

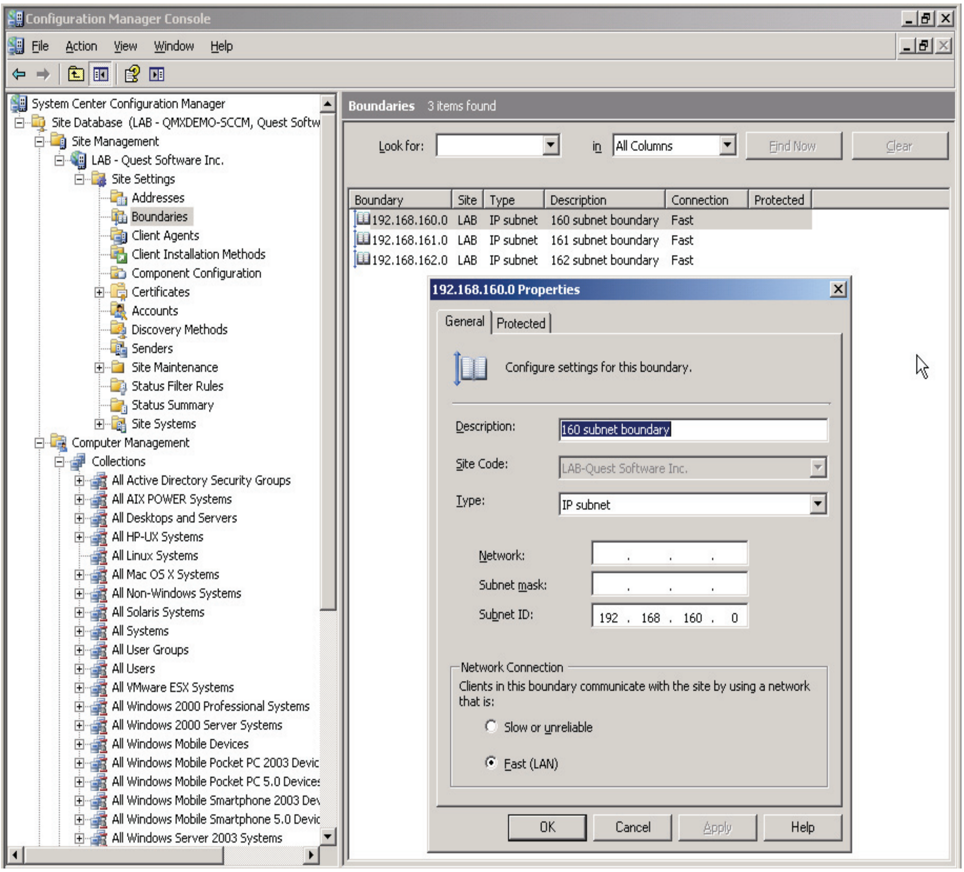
The QMX - Configuration Manager 2007 Agent client performs software metering every 10 seconds by default but a low polling interval can cause High CPU utilization.

a) First check to see if software metering is enabled. Navigate to **System Center Configuration Manager | Site Database | Site Management| <site code> - <site name> | Site Settings | Client Agents | Software Metering Client Agent**.

b) Next check the `umi.metering_poll_interval` in the `/etc/opt/quest/umi/openwbem/openwbem.conf.d/umi.conf` file

To change the software metering interval, see *Scheduling Software Metering* in the *QMX - Configuration Manager 2007 Administrator's Guide*.

3. Check the network discovery frequency. Under **Site Settings** double click **Network Discovery**.



Boundary	Site	Type	Description	Connection	Protected
192.168.160.0	LAB	IP subnet	160 subnet boundary	Fast	
192.168.161.0	LAB	IP subnet	161 subnet boundary	Fast	
192.168.162.0	LAB	IP subnet	162 subnet boundary	Fast	

192.168.160.0 Properties

General | Protected

Configure settings for this boundary.

Description: 160 subnet boundary

Site Code: LAB-Quest Software Inc.

Type: IP subnet

Network: . . .

Subnet mask: . . .

Subnet ID: 192 . 168 . 160 . 0

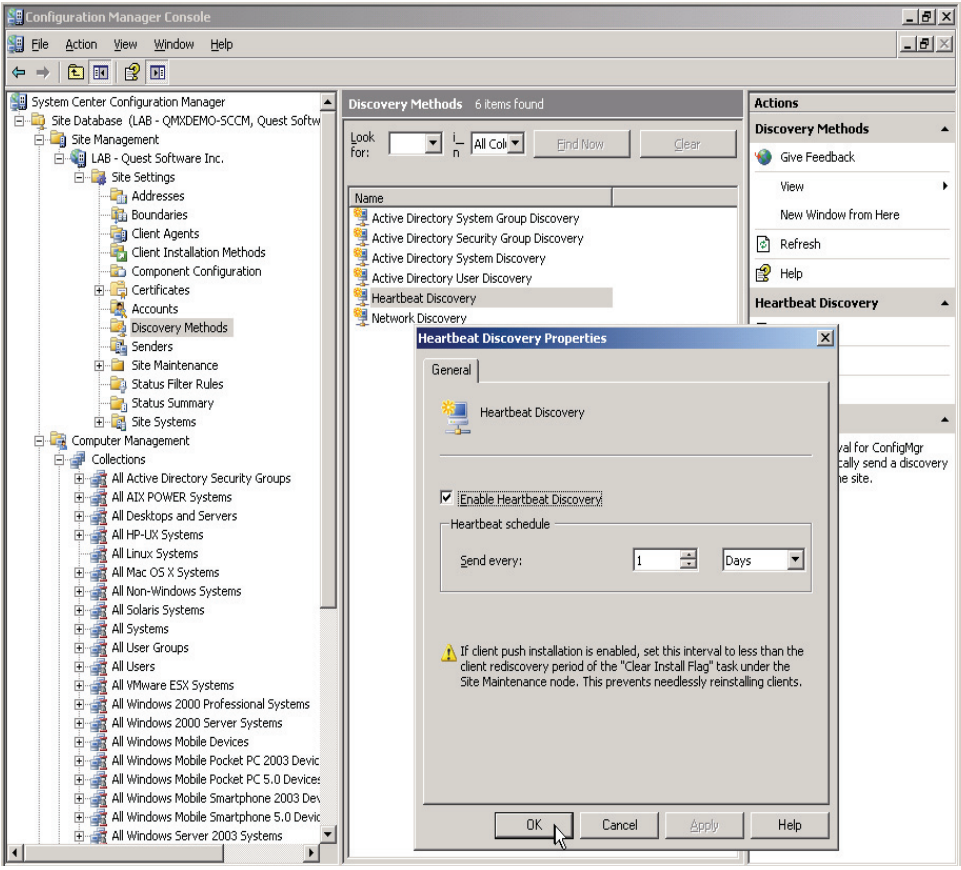
Network Connection

Clients in this boundary communicate with the site by using a network that is:

○ Slow or unreliable

● Fast (LAN)

4. Check the heartbeat discovery frequency. Under **Site Settings** double click **Heartbeat Discovery**.



Configuration Manager Console
File Action View Window Help
System Center Configuration Manager
Site Database (LAB - QMXDEMO-SCCM, Quest Softw
Site Management
LAB - Quest Software Inc.
Site Settings
Addresses
Boundaries
Client Agents
Client Installation Methods
Component Configuration
Certificates
Accounts
Discovery Methods
Senders
Site Maintenance
Status Filter Rules
Status Summary
Site Systems
Computer Management
Collections
All Active Directory Security Groups
All AIX POWER Systems
All Desktops and Servers
All HP-UX Systems
All Linux Systems
All Mac OS X Systems
All Non-Windows Systems
All Solaris Systems
All Systems
All User Groups
All Users
All VMware ESX Systems
All Windows 2000 Professional Systems
All Windows 2000 Server Systems
All Windows Mobile Devices
All Windows Mobile Pocket PC 2003 Devic
All Windows Mobile Pocket PC 5.0 Devices
All Windows Mobile Smartphone 2003 Dev
All Windows Mobile Smartphone 5.0 Devic
All Windows Server 2003 Systems
Discovery Methods 6 items found
Look for:
in
All Col
Find Now
Clear
Name
Active Directory System Group Discovery
Active Directory Security Group Discovery
Active Directory System Discovery
Active Directory User Discovery
Heartbeat Discovery
Network Discovery
Actions
Discovery Methods
Give Feedback
View
New Window from Here
Refresh
Help
Heartbeat Discovery
val for ConfigMgr
cally send a discovery
e site.
Heartbeat Discovery Properties
General
Heartbeat Discovery
OK
Cancel
Apply
Help

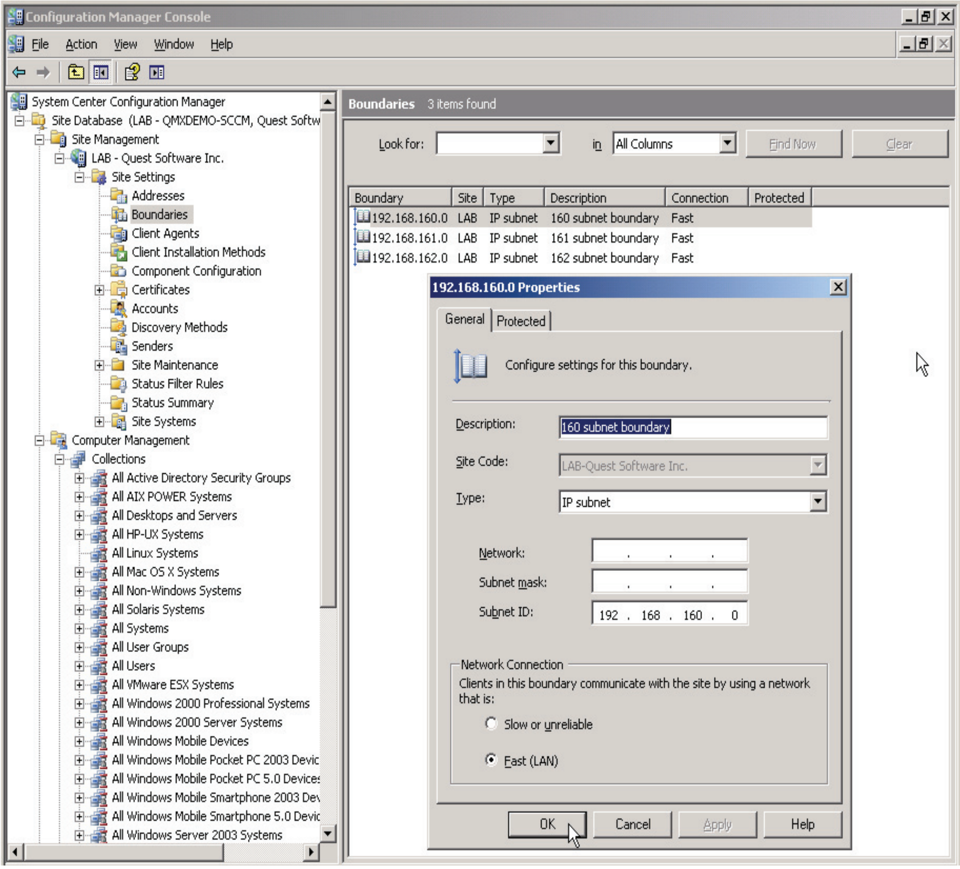
☑ Enable Heartbeat Discovery

Heartbeat schedule

Send every: 1 Days

If client push installation is enabled, set this interval to less than the client rediscovery period of the "Clear Install Flag" task under the Site Maintenance node. This prevents needlessly reinstalling clients.

5. Check to see if you have site boundaries set up under **Site Settings | Boundaries**. Double-click a site name to open the site's *Properties* dialog:



Boundaries 3 items found

Boundary	Site	Type	Description	Connection	Protected
192.168.160.0	LAB	IP subnet	160 subnet boundary	Fast	
192.168.161.0	LAB	IP subnet	161 subnet boundary	Fast	
192.168.162.0	LAB	IP subnet	162 subnet boundary	Fast	

192.168.160.0 Properties

Configure settings for this boundary.

Description: 160 subnet boundary

Site Code: LAB-Quest Software Inc.

Type: IP subnet

Network: . . .

Subnet mask: . . .

Subnet ID: 192 . 168 . 160 . 0

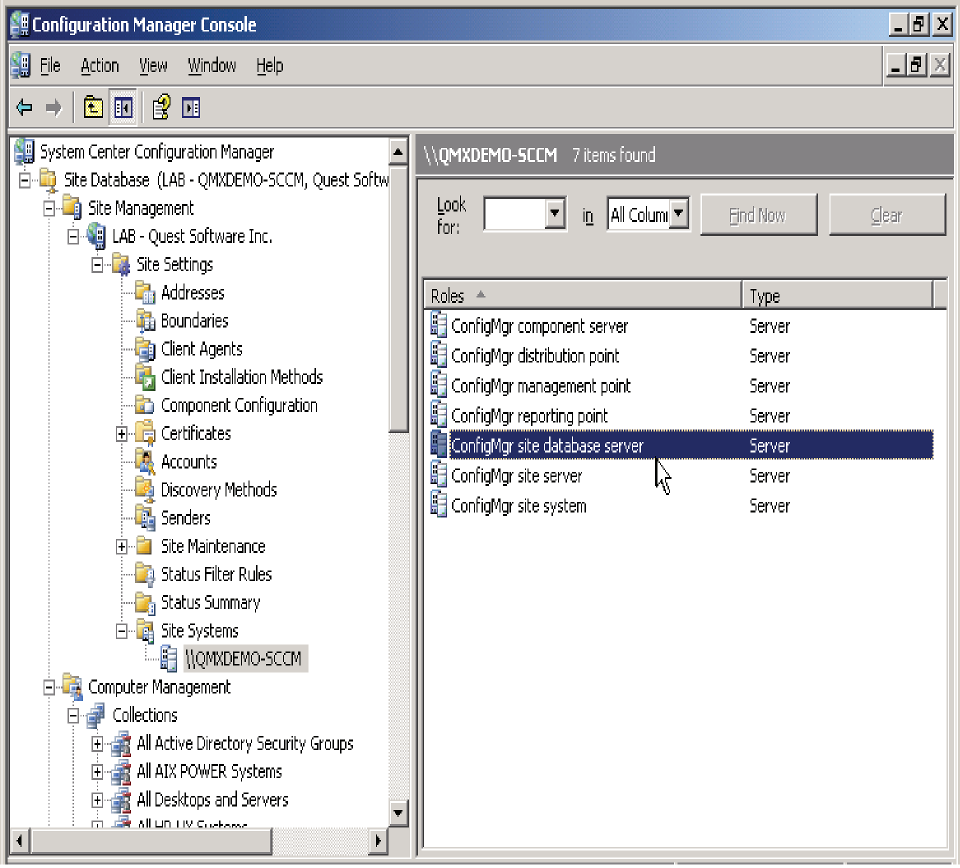
Network Connection

Clients in this boundary communicate with the site by using a network that is:

○ Slow or unreliable

● Fast (LAN)

6. Another thing you can do to check for high CPU Utilization is check that the SQL server database is on the primary site server.



Roles	Type
ConfigMgr component server	Server
ConfigMgr distribution point	Server
ConfigMgr management point	Server
ConfigMgr reporting point	Server
ConfigMgr site database server	Server
ConfigMgr site server	Server
ConfigMgr site system	Server

Changing the CPU Process Priority

Running installation and inventory processes can create CPU spikes. QMX - Configuration Manager 2007 uses the default priority for your system. However, you can temporarily change the priorities of existing processes using the `nice` or `renice` command to restrict CPU spikes.

Note: `nice` starts a new process with the specified priority, while `renice` changes the priority of a process that is already running.

To change the priorities so processes start with a lower priority

1. Enter:

```
nice -n 5 /opt/quest/qmxcm/sbin/qmxcmd_init restart
```

To lower the priority of QMX - Configuration Manager 2007 processes permanently, modify both of the following files:

- `/opt/quest/qmxcm/sbin/qmxcmd_init`
- `/opt/quest/umi/sbin/quest-owcimomd_init`

Change the "`$DAEMON $OPTIONS`" line to "`nice -n <value> $DAEMON $OPTIONS`" where <*value*> is a digit, such as 5, that increases the `nice` value of the process, causing it to run at a lower priority.

Once you modify the init scripts, use Software Distribution to distribute the scripts. The new priorities will be set after the next system reboot or you can manually restart using following commands:

```
/opt/quest/qmxcm/sbin/qmxcmd_init restart

/opt/quest/umi/sbin/quest-owcimomd_init restart
```

Lowering the priority too much will mean that there can be missed items for software metering, extremely long inventory cycles, and so forth. Changing the schedules to do the minimum amount of work required is the preferred method of controlling overall CPU load.

Remote Tools Did Not Connect

Remote tools may not connect to the correct host if the IP has changed since the last time the heartbeat discovery data was reported to System Center Configuration Manager 2007. The managed systems must be resolvable through DNS. See Resolve Hostnames for more information.

Snapshot Script

Quest has provided a special utility script called `snapshot.sh` to help you perform troubleshooting tasks. When you call Quest Support, they may ask you to run the `snapshot.sh` script to gather vital information to help them diagnose your problems. The `snapshot.sh` script creates a `.tar.gz` file in the `/tmp` directory containing basic data from your system. The description of the data it collects is in the header of the script itself. You can find this script in the `/scripts` directory at the root of the installation media and in the `/opt/quest/qmxcm/bin` directory on your client machine after you install QMX - Configuration Manager 2007.

You can run `snapshot.sh` on any version of QMX - Configuration Manager 2007 greater than 1.5.

For information about the `detach`, `disable_software_metering`, and `reenable_software_metering` scripts that are also in the `/scripts` directory refer to the *Software Metering* chapter in the *Administrator's Guide*.

Running the Snapshot Script

To execute the Snapshot script

1. At your client, change to the `/opt/quest/qmxcm/bin` directory.
2. From the command line, run:

   ```
   # ./snapshot.sh
   ```

If you run `snapshot.sh` with no parameters, it collects basic operating system and QMX - Configuration Manager 2007 data, changes the debug level to DEBUG3, restarts the client, deletes the log files, runs discovery and policy update, changes the log level back to DEBUG, and restarts the client. It also runs some other basic clienttool commands (such as `--show-schedules`) useful for troubleshooting.

3. If you run the script with an `-h` or `--help`, it displays the list of available options. For example:

   ```
   # ./snapshot.sh -h
   ```

   Note • You can run `snapshot.sh` with one or more options, separated by spaces.

SNAPSHOT SCRIPT OPTIONS

OPTIONS	**DESCRIPTION**
-h, --help	Lists a description of each `snapshot.sh` option.
--run-hardware-inventory	Runs hardware inventory and produces a log in DEBUG3 level.
--run-software-inventory	Runs software inventory and produces a log in DEBUG3 level.

OPTIONS	DESCRIPTION
--list-available-software	Prints a list of software available for installation.
--run-file-collection [arg]	Runs file collection on the specified collection and produces a log in DEBUG3 level. Use the "full" argument to collect files from all collections; use no argument to collect only the files that have changed.
--run-software-metering-usage-report	Generates the software metering usage report and produces a log in DEBUG3 level.
--run-software-distribution <Advertisement ID> <Package ID> <Program ID>	Runs software distribution for the specified Advertisement, Package, and Program, and produces a log in DEBUG3 level. To obtain the strings for this command's arguments, run the `--list-available-software` option.
--debug-class <arg>	Retrieves hardware inventory debug information for the specified class. To list debug information for all classes, specify "all".
--wql	Runs WQL queries against the local repository to assist with software metering issues.
--no-restart	Prevents the snapshot script from restarting the Agent. **Note**: When you run the snapshot script without this option, it restarts the Agent automatically and when it restarts the Agent, it deletes all log files and changes the log level to DEBUG3. So use the `--no-restart` option to preserve the log files and prevent the snapshot script from enabling DEBUG3.
--grab-current-logs	Saves the current log files before deleting them when it restarts the Agent. **Note**: If you run the snapshot script without this option, it deletes old log files and captures new log files in DEBUG3 level, the highest debug level possible.
--socket-dump	Generates a socket dump for the Agent, useful for examining data coming from the Management Point.
--no-discovery-update	Prevents Discovery and Policy Update from running.

By default `snapshot.sh` changes the configuration file so that the log files contain DEBUG3 information, then it restarts the Agent for this change to take effect.

Tips on Running the Snapshot Script

You can run `snapshot.sh` without any options to obtain useful troubleshooting information. Quest recommends that you run this script *before* opening a support case so that you can send them the output. Support may ask for additional options.

Here are some hints for using `snapshot.sh`:

1. `snapshot.sh` requires root access. It authenticates a user based on file system permissions and does not require a password. Anyone with an euid (effective user ID) of 0 (zero) may use the Snapshot script. If you use sudo or another similar tool, you can also run it.
2. Use the `--grab-current-logs` option to save the current logs files.

When you have a problem, always save the current logs *before* they have been deleted and refreshed.

3. If you are having problems with Advanced Hardware Inventory, run the `--run-hardware-inventory` option, it always retrieves the information from the `noidmofs` directory.
4. Support will ask you to send the `.tar.gz` file created in the `/tmp` directory by the `snapshot.sh` script; it contains basic data from your system as well as client data that they need to help troubleshoot your problems.

11

Getting Support

- Contacting Quest Support
- Join the Community

Contacting Quest Support

Quest Support is available to customers who have a trial version of a Quest product or who have purchased a commercial version and have a valid maintenance contract. Quest Support provides around the clock coverage with SupportLink, our web self-service.

SupportLink	www.quest.com/support
Email at	support@quest.com

From SupportLink, you can do the following:

- Quickly find thousands of solutions (Knowledgebase articles/documents)
- Access FAQs
- Download patches and upgrades
- Seek help from a Support engineer
- Update or view support requests

View the *Global Support Guide* for a detailed explanation of support programs, online services, contact information, and policy and procedures. The guide is available at http://support.quest.com/pdfs/Global Support Guide.pdf.

When you contact Support please include the following information:

1. The software you are working with.
2. The versions you have installed.
3. The Windows versions you have installed: 2000, XP, 2003 Server, 2003 Server R2.
4. The name of your Microsoft System Center Configuration Manager 2007 Contact.
5. How many non-Windows clients you have in your environment.
6. The port number that System Center Configuration Manager 2007 uses to handle requests and the port the QMX - Configuration Manager 2007 Agent uses for communications.
7. The following Log files:
    - C:\Program Files\Quest Software\QMX for ConfigMgr\push_install.log
    - /var/opt/quest/qmxcm/logs/qmxcmd.log
    - /var/opt/quest/qmxcm/owlogs/qmx_status.log
    - /var/opt/quest/qmxcm/owlogs/qmxlog.txt

- /var/opt/quest/qmxcm/owlogs/qmxlog.xml

8. The system information output from the client using an `uname -a` command.
9. Any information you feel is appropriate about your System Center Configuration Manager 2007 environment or test lab setup.

Join the Community

Get the latest product information, find helpful resources, and join a discussion with the QMX - Configuration Manager 2007 team and other community members at: http://vintela.inside.quest.com/category.jspa?categoryID=34

INDEX