

Provisioning the K1000 Agent

Agent provisioning is the task of installing the K1000 Agent on devices you want to add to K1000 inventory using the Agent.

About the K1000 Agent

The K1000 Agent is an application that can be installed on devices to enable inventory reporting and other device management features.

Agents that are installed on managed devices communicate with the K1000 appliance through AMP (Agent Messaging Protocol). Agents perform scheduled tasks, such as collecting inventory information from, and distributing software to, managed devices. Agentless management is available for devices that cannot have Agent software installed, such as printers and devices with operating systems that the Agent does not support. See [Using Agentless management](#).

Tracking changes to Agent settings

If History subscriptions are configured to retain information, you can view the details of the changes made to settings, assets, and objects.

This information includes the date the change was made and the user who made the change, which can be useful during troubleshooting. See [About history settings](#).

Methods for provisioning the K1000 Agent

You have a number of ways to deploy the K1000 Agent to the devices you want to manage.

- **Provision using the Agent Provisioning Assistant:** You can use the Agent Provisioning Assistant to perform provisioning for devices with Windows, Mac OS X, and Linux operating systems. Within the Assistant, you can choose between using the K1000 GPO Provisioning Tool for deploying the Agent to Windows devices, or using Onboard Provisioning for deploying the Agent to Windows, Mac OS X, or Linux devices.

The GPO Provisioning Tool is recommended for Windows devices because using the tool minimizes the pre-configuration that must happen on the target device. It requires an Active Directory environment. The onboard provisioning approach requires you to perform client-side configuration on the devices to be managed before you can start provisioning.

- **Provision using manual deployment:** Manual deployment is useful when automated Agent provisioning is not practical or when you want to deploy the K1000 Agent using email or logon scripts.

Related topics

[Provisioning the K1000 Agent using the GPO Provisioning Tool for Windows devices](#)

[Provisioning the K1000 Agent using onboard provisioning](#)

[Manually deploying the K1000 Agent](#)

Enabling file sharing

To provision Agent software, you must enable file sharing.

If the Organization component is enabled on your appliance, see [Enable file sharing at the System level](#). Otherwise, see [Enable file sharing without the Organization component enabled](#).

Enable file sharing at the System level

If the Organization component is enabled on your appliance, you must enable file sharing at the System level to provision the Agent.



NOTE: If the Organization component is not enabled on your appliance, follow the instructions in [Enable file sharing without the Organization component enabled](#).

1. Go to the *Security Settings* page:
 - a. Log in to the K1000 System Administration Console, http://K1000_hostname/system, or select **System** from the drop-down list in the top-right corner of the page.
 - b. On the left navigation bar, click **Settings**.
 - c. On the *Control Panel*, click **Security Settings**.
2. In the *Samba* section, specify the following settings:

Option	Description
For appliances with the Organization component enabled: Enable Organization File Shares	Use the appliance's client share to store files, such as files used to install applications on managed devices. The appliance's client share is a built-in Windows file server that the provisioning service can use to assist in distributing the Samba client on your network. Quest recommends that this file server only be enabled when you perform application installations on managed devices.
Require NTLMv2 authentication to appliance file shares	Enable NTLMv2 authentication for the K1000 files shares. When this setting is enabled, managed devices connecting to the K1000 File Shares require support for NTLMv2 and authenticate to the K1000 using NTLMv2. Even though NTLMv2 is more secure than NTLM and LANMAN, non-NTLMv2 configurations are more common and this option is usually turned off. Enabling this option disables lanman auth and ntlm auth on the Samba server. NTLMv2 Levels 1-4 are supported. If you need NTLM v2 Level 5, consider manually provisioning the K1000 Agent. See Manually deploying the K1000 Agent .
Require NTLMv2 to off-board file shares	Force certain K1000 functions that are supported through the Samba client, such as Agent Provisioning, to authenticate to offboard network file shares using NTLMv2. Even though NTLMv2 is more secure than NTLM and LANMAN, non-NTLMv2 configurations are more common and this option is usually disabled. Enabling this option enables the client ntlmv2 auth option for Samba client functions.

3. Click **Save**.
4. If prompted, restart the appliance.

When the appliance restarts, enable file sharing at the organization level. See [Enable organization-level file sharing with the Organization component enabled](#).

Enable organization-level file sharing with the Organization component enabled

If the Organization component is enabled on your appliance, you must enable file sharing at the organization level to provision the Agent.

Verify that organization file shares are enabled. For instructions, see [Enable file sharing at the System level](#).

1. Go to the Admin-level *General Settings* page:
 - a. Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
 - b. On the left navigation bar, click **Settings**.
 - c. On the *Control Panel*, click **General Settings**.
2. Select **Enable File Sharing** in the *Samba Share Settings* section.

If File Shares are disabled, you must enable them at the System level. See [Configure security settings for the appliance](#).

3. **Optional:** Enter a password for the File Share User.
4. Click **Save Samba Settings**.
5. If prompted, restart the appliance.
6. If you have multiple organizations, repeat the preceding steps for each organization.

Enable file sharing without the Organization component enabled

If the Organization component is not enabled on your appliance, you must enable file sharing in the appliance security settings to provision the Agent.

1. Go to the *Security Settings* page:
 - a. Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
 - b. On the left navigation bar, click **Settings**.
 - c. On the *Control Panel*, click **Security Settings**.
2. In the *Samba* section, select **Enable File Sharing**.
3. **Optional:** Select authentication options:

Option	Description
Require NTLMv2 to authenticate appliance file shares	Enable NTLMv2 authentication for the K1000 files shares. When this setting is enabled, managed devices connecting to the K1000 File Shares require support for NTLMv2 and authenticate to the K1000 using NTLMv2. Even though NTLMv2 is more secure than NTLM and LANMAN, non-NTLMv2 configurations are more common and this option is usually turned off. Enabling this option disables lanman auth and ntlm auth on the Samba server. NTLMv2 Levels 1-4 are supported. If you need NTLM v2 Level 5, consider manually provisioning the K1000 Agent. See Manually deploying the K1000 Agent .
Require NTLMv2 authentication to off-board file shares	Force certain K1000 functions that are supported through the Samba client, such as Agent Provisioning, to authenticate to offboard network file shares using NTLMv2. Even though NTLMv2 is more secure than NTLM and LANMAN, non-NTLMv2 configurations are more common and this option is usually disabled. Enabling this option enables the client ntlmv2 auth option for Samba client functions.

4. Click **Save**.
5. If prompted, restart the appliance.

Provisioning the K1000 Agent using the GPO Provisioning Tool for Windows devices

Of the methods for provisioning the Agent on Windows devices, Quest recommends the GPO Provisioning Tool because using the tool minimizes the pre-configuration that must happen on the target devices.

The GPO Provisioning Tool uses Active Directory® and Group Policy to distribute the installation settings and to perform the installation of the Agent. The tool creates a GPO, or modifies a pre-existing GPO to install the K1000 Agent when a device authenticates with Active Directory.

The first time a target device refreshes Group Policy after the tool has completed the creation or modification process, a new Group Policy client-side extension dll is registered on the devices applying this GPO. Then the next time that the device refreshes Group Policy, Windows triggers the newly registered client-side extension to install the K1000 Windows Agent.

For the Quest Knowledge Base article that contains the link to download the GPO Provisioning Tool, go to <https://support.quest.com/kb/133776>.

Prepare to use the GPO Provisioning Tool for Agent deployment

Before you can use the GPO Provisioning Tool to deploy Agents to Windows devices, you must ensure that your system is configured to use the tool.

The following system requirements are necessary for using the GPO Provisioning Tool:

- **Windows Vista and higher:** Remote Server Administration Tools (RSAT) enables IT administrators to remotely manage roles and features in Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 or Windows Server 2008 R2 from a computer that is running Windows 8.1, Windows 8, Windows 7, or Windows Vista.

Go to <http://social.technet.microsoft.com/wiki/contents/articles/2202.remote-server-administration-tools-rsat-for-windows-client-and-windows-server-dsforum2wiki.aspx>.

- **For Windows XP:** Install and enable the Group Policy Console for your Windows operating system.

Go to <http://microsoft.com/en-us/download/details.aspx?id=21895>.

- **.NET Framework 3.5.**
- **Windows Server 2008 or higher Active Directory Functional Level.**
- **Distribution Share:** Make sure to use a share that everyone can access. For example, do not place the .msi file on the NETLOGON share, because not every user can reach that share and the lack of access will cause your upgrade to fail in the future. This location should be a permanently accessible share. The installer is an MSI (Microsoft Installer) file. To uninstall or upgrade software, MSI needs access to the .msi file. If it is not accessible, `msiexec` will not uninstall.

Provision K1000 Agents using the K1000 GPO Provisioning Tool

You can install the K1000 Agent on a single device, or on multiple devices by using the K1000 GPO Provisioning Tool, starting within the Agent Provisioning Assistant. You can use this method to provision Windows devices.

- You have an Active Directory environment.
- You have appropriate access to set up software installations.
- You have met the system requirement spelled out in [Prepare to use the GPO Provisioning Tool for Agent deployment](#).

To complete this task, you leave the K1000 appliance to work in the Windows Group Policy Management Console or the Windows Administrative Tools using the K1000 GPO Provisioning Tool before returning to the appliance.

1. Go to the Agent Provisioning Assistant:
 - a. Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
 - b. On the left navigation bar, click **Settings**, then click **Provisioning**.
 - c. On the *Provisioning* panel, click **Agent Provisioning Assistant**.

The *Agent Provisioning Assistant: Step 1 of 3* page appears.


2. Select the check box for *Provisioning Using Windows Group Policy (recommended)*, and click **Next** to display the *Agent Provisioning Assistant: Step 2 of 3* page.
3. Click the link to the Knowledge Base article about using the K1000 GPO Provisioning Tool for Agent deployment at <https://support.quest.com/kb/133776>.

The Knowledge Base article provides a link to download the MSI for the GPO Provisioning Tool.

Installing and starting the tool requires leaving the K1000 interface.

4. Download the MSI, and start it to install the tool.
5. Start the installed tool from the **Start** menu.

The deployment wizard leads you through steps to configure and apply a GPO for software deployment. Where possible, the wizard attempts to use defaults that reduce the amount of configuration required.

 **NOTE:** Only GPOs for which you have permission to edit are displayed in the tool.

6. Return to the *Agent Provisioning: Step 2 of 3* page in the K1000 when you have completed working in the tool, and click **Next**.
7. Click **Finish** on the *Agent Provisioning: Step 3 of 3* page.

Agents are installed on the client devices after the Group Policy is refreshed on those devices. Depending on the environment, this installation takes place either when the device reboots, or after a 90-minute refresh cycle occurs for the Group Policy.

Go to the *Devices* page to keep track of the progress of devices having the agents installed and checked in.

Provisioning the K1000 Agent using onboard provisioning

You can install the K1000 Agent on multiple devices by specifying a range of IP addresses as targets for deployment (onboard provisioning). Windows, Mac OS X, and Linux devices can be targets for onboard provisioning.

After you have prepared each of your target client devices, you use the Agent Provisioning Assistant in the K1000 to identify the devices and set up a provisioning schedule.

Preparing to install the K1000 Agent

Before you install the K1000 Agent on devices using onboard provisioning, you must verify system requirements, enable file sharing, and prepare devices.

For information on file sharing, see [Enabling file sharing](#).

Verifying system requirements for the K1000 Agent installation

Before you install the K1000 Agent on devices, verify that the required ports are accessible, and that managed devices meet system requirements.

Managed devices must meet the following system requirements and be able to access the required ports:

- Go to <https://support.quest.com/technical-documents/kace-systems-management-appliance/7.2/technical-specifications-for-physical-appliances/>.
- See [Verifying port settings](#), [NTP service](#), and [website access](#).

Prepare Windows devices to have the Agent installed

Before you install the K1000 Agent on Windows devices, you must configure file sharing and User Account Control (UAC) properly.

- **Prepare a Windows Vista™, Windows 7, or Windows 8 device**

Provide Administrator credentials for each device. To install the K1000 Agent on multiple devices, the Administrator credentials must be the same for all devices.

To configure User Account Control (UAC), do one of the following:

- **Set User Account Control: Run all administrators in Admin Approval Mode to Disabled.** This option is recommended, because it is more secure and can be centrally configured using GPO. To find this setting, open the **Group Policy** (type secpol.msc into the *Search programs and files* field

under the **Start** menu), then go to **Local Policies > Security Options**. Restart the device after applying the settings.

- Disable UAC. On Windows Vista, go to **Control Panel > User Accounts > User Accounts > Turn User Account Control on or off**. On Windows 7, go to **Control Panel > System and Security > Action Center > Change User Account Control Settings**. On Windows 8, go to **Control Panel > System and Security > Administrative Tools > Local Security Policy**, then in *Security Options* in the *Local Policies* section choose **Disabled** for each of the items labeled *User Account Control*.

On the *Advanced Sharing Settings* page, enable network discovery and file and printer sharing.

- **Prepare a Windows XP device**

Turn off Simple File Sharing. For instructions, go to <http://support.microsoft.com/kb/304040> on the Microsoft Support website.

i **NOTE:** If Simple File Sharing is enabled, logon failures occur. This failure is because Simple File Sharing does not support administrative file shares and the associated access security required for provisioning. Therefore, Simple File Sharing must be turned off during Agent provisioning.

- **Prepare Windows Firewall**

If Windows Firewall is enabled, you must enable **File and Print Sharing** in the *Exceptions* list of the Firewall Configuration. For instructions, see the Microsoft Support website.

- **Verify port availability**

Verify the availability of ports 139 and 445.

The appliance verifies the availability of ports 139 and 445 on target devices before attempting to run any remote installation procedures.

i **NOTE:** On Windows devices, ports 139 and 445, File and Print Sharing, and Administrator credentials are required only during Agent installation. You can disable access to these ports and services after installation if necessary. The Agent uses port 52230 for ongoing communications.

NOTE: After installation, the Agent runs within the context of the Local System Account, which is a built-in account used by Windows operating systems.

Install the K1000 Agent on a device or multiple devices

You can install the K1000 Agent on a single device, or on multiple devices by specifying a range of IP addresses as targets for installation, using the Agent Provisioning Assistant. You can use this method to provision Windows, Mac, or Linux devices.

- You have prepared all the target devices. See [Preparing to install the K1000 Agent](#).
- You have information for the administrator account that has the necessary privileges to install Agents on the target devices.

With the Agent Provisioning Assistant, you can create provisioning schedules to specify how and when to install the K1000 Agent on devices in your network. Provisioning according to a schedule is useful to help ensure that devices in an IP address range have the Agent installed.

Provisioning schedules configure the K1000 appliance to periodically check devices in a specified IP address range and install, reinstall, or uninstall the K1000 Agent as needed.

For provisioning Windows devices, you can also use the K1000 GPO Provisioning Tool. Using the tool minimizes the pre-configuration that must happen on the target device. See [Provisioning the K1000 Agent using the GPO Provisioning Tool for Windows devices](#).

1. Go to the Agent Provisioning Assistant:
 - a. Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
 - b. On the left navigation bar, click **Settings**, then click **Provisioning**.

- c. On the *Provisioning* panel, click **Agent Provisioning Assistant**.

The *Agent Provisioning Assistant: Step 1 of 3* page appears.

2. Select *Provisioning Using IP Range (Windows, Mac, Linux)* and click **Next** to display the *Provisioning Schedule Detail* page.
3. In the *Configure* section, name the schedule, enable provisioning, and provide platform information:

Option	Description
Name	A unique name that identifies this configuration. The name appears on the <i>Provisioning Schedules</i> page.
Enabled	Enable provisioning schedules. Schedules run only if this check box is selected.
Install/Uninstall	Indicates whether the provisioning schedule deals with installing or uninstalling Agents.
Credentials	Separate rows for the credentials needed to connect to the device and run commands for the particular platform targeted by the schedule. The first column contains the operating system. The second column contains the Agent Version in place for installation. The third column contains a drop-down list from which to select existing credentials. You can select Add new credential to add credentials not already listed. See Add and edit User/Password credentials .

4. In the *Deploy* section, identify the devices to be included in the schedule:

Option	Description
Target IP addresses or Hostnames	A comma-separated list of the IP addresses or hostnames of the target devices. The Help me pick devices link enables you to add devices to the <i>Target IP addresses or Hostnames</i> list: <ul style="list-style-type: none"> • Provisioning IP Range: Use hyphens to specify individual IP address class ranges. For example: 192 168 2-5 1-200. After specifying a range, click Add All. • Select Devices from Discovery: This drop-down list is populated from the Discovery Results. To filter the contents, start typing in the field. After selecting a device, click Add All.

5. Set the time for the schedule to run.

Option	Description
None	Run in combination with an event rather than on a specific date or at a specific time.
Every n minutes/ hours	Run at a specified interval.
Every day/specific day at HH:MM	Run daily at a specified time, or run on a designated day of the week at a specified time.
On the nth of every month/	Run on the same day every month, or a specific month, at the specified time.

Option	Description
specific month at HH:MM	

6. **Optional:** Use *Advanced* settings to:
 - Customize the ports the appliance uses to deploy the Agent.
 - Designate an alternative download location for the Agent installer.
 - Enable a complete uninstall of the Agent. Selecting *Remove KUID during uninstall* results in an existing Agent being removed from the device before the Agent is installed again. In this case, the K1000 generates a new KUID for the asset, and it appears as a new device in the K1000.
7. Click **Run now** to display the *Provisioning Schedules* page and the new configuration.

The appliance saves the configuration with the name you supplied, and then runs the configuration against the targeted IP addresses.

The *Provisioning Schedules* page displays the progress of the successful installations after the schedule's start time.

Related topics

- [Power-on the appliance and log in to the Administrator Console](#)
- [Provisioning the K1000 Agent using the GPO Provisioning Tool for Windows devices](#)
- [Manually deploying the K1000 Agent](#)

Managing provisioning schedules

To streamline the Agent installation process, you can add provisioning schedules that specify how and when to install the K1000 Agent on devices. You can add, view, edit, run, duplicate, and delete provisioning schedules.

View, run, edit, or duplicate provisioning schedules

You can view provisioning schedule status and other details on the *Provisioning Schedules* page. From this page you can also run and edit provisioning schedules as needed.

When you duplicate provisioning schedule, its properties are copied into the new configuration. If you are creating a configuration that is similar to an existing configuration, starting with a duplicated schedule can be faster than creating a configuration from scratch.

1. Go to the *Provisioning Schedules* list:
 - a. Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
 - b. On the left navigation bar, click **Settings**, then click **Provisioning**.
 - c. On the *Provisioning Panel*, click **Schedules**.

The list displays the following columns:

Option	Description
Name	The name of the provisioning schedule (links to the <i>Provisioning Schedule Detail page</i>).
Targeted	The total number of target devices in the configuration (links to the <i>Provisioning Results</i> page).

Option	Description
Running	The total number of target devices on which provisioning is running (links to the <i>Provisioning Results</i> page).
Pending	The total number of target devices on which provisioning has not yet started (links to the <i>Provisioning Results</i> page).
Succeeded	The total number of target devices on which provisioning has succeeded (links to the <i>Provisioning Results</i> page).
Failed	The total number of target devices on which provisioning has failed (links to the <i>Provisioning Results</i> page).
Success Rate	The total number of target devices on which provisioning has succeeded as a percentage.
IP Range	The IP address range of the target device.
Schedule	The specified provisioning schedule. For example: Everyn minutes, Every n hours, or Never.
Enabled	Whether the configuration is enabled or disabled. A check mark indicates that the provisioning schedule is enabled.

2. Run provisioning schedules:
 - a. Select the check boxes for the schedules that you want to run.
 - b. Select **Choose Action > Run Now**.
3. Edit schedules:
 - a. Click the name of a schedule.
 - b. Edit the provisioning schedule on the schedule's *Provisioning Schedule Detail* page, and click **Save**.

See [Install the K1000 Agent on a device or multiple devices](#).
4. Duplicate schedules:
 - a. Click the name of a schedule.
 - b. In the *Advanced* section, click **Duplicate** to display the *Provisioning Schedules* page with the new schedule listed as **Copy of** Schedule Name.

Delete provisioning schedules

You can delete provisioning schedules when you want to remove schedules from the appliance.

When provisioning schedules are deleted, results associated with those schedules are also deleted. Devices provisioned using the schedules, however, are not removed from inventory.




1. Go to the *Provisioning Schedules* list:
 - a. Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
 - b. On the left navigation bar, click **Settings**, then click **Provisioning**.
 - c. On the *Provisioning Panel*, click **Schedules**.
2. Select the check box next to one or more schedules.
3. Select **Choose Action > Delete**, then click **Yes** to confirm.

View provisioning results

You can view the results of actions performed by provisioning schedules.

1. Go to the *Provisioning Schedules* list:
 - a. Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
 - b. On the left navigation bar, click **Settings**, then click **Provisioning**.
 - c. On the *Provisioning Panel*, click **Schedules**.
2. Click a link in the *Running*, *Pending*, *Succeeded*, or *Failed* column.

The *Provisioning Results* page appears with the following information:


Item	Description
Status	The status of the Agent connection to the appliance:  : An Agent-managed device is connected to the appliance.  : An Agent-managed device is not connected to the appliance.
Schedule Name	The name of the provisioning schedule.
IP Address	The IP address of the target device.
Hostname	The hostname of the target device. Click the Remote Connection button to open a Remote Desktop Connection to the target device (Internet Explorer only): 
Result	The status of the most recent provisioning attempt.
Action	I indicates a successful installation. U indicates a successful uninstallation.
Error	The failure error, such as TCP ports not accessible.
Last Run	The last time the schedule ran.

3. To view additional information about a target device, click its **IP Address**.

The *K1000 Agent Provisioning* page appears.

This page displays the results of the most recent provisioning run and includes information such as the IP address, port configuration, and the logs of each provisioning step.

4. To view inventory information, click the **[computer inventory]** link next to the **MAC address**.

 **NOTE:** The **[computer inventory]** link appears only if the provisioning process can match the MAC address of the target device with the current inventory data. See [Managing MIA devices](#).

Managing Agent communications

Communications between the appliance and Agents installed on managed devices include inventory reports, alerts, patches, scripts, and crash logs. You can configure and view communications that are queued, or pending.

Configure Agent communication and log settings

Agents installed on managed devices periodically check in to the K1000 to report inventory, update scripts, and perform other tasks.

You can configure the Agent settings, including the interval at which the Agents check in, messages displayed to users, and log retention time, as described in this section. If you have multiple organizations, you configure Agent settings for each organization separately.

1. Do one of the following:
 - If the Organization component is enabled on your appliance, log in to the K1000 System Administration Console, http://K1000_hostname/system, or select **System** in the drop-down list in the top-right corner of the page next to the login information. Then click **Organizations**. To display the organization's information, click the organization's name.
The *Organization Detail* page appears.
 - If the Organization component is not enabled on your appliance, select **Settings > Provisioning**. Then click **Communication Settings** on the *Provisioning* panel.
The *Communication Settings* page appears.

2. In the *Communications Settings* section, specify the following settings:

To reduce the load on the K1000 appliance, limit the number of Agent connections to 500 per hour. The number of connections that appears next to the inventory, scripting, and metering intervals, applies to the current organization only. If the Organization component is enabled on your appliance, the total number of Agent connections for all organizations should not exceed 500 per hour.

Option	Suggested Setting	Notes
Agent Logging	Enabled	Whether the K1000 appliance stores scripting results provided by Agents installed on managed devices. Agent logs can consume as much as 1GB of disk space in the database. If disk space is not an issue, enable <i>Agent Logging</i> to keep all log information for Agent-managed devices. These logs can be useful during troubleshooting. To save disk space, and enable faster Agent communication, disable <i>Agent Logging</i> .
Agent Debug Trace	Enabled	If selected, this option allows you to record the Agent's debug trace. This information allows administrators to monitor the Agent's performance, and to diagnose common problems.
Agent Inventory	12 hours	The frequency at which Agents on managed devices report inventory. This information is displayed in the <i>Inventory</i> section.
Agentless Inventory	1 day	The frequency at which Agentless devices report inventory. This information is displayed in the <i>Inventory</i> section.
Catalog Inventory	1 day	The frequency at which managed devices report inventory to the <i>Software Catalog</i> page.
Metering	4 hours	The frequency at which managed devices report metering information to the K1000 appliance. Requires metering to be enabled on devices and applications.
Scripting Update	4 hours	The frequency at which Agents on managed devices request updated copies of scripts that are enabled on managed devices. This interval does not affect how often scripts run.

Option	Suggested Setting	Notes
Max Download Speed	As required	The maximum download speed, as required. Choose from the available options.
Disable Wait for Bootup Tasks	Disabled	If selected, this option stops the Agent from executing boot-up tasks.
Disable Wait for Login Tasks	Disabled	If selected, this option stops the agent from executing login tasks.

3. In the *Notify* section, specify the message to use for Agent communications:

Option	Suggested Setting	Notes
Agent Splash Page Message	Default text: KACE Systems Management Appliance (K1000) is verifying your PC Configuration and managing software updates. Please Wait...	The message that appears to users when Agents are performing tasks, such as running scripts, on their devices.
Agent Splash Bitmap	As required	The path to an existing .bmp file that you want to use as the splash logo.
Disable Bootup Splash	Disabled	If selected, this option stops the agent from displaying the boot-up splash logo.
Disable Login Splash	Disabled	If selected, this option stops the agent from displaying the login splash logo.

4. In the *Schedule* section, specify the *Communication Window*:

Option	Suggested Setting	Notes
Communication Window	00:00 to 00:00 (+1 day)	The period during which Agents on managed devices are allowed to connect with the K1000 appliance. For example, to allow Agents to connect between the hours of 01:00 and 06:00 only, select 01:00 from the first drop-down list, and 06:00 from the second drop-down list. You can set the communications window to avoid times when your devices are busiest.

5. In the *Agentless Settings* section, specify communications settings for Agentless devices:

Option	Description
SNMP Timeout	The time, in seconds or minutes, after which the connection is closed if there is no activity.
SSH/Telnet Timeout	The time, in seconds, after which the connection is closed if there is no activity.
WinRM Timeout	The time, in seconds or minutes, after which the connection is closed if there is no activity.

Option	Description
Maximum Attempts	The number of times the connection is attempted.

- If the Organization component is not enabled on your appliance, specify *Agent* settings.

i **NOTE:** If the Organization component is enabled on your appliance, these *Agent* settings are located on the appliance K1000 System Administration Console *General Settings* page.

Option	Description
Last Task Throughput Update	This value indicates the date and time when the appliance task throughput was last updated.

Current Load Average	The value in this field depicts the load on an appliance at any given time. For the appliance to run normally, the value in this field must be between 0.0 and 10.0.
-----------------------------	--

Task Throughput	The value that controls how scheduled tasks, such as inventory collection, scripting, and patching updates, are balanced by the appliance.
------------------------	--

i **NOTE:** This value can be increased only if the value in the Current Load Average is not more than 10.0 and the Last Task Throughput Update time is more than 15 minutes.

- Click **Save**.

The changes take effect when Agents check in to the appliance.

- If you have multiple organizations, repeat the preceding steps for each organization.

Related topics

[View appliance logs](#)

[Configure appliance General Settings with the Organization component enabled](#)

View Agent task status

You can view the status of tasks that are currently running, or that are scheduled to run, on Agent-managed devices.

- Go to the appliance *Control Panel*:
 - If the Organization component is not enabled on the appliance, log in to the K1000 Administrator Console, `http://K1000_hostname/admin`, then click **Settings**.
 - If the Organization component is enabled on the appliance, log in to the K1000 System Administration Console, `http://K1000_hostname/system`, or select **System** in the drop-down list in the top-right corner of the page, then click **Settings**.
- On the left navigation bar, click **Support** to display the *Support* page.
- In the *Troubleshooting Tools* section, click **Display Agent task status** to display the *Agent Tasks* page.

By default, *In Progress* tasks are listed. To view other tasks, select different filtering options in the *View By* drop-down list, which appears above the list on the right. Task information includes:

Column	Description
Device Name	The name of the device that is the target of the task.
Type	The type of task. Depending on appliance configuration, task types include alerts, inventory, kbot, crash upload, and scripting updates.

Column	Description
Started	The start time of the task.
Completed	The completion time of the task.
Next Run	The next scheduled run time for the task.
Run Time	How long it took to run the task.
Timeout	The time limit for completing the task.
Priority	The importance or rank of the task.

The options displayed depend on type of tasks available on your appliance. Typical options include:

- **Ready to Run (connected):** Tasks that are connected through the messaging protocol and about to run.
 - **Ready to Run:** Tasks that are queued to run when an messaging protocol connection is established.
 - **Longer than 10 minutes:** Tasks that have been waiting longer than 10 minutes for a protocol connection.
4. To view details about a device, click its name in the *Device Name* column.
The *Device Detail* page appears.

View the Agent Command Queue

The Agent Command Queue list shows messages, such as pop-ups and alerts, that have been queued for distribution from the appliance to Agent-managed devices.

1. Go to the appliance *Control Panel*:
 - If the Organization component is not enabled on the appliance, log in to the K1000 Administrator Console, `http://K1000_hostname/admin`, then click **Settings**.
 - If the Organization component is enabled on the appliance, log in to the K1000 System Administration Console, `http://K1000_hostname/system`, or select **System** in the drop-down list in the top-right corner of the page, then click **Settings**.
2. On the left navigation bar, click **Support** to display the *Support* page.
3. In the *Troubleshooting Tools* section, click **View Agent command queue** to display the *Agent Command Queue* page.

Pending messages appear in this queue only during continuous connection between the Agent and the appliance.

i **NOTE:** Pending alerts appear on the *Agent Command Queue* page even if there is no connection between the Agent and the K1000.

The *Agent Command Queue* page contains the following fields:

Option	Description
Device Name	The name of the device. Click a name to view device details.
Type [Plug-in, Source]	The type of message, such as <i>Run Process</i> .

Option	Description
Command	The content and information contained in the message.
Expiration	The date and time when the message expires, also called <i>Keep Alive</i> time. Messages are deleted from the queue automatically when they expire.
Status	The status of the message, such as <i>Completed</i> or <i>Received</i> .

Related topics

[Broadcasting alerts to managed devices](#)

Delete messages from the Agent command queue

You can delete messages that are no longer needed from the Agent command queue.

1. Go to the appliance *Control Panel*:
 - If the Organization component is not enabled on the appliance, log in to the K1000 Administrator Console, http://K1000_hostname/admin, then click **Settings**.
 - If the Organization component is enabled on the appliance, log in to the K1000 System Administration Console, http://K1000_hostname/system, or select **System** in the drop-down list in the top-right corner of the page, then click **Settings**.
2. On the left navigation bar, click **Support** to display the *Support* page.
3. In the *Troubleshooting Tools* section, click **View Agent command queue** to display the *Agent Command Queue* page.
4. Select the check box next to one or more messages.
5. Select **Choose Action > Delete**, then click **Yes** to confirm.

Updating the K1000 Agent on managed devices

The K1000 appliance automatically checks with Quest for K1000 Agent updates at approximately 03:40 every day. In addition, the appliance checks Quest for Agent updates whenever the appliance is rebooted.

When Agent updates are available, they are automatically downloaded to the K1000 appliance, provided that the appliance is connected to the Internet, and an alert appears on the *Home* page of the K1000 Administrator Console. Until you configure deployment settings, however, Agent updates are not automatically deployed to managed devices. Click the link in the alert to configure deployment settings.

In addition, you can check for Agent software updates, obtain Agent updates manually, and configure Agent update settings any time. Obtaining updates manually is useful if your appliance is not connected to the Internet.

View K1000 Agent updates

You can view K1000 Agent updates in the Administrator Console.

1. Go to the appliance *Control Panel*:
 - If the Organization component is not enabled on the appliance, log in to the K1000 Administrator Console, http://K1000_hostname/admin, then click **Settings**.
 - If the Organization component is enabled on the appliance, log in to the K1000 System Administration Console, http://K1000_hostname/system, or select **System** in the drop-down list in the top-right corner of the page, then click **Settings**.
2. On the left navigation bar, click **Appliance Updates**.
The *Appliance Updates* page appears. The current Agent bundle appears in the *Agent* section.
3. **Optional:** To check for updates: In the *Agent* section, click **Check for Update**.

The appliance checks for updates, and the results appear on the *Logs* page.

Configure Agent update settings

After Agents are installed on devices, they are designed to update themselves automatically based on the Agent update settings you choose on the *Update Agent Settings* page. This is true regardless of the provisioning methods used to deploy the Agents, including K1000 provisioning, GPO wizard, other GPO deployments, or image deployment.

If you have multiple organizations, you configure Agent update settings for each organization separately.

1. Go to the *Update Agent Settings* page:
 - a. Log in to the K1000 Administrator Console, http://K1000_hostname/admin. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
 - b. On the left navigation bar, click **Settings**, then click **Provisioning**.
 - c. On the *Provisioning Panel*, click **Update Agents**.

If a new Agent update is available, it appears in the *Available Agent Bundle* section.

2. Click **Apply** in the *Available Agent Bundle* section.

The new Agent version number appears in the *Advertised Updates* section, and the *Enabled* check box in the *Agent Settings* section is cleared, disabling automatic updates. This enables you to test the updates on selected devices before deploying them system-wide.

3. View or specify the following Agent update settings:

Option	Description
Enabled	Deploy the update to the selected K1000 devices during the next scheduled inventory interval. Clear the check box to prevent updates from being installed.
Modified	Read-only: The time the most recent Agent bundle was downloaded.
All Devices	Deploy the update to all devices that have the K1000 Agent installed. If this option is selected, the <i>Devices</i> and <i>Labels</i> elements do not appear on the page.
Devices	Update only specific devices. Select the device names in the drop-down list that appears when you click in the field, or type the first few characters of a device name to sort the list. For example, type Dev to list matching device names such as Device-1, Device-2, and so on. This option is not available when you select All Devices .
Manage Associated Labels	Display the <i>Edit Labels</i> dialog. Search for and select labels, and update devices assigned to the selected labels. This option is not available when you select All Devices .
Notes	Any additional information you want to provide.

4. Click **Save**.

The update is deployed to the selected devices during the next scheduled inventory interval. If you use Replication Shares, and failover to the K1000 is not selected, Agents are updated after the Replication Shares are updated.

5. If you limited deployment to specified devices for testing, select additional devices in the *Agent Settings* section of the *Update Agent Settings* page when your testing is complete.

The update is deployed to the selected devices during the next scheduled inventory interval.

6. If you have multiple organizations, repeat the preceding steps for each organization.

Related topics

[Setting up and using labels to manage groups of items](#)

Upload Agent updates manually

In most cases, Agent updates are automatically downloaded to the K1000 appliance when they become available. However, you can download updates from Quest and manually upload Agent updates to the appliance as needed. This is useful if your appliance is not connected to the Internet, or if Agent updates are available but have not yet been downloaded to the appliance automatically.

To download Agent updates from Quest, you must obtain customer login credentials by contacting Quest Support at <https://support.quest.com/contact-support>.

1. To manually check for updates, go to the appliance *Control Panel*:
 - If the Organization component is not enabled on the appliance, log in to the K1000 Administrator Console, `http://K1000_hostname/admin`, then click **Settings**.
 - If the Organization component is enabled on the appliance, log in to the K1000 System Administration Console, `http://K1000_hostname/system`, or select **System** in the drop-down list in the top-right corner of the page, then click **Settings**.
2. On the left navigation bar, click **Appliance Updates** to display the *Appliance Updates* page.

The version of the current Agent bundle appears in the *Agent* section.
3. Click **Check for Update** in the *Agent* section.

The appliance checks for updates, and the results appear on the *Logs* page.
4. To obtain updates:
 - a. Log in to the Quest Support site using your customer login credentials:
<https://support.quest.com/kace-systems-management-appliance/download-new-releases>.
 - b. Download the Agent update bundle and save the file locally.
5. Go to the *Update Agent Settings* page:
 - a. Log in to the K1000 Administrator Console, `http://K1000_hostname/admin`. Or, if the *Show organization menu in admin header* option is enabled in the appliance General Settings, select an organization in the drop-down list in the top-right corner of the page next to the login information.
 - b. On the left navigation bar, click **Settings**, then click **Provisioning**.
 - c. On the *Provisioning Panel*, click **Update Agents**.
6. Do one of the following:
 - If a new update appears in the *Available Agent Bundle* section, click **Apply**.
 - If you manually downloaded an update, go to the *Manually Upload Agent Bundle* section, click **Browse** or **Choose File**, locate the file that you downloaded, then click **Upload**.

The new Agent version number appears in the *Advertised Updates* section, and the *Enabled* check box in the *Agent Settings* section is cleared, disabling automatic updates. This enables you to test the updates on selected devices before deploying them system-wide.

7. Specify deployment options in the *Agent Settings* section. See [Configure Agent update settings](#).
8. If you have multiple organizations, repeat 6 and 7 for each organization.

Manually deploying the K1000 Agent

Manual deployment is useful when automated Agent provisioning is not practical or when you want to deploy the K1000 Agent using email, logon scripts, GPO (Group Policy Objects), or Active Directory.

- **Email:** To deploy K1000 Agents through email, you would send an email to your users that contains one of the following:
 - The Agent installation file.
 - A link to the appliance where the Agent file can be downloaded.
 - A web location where the required installation file can be downloaded.
- **Logon scripts:** Logon scripts enable you to deploy the K1000 Agent when users log on to a device. If you use logon scripts, you would upload the appropriate file in an accessible directory and create a logon script to retrieve it.

Obtaining Agent installation files

Agent installation files are available on the appliance.

You can find the K1000 Agent installers for Windows, Mac OS X, and Linux devices on the K1000 appliance in the following directory:

```
\\k1000_hostname\client\agent_provisioning
```



NOTE: File sharing must be enabled to access the installers. See [Enable file sharing at the System level](#).

Manually deploying the K1000 Agent on Windows devices

You can manually deploy the K1000 Agent on Windows devices using the installation wizard or from the command line on devices.

When you install the Agent manually, the Agent executable files must be installed in the following locations:

- Windows 32-bit devices: `C:\Program Files\Dell\KACE\`
- Window 64-bit devices: `C:\Program Files (x86)\Dell\KACE\`

The Agent configuration files, logs, and other data are stored in:

- Windows 32-bit devices: `C:\Documents and Settings\All Users\Dell\KACE`
- Window 64-bit devices: `C:\ProgramData\Dell\KACE`

Manually deploy the K1000 Agent on Windows devices using the installation wizard

You can manually deploy the K1000 Agent on Windows devices by running the installation wizard on devices.

1. Go to the shared directory of the appliance:

```
\\k1000_hostname\client\agent_provisioning\windows_platform
```

2. Copy the `ampagent-6.x.xxxxx-x86.msi` file to the device.
3. Double-click the file to start the installation and follow the instructions in the installation wizard.

The device information appears in the appliance Inventory within a few minutes. See [Managing applications on the Software page](#).

Manually deploy the K1000 Agent on Windows devices using the Command line

There are several ways to deploy the Agent from the command line on Windows devices.

For example:

- In a batch file as part of a logon script that runs the installer (`msiexec`) and sets various parameters, such as the value of the host.
- Set an environment variable for the server name then run the installer.
- Change name of the installer, which automatically sets the server name during the installation.

The following table shows command line parameters used to deploy the Agent.

Table 20. Command line parameters for the Agent

Description	Parameter
Windows Installer Tool	<code>msiexec</code> or <code>msiexec.exe</code>
Install flag	<code>/i</code> Example: <code>msiexec /i ampagent-6.x.xxxxx-x86</code>
Uninstall flag	<code>/x</code> Example: <code>msiexec /x ampagent-6.x.xxxxx-x86</code>
Silent install	<code>/qn</code> Example: <code>msiexec /qn /i ampagent-6.x.xxxxx-x86</code>
Log verbose output	<code>/L*v log.txt</code> Example: <code>msiexec /qn /L*v C:\temp\log.txt /i ampagent-6.x.xxxxx-x86</code>
Auto set hostname: Rename the installation file to the name of the server name, which automatically sets the hostname	<code>rename agent_installer.msi_hostname.msi</code> Example: <code>msiexec /qn /i ampagent-6.x.xxxxx-x86_k1000.example.com.msi</code>
Set properties	<code>PROPERTY=value (Must use ALL CAPS)</code> Example: <code>msiexec /qn /i ampagent-6.x.xxxxx-x86.msi HOST=k1000.example.com</code>
Set server name	<code>set KACE_SERVER=k1000name</code> Must be followed by an <code>msiexec</code> call to install Example: <code>set KACE_SERVER=kboxmsiexec /i ampagent-6.x.xxxxx-x86</code>

Description	Parameter
Prevent the installation of logon or bootup hooks, and preserve existing userinit.exe files	NOHOOKS=1 Example: <pre>msiexec /qn /i ampagent-6.x.xxxxx-x86.msi HOST=k1000.example.com NOHOOKS=1</pre>
Install the Agent but do not start the service. This enables the Agent to be imaged and cloned to other devices	CLONEPREP=yes/no Example: <pre>msiexec /qn /i ampagent-6.x.xxxxx-x86.msi HOST=k1000.example.com CLONEPREP=yes</pre>
Set the debug level for the Agent when it generates logs	DEBUG=true/all Example: <pre>msiexec /qn /i ampagent-6.x.xxxxx-x86.msi HOST=k1000.example.com DEBUG=true</pre>
Force the Agent to communicate through HTTPS only. It cannot fall back to HTTP if HTTPS is unavailable	SSLREQUIRED=true Example: <pre>msiexec /qn /i ampagent-6.x.xxxxx-x86.msi HOST=k1000.example.com SSLREQUIRED=true</pre>

The system looks for the value of host in these locations in the order shown:

1. The installer file
2. The `HOST` property value
3. `KACE_SERVER` (environment variable)
4. The `amp.conf` file

CAUTION: If you leave the host value empty, you must set the environment variable. Otherwise, the Agent will not connect to the appliance. Quest recommends that you use the fully qualified domain name as the hostname.

Manually deploying and upgrading the K1000 Agent on Linux devices

You can manually deploy or upgrade the K1000 Agent on Linux devices as needed.

Manually deploy the K1000 Agent on Linux devices

You can manually deploy the K1000 Agent on Linux devices by copying the Agent installation files to the devices and running installation commands.

1. Copy the K1000 Agent installation file to the device.

See [Obtaining Agent installation files](#).

2. Open a terminal window from **Applications > System Tools**.
3. At the command prompt, set the name of the server and install the Agent:

```
sudo KACE_SERVER=k1000name rpm -Uvh ampagent-6.x.xxxxx-x.i386.rpm
```

The Agent is installed in the following directories:

- `/opt/dell/kace/bin/` where the Agent executable files are installed.
- `/var/dell/kace/` where the Agent configuration, logs, and other data is stored.

The device information appears in the appliance Inventory within a few minutes. See [Managing applications on the Software page](#).

Deploy the K1000 Agent on Linux devices at startup or login

You can schedule the Agent to be deployed when users start or log in to Linux devices.

- Set the name by adding the following command to the root directory:

```
export KACE_SERVER=k1000name
```

The `export` call must precede the call to the installer. For example: `export KACE_SERVER=k1000name rpm -Uvh k1000agent-12345.i386.rpm`

The system looks for the value of `host` in these locations in the order shown:

1. The installer file
2. `KACE_SERVER` (environment variable)
3. The `amp.conf` file

• **CAUTION:** If you leave the `host` value empty, you must set the environment variable. Otherwise, the Agent does not connect to the appliance. Quest recommends that you use the fully qualified domain name as the hostname.

Upgrade the K1000 Agent on Linux devices

You can manually upgrade the K1000 Agent on Linux devices by running commands on the devices.

1. Copy the K1000 Agent installation file to the device. See [Obtaining Agent installation files](#).
2. Open a terminal window from **Applications > System Tools**.
3. At the command prompt, enter:

```
rpm -uvh k1000agent-linux_buildnumber.rpm
```

Performing Agent operations on Linux devices

You can run commands on Agent-managed Linux devices to perform various Agent operations.

Start and stop the Agent on Linux devices

You can run commands on Linux devices to start and stop the Agent. This procedure is useful in troubleshooting Agent-related issues.

1. Open a terminal window from **Applications > System Tools**.
2. To start the Agent, enter:

```
/opt/dell/kace/bin/AMPTools start
```

3. To stop the Agent, enter:

```
/opt/dell/kace/bin/AMPTools stop
```

Manually remove the Agent from Linux devices

You can remove the Agent from Linux devices manually by running commands on the devices.

1. Open a terminal window from **Applications > System Tools**.
2. At the command prompt, enter:

```
sudo rpm -e ampagent
```

3. **Optional:** Remove the `kace` directory:

```
rm -rf /var/dell/kace/
```

Verify that the Agent is running on Linux devices

You can run a command on Linux devices to determine whether the Agent is running.

1. Open a terminal window from **Applications > System Tools**.
2. At the command line prompt, enter:

```
ps aux | grep AMPAgent
```

This output indicates that the process is running:

```
root 6100 0.0 3.9 3110640 20384 ? Ssl Mar03 0:00 /opt/dell/kace/bin/AMPAgent --  
daemon
```

View the Agent version on Linux devices

You can run a command on Linux devices to verify the version of the Agent installed on those devices.

1. Open a terminal window from **Applications > System Tools**.
2. At the command line prompt, enter:

```
rpm -q ampagent
```

The version number is displayed.

Collecting inventory information

You can manually collect inventory on Linux devices by forcing inventory updates.

See [Forcing inventory updates](#).

Manually deploying and upgrading the K1000 Agent on Mac devices

You can manually deploy or upgrade the Agent on Mac devices as needed.

This section provides information for manually deploying the K1000 Agent on Mac OS X devices. Additional options are described in [Use shell scripts to deploy the K1000 Agent](#).



NOTE: Some commands must be run as **root**.

NOTE: Proceed with `su` or `sudo` as required.

Deploy or upgrade the K1000 Agent to Mac devices using the Agent installer

You can manually deploy the K1000 Agent on Mac devices by copying the Agent installation files to the devices and running the installer.

1. Copy the K1000 Agent installation file to the device.
See [Obtaining Agent installation files](#).
2. Double-click **ampagent-6.x.build_number.dmg**.
3. Double-click **AMPAgent.pkg**.
4. Follow the instructions in the installer.

Be sure to enter the name of your K1000 appliance.

The installer creates the following directories on your device:

- `/Library/Application Support/Dell/KACE/bin` where the Agent executable files are installed.
- `/Library/Application Support/Dell/KACE/data/` where the Agent configuration, logs, and other data is stored.

Deploy the Agent to Mac devices using the terminal window

You can manually deploy the K1000 Agent on Mac devices by copying the Agent installation files to the devices and running commands.

1. Copy the K1000 Agent installation file to the device.
See [Obtaining Agent installation files](#).
2. Open a terminal window from **Applications > Utilities**.
3. At the command prompt, enter the following commands to set the name of the server and install the Agent:

```
hdiutil attach ./ampagent-6.x.xxxxx-all.dmg

sudo sh -c 'KACE_SERVER=k1000name installer -pkg /Volumes/Dell_KACE/
AMPAgent.pkg -target /'

hdiutil detach '/Volumes/Dell_KACE'
```

Use shell scripts to deploy the K1000 Agent

You can run shell scripts to deploy the Agent to Mac devices.

When using shell scripts to deploy the Agent, you can use the following command line options:

- `hdiutil attach ./ampagent-6.x.xxxxx-all.dmg`
- `sudo sh -c 'KACE_SERVER=k1000name installer -pkg`
- `/Volumes/Dell_KACE/AMPAgent.pkg -target /'`
- `hdiutil detach '/Volumes/Dell_KACE'`

i **NOTE:** The `export` call must precede the `install` call. For example: `sudo export KACE_SERVER=k1000name installer -pkg '/Volumes/Dell_KACE/AMPAgent.pkg' -target /`

The system looks for the value of `host` in these locations in the following order shown:

1. The installer file
2. `KACE_SERVER` (environment variable)
3. The `amp.conf` file

For information about using shell scripts and command lines, go to <http://developer.apple.com>.

! **CAUTION:** If you leave the `host` value empty, you must set the environment variable. Otherwise, the Agent will not connect to the appliance. Quest KACE recommends that you use the fully qualified domain name as the hostname.

Performing other Agent operations on Mac devices

You can run commands on Agent-managed Mac devices to perform various operations.

Start or stop the Agent on Mac devices

You can run commands on Mac devices to start and stop the Agent. This procedure is useful in troubleshooting Agent-related issues.

1. Open a terminal window from **Applications > Utilities**.
2. Type the following:

```
cd "/Library/Application Support/Dell/KACE/bin"
```

3. To start the Agent, enter:

```
./AMPTools start
```

4. To stop the Agent, enter:

```
./AMPTools stop
```

Manually remove the Agent from Mac devices

You can remove the Agent from Mac devices manually by running commands on the devices.

1. Open a terminal window from **Applications > Utilities**.
2. Type the following:

```
sudo "/Library/Application Support/Dell/KACE/bin/AMPTools" uninstall
```

The Agent is removed.

Verify that the Agent is running on Mac devices

You can run a command on Mac devices to determine whether the Agent is running.

1. Open a terminal window from **Applications > Utilities**.
2. Enter the following command:

```
ps aux | grep AMPAgent
```

This output indicates that the process is running:

```
root 2159 0.0 1.1 94408 12044 p2 S 3:26PM 0:10.94 /Library/Application Support/  
Dell/KACE/AMPAgent
```

Verify the version of the Agent on Mac devices

You can run a command on Mac devices to verify the version of the Agent installed on those devices.

1. Open a terminal window from **Applications > Utilities**.
2. Enter the following command:

```
cat /Library/Application\ Support/Dell/KACE/data/version
```

The version number is displayed.

Collecting inventory information from Mac devices

You can manually collect information from Mac devices by forcing inventory updates.

See [Forcing inventory updates](#).

Viewing information collected by the Agent

You can view inventory information collected by the Agent on the *Device Detail* page.

See [Managing inventory information](#).